Response to Pre-Bid Queries/Suggestions/Clarifications of RFP for Supply, Installation, Integration & Commissioning of new firewall and buyback of existing firewall for Rajasthan State Data Centre (RSDC) P-III
NIB F4.14(7)/RISL/Tech/e-Proc/2022/00177 dated 28.06.2022 ~ Tender ID: 2022_RISL_283888_1

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
1	15	3. Pre qualification/ Eligibility Criteria 3.1	3. PRE-QUALIFICATION / ELIGIBILITY CRITERIA Pt No 4 Technical Capability & Experience	The bidder must have successfully completed 2 project of Govt / PSU / Bank for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.) of minimum value of Rs. 1.00 Crore per project or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22. OR The bidder must have successfully completed 1 projects of Govt / PSU / Bank for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.) of value of Rs. 2.00 Crores or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22.	**Request you to clarify :** We have to showcase all IT equipment (like Router, Firewall, Network Switch etc.) in a single PO or we can submit multiple PO's with a value of Rs. 2.00 Crores or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22.. Or We can submit only Firewall PO with a value of Rs. 2.00 Crores or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22.	Clause Ammended	Refer Final RFP
2	15	3. Pre qualification/ Eligibility Criteria 3.1	4. Technical Capability & Experience	The bidder must have successfully completed 2 project of Govt / PSU /Bank for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.) of minimum value of Rs. 1.00 Crore per project or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22. OR The bidder must have successfully completed 1 projects of Govt / PSU /Bank for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.) of value of Rs. 2.00 Crores or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22.	Here the department has asked for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.). This will restrict the bidders to participate. **Hence we request to change this clause as Supply, Installation & Maintenance of IT/ITes projects for healthy competition.**	Clause Ammended	Refer Final RFP
3	15	3. PRE-QUALIFICATION / ELIGIBILITY CRITERIA 3.1	4. Technical Capability & Experience	The bidder must have successfully completed 2 project of Govt / PSU /Bank for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.) of minimum value of Rs. 1.00 Crore per project or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22. OR The bidder must have successfully completed 1 projects of Govt / PSU /Bank for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.) of value of Rs. 2.00 Crores or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22.	We request the department to amend this clause to increase the participation as " The bidder must have successfully completed or partial completed with requisite amount,two project of supply and installation of IT Hardware infra and Maintenance of value of Rs. 1.00 Crore per project or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22." OR The bidder must have successfully completed or partial completed with requisite amount,one project of supply and installation of IT Hardware infra and Maintenance of value of Rs. 2.00 Crore per project or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22."	Clause Ammended	Refer Final RFP
4	15	3.1 Pre Qualification/ Eligibility Criteria	4. Technical Capability & Experience	The bidder must have successfully completed 2 project of Govt / PSU /Bank for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.) of minimum value of Rs. 1.00 Crore per project or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22. OR The bidder must have successfully completed 1 projects of Govt / PSU /Bank for Supply, Installation & Maintenance of IT Equipment's (like Router, Firewall, Network Switch etc.) of value of Rs. 2.00 Crores or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22.	The bidder must have successfully completed 2 project of Govt / PSU /Bank for Supply, Installation & Maintenance of IT Equipment's of minimum value of Rs. 1.00 Crore per project or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22. OR The bidder must have successfully completed 1 projects of Govt / PSU /Bank for Supply, Installation & Maintenance of IT Equipment's of value of Rs. 2.00 Crores or more during the last four financial years i.e., FY's 2018-19, 2019-20, 2020-21, 2021-22.	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
5	65	project deliverables	7.1	60 Days	we would requst you to kindlly consider and extenstion on delivery time line by additonal of 90 days (150 days from PO). Due to the ongoing COVID-19 pandamic there is worldwide shortage of semiconductor chips, this has severely impacted the delivery timelines for all IT components. we requst you to kindlly consider as delivery within 60 days is a difficult challenge.	Clause Ammended	Refer Final RFP
6	65	SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	7.1	Supply &Installation On Go-Live - 90 % Remaining 10% of order value, in equated 4 installments payable at end of each year i.e., 2.5% annually	we would request you please release the 90% payment againts delivery and remaning 10 % againts installation. Because you are already holding our 10% BG for 4 year.	No Change	As per RFP
7	65	7. Special Terms and Conditions of Tender & Contract	7.1. Payment Terms and Schedule	Phase 1: 90% of Order Value Phase2: Remaining 10% of order value, in equated 4 installments payable at end of each year i.e., 2.5% annually	**We request the deaprtment to change this clause as 100 % payment after Supply & Installation On Go-Live of project.** As the Department has asked for Security Deposit from the bidders and considering that this deposit will be retained by the department for the service period. The current payment terms will substantially increase the cost of investment of the partners as OEMs and distributor do not give credit of more than 30 days for 100% payment. As a result of this bidders will be forced to quote extremely high prices to cover their costs. The present economic conditions have adversely affected the cash flow of various organizations which would deter them from participating in this tender with the current payment term. Hence we request for 100% of the total amount quoted on Delivery, Installation, OEM Support Certificate and Escalation Matrix.	No Change	As per RFP
8	65	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	7.1. Payment Terms and Schedule	Supply & Installation On Go-Live	We request you to amend this clause as under:- 96% of Order Value	No Change	As per RFP
9	65	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	7.1. Payment Terms and Schedule	Support Service	We request you to amend this clause as under:- Remaining 4% of order value, in equated 4 installments payable at end of each year i.e., 1% annually	No Change	As per RFP
10	95	Internet Firewall - Description of Requirement	2	Vendor shouldn't have reported any backdoor vulnerability in their product or OS for past 3years.	Query - Today any security OEM including Palo Alto, Cisco, etc have reported minor vulnerabilities which are being fixed by them. Palo Alto - https://www.cvedetails.com/vulnerability-list/vendor_id-12836/product_id-26167/Paloaltonetworks-Pan-os.html Cisco - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32730/Cisco-Firepower-Management-Center.html Revision request - Kindly revise the clause - The proposed NGFW OS should not have any severe vulnerability reported in last 3 years which has resulted in security breach	Clause Removed	Refer Final RFP
11	95	Internet Firewall - Description of Requirement	2	Vendor shouldn't have reported any backdoor vulnerability in their product or OS for past 3years.	Query - Today any security OEM including Palo Alto, Cisco, etc have reported minor vulnerabilities which are being fixed by them. Palo Alto - https://www.cvedetails.com/vulnerability-list/vendor_id-12836/product_id-26167/Paloaltonetworks-Pan-os.html Cisco - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32730/Cisco-Firepower-Management-Center.html Revision request - Kindly revise the clause - The proposed NGFW OS should not have any severe vulnerability reported in last 3 years which has resulted in security breach	Clause Removed	Refer Final RFP
12	95	Internet Firewall -Description of Requirement	2	Vendor shouldn't have reported any backdoor vulnerability in their product or OS for past 3years.	Query - Today any security OEM including Palo Alto, Cisco, etc have reported minor vulnerabilities which are being fixed by them. Palo Alto - https://www.cvedetails.com/vulnerability-list/vendor_id-12836/product_id-26167/Paloaltonetworks-Pan-os.html Cisco - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32730/Cisco-Firepower-Management-Center.html Revision request - Kindly revise the clause - The proposed NGFW OS should not have any severe vulnerability reported in last 3 years which has resulted in security breach	Clause Removed	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
13	95	Internet Firewall -Description of Requirement	2	Vendor shouldn't have reported any backdoor vulnerability in their product or OS for past 3years.	Query - Today any security OEM including Palo Alto, Cisco, etc have reported minor vulnerabilities which are being fixed by them. Palo Alto - https://www.cvedetails.com/vulnerability-list/vendor_id-12836/product_id-26167/Paloaltonetworks-Pan-os.html Cisco - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32730/Cisco-Firepower-Management-Center.html Revision request - Kindly revise the clause - The proposed NGFW OS should not have any severe vulnerability reported in last 3 years which has resulted in security breach	Clause Removed	Refer Final RFP
14	95	Internet Firewall - General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	Equal Multiple path would not be required in Internal Firrewall as there would be ISP/link is terminating on same Firewaal. Moreover, if ISP/links are terminating on Internal Firewaal, SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
15	95	Internet Firewall -General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	Equal Multiple path would not be required in Internal Firrewall as there would be ISP/link is terminating on same Firewaal. Moreover, if ISP/links are terminating on Internal Firewaal, SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
16	95	Internet Firewall -General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	Equal Multiple path would not be required in Internal Firrewall as there would be ISP/link is terminating on same Firewaal. Moreover, if ISP/links are terminating on Internal Firewaal, SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
17	95	Internet Firewall -General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	Equal Multiple path would not be required in Internal Firrewall as there would be ISP/link is terminating on same Firewaal. Moreover, if ISP/links are terminating on Internal Firewaal, SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
18	95	Internet Firewall -General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	Equal Multiple path would not be required in Internal Firrewall as there would be ISP/link is terminating on same Firewaal. Moreover, if ISP/links are terminating on Internal Firewaal, SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
19	95	Internet Firewall -General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
20	95	Internet Firewall -General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
21	95	Internet Firewall -General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
22	95	Internet Firewall -General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
23	95	Internet Firewall - General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
24	95	Internet Firewall - General Requirements	1,2	Proposed NGFW vendor must be Leader in latest published Gartner Magic Quadrant for Enterprise Network NGFW's.	Proposed NGFW vendor must be Leader in published Gartner Magic Quadrant for Enterprise Network NGFW's for last 5 consecutive years	No Change	As per RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
25	95	Internet Firewall	General Requirements	Proposed NGFW vendor must be Leader in latest published Gartner Magic Quadrant for Enterprise Network NGFW's.	Proposed NGFW vendor must be Leader in published Gartner Magic Quadrant for Enterprise Network NGFW's for last 5 consecutive years	No Change	As per RFP
26	95	7.1 Annexure 18	Internet Firewall - General Requirements - Sl. No. 1	Proposed NGFW vendor must be Leader in latest published Gartner Magic Quadrant for Enterprise Network NGFW's.	As per PPP order from Govt. of India, Ministry of Commerce and Industy order dated 06th Sept 2020 asking for foreign certification is discriminatory/restrictive as per clause 10(e) hence we request to remove this certifcation requirement and subsequent order from MeiTy, and other ministry of Govt. of India. Please remove the clause. This will help for broader participation.	No Change	As per RFP
27	95	7.1 Annexure 18	Internet Firewall - General Requirements - Sl. No. 1	Proposed NGFW vendor must be Leader in latest published Gartner Magic Quadrant for Enterprise Network NGFW's.	As per PPP order from Govt. of India, Ministry of Commerce and Industy order dated 06th Sept 2020 asking for foreign certification is discriminatory/restrictive as per clause 10(e) hence we request to remove this certifcation requirement and subsequent order from MeiTy, and other ministry of Govt. of India. Please remove the clause. This will help for broader participation.	No Change	As per RFP
28	95	7.1 Annexure 18	Internet Firewall - General Requirements - Sl. No. 14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	It is important to have hotfixes for the software. In automatic roll back function, such hotfixes may get lost and could affect the current working configuration. Instead auto hotfixes option should be control by admin. If enabled, all the hotfixes will be downloaded and implemented automatically. If disabled, admin can manually look for updates. And for backup of configuration, automated backup should be the option.But applying the same should be manual as it can affect the current working configuration. Hence requesting to change clause to "Automatic updates/hotfixes and automatic backup generation"	Clause Removed	Refer Final RFP
29	95	7.1 Annexure 18	Internet Firewall - General Requirements - Sl. No. 14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	It is important to have hotfixes for the software. In automatic roll back function, such hotfixes may get lost and could affect the current working configuration. Instead auto hotfixes option should be control by admin. If enabled, all the hotfixes will be downloaded and implemented automatically. If disabled, admin can manually look for updates. And for backup of configuration, automated backup should be the option.But applying the same should be manual as it can affect the current working configuration. Hence requesting to change clause to "Automatic updates/hotfixes and automatic backup generation"	Clause Removed	Refer Final RFP
30	96	Performance Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 15 Gbps.	Request is to consider 9 Gbps next generation firewall throughput.	Clause Ammended	Refer Final RFP
31	96	Performance Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 15 Gbps.	Request is to consider 9 Gbps next generation firewall throughput.	Clause Ammended	Refer Final RFP
32	96	Performance Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 15 Gbps.	Request is to consider 9 Gbps next generation firewall throughput.	Clause Ammended	Refer Final RFP
33	96	Performance Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 15 Gbps.	Request is to consider 9 Gbps next generation firewall throughput.	Clause Ammended	Refer Final RFP
34	96	Data Center (DC) Firewall	1	Proposed NGFW vendor must be Leader in latest published Gartner Magic Quadrant for Enterprise Network NGFW's.	Proposed NGFW vendor must be Leader in published Gartner Magic Quadrant for Enterprise Network NGFW's from last consecutive 5 years	No Change	As per RFP
35	96	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one.	Request to consider 2x 40GE QSFP+, 4x 25GE SFP28, 4x 10GE SFP+, 8x GE SFP, 18x GE RJ45	No Change	As per RFP
36	96	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one.	Request to consider 2x 40GE QSFP+, 4x 25GE SFP28, 4x 10GE SFP+, 8x GE SFP, 18x GE RJ45	No Change	As per RFP
37	96	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one.	Request to consider 2x 40GE QSFP+, 4x 25GE SFP28, 4x 10GE SFP+, 8x GE SFP, 18x GE RJ45	No Change	As per RFP
38	96	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one.	Request to consider 2x 40GE QSFP+, 4x 25GE SFP28, 4x 10GE SFP+, 8x GE SFP, 18x GE RJ45	No Change	As per RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
39	96	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one.	**Requested Change:** The platform must be supplied with at least 12 x 10G RJ45 interfaces along with 10x10G SFP+ and minimum 4*25G SFP28 (transceiver should be at least 4 SR and 2 LR) interfaces fully populated ports from day one **Justification:** This is an investment by the department for the next 4-5 years and today's traffic patterns demand higher bandwidth requirements. So, minimum 4*25G interfaces for the backbone traffic should be defined as above for uplink connectivity. Defining this ask for more number of 10G and even 25G ports from day 1 will ensure the interface backbone scalability and will meet the future traffic/ bandwidth requirements on this new NGFW investment	No Change	As per RFP
40	96	Performance Requirements	2	The NGFW must support at least 2 million concurrent connections.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. "It is suggested that the "Firewall should support at least 20 Million concurrent sessions and minimum 400 connections per/ second to cater to present and future requirements	Clause Ammended	Refer Final RFP
41	96	Performance Requirements	2	The NGFW must support at least 2 million concurrent connections.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. "It is suggested that the "Firewall should support at least 20 Million concurrent sessions and minimum 400 connections per/ second to cater to present and future requirements	Clause Ammended	Refer Final RFP
42	96	Performance Requirements	2	The NGFW must support at least 2 million concurrent connections.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. "It is suggested that the "Firewall should support at least 20 Million concurrent sessions and minimum 400 connections per/ second to cater to present and future requirements	Clause Ammended	Refer Final RFP
43	96	Performance Requirements	2	The NGFW must support at least 2 million concurrent connections.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. "It is suggested that the "Firewall should support at least 20 Million concurrent sessions and minimum 400 connections per/ second to cater to present and future requirements	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
44	96	Internet Firewall	2	The NGFW must support at least 2 million concurrent connections.	**Requested Change:**The NGFW must support at least 1 million Layer 7 concurrent connections/sessions **Justification:** The traffic flow within the RajCom datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, the session count calculation should also be defined for Layer 7 traffic rather than keeping it generic where OEMs can even interpret this as a Layer 4 session count and such derived references will impact the RajComp Perimeter Security Layer devices from performance standpoint during traffic throttling	Clause Ammended	Refer Final RFP
45	96	Data Center (DC) Firewall- General Requirements	2	Vendor shouldn't have reported any backdoor vulnerability in their product or OS for past 3years.	Query - Today any security OEM including Palo Alto, Cisco, etc have reported minor vulnerabilities which are being fixed by them. Palo Alto - https://www.cvedetails.com/vulnerability-list/vendor_id-12836/product_id-26167/Paloaltonetworks-Pan-os.html Cisco - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32730/Cisco-Firepower-Management-Center.html Revision request - Kindly revise the clause - The proposed NGFW OS should not have any severe vulnerability reported in last 3 years which has resulted in security breach	Clause Removed	Refer Final RFP
46	96	Data Center (DC) Firewall- General Requirements	2	Vendor shouldn't have reported any backdoor vulnerability in their product or OS for past 3years.	Query - Today any security OEM including Palo Alto, Cisco, etc have reported minor vulnerabilities which are being fixed by them. Palo Alto - https://www.cvedetails.com/vulnerability-list/vendor_id-12836/product_id-26167/Paloaltonetworks-Pan-os.html Cisco - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32730/Cisco-Firepower-Management-Center.html Revision request - Kindly revise the clause - The proposed NGFW OS should not have any severe vulnerability reported in last 3 years which has resulted in security breach	Clause Removed	Refer Final RFP
47	96	Data Center (DC) Firewall- General Requirements	2	Vendor shouldn't have reported any backdoor vulnerability in their product or OS for past 3years.	Query - Today any security OEM including Palo Alto, Cisco, etc have reported minor vulnerabilities which are being fixed by them. Palo Alto - https://www.cvedetails.com/vulnerability-list/vendor_id-12836/product_id-26167/Paloaltonetworks-Pan-os.html Cisco - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32730/Cisco-Firepower-Management-Center.html Revision request - Kindly revise the clause - The proposed NGFW OS should not have any severe vulnerability reported in last 3 years which has resulted in security breach	Clause Removed	Refer Final RFP
48	96	Data Center (DC) Firewall- General Requirements	2	Vendor shouldn't have reported any backdoor vulnerability in their product or OS for past 3years.	Query - Today any security OEM including Palo Alto, Cisco, etc have reported minor vulnerabilities which are being fixed by them. Palo Alto - https://www.cvedetails.com/vulnerability-list/vendor_id-12836/product_id-26167/Paloaltonetworks-Pan-os.html Cisco - https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32730/Cisco-Firepower-Management-Center.html Revision request - Kindly revise the clause - The proposed NGFW OS should not have any severe vulnerability reported in last 3 years which has resulted in security breach	Clause Removed	Refer Final RFP
49	96	Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 400 GB SSD , RAID with 64 GB RAM.	Every OEM has their own architecture with required Memory to handle the max concurrent sessions. Mentioning 64GB will unnecessarily inflate the competition model and will give liberty to single OEM to inflate their bidding price. This will not give any competitive advantage to customer and will have to pay higher price. Kindly revise the clause to - Should have adequate memory on day 1 to handle concurrent connections requirement asked..	Clause Ammended	Refer Final RFP
50	96	Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 400 GB SSD , RAID with 64 GB RAM.	Every OEM has their own architecture with required Memory to handle the max concurrent sessions. Mentioning 64GB will unnecessarily inflate the competition model and will give liberty to single OEM to inflate their bidding price. This will not give any competitive advantage to customer and will have to pay higher price. Kindly revise the clause to - Should have adequate memory on day 1 to handle concurrent connections requirement asked..	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
51	96	Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 400 GB SSD , RAID with 64 GB RAM.	Every OEM has their own architecture with required Memory to handle the max concurrent sessions. Mentioning 64GB will unnecessarily inflate the competition model and will give liberty to single OEM to inflate their bidding price. This will not give any competitive advantage to customer and will have to pay higher price. Kindly revise the clause to - Should have adequate memory on day 1 to handle concurrent connections requirement asked..	Clause Ammended	Refer Final RFP
52	96	Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 400 GB SSD , RAID with 64 GB RAM.	Every OEM has their own architecture with required Memory to handle the max concurrent sessions. Mentioning 64GB will unnecessarily inflate the competition model and will give liberty to single OEM to inflate their bidding price. This will not give any competitive advantage to customer and will have to pay higher price. Kindly revise the clause to - Should have adequate memory on day 1 to handle concurrent connections requirement asked..	Clause Ammended	Refer Final RFP
53	96	Internet Firewall Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 400 GB SSD, RAID with 64 GB RAM.	**Requested Change:** NGFW Appliance should have minimum Log storage of 480 GB SSD with minimum 48 GB RAM **Justification:** Every OEM has a different Hardware reference architecture and each OEM meets same FW performance with different HW configuration. So, CPU cores and RAM varies for different OEMs. Please specify minimum value of 48GB RAM because ideally platform should meet the desired throughput/ session count requirements for better performance and security efficacy	Clause Ammended	Refer Final RFP
54	96	Internet Firewall Performance Requirements	3	The NGFW must support more than 200,000 new connections per second processing	**Requested Change:**The NGFW must support at least 100,000 new Layer 7 connections per second considering 1 byte HTTP transaction **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, the session count calculation should also be defined for Layer 7 traffic rather than keeping it generic where OEMs can even interpret this as a Layer 4 session count and such derived references will impact the RajComp Perimeter Security Layer devices from performance standpoint during traffic throttling	Clause Ammended	Refer Final RFP
55	96	Performance Requirements	3	The NGFW must support more than 200,000 new connections per second processing .		Clause Ammended	Refer Final RFP
56	96	Performance Requirements	3	The NGFW must support more than 200,000 new connections per second processing .		Clause Ammended	Refer Final RFP
57	96	Performance Requirements	3	The NGFW must support more than 200,000 new connections per second processing .		Clause Ammended	Refer Final RFP
58	96	Performance Requirements	3	The NGFW must support more than 200,000 new connections per second processing .		Clause Ammended	Refer Final RFP
59	96	7.1 Annexure 18	Data Center (DC) Firewall - General Requirements - Sl. No. 1	Proposed NGFW vendor must be Leader in latest published Gartner Magic Quadrant for Enterprise Network NGFW's.	As per PPP order from Govt. of India, Ministry of Commerce and Industy order dated 06th Sept 2020 asking for foreign certification is discriminatory/restrictive as per clause 10(e) hence we request to remove this certifcation requirement and subsequent order from MeiTy, and other ministry of Govt. of India. Please remove the clause. This will help for broader participation.	No Change	As per RFP
60	96	7.1 Annexure 18	Data Center (DC) Firewall - General Requirements - Sl. No. 1	Proposed NGFW vendor must be Leader in latest published Gartner Magic Quadrant for Enterprise Network NGFW's.	As per PPP order from Govt. of India, Ministry of Commerce and Industy order dated 06th Sept 2020 asking for foreign certification is discriminatory/restrictive as per clause 10(e) hence we request to remove this certifcation requirement and subsequent order from MeiTy, and other ministry of Govt. of India. Please remove the clause. This will help for broader participation.	No Change	As per RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
61	96	Data Center (DC) Firewall	General Requirements	Proposed NGFW vendor must be Leader in latest published Gartner Magic Quadrant for Enterprise Network NGFW's.	Proposed NGFW vendor must be Leader in published Gartner Magic Quadrant for Enterprise Network NGFW's from last consecutive 5 years	No Change	As per RFP
62	96	Internet Firewall	Hardware and Interface Requirements	NGFW Appliance should have Log storage of 400 GB SSD, RAID with 64 GB RAM.	**Requested Change:** NGFW Appliance should have minimum Log storage of 480 GB SSD with minimum 48 GB RAM **Justification:** Every OEM has a different Hardware reference architecture and each OEM meets same FW performance with different HW configuration. So, CPU cores and RAM varies for different OEMs. Please specify minimum value of 48GB RAM because ideally platform should meet the desired throughput/ session count requirements for better performance and security efficacy	Clause Ammended	Refer Final RFP
63	96	Internet Firewall	Hardware and Interface Requirements	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one.	**Requested Change:** The platform must be supplied with at least 12 x 10G RJ45 interfaces along with 10x10G SFP+ and minimum 4*25G SFP28 (transceiver should be at least 4 SR and 2 LR) interfaces fully populated ports from day one **Justification:** This is an investment by the department for the next 4-5 years and today's traffic patterns demand higher bandwidth requirements. So, minimum 4*25G interfaces for the backbone traffic should be defined as above for uplink connectivity. Defining this ask for more number of 10G and even 25G ports from day 1 will ensure the interface backbone scalability and will meet the future traffic/ bandwidth requirements on this new NGFW investment	No Change	As per RFP
64	96	7.1 Annexure 18	Internet Firewall - General Requirements - Sl. No. 15	The admins must be able to view report on the CPU usage for management activities and CPU usage for other activities.	It is essential to view the current CPU usage on the firewall instead of, it is getting utilised for what purpose. Also CPU usage shown on dashboard is very easy for admins to track the same. Hence requesting to change the clause to incorporate "CPU utilization status on dashboard"	No Change	As per RFP
65	96	7.1 Annexure 18	Internet Firewall - General Requirements - Sl. No. 15	The admins must be able to view report on the CPU usage for management activities and CPU usage for other activities.	It is essential to view the current CPU usage on the firewall instead of, it is getting utilised for what purpose. Also CPU usage shown on dashboard is very easy for admins to track the same. Hence requesting to change the clause to incorporate "CPU utilization status on dashboard"	No Change	As per RFP
66	96	7.1 Annexure 18	Internet Firewall -Hardware and Interface Requirements Sl. No. 3	NGFW Appliance should have Log storage of 400 GB SSD , RAID with 64 GB RAM.	RAID should not be made compulsory as availability of storage totally depends upon quality of SSD provided. Also if more disk space is provided along with appliance then working of the SSD is faultless. In case of RAM, appliance is tested by labs for better perfomance and approprate RAM is installed in the appliance. So specific value of RAM should not be mentioned. Hence requesting to change the clause "to remove RAID requirment and storage should be increased to 1TB SSD." Also for RAM mention "Appropriate RAM should be used to maintain the performance of the appliance"	Clause Ammended	Refer Final RFP
67	96	7.1 Annexure 18	Internet Firewall -Hardware and Interface Requirements Sl. No. 3	NGFW Appliance should have Log storage of 400 GB SSD , RAID with 64 GB RAM.	RAID should not be made compulsory as availability of storage totally depends upon quality of SSD provided. Also if more disk space is provided along with appliance then working of the SSD is faultless. In case of RAM, appliance is tested by labs for better perfomance and approprate RAM is installed in the appliance. So specific value of RAM should not be mentioned. Hence requesting to change the clause "to remove RAID requirment and storage should be increased to 1TB SSD." Also for RAM mention "Appropriate RAM should be used to maintain the performance of the appliance"	Clause Ammended	Refer Final RFP
68	96	7.1 Annexure 18	Internet Firewall -NGFW Filtering Requirements Sl. No. 2	NGFW updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time.	All the updates should happen automatic and should happen daily basis to maintain security level on the appliance. Hence requesting to change the clause to " scheduling for specific time only"	No Change	As per RFP
69	96	7.1 Annexure 18	Internet Firewall -NGFW Filtering Requirements Sl. No. 2	NGFW updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time.	All the updates should happen automatic and should happen daily basis to maintain security level on the appliance. Hence requesting to change the clause to " scheduling for specific time only"	No Change	As per RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
70	96	7.1 Annexure 18	Internet Firewall -NGFW Filtering Requirements Sl. No. 5	The NGFW should support authentication protocols like LDAP, RADIUS and have support for NGFW passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.	LDAP, RADIUS, TACACS+ , Tokens are commonly used for authentication. Smart cards and digital certificates are very rarely used. So requesting to remove "smart cards and digital certificates" from the clause.	No Change	As per RFP
71	96	7.1 Annexure 18	Internet Firewall -NGFW Filtering Requirements Sl. No. 5	The NGFW should support authentication protocols like LDAP, RADIUS and have support for NGFW passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.	LDAP, RADIUS, TACACS+ , Tokens are commonly used for authentication. Smart cards and digital certificates are very rarely used. So requesting to remove "smart cards and digital certificates" from the clause.	No Change	As per RFP
72	96	ANNEXURE-18: TECHNICAL SPECIFICATIONS	Item no. 1: Internet Firewall Hardware & Interface Requirements	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one.	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one. Dedicated out of bond management port with 10/100/1000 Base-T Port along with dedicated sync port of 10/100/1000 Base-T Port. - Additionally, there should be dedicated out of band management port with 10/100/1000 Base-T Port. - Primary benefit of an out-of-band management interface **is its availability when the device is down**, a device is turned off, in sleep mode, hibernating, or otherwise inaccessible. OOBM can be used to remotely reboot devices that have crashed and manage powered-down devices. - Dedicated Sync Port require in order to ensure all the available ports should be optimized.	No Change	As per RFP
73	96	ANNEXURE-18: TECHNICAL SPECIFICATIONS	Item no. 1: Internet Firewall Hardware & Interface Requirements	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one.	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 6x10G(transceiver should be 4 SR and 2 LR) interfaces fully populated ports from day one. Dedicated out of bond management port with 10/100/1000 Base-T Port along with dedicated sync port of 10/100/1000 Base-T Port. - Additionally, there should be dedicated out of band management port with 10/100/1000 Base-T Port. - Primary benefit of an out-of-band management interface **is its availability when the device is down**, a device is turned off, in sleep mode, hibernating, or otherwise inaccessible. OOBM can be used to remotely reboot devices that have crashed and manage powered-down devices. - Dedicated Sync Port require in order to ensure all the available ports should be optimized.	No Change	As per RFP
74	96	Internet Firewall	Performance Requirements	NGFW must have minimum Next Generation Firewall throughput of 15 Gbps.	**Requested Change:**NGFW must have minimum Next Generation Firewall throughput of 12 Gbps with application-identification/AVC/application control and logging enabled considering transaction size of 64KB HTTP packet **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, The NGFW throughput should clearly mention App-ID/AVC/App Control and logging to be enabled while the throughput is computed with a packet size reference of 64KB HTTP to evaluate equivalent platforms on performance. Packet size will define the baseline for deriving these throughput values and is a critical aspect in the throughput calculation	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
75	96	Internet Firewall	Performance Requirements	The NGFW must support at least 2 million concurrent connections.	**Requested Change:**The NGFW must support at least 1 million Layer 7 concurrent connections/sessions **Justification:** The traffic flow within the RajCom datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, the session count calculation should also be defined for Layer 7 traffic rather than keeping it generic where OEMs can even interpret this as a Layer 4 session count and such derived references will impact the RajComp Perimeter Security Layer devices from performance standpoint during traffic throttling	Clause Ammended	Refer Final RFP
76	96	Internet Firewall	Performance Requirements	The NGFW must support more than 200,000 new connections per second processing	**Requested Change:**The NGFW must support at least 100,000 new Layer 7 connections per second considering 1 byte HTTP transaction **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, the session count calculation should also be defined for Layer 7 traffic rather than keeping it generic where OEMs can even interpret this as a Layer 4 session count and such derived references will impact the RajComp Perimeter Security Layer devices from performance standpoint during traffic throttling	Clause Ammended	Refer Final RFP
77	96	Performance Requirements		NGFW must have minimum Next Generation Firewall throughput of 15 Gbps.	**Requested Change:**NGFW must have minimum Next Generation Firewall throughput of 12 Gbps with application-identification/AVC/application control and logging enabled considering transaction size of 64KB HTTP packet **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, The NGFW throughput should clearly mention App-ID/AVC/App Control and logging to be enabled while the throughput is computed with a packet size reference of 64KB HTTP to evaluate equivalent platforms on performance. Packet size will define the baseline for deriving these throughput values and is a critical aspect in the throughput calculation	Clause Ammended	Refer Final RFP
78	97	Performance Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 25 Gbps.	Pls change "the next generation throughput to 11Gbps".	Clause Ammended	Refer Final RFP
79	97	Performance Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 25 Gbps.	We request you to change "the next generation throughput to 11Gbps".	Clause Ammended	Refer Final RFP
80	97	Performance Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 25 Gbps.	Pls change "the next generation throughput to 11Gbps".	Clause Ammended	Refer Final RFP
81	97	Performance Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 25 Gbps.	Pls change "the next generation throughput to 11Gbps".	Clause Ammended	Refer Final RFP
82	97	Data Center (DC) Firewall Hardware and Interface Requirements	1	NGFW must have minimum Next Generation Firewall throughput of 25 Gbps.	**Requested Change:**NGFW must have minimum Next Generation Firewall throughput of 25 Gbps with application-identification/AVC/application control and logging enabled considering transaction size of 64KB HTTP packet **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, The NGFW throughput should clearly mention App-ID/AVC/App Control and logging to be enabled while the throughput is computed with a packet size reference of 64KB HTTP to evaluate equivalent platforms on performance. Packet size will define the baseline for deriving these throughput values and is a critical aspect in the throughput calculation	Clause Ammended	Refer Final RFP
83	97	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 12x10G (transceiver should be 8 SR and 4 LR) interfaces fully populated ports from day one.	4x 40 GE QSFP+, 12x 25 GE SFP28, 2x10 GE SFP+, 8x GE SFP, 18x GE RJ45	No Change	As per RFP
84	97	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 12x10G (transceiver should be 8 SR and 4 LR) interfaces fully populated ports from day one.	4x 40 GE QSFP+, 12x 25 GE SFP28, 2x10 GE SFP+, 8x GE SFP, 18x GE RJ45	No Change	As per RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
85	97	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 12x10G (transceiver should be 8 SR and 4 LR) interfaces fully populated ports from day one.	4x 40 GE QSFP+, 12x 25 GE SFP28, 2x10 GE SFP+, 8x GE SFP, 18x GE RJ45	No Change	As per RFP
86	97	Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 12x10G (transceiver should be 8 SR and 4 LR) interfaces fully populated ports from day one.	4x 40 GE QSFP+, 12x 25 GE SFP28, 2x10 GE SFP+, 8x GE SFP, 18x GE RJ45	No Change	As per RFP
87	97	Data Center (DC) Firewall Hardware and Interface Requirements	1	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 12x10G (transceiver should be 8 SR and 4 LR) interfaces fully populated ports from day one.	**Requested Change:** The platform must be supplied with at least 12 x 10G RJ45 interfaces along with 10x10G SFP+, minimum 4*25G SFP28 and at least 2*40G/100G interfaces (transceiver should be at least 8 SR and 4 LR) interfaces fully populated ports from day 1 **Justification:** This is an investment by the department for the next 4-5 years and today's traffic patterns demand higher bandwidth requirements. So,minimum 2*40G/100G interfaces for the backbone traffic should be defined as above for uplink connectivity. Defining ask for more 10G and even 40G/100GG ports from day 1 will ensure the interface backbone scalability and will meet the traffic/bandwidth requirements for any upgraded future requirements on this new NGFW investment	No Change	As per RFP
88	97	Performance Requirements	2	The NGFW must support at least 8 million concurrent connections.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. "It is suggested that the "Firewall should support at least 12 Million concurrent sessions and minimum 750 connections per/ second to cater to present and future requirements	Clause Ammended	Refer Final RFP
89	97	Performance Requirements	2	The NGFW must support at least 8 million concurrent connections.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. "It is suggested that the "Firewall should support at least 12 Million concurrent sessions and minimum 750 connections per/ second to cater to present and future requirements	Clause Ammended	Refer Final RFP
90	97	Performance Requirements	2	The NGFW must support at least 8 million concurrent connections.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. "It is suggested that the "Firewall should support at least 12 Million concurrent sessions and minimum 750 connections per/ second to cater to present and future requirements	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
91	97	Performance Requirements	2	The NGFW must support at least 8 million concurrent connections.	Today there are many applications which keep running on PCs / Servers / Laptops and which try to connect to internet for various downloads like windows updates / antivirus updates and other online applications. These application keeps opening sessions automatically. The firewall should not become a bottleneck in case of a virus or trojan generating huge nos of connections. To ensure that the firewall is capable of handling such traffic scenarios it is important that firewall is capable of handling very high concurrent sessions and new sessions per second. "It is suggested that the "Firewall should support at least 12 Million concurrent sessions and minimum 750 connections per/ second to cater to present and future requirements	Clause Ammended	Refer Final RFP
92	97	Data Center (DC) Firewall Performance Requirements	2	The NGFW must support at least 8 million concurrent connections..	**Requested Change:**The NGFW must support at least 2.5 million Layer 7 concurrent connections/sessions **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, the session count calculation should also be defined for Layer 7 traffic rather than keeping it generic where OEMs can even interpret this as a Layer 4 session count and such derived references will impact the RajComp Perimeter Security Layer devices from performance standpoint during traffic throttling	Clause Ammended	Refer Final RFP
93	97	Data Center (DC) Firewall Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 500 GB HDD, RAID with 128 GB RAM.	**Requested Change:** NGFW Appliance should have minimum Log storage of 480 GB SSD with minimum 64 GB RAM **Justification:** Every OEM has a different Hardware reference architecture. So, CPU cores and RAM will vary as per the OEM platform.Please specify minimum value of 48GB RAM because ideally platform should meet the desired throughput/session count requirements for better performance and security efficacy	Clause Ammended	Refer Final RFP
94	97	Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 500 GB HDD, RAID with 128 GB RAM.	Every OEM has their own architecture with required Memory to handle the max concurrent sessions. Mentioning 64GB will unnecessarily inflate the competition model and will give liberty to single OEM to inflate their bidding price. This will not give any competitive advantage to customer and will have to pay higher price. Kindly revise the clause to - Should have adequate memory on day 1 to handle concurrent connections requirement asked..	Clause Ammended	Refer Final RFP
95	97	Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 500 GB HDD, RAID with 128 GB RAM.	Every OEM has their own architecture with required Memory to handle the max concurrent sessions. Mentioning 64GB will unnecessarily inflate the competition model and will give liberty to single OEM to inflate their bidding price. This will not give any competitive advantage to customer and will have to pay higher price. Kindly revise the clause to - Should have adequate memory on day 1 to handle concurrent connections requirement asked..	Clause Ammended	Refer Final RFP
96	97	Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 500 GB HDD, RAID with 128 GB RAM.	Every OEM has their own architecture with required Memory to handle the max concurrent sessions. Mentioning 64GB will unnecessarily inflate the competition model and will give liberty to single OEM to inflate their bidding price. This will not give any competitive advantage to customer and will have to pay higher price. Kindly revise the clause to - Should have adequate memory on day 1 to handle concurrent connections requirement asked..	Clause Ammended	Refer Final RFP
97	97	Hardware and Interface Requirements	3	NGFW Appliance should have Log storage of 500 GB HDD, RAID with 128 GB RAM.	Every OEM has their own architecture with required Memory to handle the max concurrent sessions. Mentioning 64GB will unnecessarily inflate the competition model and will give liberty to single OEM to inflate their bidding price. This will not give any competitive advantage to customer and will have to pay higher price. Kindly revise the clause to - Should have adequate memory on day 1 to handle concurrent connections requirement asked..	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
98	97	Data Center (DC) Firewall Performance Requirements	3	The NGFW must support more than 300,000 new connections per second processing.	**Requested Change:**The NGFW must support at least 250,000 new Layer 7 connections per second considering 1 byte HTTP transaction **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, the session count calculation should also be defined for Layer 7 traffic rather than keeping it generic where OEMs can even interpret this as a Layer 4 session count and such derived references will impact the RajComp Perimeter Security Layer devices from performance standpoint during traffic throttling	Clause Ammended	Refer Final RFP
99	97	Performance Requirements	3	The NGFW must support more than 300,000 new connections per second processing.		Clause Ammended	Refer Final RFP
100	97	Performance Requirements	3	The NGFW must support more than 300,000 new connections per second processing.		Clause Ammended	Refer Final RFP
101	97	Performance Requirements	3	The NGFW must support more than 300,000 new connections per second processing.		Clause Ammended	Refer Final RFP
102	97	Performance Requirements	3	The NGFW must support more than 300,000 new connections per second processing.		Clause Ammended	Refer Final RFP
103	97	Data Center (DC) Firewall- General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
104	97	Data Center (DC) Firewall- General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
105	97	Data Center (DC) Firewall- General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
106	97	Data Center (DC) Firewall- General Requirements	7	Solution should support Session based load sharing (not packet based) over multiple equal cost paths. It should work with both static and dynamic routing.	SD WAN is a feature which will help to optimise uses of all available link/ISP, it is automated process and better than asked feature ECMP. Request you to add SD WAN feature in the asked.	No Change	As per RFP
107	97	Data Center (DC) Firewall- General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
108	97	Data Center (DC) Firewall- General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
109	97	Data Center (DC) Firewall- General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
110	97	Data Center (DC) Firewall- General Requirements	14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	Any OS upgrades / hotfixes require reboot of NGFW. If the hotfixes are installed automatically, there will be severe downtime while the NGFW reboots to activate the new hotfixes / upgrades. Kindly remove this clause as the upgrades needs proper planning and scheduled downtime in advance.	Clause Removed	Refer Final RFP
111	97	7.1 Annexure 18	Data Center (DC) Firewall - General Requirements - Sl. No. 14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	It is important to have hotfixes for the software. In automatic roll back function, such hotfixes may get lost and could affect the current working configuration. Instead auto hotfixes option should be control by admin. If enabled, all the hotfixes will be downloaded and implemented automatically. If disabled, admin can manually look for updates. And for backup of configuration, automated backup should be the option.But applying the same should be manual as it can affect the current working configuration. Hence requesting to change clause to incorporate "Automatic updates/hotfixes and automatic backup generation only"	Clause Removed	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
112	97	7.1 Annexure 18	Data Center (DC) Firewall - General Requirements - Sl. No. 14	Device must support automatic search, downloading and install software hotfixes without any administrator efforts System should have provision to automatically roll back last saved config.	It is important to have hotfixes for the software. In automatic roll back function, such hotfixes may get lost and could affect the current working configuration. Instead auto hotfixes option should be control by admin. If enabled, all the hotfixes will be downloaded and implemented automatically. If disabled, admin can manually look for updates. And for backup of configuration, automated backup should be the option.But applying the same should be manual as it can affect the current working configuration. Hence requesting to change clause to incorporate "Automatic updates/hotfixes and automatic backup generation only"	Clause Removed	Refer Final RFP
113	97	7.1 Annexure 18	Data Center (DC) Firewall - General Requirements - Sl. No. 15	The admins must be able to view report on the CPU usage for management activities and CPU usage for other activities.	It is essential to view the current CPU usage on the firewall instead of, it is getting utilised for what purpose. Also CPU usage shown on dashboard is very easy for admins to track the same. Hence requesting to change the clause to incorporate "CPU utilization status on dashboard"	No Change	As per RFP
114	97	7.1 Annexure 18	Data Center (DC) Firewall - General Requirements - Sl. No. 15	The admins must be able to view report on the CPU usage for management activities and CPU usage for other activities.	It is essential to view the current CPU usage on the firewall instead of, it is getting utilised for what purpose. Also CPU usage shown on dashboard is very easy for admins to track the same. Hence requesting to change the clause to incorporate "CPU utilization status on dashboard"	No Change	As per RFP
115	97	7.1 Annexure 18	Data Center (DC) Firewall - NGFW Filtering Requirements Sl. No. 2	NGFW updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time.	All the updates should happen automatic and should happen daily basis to maintain security level on the appliance. Hence requesting to change the clause to " scheduling for specific time only"	No Change	As per RFP
116	97	7.1 Annexure 18	Data Center (DC) Firewall - NGFW Filtering Requirements Sl. No. 2	NGFW updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time.	All the updates should happen automatic and should happen daily basis to maintain security level on the appliance. Hence requesting to change the clause to " scheduling for specific time only"	No Change	As per RFP
117	97	7.1 Annexure 18	Data Center (DC) Firewall - NGFW Filtering Requirements Sl. No. 5	The NGFW should support authentication protocols like LDAP, RADIUS and have support for NGFW passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.	LDAP, RADIUS, TACACS+ , Tokens are commonly used for authentication. Smart cards and digital certificates are very rarely used. So requesting to remove "smart cards and digital certificates" from the clause.	No Change	As per RFP
118	97	7.1 Annexure 18	Data Center (DC) Firewall - NGFW Filtering Requirements Sl. No. 5	The NGFW should support authentication protocols like LDAP, RADIUS and have support for NGFW passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.	LDAP, RADIUS, TACACS+ , Tokens are commonly used for authentication. Smart cards and digital certificates are very rarely used. So requesting to remove "smart cards and digital certificates" from the clause.	No Change	As per RFP
119	97	7.1 Annexure 18	Data Center (DC) Firewall- Hardware and Interface Requirements Sl. No. 3	NGFW Appliance should have Log storage of 500 GB HDD, RAID with 128 GB RAM.	RAID should not be made compulsory as availability of storage totally depends upon quality of SSD provided. Also if more disk space is provided along with appliance then working of the SSD is faultless. In case of RAM, appliance is tested by labs for better perfomance and approprate RAM is installed in the appliance. So specific value of RAM should not be mentioned. Hence requesting to change the clause "to remove RAID requirment and storage should be increased to 1TB SSD." Also for RAM mention "Appropriate RAM should be used to maintain the performance of the appliance"	Clause Ammended	Refer Final RFP
120	97	7.1 Annexure 18	Data Center (DC) Firewall- Hardware and Interface Requirements Sl. No. 3	NGFW Appliance should have Log storage of 500 GB HDD, RAID with 128 GB RAM.	RAID should not be made compulsory as availability of storage totally depends upon quality of SSD provided. Also if more disk space is provided along with appliance then working of the SSD is faultless. In case of RAM, appliance is tested by labs for better perfomance and approprate RAM is installed in the appliance. So specific value of RAM should not be mentioned. Hence requesting to change the clause "to remove RAID requirment and storage should be increased to 1TB SSD." Also for RAM mention "Appropriate RAM should be used to maintain the performance of the appliance"	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
121	97	Data Center (DC) Firewall	Hardware and Interface Requirements	NGFW Appliance should have Log storage of 500 GB HDD, RAID with 128 GB RAM.	**Requested Change:** NGFW Appliance should have minimum Log storage of 480 GB SSD with minimum 64 GB RAM **Justification:** Every OEM has a different Hardware reference architecture. So, CPU cores and RAM will vary as per the OEM platform.Please specify minimum value of 48GB RAM because ideally platform should meet the desired throughput/session count requirements for better performance and security efficacy	Clause Ammended	Refer Final RFP
122	97	Data Center (DC) Firewall	Hardware and Interface Requirements	The platform must be supplied with at least 2x RJ45(100/1000 MB) interfaces along with 12x10G (transceiver should be 8 SR and 4 LR) interfaces fully populated ports from day one.	**Requested Change:** The platform must be supplied with at least 12 x 10G RJ45 interfaces along with 10x10G SFP+, minimum 4*25G SFP28 and at least 2*40G/100G interfaces (transceiver should be at least 8 SR and 4 LR) interfaces fully populated ports from day 1 **Justification:** This is an investment by the department for the next 4-5 years and today's traffic patterns demand higher bandwidth requirements. So,minimum 2*40G/100G interfaces for the backbone traffic should be defined as above for uplink connectivity. Defining ask for more 10G and even 40G/100GG ports from day 1 will ensure the interface backbone scalability and will meet the traffic/bandwidth requirements for any upgraded future requirements on this new NGFW investment	No Change	As per RFP
123	97	ANNEXURE-18: TECHNICAL SPECIFICATIONS	Item no. 1: Internet Firewall	Storage for Data Center Firewall is 500 GB HDD	Storage for Data Center should be 500 GB HDD/SSD. SSD provide better performance and all new appliances are now embedded with SSD storage for better functionality.	Clause Ammended	Refer Final RFP
124	97		Item no. 1: Internet Firewall NGFW Filtering Requirements	Storage for Data Center Firewall is 500 GB HDD	Storage for Data Center should be 500 GB HDD/SSD. SSD provide better performance and all new appliances are now embedded with SSD storage for better functionality.	Clause Ammended	Refer Final RFP
125	97	Data Center (DC) Firewall	Performance Requirements	NGFW must have minimum Next Generation Firewall throughput of 25 Gbps.	**Requested Change:**NGFW must have minimum Next Generation Firewall throughput of 25 Gbps with application-identification/AVC/application control and logging enabled considering transaction size of 64KB HTTP packet **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, The NGFW throughput should clearly mention App-ID/AVC/App Control and logging to be enabled while the throughput is computed with a packet size reference of 64KB HTTP to evaluate equivalent platforms on performance. Packet size will define the baseline for deriving these throughput values and is a critical aspect in the throughput calculation	Clause Ammended	Refer Final RFP
126	97	Data Center (DC) Firewall	Performance Requirements	The NGFW must support at least 8 million concurrent connections..	**Requested Change:**The NGFW must support at least 2.5 million Layer 7 concurrent connections/sessions **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, the session count calculation should also be defined for Layer 7 traffic rather than keeping it generic where OEMs can even interpret this as a Layer 4 session count and such derived references will impact the RajComp Perimeter Security Layer devices from performance standpoint during traffic throttling	Clause Ammended	Refer Final RFP
127	97	Data Center (DC) Firewall	Performance Requirements	The NGFW must support more than 300,000 new connections per second processing.	**Requested Change:**The NGFW must support at least 250,000 new Layer 7 connections per second considering 1 byte HTTP transaction **Justification:** The traffic flow within the RajComp datacenter will be application oriented and NGFW appliances are built around L7 inspection and control. So, the session count calculation should also be defined for Layer 7 traffic rather than keeping it generic where OEMs can even interpret this as a Layer 4 session count and such derived references will impact the RajComp Perimeter Security Layer devices from performance standpoint during traffic throttling	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
128	98	Management Appliance	3	Management Server and Logging module must be single solution. It must allow administrator to choose to login in read-only or read-write mode. Option must be available at Authentication window itself.	Every OEM has it's own architecture to have separate or single management server and logging module. It's recommended to have separate logging module for optimized performance of the applinace. Geretaing the report tidious task and need good memory and CPU of the appliance and it will createissue/problem to use the same applinace as management server during same time. Would request to change the clause as "Management Server and Logging module must be single /seperate solution" so that Fortinet can also participate in this RFP.	Clause Ammended	Refer Final RFP
129	98	Management Appliance	3	Management Server and Logging module must be single solution. It must allow administrator to choose to login in read-only or read-write mode. Option must be available at Authentication window itself.	Every OEM has it's own architecture to have separate or single management server and logging module. It's recommended to have separate logging module for optimized performance of the applinace. Geretaing the report tidious task and need good memory and CPU of the appliance and it will createissue/problem to use the same applinace as management server during same time. Would request to change the clause as "Management Server and Logging module must be single /seperate solution" so that Fortinet can also participate in this RFP.	Clause Ammended	Refer Final RFP
130	98	Management Appliance	3	Management Server and Logging module must be single solution. It must allow administrator to choose to login in read-only or read-write mode. Option must be available at Authentication window itself.	Every OEM has it's own architecture to have separate or single management server and logging module. It's recommended to have separate logging module for optimized performance of the applinace. Geretaing the report tidious task and need good memory and CPU of the appliance and it will createissue/problem to use the same applinace as management server during same time. Would request to change the clause as "Management Server and Logging module must be single /seperate solution" so that Fortinet can also participate in this RFP.	Clause Ammended	Refer Final RFP
131	98	Management Appliance	3	Management Server and Logging module must be single solution. It must allow administrator to choose to login in read-only or read-write mode. Option must be available at Authentication window itself.	Every OEM has it's own architecture to have separate or single management server and logging module. It's recommended to have separate logging module for optimized performance of the applinace. Geretaing the report tidious task and need good memory and CPU of the appliance and it will createissue/problem to use the same applinace as management server during same time. Would request to change the clause as "Management Server and Logging module must be single /seperate solution" so that Fortinet can also participate in this RFP.	Clause Ammended	Refer Final RFP
132	98	Management Appliance	3	Management Server and Logging module must be single solution. It must allow administrator to choose to login in read-only or read-write mode. Option must be available at Authentication window itself.	Every OEM has it's own architecture to have separate or single management server and logging module. It's recommended to have separate logging module for optimized performance of the applinace. Geretaing the report tidious task and need good memory and CPU of the appliance and it will createissue/problem to use the same applinace as management server during same time. Would request to change the clause as "Management Server and Logging module must be single /seperate solution" so that Fortinet can also participate in this RFP.	Clause Ammended	Refer Final RFP
133	98	Management Appliance	9	NGFW Management should support minimum 10,0000 peak log per sec with 3TB storage.	The asked peak log per sec is too high and storage is too low and and would request to change it to 4000 peak log/sec. and storage to 16TB.	Clause Ammended	Refer Final RFP
134	98	Management Appliance	9	NGFW Management should support minimum 10,0000 peak log per sec with 3TB storage.	The asked peak log per sec is too high and storage is too low and and would request to change it to 4000 peak log/sec. and storage to 16TB.	Clause Ammended	Refer Final RFP
135	98	Management Appliance	9	NGFW Management should support minimum 10,0000 peak log per sec with 3TB storage.	The asked peak log per sec is too high and storage is too low and and would request to change it to 4000 peak log/sec. and storage to 16TB.	Clause Ammended	Refer Final RFP
136	98	Management Appliance	9	NGFW Management should support minimum 10,0000 peak log per sec with 3TB storage.	The asked peak log per sec is too high and storage is too low and and would request to change it to 4000 peak log/sec. and storage to 16TB.	Clause Ammended	Refer Final RFP
137	98	Management Appliance	9	NGFW Management should support minimum 10,0000 peak log per sec with 3TB storage.	The asked peak log per sec is too high and storage is too low and and would request to change it to 4000 peak log/sec. and storage to 16TB.	Clause Ammended	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
138	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 1	Management Server should be sperate sever to manage the NGFW & must be hardware based multi-tenant appliance. Multi-tenant Security Management hardware platform must provides more security and control by segmenting security management into multiple virtual domains based on geography, business unit, security functions to strengthen security and simplify management. for instance the Internet and the Data Center firewalls should have dedicated management and logging tenant on the security managemnet with segregated security policy database protected with role based access control	In case of hardware based management server, scalability will be a challenge. Same can be easily achieved in virtual management server. Also the management will be much more easy. Also in order to transfer management server to open server in case of failure, virtual managment server will be useful. As we can simply deploy virtual managment server on open server and then install last taken backup on the same. Hence requesting to remove "hardware based" from the clause.	Clause Ammended	Refer Final RFP
139	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 1	Management Server should be sperate sever to manage the NGFW & must be hardware based multi-tenant appliance. Multi-tenant Security Management hardware platform must provides more security and control by segmenting security management into multiple virtual domains based on geography, business unit, security functions to strengthen security and simplify management. for instance the Internet and the Data Center firewalls should have dedicated management and logging tenant on the security managemnet with segregated security policy database protected with role based access control	In case of hardware based management server, scalability will be a challenge. Same can be easily achieved in virtual management server. Also the management will be much more easy. Also in order to transfer management server to open server in case of failure, virtual managment server will be useful. As we can simply deploy virtual managment server on open server and then install last taken backup on the same. Hence requesting to remove "hardware based" from the clause.	Clause Ammended	Refer Final RFP
140	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 3	Management Server and Logging module must be single solution. It must allow administrator to choose to login in read-only or read-write mode. Option must be available at Authentication window itself.	Instead of controlling the access while logging the management server, it is better to control the same while creating administrative users. Hence requesting to change the same clause to " capability of Role based administration"	Clause Ammended	Refer Final RFP
141	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 3	Management Server and Logging module must be single solution. It must allow administrator to choose to login in read-only or read-write mode. Option must be available at Authentication window itself.	Instead of controlling the access while logging the management server, it is better to control the same while creating administrative users. Hence requesting to change the same clause to " capability of Role based administration"	Clause Ammended	Refer Final RFP
142	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 4	Management Server must support backup with all configuration, certificates etc. It should be possible to restore management server configuration on normal open server to manage network security in case of failure.	In order to transfer management server to open server in case of failure, virtual managment server will be useful. As we can simply deploy virtual managment server on open server and then install last taken backup on the same. Hence requesting to remove "hardware based" from the clause.	No Change	As per RFP
143	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 4	Management Server must support backup with all configuration, certificates etc. It should be possible to restore management server configuration on normal open server to manage network security in case of failure.	In order to transfer management server to open server in case of failure, virtual managment server will be useful. As we can simply deploy virtual managment server on open server and then install last taken backup on the same. Hence requesting to remove "hardware based" from the clause.	No Change	As per RFP
144	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 5	Solution must support multiple administrators to work on policies on session based, All the policies and objects on which Administrator 1 is working should be locked for all other administrator, however other administrator can work on other policy rules and objects in their respective sessions. Changes done by Administrator-1 should not be visible to other administrators till the time Administrator-1 publish changes.	Such clashes can be managed while creating admins for the management server. Role based administration can easliy help to manage the management server. So requesting to remove this clause. Or change it to "Role based administration"	No Change	As per RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
145	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 5	Solution must support multiple administrators to work on policies on session based, All the policies and objects on which Administrator 1 is working should be locked for all other administrator, however other administrator can work on other policy rules and objects in their respective sessions. Changes done by Administrator-1 should not be visible to other administrators till the time Administrator-1 publish changes.	Such clashes can be managed while creating admins for the management server. Role based administration can easliy help to manage the management server. So requesting to remove this clause. Or change it to "Role based administration"	No Change	As per RFP
146	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 9	NGFW Management should support minimum 10,0000 peak log per sec with 3TB storage.	Hardware appliance has limitation in case of storage, if virtual management server is deployed storage can be upgraded time to time as per requirement. Hence either change storage to 2TB or change appliance type to virtual.	Clause Ammended	Refer Final RFP
147	98	7.1 Annexure 18	Management Appliance - Management & Logging- Sl. No. 9	NGFW Management should support minimum 10,0000 peak log per sec with 3TB storage.	Hardware appliance has limitation in case of storage, if virtual management server is deployed storage can be upgraded time to time as per requirement. Hence either change storage to 2TB or change appliance type to virtual.	Clause Ammended	Refer Final RFP
148	96	ANNEXURE-18: TECHNICAL SPECIFICATIONS	Item no. 1: Internet Firewall		**We request the department to incorporate this point**: Based on the hardware specifications 8 physical cores are required for internet firewall. We request the deaprtment to incorporate this point as 8 cores processor required.	No Change	As per RFP
149	97	ANNEXURE-18: TECHNICAL SPECIFICATIONS	Item no. 2: Data Center (DC) Firewall		**We request the department to incorporate this point**: Based on the hardware specifications 24 physical cores are required for data center firewalls.We request the deaprtment to incorporate this point as 24 cores processor required.	No Change	As per RFP
150	NA	Internet Firewall & Data Center (DC) Firewall	General	Additional Clause to be incorporated	The proposed solution must support policy optimization feature and allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters. Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis	No Change	As per RFP
151	NA	Internet Firewall & Data Center (DC) Firewall	General	Additional Clause to be incorporated	The proposed solution must support policy optimization feature and allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters. Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis	No Change	As per RFP
152	NA	Internet Firewall & Data Center (DC) Firewall	General	Additional Clause to be incorporated	The proposed device should be futuristic with support for machine learning capabilities from day and support for AI based operations, IoT, OT and DNS tunnel inspection, VXLAN inspection as and when required	No Change	As per RFP
153	NA	Internet Firewall & Data Center (DC) Firewall	General	Additional Clause to be incorporated	The proposed device should be futuristic with support for machine learning capabilities from day and support for AI based operations, IoT, OT and DNS tunnel inspection, VXLAN inspection as and when required	No Change	As per RFP
154	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	It is highly recommended to have Internet and DC NGFW from two different OEMs to safeguard the critical assets from expanding attack surface and exploits. If one NGFW bypasses a threat there are high chances of being bypassed by second layer NGFW also if they are from same OEM as they will have same IPS signature / anti-malware updates. If both NGFWs are from different OEMs, it will ensure robust security to the critical DC as if one NGFW misses a threat, it will be surely deleted and mitigated by the other NFGW that is from different OEM	Refer Ammended RFP	Refer Final RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
155	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	It is highly recommended to have Internet and DC NGFW from two different OEMs to safeguard the critical assets from expanding attack surface and exploits. If one NGFW bypasses a threat there are high chances of being bypassed by second layer NGFW also if they are from same OEM as they will have same IPS signature / anti-malware updates. If both NGFWs are from different OEMs, it will ensure robust security to the critical DC as if one NGFW misses a threat, it will be surely deleted and mitigated by the other NFGW that is from different OEM	Refer Ammended RFP	Refer Final RFP
156	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	It is highly recommended to have Internet and DC NGFW from two different OEMs to safeguard the critical assets from expanding attack surface and exploits. If one NGFW bypasses a threat there are high chances of being bypassed by second layer NGFW also if they are from same OEM as they will have same IPS signature / anti-malware updates. If both NGFWs are from different OEMs, it will ensure robust security to the critical DC as if one NGFW misses a threat, it will be surely deleted and mitigated by the other NFGW that is from different OEM	Refer Ammended RFP	Refer Final RFP
157	NA	General	General	NEW CLAUSE	Based on the hardware specifications, 8 physical cores are required for internet firewall and 24 physical cores for data center firewalls.	No Change	As per RFP
158	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	Since the ask is for DC NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 50 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
159	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	Since the ask is for DC NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 50 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
160	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	Since the ask is for DC NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 50 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
161	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	Since the ask is for Internet NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 40 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
162	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	Since the ask is for Internet NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 40 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
163	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	Since the ask is for Internet NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 40 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
164	NA	General	General	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	Since the ask is for Internet NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 40 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
165	NA	General	General	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	Since the ask is for DC NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 50 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP

Sl. No.	RFP Page No.	RFP Chapter No.	RFP Clause No.	Clause Details as per RFP	Query/Clarification/Suggestion	Comments	Department Remark
166	NA	General	General	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	It is highly recommended to have Internet and DC NGFW from two different OEMs to safeguard the critical assets from expanding attack surface and exploits. If one NGFW bypasses a threat there are high chances of being bypassed by second layer NGFW also if they are from same OEM as they will have same IPS signature / anti-malware updates. If both NGFWs are from different OEMs, it will ensure robust security to the critical DC as if one NGFW misses a threat, it will be surely deleted and mitigated by the other NFGW that is from different OEM	Refer Ammended RFP	Refer Final RFP
167	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	Since the ask is for Internet NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 40 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
168	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	Since the ask is for DC NGFW, The proposed solution shall support the client to site VPN to provide secure connectivity for users from "work from any where". Would request to include this rerquirement and proposed solution should support 50 Gbps VPN throughput and 50000 client to site VPN license.	No Change	As per RFP
169	NA	Suggestion- Addition - Data Center (DC) Firewall and Internet Firewall	General	General	It is highly recommended to have Internet and DC NGFW from two different OEMs to safeguard the critical assets from expanding attack surface and exploits. If one NGFW bypasses a threat there are high chances of being bypassed by second layer NGFW also if they are from same OEM as they will have same IPS signature / anti-malware updates. If both NGFWs are from different OEMs, it will ensure robust security to the critical DC as if one NGFW misses a threat, it will be surely deleted and mitigated by the other NFGW that is from different OEM	Refer Ammended RFP	Refer Final RFP