Responses to Pre-bid Queries

Bid for Supply, Installation, Commissioning & Maintenance of Firewall Appliances on behalf of Directorate of Technical Education, Gandhinagar
(Tender No. HWT180818508)

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Vendors	Responses to the Queries
	Page No. / Section No. / Clause No.	Tender Description		
1	Page No. 13 & 14 / Section 4 / Technical Specification / Item No. 1: Firewall Appliance (Type 1)	The proposed system should support IPsec VPN throughput of 5 Gbps	The proposed system should support IPsec VPN throughput of 10 Gbps	No change, As per RFP
2		The proposed system should support IPS throughput of 2 Gbps	The proposed system should support IPS throughput of 10 Gbps	No change, As per RFP
3		The proposed system should support AV + IPS + App control enabled throughput of 1 Gbps	The proposed system should support IPS throughput of 4 Gbps	No change, As per RFP
4		Web Filtering: Keyword, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL.	Web Filtering: Keyword, Block Java applets, cookies, ActiveX, Block malware,	No change, As per RFP
5		Appliance should support Virtual Firewall feature or should support direct termination of NKN (National Knowledge Network) link at college.	Has to be deleted	No change, As per RFP
6	Page No. 13 & 14 / Section 4 / Technical Specification / Item No. 1: Firewall Appliance (Type 1)	Device should have minimum firewall throughput of 30 Gbps	Device should have minimum firewall throughput of 28 Gbps	No change, As per RFP
7		Should support at least 40,00,000 concurrent sessions	Should support at least 30,00,000 concurrent sessions	No change, As per RFP
8		The proposed system should support IPsec VPN throughput of 8 Gbps	The proposed system should support IPsec VPN throughput of 14 Gbps	No change, As per RFP
9		The proposed system should support IPS throughput of 4 Gbps	The proposed system should support IPS throughput of 18 Gbps	No change, As per RFP
10		The proposed system should support AV + IPS + App control enabled throughput of 2.7 Gbps	The proposed system should support AV + IPS + App control enabled throughput of 9 Gbps	No change, As per RFP
11		Web Filtering: Keyword, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL.	Web Filtering: Keyword, Block Java applets, cookies, ActiveX, Block malware,	No change, As per RFP
12		Appliance should support Virtual Firewall feature or should support direct termination of NKN (National Knowledge Network) link at college.	Has to be deleted	No change, As per RFP
13	Page No. 5 / Section 1 / Eligibility Criteria	OEM of the Proposed Security Appliances should be in the Leadership / Challengers / Visionaries quadrant in the Gartner Magic Quadrant for UTM, June 2017 OR should be among the top five positions in terms of worldwide market share as per IDC report for worldwide quarterly security appliance tracker, Q12018. Documentary proof to be submitted for the same.	OEM of the Proposed Security Appliances should be in the Leadership / Challengers / Visionaries quadrant in the Gartner Magic Quadrant for UTM, June 2017 OR should be among the top five positions in terms of worldwide market share as per IDC report for worldwide quarterly security appliance tracker, Q12018. Documentary proof to be submitted for the same. Also proposed solution must be recommended by NSS SVM NGFW latest report.

Gartner & IDC are both sales/commercial criteria. As Firewall is core technical product we request you to ask NSS recommendation also which is well-accepted technical certificate across industry. | No change, As per RFP |

Sr. No.	Page No. / Section No. / Clause No.	Tender Description	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
		Tender Reference		
14	Page No. 13 / Section 4 / Technical Specification / Item No. 1: Firewall Appliance (Type 1)	The proposed system should support IPS throughput of 2 Gbps	The proposed system should support IPS throughput of 2 Gbps Real world/enterprise mix traffic. Many OEM degrades for 10 times when tested with Enterprise world traffic. Datasheets values are tested with some recommended profiles & its very impractical to get the nearby throughput in real deployment. Enterprise world throughput are testing with realistic policies & can be achievable after deployment. Request you to ask for real world/enterprise mix traffic for this clause. Almost all the well-known OEM published this values who are tested with well accepted technical bodies & are confident in their performance. Request for your consideration for the same.	No change, As per RFP
15		The proposed system should support AV + IPS + App control enabled throughput of 1 Gbps	The proposed system should support AV + IPS + App control enabled throughput of 1 Gbps real world/Enterprise mix Traffic. Many OEM degrades for 10 times when tested with Enterprise world traffic. Datasheets values are tested with some recommended profiles & its very impractical to get the nearby throughput in real deployment. Enterprise world throughput are testing with realistic policies & can be achievable after deployment. Request you to ask for real world/enterprise mix traffic for this clause. Almost all the well-known OEM published this values who are tested with well accepted technical bodies & are confident in their performance. Request for your consideration for the same.	No change, As per RFP
16	Page No. 14 / Section 4 / Technical Specification / Item No. 2: Firewall Appliance (Type 2)	The proposed system should support IPS throughput of 4 Gbps	The proposed system should support IPS throughput of 4 Gbps real world/Enterprise mix Traffic. Many OEM degrades for 10 times when tested with Enterprise world traffic. Datasheets values are tested with some recommended profiles & its very impractical to get the nearby throughput in real deployment. Enterprise world throughput are testing with realistic policies & can be achievable after deployment. Request you to ask for real world/enterprise mix traffic for this clause. Almost all the well-known OEM published this values who are tested with well accepted technical bodies & are confident in their performance. Request for your consideration for the same.	No change, As per RFP
17		The proposed system should support AV + IPS + App control enabled throughput of 2.7 Gbps	The proposed system should support AV + IPS + App control enabled throughput of 2.7 Gbps real world/Enterprise mix Traffic. Many OEM degrades for 10 times when tested with Enterprise world traffic. Datasheets values are tested with some recommended profiles & its very impractical to get the nearby throughput in real deployment. Enterprise world throughput are testing with realistic policies & can be achievable after deployment. Request you to ask for real world/enterprise mix traffic for this clause. Almost all the well-known OEM published this values who are tested with well accepted technical bodies & are confident in their performance. Request for your consideration for the same.	No change, As per RFP

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference		Query / Clarification / Suggestions from the Vendors	Responses to the Queries
		Tender Description			
18	Page No. 15 / Section 4 / Technical Specification / Item No. 3: Firewall Appliance (Type 3)	The proposed system should support IPS throughput of 5 Gbps		The proposed system should support IPS throughput of 5 Gbps real world/Enterprise mix Traffic. Many OEM degrades for 10 times when tested with Enterprise world traffic. Datasheets values are tested with some recommended profiles & its very impractical to get the nearby throughput in real deployment. Enterprise world throughput are testing with realistic policies & can be achievable after deployment. Request you to ask for real world/enterprise mix traffic for this clause. Almost all the well-known OEM published this values who are tested with well accepted technical bodies & are confident in their performance. Request for your consideration for the same.	No change, As per RFP
19		The proposed system should support AV + IPS + App control enabled throughput of 4 Gbps		The proposed system should support AV + IPS + App control enabled throughput of 4 Gbps real world/Enterprise mix Traffic. Many OEM degrades for 10 times when tested with Enterprise world traffic. Datasheets values are tested with some recommended profiles & its very impractical to get the nearby throughput in real deployment. Enterprise world throughput are testing with realistic policies & can be achievable after deployment. Request you to ask for real world/enterprise mix traffic for this clause. Almost all the well-known OEM published this values who are tested with well accepted technical bodies & are confident in their performance. Request for your consideration for the same.	No change, As per RFP
20	Page No. 16 / Section 4 / Technical Specification / Note	Bidder is responsible for providing required hardware (having storage capacity to store the logs of minimum last 1-year period), software and licenses (valid perpetual for life) for storing the logs.		Bidder is responsible for providing required dedicated & out of the box solution for logging in the form of hardware/Software/Cloud of the same Firewall OEM (having storage capacity to store the logs of minimum last 1 year period or with Minimum 2TB storage), License must be provide with support for same no. of years as per Firewall ask with support. Bidder proposing Software/Cloud option must also supply required hardware & license for every respective locations. Solution must be separate for every location. Dedicated & Out of the FW box logging is recommended as in case Firewall is down due to any attack & logs stored under FW (which is already down) there is no way to Tshoot the event & not possible to know the exact cause of the issue. Also due to this reason, all the historical logs are also lost if Firewall is replaced. So we highly recommends to ask dedicated & out of the FW box logging solution. Logging solution must from the same OEM for better Integration, visibility & single point support. There are few flavors of Logging solution available like Hardware/Software/Cloud. Request you to allow all the available forms from same OEM. Required hardware/software/licenses for proposed form can be provided by bidder from the day 1. It is difficult to say how many log is recd in 1 year. So request you to allow confirmation of storing 1 Year logs or at least 2TB storage which is quite good to store decent amount of logs. Admins & management for every location is different, so request you to consider this point for every respective location.	No change, As per RFP. Additionally, device has to provide for log and MIS reports also.

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
		Tender Description		
21		Additional Point Request	Proposed solution must offer cloud based sandbox for zero day detection & Mitigation. As today Zero day seems like a mandate for every organization to detect & mitigate. We highly recommends to ask for the same due to security reasons. Almost all the OEM's in the market are proposing the same.	No change, As per RFP
22		Additional Point Request	Proposed solution must offer 16GB flash drive for storing of multiple Firmware images & other required stuff into it. As Disk is not asked in the solution & also disk is vulnerable part so it is better not to have. We recommends to ask at least 16GB flas drive to store multiple Firmware images into it & other required stuffs.	No change, As per RFP
23	Page No. 13 to 16 / Section 4 / Technical Specification / On all 3 types Firewall	Additional Point Request	Proposed firewall must offer at least 2 Soft tokens/SMS gateway for 5 years for admin user for 2Factor authentication license for every location for admin to login into FW GUI. We all speak that Username & password are dead but when it comes to our secure our own security forgot its mainly not asked. We highly recommends to have 2FA to login into FW via Soft token or SMS so that if Username password compromise, still no one else can login into the unit.	No change, As per RFP
24		Additional Point Request	Proposed solution must offer performance based load balancing of multiple ISP in terms of Packet drops & latency. For example if there 10% packet drop on ISP A it should shift to ISP B. Or if there is more than 100ms latency observe in ISP A it should failover to ISP B. Today world moves on different level of Load balancing method. Just pingging IP & check for link & than failover is purely outdated method. Request you to ask for advance load balancing methods.	No change, As per RFP
25	Page No. 7 / Section 2 / Scope of Work	The Bidder may quote only one option (i.e. only one product can be quoted) against each item. Bidders are required to mention make & model of the product. (Do not write "OEM" against items as bidders are expected to give make & model of the product).	The Bidder may quote only one option (i.e. only one product can be quoted) against each item. Bidders are required to mention make & model of the product. (Do not write "OEM" against items as bidders are expected to give make & model of the product). All 3 types must be from same OEM. It is always recommended to have Same OEM brand at all 3 types for better support, easy management & integration part (if required in future). Request for your consideration.	No change, As per RFP
26	Page No. 13 / Section 4 / Technical Specification / Item No. 1: Firewall Appliance (Type 1)	Device should have minimum firewall throughput of 20 Gbps	Please remove this clause. This clause contradict the other clauses like IPS throughput and AV+IPS+App throughput which is 2 Gbps and 1 Gbps resp already mentioned in RFP	No change, As per RFP
27		Firewall should support at least 1,25,000 new connections per second	Please change the clause to "Firewall should support at least 20000 new connections per second". Considering the number of students and faculty in college/institute access internet simultaneously is going to be quite lower and hence we reques to change the clause	No change, As per RFP

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference		Query / Clarification / Suggestions from the Vendors	Responses to the Queries
		Tender Description			
28		The proposed system should support IPsec VPN throughput of 5 Gbps		Please change the clause to "The proposed system should support IPsec VPN throughput of 1 Gbps" Objective of VPN is to provide access the network from remote location and probabiliy for remote location faculties and admins managing network. The overall throughput of VPN can not be more than IPS. Hence requesting change	No change, As per RFP
29		The proposed system should support IPS throughput of 2 Gbps		Kindly remove this clause Since the throughput of NGFW which includes FW+ AVC + IPS is already mentioned. Request you to remove this clause	No change, As per RFP
30		Firewall should support user & admin authentication via captive portal & should be integrate with **LDAP, RADIUS, AD for SSO**		Please change the clause to "Firewall should support user & admin authentication via captive portal & should be integrate with **LDAP/ RADIUS/ AD for SSO"**. Firewall deployed at perimeter is to protect College/institute from outside threats and users/students should be authenticate before even then given access to network and hence requesting change	**Clause is revised as mentioned below:** Firewall should support user & admin authentication via captive portal & should be integrate with **LDAP/RADIUS/AD for SSO**
31		The proposed system should support AV + IPS + App control enabled throughput of 1 Gbps		Please change the clause to "The proposed system should support AV / Zero-Day Protection + IPS + App control enabled throughput of 1 Gbps". As per our understanding the objective of mentioning AV is to ensure that solution should provide protection against zero-day and unknown threat. Different OEM have different approach to meet the functional requirement and hence requesting change	No change, As per RFP
32		Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection		Please confirm whether solution proposed DDoS solution should support automatic Real Time Signature generation based on Rate Variant, Rate Invariant algorithms & Challenge Response Mechnanisms; within few seconds, without human intervention. This ensure that DDoS solution help college/institute protect against latest threat without human intervention	No change, As per RFP
33	Page No. 14 / Section 4 / Technical Specification / Item No. 1: Firewall Appliance (Type 1)	Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection		Please confirm whether proposed solution should support more than 25,000 (excluding custom signatures) IPS signatures or more. This ensure that IPS protect college/institute against broad range of threats	No change, As per RFP
34		Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection		Please confirm whether DDoS solution should also support 1 Gbps of throughput along with FW+IPS+AVC functionality. This ensure that college/institute is protected against 1 Gbps of DDoS attack	No change, As per RFP
35		Appliance should have ICSA certification for Firewall.		Please change the clause to "Appliance should have ICSA / EAL / NSS certification for Firewall." Different OEM support different certification and hence requested change	**Clause is revised as mentioned below:** Appliance should have **latest** ICSA / NSS certification for Firewall **at the time of bid submission.**

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Vendors	Responses to the Queries
	Page No. / Section No. / Clause No.	Tender Description		
36		Proposed device should also perform activities like Intrusion prevention, IP Reputation, URL filtering, Web filtering, content filtering, Anti-BOT control and Antivirus from day one with required Licenses valid perpetual for life and 24*7 support valid for 7 Years .	Please change the clause to "Proposed device should also perform activities like Intrusion prevention, IP Reputation, URL filtering, Web filtering, content filtering, Anti-BOT control and Antivirus / Zero-day protection from day one with required Licenses valid perpetual for life and 24*7 support valid for 7 Years ." As per our understanding the objective of mentioning AV is to ensure that solution should provide protection against zero-day and unknown threat. Different OEM have different approach to meet the functional requirement and hence requesting change	No change, As per RFP
37	Page No. 14 & 15 / Section 4 / Technical Specification / Item No. 2: Firewall Appliance (Type 2)	Device should have minimum firewall throughput of 30 Gbps	Please remove this clause. This clause contradict the other clauses like IPS throughput and AV+IPS+App throughput which is 4 Gbps and 2.7 Gbps resp already mentioned in RFP	No change, As per RFP
38		Firewall should support at least 2,25,000 new connections per second	Please change the clause to "Firewall should support at least 20000 new connections per second". Considering the number of students and faculty in college/institute access internet simultaneously is going to be quite lower and hence we reques to change the clause	No change, As per RFP
39		Should support at least 40,00,000 concurrent sessions	Please change the clause to "Firewall should support at least 20,00,000 new connections per second". Considering the number of students and faculty in college/institute access internet simultaneously is going to be quite lower and hence we reques to change the clause	No change, As per RFP
40		The proposed system should support IPsec VPN throughput of 5 Gbps	Please change the clause to "The proposed system should support IPsec VPN throughput of 1 Gbps". Objective of VPN is to provide access the network from remote location and probabiliy for remote location faculties and admins managing network. The overall throughput of VPN can not be more than IPS. Hence requesting change	No change, As per RFP
41		The proposed system should support IPS throughput of 4 Gbps	Kindly remove this clause. Since the throughput of NGFW which includes FW+ AVC + IPS is already mentioned. Request you to remove this clause	No change, As per RFP
42		Appliance should have ICSA certification for Firewall.	Please change the clause to "Appliance should have ICSA / EAL / NSS certification for Firewall." Different OEM support different certification and hence requested change	**Clause is revised as mentioned below:** Appliance should have **latest** ICSA / NSS certification for Firewall **at the time of bid submission.**
43		Proposed device should also perform activities like Intrusion prevention, IP Reputation, URL filtering, Web filtering, content filtering, Anti-BOT control and Antivirus from day one with required Licenses valid perpetual for life and 24*7 support valid for 7 Years .	Please change the clause to "Proposed device should also perform activities like Intrusion prevention, IP Reputation, URL filtering, Web filtering, content filtering, Anti-BOT control and Antivirus / Zero-day protection from day one with required Licenses valid perpetual for life and 24*7 support valid for 7 Years ." As per our understanding the objective of mentioning AV is to ensure that solution should provide protection against zero-day and unknown threat. Different OEM have different approach to meet the functional requirement and hence requesting change	No change, As per RFP

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
		Tender Description		
44		Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection	Please confirm whether solution proposed DDoS solution should support automatic Real Time Signature generation based on Rate Variant, Rate Invariant algorithms & Challenge Response Mechnanisms; within few seconds, without human intervention. This ensure that DDoS solution help college/institute protect against latest threat without human intervention	No change, As per RFP
45		Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection	Please confirm whether proposed solution should support more than 25,000 (excluding custom signatures) IPS signatures or more. This ensure that IPS protect college/institute against broad range of threats	No change, As per RFP
46		Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection	Please confirm whether DDoS solution should also support 1 Gbps of throughput along with FW+IPS+AVC functionality. This ensure that college/institute is protected against 2 Gbps of DDoS attack	No change, As per RFP
47		Firewall should support user & admin authentication via captive portal & should be integrate with LDAP, RADIUS, AD for SSO	Please change the clause to "Firewall should support user & admin authentication via captive portal & should be integrate with LDAP/ RADIUS/ AD for SSO". Firewall deployed at perimeter is to protect College/institute from outside threats and users/students should be authenticate before even then given access to network and hence requesting change	**Clause is revised as mentioned below:** Firewall should support user & admin authentication via captive portal & should be integrate with **LDAP/RADIUS/AD for SSO**
48	Page No. 15 & 16 / Section 4 / Technical Specification / Item No. 3: Firewall Appliance (Type 3)	Device should have minimum firewall throughput of 35 Gbps	Please remove this clause. This clause contradict the other clauses like IPS throughput and AV+IPS+App throughput which is 5 Gbps and 4 Gbps resp already mentioned in RFP	No change, As per RFP
49		Should support at least 80,00,000 concurrent sessions	Please change the clause to "Firewall should support at least 20000 new connections per second". Considering the number of students and faculty in college/institute access internet simultaneously is going to be quite lower and hence we reques to change the clause	No change, As per RFP
50		Firewall should support at least 2,75,000 new connections per second	Please change the clause to "Firewall should support at least 20,00,000 new connections per second". Considering the number of students and faculty in college/institute access internet simultaneously is going to be quite lower and hence we reques to change the clause	No change, As per RFP
51		The proposed system should support IPsec VPN throughput of 10 Gbps	Please change the clause to "The proposed system should support IPsec VPN throughput of 1 Gbps". Objective of VPN is to provide access the network from remote location and probabiliy for remote location faculties and admins managing network. The overall throughput of VPN can not be more than IPS. Hence requesting change	No change, As per RFP
52		The proposed system should support IPS throughput of 5 Gbps	Kindly remove this clause. Since the throughput of NGFW which includes FW+ AVC + IPS is already mentioned. Request you to remove this clause	No change, As per RFP

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference Tender Description	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
53		Appliance should have ICSA certification for Firewall.	Please change the clause to "Appliance should have ICSA / EAL / NSS certification for Firewall." Different OEM support different certification and hence requested change	**Clause is revised as mentioned below:** Appliance should have **latest** ICSA / NSS certification for Firewall **at the time of bid submission.**
54		Proposed device should also perform activities like Intrusion prevention, IP Reputation, URL filtering, Web filtering, content filtering, Anti-BOT control and Antivirus from day one with required Licenses valid perpetual for life and 24*7 support valid for 7 Years .	Please change the clause to "Proposed device should also perform activities like Intrusion prevention, IP Reputation, URL filtering, Web filtering, content filtering, Anti-BOT control and Antivirus / Zero-day protection from day one with required Licenses valid perpetual for life and 24*7 support valid for 7 Years ." As per our understanding the objective of mentioning AV is to ensure that solution should provide protection against zero-day and unknown threat. Different OEM have different approach to meet the functional requirement and hence requesting change	No change, As per RFP
55		Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection	Please confirm whether solution proposed DDoS solution should support automatic Real Time Signature generation based on Rate Variant, Rate Invariant algorithms & Challenge Response Mechanisms; within few seconds, without human intervention. This ensure that DDoS solution help college/institute protect against latest threat without human intervention	No change, As per RFP
56		Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection	Please confirm whether proposed solution should support more than 25,000 (excluding custom signatures) IPS signatures or more. This ensure that IPS protect college/institute against broad range of threats	No change, As per RFP
57		Intrusion Prevention System (IPS): should be able to mitigate attacks like FTP Attack, HTTP Attack, DNS Attack, ICMP Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures, IPS Policies, Automatic real-time updates, Protocol Anomaly Detection	Please confirm whether DDoS solution should also support 1 Gbps of throughput along with FW+IPS+AVC functionality. This ensure that college/institute is protected against 2 Gbps of DDoS attack	No change, As per RFP
58		Firewall should support user & admin authentication via captive portal & should be integrate with LDAP, RADIUS, AD for SSO	Please change the clause to "Firewall should support user & admin authentication via captive portal & should be integrate with LDAP/ RADIUS/ AD for SSO". Firewall deployed at perimeter is to protect College/institute from outside threats and users/students should be authenticate before even then given access to network and hence requesting change	**Clause is revised as mentioned below:** Firewall should support user & admin authentication via captive portal & should be integrate with **LDAP/RADIUS/AD for SSO**
59	Page No. 5 / Section 1 / Eligibility Criteria	OEM of the Proposed Security Appliances should be in the Leadership / Challengers / Visionaries quadrant in the Gartner Magic Quadrant for UTM, June 2017 OR should be among the top five positions in terms of worldwide market share as per IDC report for worldwide quarterly security appliance tracker, Q12018. Documentary proof to be submitted for the same.	OEM should be in Gartner's leader/Challengers for Enterprise firewall	No change, As per RFP
60		Additional	Since the NKN link/ internet link will be terminated on the firewall, request you to add the support for BGPv6	No change, As per RFP

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference Tender Description	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
61	Page No. 10 / Section 3 / General Terms & Conditions: Pt no 32	32. Delivery & Installation: Within 45 working days from the date of confirmed purchase order.	Request to change the timeline as within 10 weeks from the date of confirm purchase order.	**Clause is revised as mentioned below:** **Delivery & Installation:** Within 60 days from the date of signing of contract agreement.
62	Page No. 10 / Section 3 / General Terms & Conditions: Pt no 36	36. The successful Bidder will be required to co-ordinate with software vendor and/or do liasioning with other service provider to achieve the end-to-end connectivity. This also includes OS configuration with respect to LAN/WAN technologies implementation.	It is suggested to have central SPOC (SPOC - single point of contact) person for coordination between all stakeholders. Bidder will definitely support with all technical aspects.	No change, As per RFP
63	Page No. 7 / Section 3 / General Terms & Conditions: Pt no 4	4. The successful bidder will have to supply & install and provide operational training for supplied hardware to the purchasing department / end user staff.	Training should be at central location. All related expenses of department person to be owned by department only. Bidder will not be responsible for any kind of expenses related to department for this training.	No change, As per RFP
64	Page No. 7 / Section 3 / General Terms & Conditions: Pt no 37.2	37.2. Bidder must ensure that the warranty support & service should be available up to delivery locations to provide repairing cum replacement services of faulty equipments within 48 hrs.	Request to change the timeline for replacement as 4 working days. OR it should be as per OEM policy.	No change, As per RFP
65	General	General	Acceptance and testing criteria and time lines are not mentioned.	As per RFP
66		General	Acceptance will be released site wise or after complete delivery.	As per RFP
67		General	Who will provide the acceptance and test after the delivery and installation?.	As per RFP
68		General	What all documents need to be submit by the bidder to get the acceptance?.	As per RFP
69		General	Softcopies of all required documents must be acceptable to customer.	As per RFP
70		General	What will be the Plan of action if the site is not ready or the connectivity is down ? This will impact on implementation timeline & shall impact on cost for multiple time site visit.	As per RFP
71		General	Space, UPS power and other pre-requites will be arranged and managed by the customer at each location & post that customer should confirm to bidder so that bidder can send the engineer for device power on & further configuration & testing.	As per RFP
72		General	Configuration to be provided by customer OR bidder to define ?	As per RFP

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference		Query / Clarification / Suggestions from the Vendors	Responses to the Queries
		Tender Description			
73	Page No. 5 / Section 1 / Eligibility Criteria	OEM of the Proposed Security Appliances should be in the Leadership / Challengers / Visionaries quadrant in the Gartner Magic Quadrant for UTM, June 2017 OR should be among the top five positions in terms of worldwide market share as per IDC report for worldwide quarterly security appliance tracker, Q12018. Documentary proof to be submitted for the same.		OEM of the Proposed Security Appliances should be in the Leadership / Challengers / Visionaries quadrant in the Gartner Magic Quadrant for UTM/Enterprise, June 2017 OR should be among the top five positions in terms of worldwide market share as per IDC report for worldwide quarterly security appliance tracker, Q12018.Documentary proof to be submitted for the same. Gartner Magic Quadrant for Enterprise is the most commonly used Criteria in evaluation of NGFW.Most of the GOVT RFPs consider this evaluations. Request you to please include the Enterprise also so that we can comfortably qualify in tender.	No change, As per RFP
74	Page No. 13 & 14 / Section 4 / Technical Specification / Item No. 1: Firewall Appliance (Type 1)	Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and Nat46 (IPv4-to-IPv6)functionality, NAT66		Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and , NAT44. We all are aware of the fact that IPv6 is not fully in implementation across most of the Customers. However the practical implementations which uses IPv6 uses eith NAT 44 or NAT 66. Request you to remove NAT46	**Please refer revised clause:** Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6), Nat46 (IPv4-to-IPv6) and Nat64 (IPv6-to-IPv4) or equivalent functionality from day1. **Note:** Acceptable solution i.e. OEM/Bidder can achieve the same through providing additional hardware like Router (from Day 1 itself) of capacity equivalent to the firewall thus without compromising on any of the parameter like throughput, Ports etc. of the solution, as asked in the bid.
75		Web Filtering: Keyword, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL.		Web Filtering: Custom URL Block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL. Keywork Search is not a URL Capability ,its most of DLP feature. Ultimately any keyword search will link to a URL and will ultimately be blocked. Request you to change this to a Custom URL/Application control	No change, As per RFP
76		Appliance should have ICSA certification for Firewall.		Appliance should have ICSA/Common Criteria/ NSS Labs certification for Firewall. Every OEM has different certifications pertaining to FW certifications. Please relax for Common Criteria	**Clause is revised as mentioned below:** Appliance should have **latest** ICSA / NSS certification for Firewall **at the time of bid submission.**
77	Page No. 14 & 15 / Section 4 / Technical Specification / Item No. 2: Firewall Appliance (Type 2)	Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and Nat46 (IPv4-to-IPv6)functionality, NAT66		Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and , NAT44. We all are aware of the fact that IPv6 is not fully in implementation across most of the Customers. However the practical implementations which uses IPv6 uses eith NAT 44 or NAT 66. Request you to remove NAT46	**Please refer revised clause:** Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6), Nat46 (IPv4-to-IPv6) and Nat64 (IPv6-to-IPv4) or equivalent functionality from day1. **Note:** Acceptable solution i.e. OEM/Bidder can achieve the same through providing additional hardware like Router (from Day 1 itself) of capacity equivalent to the firewall thus without compromising on any of the parameter like throughput, Ports etc. of the solution, as asked in the bid.
78		Web Filtering: Keyword, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL.		Web Filtering: , Custom URL Block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL. Keywork Search is not a URL Capability ,its most of DLP feature. Ultimately any keyword search will link to a URL and will ultimately be blocked. Request you to change this to a Custom URL/Application control	No change, As per RFP

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference Tender Description	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
79	Page No. 15 & 16 / Section 4 / Technical Specification / Item No. 3: Firewall Appliance (Type 3)	Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and Nat46 (IPv4-to-IPv6)functionality, NAT66	Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and , NAT44. We all are aware of the fact that IPv6 is not fully in implementation across most of the Customers. However the practical implementations which uses IPv6 uses eith NAT 44 or NAT 66. Request you to remove NAT46	**Please refer revised clause:** Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6), Nat46 (IPv4-to-IPv6) and Nat64 (IPv6-to-IPv4) or equivalent functionality from day1. **Note:** Acceptable solution i.e. OEM/Bidder can achieve the same through providing additional hardware like Router (from Day 1 itself) of capacity equivalent to the firewall thus without compromising on any of the parameter like throughput, Ports etc. of the solution, as asked in the bid.
80		Web Filtering: Keyword, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL.	Web Filtering: ,Custom URL Block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL. Keywork Search is not a URL Capability ,its most of DLP feature. Ultimately any keyword search will link to a URL and will ultimately be blocked. Request you to change this to a Custom URL/Application control	No change, As per RFP
81	Page No. 5 / Section 1 / Eligibility Criteria	The bidder should be an established IT/ITeS System integrator and should have experience of Setting-up and O&M services of Network (Active & Passive) and Data Center and should have executed at least 2 projects of Network Integration/System integration/ Data Center (Setting up or O&M) anytime in India during last five years as on bid issuance date having minimum value of Rs. 5 Crore each. Customer references & Purchase orders must be attached along with the bid. (Form no. E-3)	1) Kindly confirm that project/work order experience of Active & Passive must be in last 07 Years. 2) Request you to confirm that the Rate Contract work which has multiple P.O for project would be consider for the said Minimum value of 5 Crore each. 3) In case of RC for active/passive network for multiple zone with each more then required asked value of 5 Crs, would be consider for individual order per zone. 4) Request you to kindly keep the minimum 02 order value experience for Rs 4 Crores/04 orders of 2.5 Crores/05 Orders of 2 Crores in last 07 years. 5) As experience of setting up Network & Data Center is asked, Pls clarify, wherein individual order of Network work qualifying for minimum order value would be eligible. Separate order of DC with lower Order value would be submitted to express the relevant experience.	As per RFP
82		The proposed system should support IPsec VPN throughput of 5 Gbps	VPN is not the most commonly used feature in Education institute/collage, having said that with our VPN technologies we can support many concurrent VPN tunnels with lower VPN throughput also. So request you change this to "The proposed system should support IPsec VPN throughput of Minimum 1.5 Gbps or should support Min. 2000 Concurrent VPN tunnels"	No change, As per RFP
83	Page No. 13 & 14 / Section 4 / Technical Specification / Item No. 1: Firewall Appliance (Type 1)	Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and Nat46 (IPv4-to-IPv6), functionality, NAT66	NAT46 is needed when yo have LAN on IPv4 and WAN on IPv6 which is very uncommon, request you to change this to "Firewall should support 6in4, 6to4, 4in6 and 6rd IP tunneling to promote interoperability between IPv4 and IPv6 networks along with NAT & PAT functionality"	**Please refer revised clause:** Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6), Nat46 (IPv4-to-IPv6) and Nat64 (IPv6-to-IPv4) or equivalent functionality from day1. **Note:** Acceptable solution i.e. OEM/Bidder can achieve the same through providing additional hardware like Router (from Day 1 itself) of capacity equivalent to the firewall thus without compromising on any of the parameter like throughput, Ports etc. of the solution, as asked in the bid.

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference Tender Description	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
84		Firewall should support at least 2,25,000 new connections per second	New session is mainly first negotiations done by client with server. Hence it wont play major role in supporting more no of users whereas **concurrent session per sec** play huge role in supporting more concurrent users, hence it should be more. So request you to change this to "Firewall should support at least 2,00,000 new connections per second" or Increase the number of session to 10,000,000 (10 Million)	No change, As per RFP
85	Page No. 14 & 15 / Section 4 / Technical Specification / Item No. 2: Firewall Appliance (Type 2)	The proposed system should support IPsec VPN throughput of 8 Gbps	VPN is not the most commonly used feature in institute/collage, having said that with our VPN technologies we can support many concurrent VPN tunnels with lower VPN throughput also. So request you to change this to "The proposed system should support IPsec VPN throughput of Minimum 3 Gbps or should support Min. 3500 Concurrent VPN tunnels"	No change, As per RFP
86		Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and Nat46 (IPv4-to-IPv6) functionality, NAT66	NAT46 is needed when yo have LAN on IPv4 and WAN on IPv6 which is rarest case, request you to change this to "Firewall should support 6in4, 6to4, 4in6 and 6rd IP tunneling to promote interoperability between IPv4 and IPv6 networks along with NAT & PAT functionality"	**Please refer revised clause:** Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6), Nat46 (IPv4-to-IPv6) and Nat64 (IPv6-to-IPv4) or equivalent functionality from day1. **Note:** Acceptable solution i.e. OEM/Bidder can achieve the same through providing additional hardware like Router (from Day 1 itself) of capacity equivalent to the firewall thus without compromising on any of the parameter like throughput, Ports etc. of the solution, as asked in the bid.
87		Firewall should support at least 2,75,000 new connections per second	New session is mainly first negotiations done by client with server. Hence it wont play major role in support more no of users whereas **concurrent session per sec** play huge role in supporting more concurrent users, hence it should be more. So request you to change this to "Firewall should support at least 2,20,000 new connections per second" or Increase the number of session to 12,000,000 (12million)	No change, As per RFP
88	Page No. 15 & 16 / Section 4 / Technical Specification / Item No. 3: Firewall Appliance (Type 3)	The proposed system should support IPsec VPN throughput of 10 Gbps	VPN is not the most commonly used feature in institute/collage, having said that with our VPN technologies we can support many concurrent VPN tunnels with lower VPN throughput also. So request you to change this to "The proposed system should support IPsec VPN throughput of Minimum 8 Gbps or should support Min. 4000 Concurrent VPN tunnels"	No change, As per RFP
89		Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6) and Nat46 (IPv4-to-IPv6) functionality, NAT66	NAT46 is needed when yo have LAN on IPv4 and WAN on IPv6 which is rarest case, request you to change this to "Firewall should support 6in4, 6to4, 4in6 and 6rd IP tunneling to promote interoperability between IPv4 and IPv6 networks along with NAT & PAT functionality"	**Please refer revised clause:** Firewall should support NAT, PAT, Nat66 (IPv6-to-IPv6), Nat46 (IPv4-to-IPv6) and Nat64 (IPv6-to-IPv4) or equivalent functionality from day1. **Note:** Acceptable solution i.e. OEM/Bidder can achieve the same through providing additional hardware like Router (from Day 1 itself) of capacity equivalent to the firewall thus without compromising on any of the parameter like throughput, Ports etc. of the solution, as asked in the bid.

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
		Tender Description		
90	Page No. 5 / Section 1 / Eligibility Criteria	The bidder should be an established IT/ITeS System integrator and should have experience of Setting-up and O&M services of Network (Active & Passive) and Data Center and should have executed at least 2 projects of Network Integration/System integration/ Data Center (Setting up or O&M) anytime in India during last five years as on bid issuance date having minimum value of Rs. 5 Crore each. Customer references & Purchase orders must be attached along with the bid. (Form no. E-3)	Pl put the date , as financial year starting from 01.04.2013 onwards	As per RFP
91	Page No. 6 / Section 2 / Scope of Work	Bidder should include any other components like wire, patch cords, power cables, connector etc. in the BOM for successful implementation and integration with existing Campus Wide Area Network (CWAN).	We assume data racks are available at each site and customer will provide space for installation of firewall.	As per RFP
92	Page No. 6 / Section 2 / Scope of Work	The Bidder shall ensure that the products quoted should not be declared "End of Production" for next 2 years and "End of support" for the next 7 years by the OEM from the date of bid submission. However, if OEM declares any equipment as end of support for any reasons, then in that case OEM has to replace that equipment with better or equivalent products without any cost to purchaser. OEM has to also submit on their letter head, complete details on the support available for the equipment, their end of support dates and replacement model, if any.	Pl revise this clause to "The Bidder shall ensure that the products quoted should not be declared "End of Production" for next 2 years and "End of support" for the next 7 years by the OEM from the date of bid submission. However, if OEM declares any equipment as end of support for any reasons **and the said equipment goes faulty or beyond repairs before the next 7 years,** then in that case OEM has to replace that equipment with better or equivalent products without any cost to purchaser. OEM has to also submit on their letter head, complete details on the support available for the equipment, their end of support dates and replacement model, if any.	As per RFP
93	Page No. 7 / Section 3 / General Terms & Conditions	3. The Bidder may quote only one option (i.e. only one product can be quoted) against each item. Bidders are required to mention make & model of the product. (Do not write "OEM" against items as bidders are expected to give make & model of the product).	Pl insert : "Bidders should quote the solution from same OEM for all the three types/model."	No change, As per RFP
94	Page No. 11 / Section 3 / General Terms & Conditions	38.2. Operational / Warranty period Penalties: c) Successful bidder should submit the Performance Bank Guarantee @ 10 % of total order value for the duration of warranty period + extra 3 months as per bid requirements. In any case, bidder is required to maintain 10 % PBG at all time during the period of contract.	Can we submit PBG for first 3 years and renew it thereafter for the next 2 years.	No change, As per RFP
95	Page No. 11 / Section 3 / General Terms & Conditions	39. Payment: Payment for Goods and Services shall be made by purchasing department in Indian Rupees as follows: 39.1. No advance payment will be made. 39.2. 90 % payment after inspection and successful delivery of ordered goods. The inspection will be done by GIL. 39.3. Remaining 10% payment will be made after installation, commissioning, FAT & user's functional training of the ordered goods.	Can Are we supposed to delivery at goods at central site for inspection ?	As per RFP

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Vendors	Responses to the Queries
	Page No. / Section No. / Clause No.	Tender Description		
96	Page No. 5 / Section 1 / Eligibility Criteria	OEM of the Proposed Security Appliances should be in the Leadership / Challengers / Visionaries quadrant in the Gartner Magic Quadrant for UTM, June 2017 OR should be among the top five positions in terms of worldwide market share as per IDC report for worldwide quarterly security appliance tracker, Q12018. Documentary proof to be submitted for the same.	OEM of the Proposed Security Appliances should be in the Leadership / Challengers / Visionaries quadrant in the Gartner Magic Quadrant for Enterprise Firewall, June 2017 OR should be among the top five positions in terms of worldwide market share as per IDC report for worldwide quarterly security appliance tracker, Q12018. Documentary proof to be submitted for the same. Also proposed solution must be recommended by NSS SVM NGFW latest report. NSS is Technical Certification and shows effectiveness of the solution.	No change, As per RFP
97	Page No. 13, 14 & 15 / Section 4 / Technical Specification / Item No. 1, 2 & 3: Firewall Appliance	The proposed system should support IPS throughput of 2 Gbps; The proposed system should support IPS throughput of 4 Gbps; The proposed system should support IPS throughput of 5 Gbps	The proposed system should support IPS throughput of 2 Gbps Real world/enterprise mix traffic; The proposed system should support IPS throughput of 4 Gbps real world/Enterprise mix Traffic ; The proposed system should support IPS throughput of 5 Gbps real world/Enterprise mix Traffic. Real World / Enterprise Mix is the real world throughput which customer will get in real time scenario . Otherwise the throughputs are mentioned in best cae scenario and drops drastically as large as 70-90% when compared to real world throughput.	No change, As per RFP
98	Page No. 13, 14 & 15 / Section 4 / Technical Specification / Item No. 1, 2 & 3: Firewall Appliance	The proposed system should support AV + IPS + App control enabled throughput of 1 Gbps ; The proposed system should support AV + IPS + App control enabled throughput of 2.7 Gbps ; The proposed system should support AV + IPS + App control enabled throughput of 4 Gbps	The proposed system should support AV + IPS + App control enabled throughput of 1 Gbps real world/Enterprise mix Traffic ; The proposed system should support AV + IPS + App control enabled throughput of 2.7 Gbps real world/Enterprise mix Traffic ; The proposed system should support AV + IPS + App control enabled throughput of 4 Gbps real world/Enterprise mix Traffic. Real World / Enterprise Mix is the real world throughput which customer will get in real time scenario . Otherwise the throughputs are mentioned in best cae scenario and drops drastically as large as 70-90% when compared to real world throughput.	No change, As per RFP
99	Page No. 16 / Section 4 / Technical Specification / Note	Bidder is responsible for providing required hardware (having storage capacity to store the logs of minimum last 1-year period), software and licenses (valid perpetual for life) for storing the logs.	Bidders are responsible for providing Logs of 1 Year with no cap on storage limitation. Logs should be provided by an external solution from the same OEM for better integration and compliance . Logs can be provided by giving external Hardware / Software/ Cloud and all relevant Licenses and hardware should be quoted for tender terms (Seven Years - 5+ 2 years). If Storage is provided internally in UTM and device goes down all logs will be gone and as per government rules logs of one year has to be maintained . Secondly there is limited disk space if logs are taken internally . Having an external solution for logs will save from both the problems . Secondly if logs is provided by different OEMS there will be integration issue considering the procurement is for Seven Years . Kindly clarify if only one log solution can be provided for all 42 Campus or Separate solution is required for all 42 Locations.	No change, As per RFP. Additionally, device has to provide for log and MIS reports also.

Sr. No.	Page No. / Section No. / Clause No.	Tender Reference Tender Description	Query / Clarification / Suggestions from the Vendors	Responses to the Queries
100	Page No. 13, 14 & 15 / Section 4 / Technical Specification / Item No. 1, 2 & 3: Firewall Appliance	Additional Point	Proposed solution must offer cloud based sandbox for zero day detection & Mitigation. New type of attacks are Zero Day Attacks - Any security UTMsolution is signature based device and is not able to protect the organization from Zero Day Attack. For Protection there is a dedicated solution claaed as SandBox which is required- Physical sandbox at all location will increase the tender cost where as cloud based sandbox will hardly make any difference in the commercials.	No change, As per RFP
101	Page No. 13 / Section 4 / Technical Specification / Item No. 1: Firewall Appliance (Type 1)	Firewall should support at least 1,25,000 new connections per second	Firewall should support at least 1,30,000 new connections per second. Ask new Connection per Second is less as compared to other throughputs	No change, As per RFP
102		The proposed system should support IPsec VPN throughput of 5 Gbps	The proposed system should support IPsec VPN throughput of 7 Gbps. With the adaptability of Advance technology- Dependability on IPSec VPN is increasing day by Day.	No change, As per RFP
103		The proposed system should support AV + IPS + App control enabled throughput of 1 Gbps	The proposed system should support AV + IPS + App control enabled throughput of 1.2 Gbps. Ask Throughput is less.	No change, As per RFP
104	Page No. 14 / Section 4 / Technical Specification / Item No. 2: Firewall Appliance (Type 2)	Firewall should support at least 2,25,000 new connections per second	Firewall should support at least 2,75,000 new connections per second. Ask new Connection per Second is less as compared to other throughputs	No change, As per RFP
105		The proposed system should support IPsec VPN throughput of 8 Gbps	The proposed system should support IPsec VPN throughput of 12 Gbps. With the adaptability of Advance technology- Dependability on IPSec VPN is increasing day by Day.	No change, As per RFP
106		The proposed system should support AV + IPS + App control enabled throughput of 2.7 Gbps	The proposed system should support AV + IPS + App control enabled throughput of 3.0 Gbps. Ask Throughput is less.	No change, As per RFP
107	Page No. 15 / Section 4 / Technical Specification / Item No. 3: Firewall Appliance (Type 3)	The proposed system should support IPsec VPN throughput of 10 Gbps	The proposed system should support IPsec VPN throughput of 15 Gbps. With the adaptability of Advance technology- Dependability on IPSec VPN is increasing day by Day.	No change, As per RFP
108		The proposed system should support AV + IPS + App control enabled throughput of 4 Gbps	The proposed system should support AV + IPS + App control enabled throughput of 4.5 Gbps. Ask Throughput is less.	No change, As per RFP
109	Page No. 5 / Section 1 / Eligibility Criteria	The bidder should be an established IT/ITeS System integrator and should have experience of Setting-up and O&M services of Network (Active & Passive) and Data Center and should have executed at least 2 projects of Network Integration/System integration/ Data Center (Setting up or O&M) anytime in India during last five years as on bid issuance date having minimum value of Rs. 5 Crore each. Customer references & Purchase orders must be attached along with the bid. (Form no. E-3)	Request for the Revision: The bidder should be an established IT/ITeS System integrator and should have experience of Setting-up and O&M services of Network (Active & Passive) and Data Center and should have executed at least 1 project of Network Integration/System integration/ Data Center (Setting up or O&M) anytime in India during last five years as on bid issuance date having minimum value of Rs. 10 crore for one project OR two projects of RS. 5 Crore each. Customer references & Purchase orders must be attached along with the bid. (Form no. E-3)	As per RFP

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Vendors	Responses to the Queries
	Page No. / Section No. / Clause No.	Tender Description		
110	Page No. 10 / Section 3 / General Terms & Conditions	Delivery & Installation: Within 45 working days from the date of confirmed purchase order.	Request for the Revision: Delivery & Installation: Within 60 working days from the date of confirmed purchase order.	**Clause is revised as mentioned below:** **Delivery & Installation:** Within 60 days from the date of signing of contract agreement.
111	Section 1 (Page 5/27)	Clause 3 Section 1	We hereby request to allow consortium bids to meet this criteria to qualify.	No change, As per RFP
112	Section 1 (Page 5/27)	The bidder should have average annual turnover of Rs. 25 Crore (Minimum) in the last three financial years as on 31st March 2018	We hereby request to allow annual average turnover of Rs 15 Crore in the last 3 financial Years as on 31 March 2018.	No change, As per RFP
113	Clause 32 (Page 10/27) Clause 16 (Page 8/27)	Delivery & Installation: Within 45 working days from the date of confirmed purchase order.	We hereby request that delivery & installation & PBG Submission timelines should start from Contract signing date.	**Clause is revised as mentioned below:**
114	Clause 32 (Page 10/27)		Delivery & Installation timelines are very skewed, request you to extend these by at least 4 weeks.	**Delivery & Installation:** Within 60 days from the date of signing of contract agreement.
115	Annx B 26/27	Delivery locations	Delivery locations readiness, whether all sites are ready & supplied goods will not have any site readiness issue	As per RFP
116	Page 6/27	Installation & Training : Onsite training is to be given by the Bidder to respective Institute persons for the equipments to be supply, on operation and troubleshooting during the time of supply.	Our understanding is that bidder has to provide basic training on Operation, L1 level troubleshooting if required & complaint logging, we hope our understanding is correct.	As per RFP
117	clause 18, 19 (Page no.8/27)	EMD	Pls clarify on submission of any deviation & any such deviation will not put EMD at risk.	As per RFP
118	CLAUSE 20.1 (Page 9/27)		We hereby Request you to increase the notice period to 90 days. Termination should only be for the portion where there has been a default. Please include Bidder's right to terminate for non-payment of dues in time and right to claim late payment interest @ 1.5% per month. PBG SHOULD NOT BE INVOKED IN FULL; it should be limited to goods and services that are undelivered and subject to penalty capping. This clause of termination should be linked / subject to : a) Material Breach of SLA and therefore a breach of cap of 10% of LD/penalties for four successive quarters; b) Only the affected portion of the Contract/ Order should be terminated c) the capping of additional cost incurred by customer should be limited to PBG value.	No change, As per RFP
119	Clause 38.1 (d) (Page No. 11/25), Clause 20.2 (Page9/27)	In case, the selected bidder does not supply the ordered items for any reason, he will be liable to pay the difference amount i.e. between L1-L2 and so on to the purchaser, over and above the Performance Guarantee, which indenter departments\Boards\Corporations have to pay to the next or other selected bidder for purpose of the said items.	We request recovery of differential/excess cost should be capped at 10% of the work that was undelivered. If the contract is terminated, the Supplier shall be entitled to receive: the outstanding balance of the Contract value of the Goods which have been delivered or the Services performed up to the effective date of such termination.	No change, As per RFP

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Vendors	Responses to the Queries
	Page No. / Section No. / Clause No.	**Tender Description**		
120	Clause 38.1 (b), & 38.2 (b) Page 11/27	The amount of penalties for delay in delivery and installation shall be subject to a maximum limit of 10% of the total contract value. The amount of Operational/Warranty period Penalty shall be subject to a maximum limit of 10% of the total contract value	We hereby requests that Penalty should be kept @ 10% of the undelivered portion of the equipment and/or services. Please clarify that LD/penalty shall be the sole and exclusive remedy. This obligation shall not apply to delays arising from actions or inactions of the Purchaser or any third party. Payment of liquidated damages under the agreement shall be in full and final satisfaction of all claims and liabilities arising from lateness or defective performance.	No change, As per RFP
121	Clause 45/Page 12	It will be prerogative of Purchaser / GoG to take the decision on force major conditions and Purchaser	As all decisions are subject to arbitration as per law. So these lines in the said clause is not applicabel.Bidder shall be paid for supply and services till last date of termination in case of force majeure.	As per RFP
122	Clause 31/Page 10	The Indenter's right to inspect, test and, where necessary, reject the Goods after the Goods arrival at Customer Site shall in no way be limited or waived by reason of the Goods having previously been inspected, tested and passed by the Purchaser or its representative prior to the Goods shipment	Pls check the acceptance criteria of Goods. Supplied Goods cannot be rejected, they canbe repaired or replaced as per various OEM Policies. Payment of supplied & inspected ok Goods should not be withheld due to any such replacement	No change, As per RFP
123	Clause 45/Page 12	Additional clause	Pls add Arbitration, Jurisdiction clause as they are standard clauses which needs to be present in every Tender. In case of any disputes ,it should be settled by the Arbitration and Conciliation Act 1996 (as amended by latest amendments). Arbitration should be held at Mumbai/ Delhi.	In case of any disputes, Arbitration should be held at Gandhinagar Jurisdiction as per Arbitration Rules.
Note:	**All other Bid terms & conditions and technical specifications remain unchanged.**			