S.N.	Bidding Document Reference(s) (Clause/Section No/ Page)	Existing Clause in RFP (Content of RFP Requiring Clarification)	Query/ Clarification, Change required /sought	Response by Air India
	BIDDERS - FORCEPOINT / I Value Info Solutions Pvt. Ltd (iStorm)/ TECHWIZARD SERVICES.COM & M/S SISL INFOTECH PVT LTD.			
1	Clause 5.4.2 - Technical Requirements - Solution 'B' - Secure Web Gateway and Content Filtering Solution, 2(B), page 55 (Point 3)	Should support Forward Proxy, Reverse Proxy, Transparent, Bridge Mode, WCCP, ICAP	Should support Forward ProxyTransparent ,WCCP, ICAP	No change
2	Secure Web Gateway and Content Filtering Solution, 2(B), page 55 (Point 4)	Should Support external Load balancer as High Availability option	Should Support external Load balancer as High Availability option	Change to :- Solution should Support external Load balancer as High Availability option if required in future.
3	Secure Web Gateway and Content Filtering Solution, 2(B), page 55 (Point 10)	Quota Filtering, Thumbnail / Image Blocking, Compressed File Filtering - Should Block, Pass, Quarantine	Quota Filtering, Thumbnail / Image Blocking, Compressed File Filtering - Should Block, Pass, Quarantine	No Change
4	Secure Web Gateway and Content Filtering Solution, 2(B), page 55 (Point 11)	Should have following FTP Scanning functionality, Reverse FTP Proxy, Passive FTP Support, Active FTP Support, Should Support IP Address based FTP Access Control, FTP Port Filtering	Should have following FTP Scanning functionalityPassive FTP Support, Active FTP Support, Should Support IP Address based FTP Access Control, FTP Port Filtering	No Change
5	Secure Web Gateway and Content Filtering Solution, 2(B), page 55 (Point 14)	Heuristic Scanning, Signature Matching, Customizable File Filters for Scanning, Large file handling, Compressed File Support - with block, bypass and quarantine modes	Heuristic Scanning, Signature Matching, Customizable File Filters for Scanning, Large file handling, Compressed File Support - with block, bypass .	No change
6	Secure Web Gateway and Content Filtering Solution, 2(B), page 55 (Point 15)	Quarantine File Support, Real-time Page Analysis (content scan), Automatic Signature Updates, Incremental Updates, Rollback Updates, Solution should be able to detect and block Brute Force Attacks against Passwords, Manual and Automated Updates, Botnet Detection Technology	Real-time Page Analysis (content scan), Automatic Signature Updates, Incremental Updates, Rollback Updates, Solution should be able to detect and block Brute Force Attacks against Passwords, Manual and Automated Updates, Botnet Detection Technology	No Change
7	Secure Web Gateway and Content Filtering Solution, 2(B), page 55 (Point 16)	Solution should have Web cache acceleration with File Cache, Dynamic Object Cache and Static Object Cache and Selective Category Logging, full URL Logging	Solution should have File Cache, Dynamic Object Cache and Static Object Cache and Selective Category Logging, full URL Logging	No change
8	Secure Web Gateway and Content Filtering Solution, 2(B), page 55 (Point 21)	Should integrate with Anti-APT solution to receive IOC's and both solution should have central management console for central visibility.	Should integrate with Anti-APT solution to receive IOC's and provide protection.	No change
	New	The solution should have ability to protect the sentisitve data exfilatration based on geo-location. The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and uknown encryption files		As per RFP
	New	The solution should have ability to block anonymizer sites or proxy avoidance tools. Below mentioned tools should be blocked from first day and should be provided in default protocol database Ghostsurf, Google web accelerator, Hopster, Jap, Realtunnel, Socksonline, Tongtongtong, Toonel, Tor, Yourfreedom.		As per RFP
	New	The solution provide the Shadow IT vsibility for the sactioned and un sactioned application and provide the visibility and control for the same.		As per RFP
	New	The solution should be in the latest Gartner Leaders and Challenges for the Secure Web Gateway.		As per RFP

BIDDER - SISL INFOTECH PVT LTD - Additional Queries

S.N.	Bidding Document Reference(s) (Clause/Section No/ Page)	Existing Clause in RFP (Content of RFP Requiring Clarification)	Query/ Clarification, Change required /sought	Response by Air India
1	Technical Solutions – Broad General Requirements for Security Architecture Project, Clause 3.1, Page 26	OEM should attain ISO 27001 Certification as well as should attain ISO for its Support Services	Requested to delete this clause as ISO 270001 is a DC security standard not applicable to support services	Accepted and Clause Removed
2	Technical Solutions – Broad General Requirements for Security Architecture Project, Clause 3.8, Page 26	Proposed OEMs for Security solution must comply to at least one of the following two requirements a. Proposed OEM must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Next Generation Firewall with IPS(UTM) published by Gartner or in Latest NSS Lab Report. b. Proposed OEM for Anti-APT must have scored equal or more than 98.5% 'Security Effectiveness' in latest NSS Breach Detection Systems (BDS) report	**Proposed Change**: Proposed OEMs for Security solution must comply to ~~at least one of~~ the following two requirements a. Proposed OEM must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Next Generation Firewall with IPS(UTM) published by Gartner or in Latest NSS Lab Report. b. Proposed OEM for Anti-APT must have scored equal or more than 98.5% 'Security Effectiveness' in latest NSS Breach Detection Systems (BDS) report and recommended rating.	No Change
3	Next Generation Security Architecture-UTM (Firewall with IPS), Clause 1a, Page 32	OEM should attain ISO 27001 certification as well as should attain ISO for its Support Services	Requested to delete this clause as ISO 270001 is a DC security standard not applicable to support services	Accepted and Clause Removed
4	Basic Criteria, clause 1f, page 33	Firewall throughput of 100,000 Gbps	Proposed Change: Firewall Throughput of 70 Gbps	May be read as :- Firewall throughput of 100 Gbps
5	Basic Criteria, Clause 1g page 33	Minimum 17 Gbps of Antivirus Throughput	Proposed Change : UTM Throughput of 13 Gbps	No Change
6	Basic Criteria, Clause 1h, page33	Minimum 30,000,000 Concurrent sessions	Proposed Change : Min 25 Million concurrent sessions	No Change
7	Basic Criteria, Clause 1j, page 33	Minimum 300,000 New Sessions/second	Proposed Change ; Min 185,000 New sessions/second	No Change
8	Basic Criteria, Clause 1m, Page 33	Minimum of 8 x GBE Interfaces and 2 x GE SFP and 4 x 10 GE SFPwith expansion slot to accommodate more ports if required.	Proposed Change : Minimum of 8 x GBE Interfaces and 4 x 10 GE SFP with support for addition of 2 more 10G/ 40G interfaces	No Change
9	Basic Criteria, clause 1n, Page 33	Should have minimum of 500 GB SSD drives in RAID	Proposed Changes : Should have minimum of 500 GB HDD/SSD drives in RAID	No Change
10	General Features, Clause 2g, Page 33	Web Application Firewall	Requested to delete this clause as specific to certain OEMs	No Change
11	General Features, Clause 2n, Page 33	4 Eye Authentication feature for data integrity.	Requested to delete this clause as specific to certain OEMs	Accepted and Clause Removed
12	General Features, Clause 2o, Page 33	Should have an integrated wireless controller and should be able to manage multiple wireless access points centrally from web admin console	Requested to delete this clause as specific to certain OEMs	No Change
13	Gateway Antivirus, Anti-Spyware and Anti-Spam, Clause 3, Page 33	Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area. Should have dual AV engine, Email Encryption, Recipient self-registration SPX password management, DLP engine with automatic scanning of emails and attachments for sensitive data	Propsoed Change: Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, ~~and Redirect spam mails to dedicated email address~~, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. ~~Recurrent pattern Detection Technology for AS. Self Service Quarantine area. Should have dual AV engine, Email Encryption, Recipient self-registration SPX password management,~~ DLP engine with automatic scanning of emails and attachments for sensitive data	May be read as :- Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Should have dual AV engine, Email Encryption, Recipient self-registration, SPX password management, data protection engine with automatic scanning of emails and attachments for sensitive data.
14	Wireless Security and Control, Clause 5, Page 33	Should act as a wireless controller, Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center, Central monitor and manage all APs and wireless clients through the built-in wireless controller, Support for IEEE 802.1X (RADIUS authentication), Wireless repeating and bridging meshed network mode with supported Aps	Requested to delete this clause as specific to certain OEMs	No Change

15	Web Application Firewall (WAF), Clause 7, page 33	Should have an option of WAF with Positive Protection Module, Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Reverse Proxy, Dual AV Engine, Extensive Logging and reporting. If external, then has to be quoted separately.	Proposed Changes : Should have an option of WAF/IPS signatures with ~~Positive Protection Module,~~ Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Reverse Proxy, Dual AV Engine, Extensive Logging and reporting. If external, then has to be quoted separately.	No Change
16	Monitoring and Reporting System, clause 12a, page 34	Includes Integrated Web Based reporting,, Monitoring & Logging, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. IPS, Web filter, Antivirus, Anti-spam system reports. IP and User basis report, 45+ Compliance reports and 1200+ drilled down reports on the appliance.	Proposed Change : Includes Integrated Web/GUI Based reporting,, Monitoring & Logging, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. IPS, Web filter, Antivirus, Anti-spam system reports. IP and User basis report, ~~45+ Compliance reports and 1200+ drilled down reports on the appliance.~~	No Change
17	Anti APT Solution , Clause 12, pg 35	The proposed solution should use customizable OS sandboxes for detecting zeroday malwares, This should not be a CPU or chip based function.	Proposed Change : The proposed solution should use customizable OS sandboxes for detecting zeroday malwares, ~~This should not be a CPU or chip based function.~~	No Change
18	Anti APT Solution , Clause 19, page 36	The proposed solution should be able to detect lateral movement (East-West) of the attacker without the need of installing agents on endpoint/server machines.	Requested to delete this clause as specific to certain OEMs	No Change
19	Anti APT Solution , clause 31, pg 36	The Proposed solution should support remote packet capturing for Kerberos traffic from the remote location for analysis.	Requested to delete this clause as specific to certain OEMs	No Change
20	Anti APT Solution , clause 32, pg 36	The Proposed solution should monitor Inter-VM traffic on a Port Mirror Session.	Requested to delete this clause as specific to certain OEMs	No Change
21	Anti APT Solution , clause 36, page 37	The proposed solution should be able to run atleast 60 parallel sandboxes for analysis of payload and on-premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	Proposed Change : The proposed solution should be able to run multiple parallel sandboxes(min 28) for analysis of payload and on-premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	No Change
22	Anti APT Solution , clause 38, page 37	Customized sandbox solution should support following operating systems (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008 & 2012)	Proposed Change : Customized sandbox solution should support following operating systems (Windows XP, Win7, Win8/8.1, Win 10, ~~Windows Server 2003, 2008 & 2012)~~	No Change
23	Anti APT Solution , clause 42, page 37	The Proposed solution should support customizable Windows 7/8/10 and Microsoft 2008/12 operating environments for Sandboxing. This requirement should be based on virtual execution and should not be a Hardware or chip based function.	Proposed Change : The Proposed solution should support customizable Windows 7/8/10 ~~and Microsoft 2008/12~~ operating environments for Sandboxing. This requirement should be based on virtual execution and should not be a Hardware or chip based function.	No Change
24	Anti APT Solution , clause 47, page 37	The proposed solution should have option to configure unrestricted internet for sandboxes and proposed solution must have capabilities to detect Mac, Linux and mobile malwares.	Proposed Change : The proposed solution should have work without the need for internet access option ~~to configure unrestricted internet for sandboxes and proposed solution must have capabilities to detect Mac, Linux and mobile malwares.~~	No Change
25	Anti APT Solution , clause 50, page 38	The Proposed solution should have option to share Indicators of compromise for mitigation and clean up with AV endpoint and Web gateway to block threat at web gateway level. Anti-APT solution should share intelligence with endpoint and security web gateway solution, similarly endpoint and security web gateway should submit files to anti-APT solution for analysis and all three solution should manage through single management console.	Proposed Change : The Proposed solution should have option to share Indicators of compromise for mitigation and clean up with AV endpoint and Web gateway/NGFW to block threat at web gateway/NGFW level. Anti-APT solution should share intelligence with endpoint and security web gateway/NGFW solution, ~~similarly endpoint and security web gateway should submit files to anti-APT solution for analysis and all three solution should manage through single management console.~~	No Change

BIDDER - CIPL / UV TECHNOLOGIES PVT LTD

S.N.	Bidding Document Reference(s) (Clause/Section No/ Page)	Existing Clause in RFP (Content of RFP Requiring Clarification)	Query/ Clarification, Change required /sought	Response by Air India
1	Page 26, Point 3.1	OEM should attain ISO 27001 Certification as well as should attain ISO for its Support Services	It should be changed to "Bidder/OEM should attain ISO 27001"	Accepted and Clause Removed
2	Page 32, Point 1 (a)	OEM should attain ISO 27001 certification as well as should attain ISO for its Support Services	It should be changed to "Bidder/OEM should attain ISO 27001"	Accepted and Clause Removed

3	Page 5, Point 3	A bidder should be a Company, registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013 with a minimum of 05 years into Operation having experience in providing complete IT security solutions architecture in any large company with Pan India infrastructure setup.	It should be changed to "A bidder should be a Company, registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013 with a minimum of 05 years into Operation having experience in providing complete IT security/ IT Infrastructure solutions."	Accepted and may be read as :- Bidder should be a Company, registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013 with a minimum of 05 years into Operation having experience in providing complete IT security/ IT Infrastructure solutions.
4	Page 5, Point 3	Bidder should be having domain expertise as IT security solution architecture provider. Vendor or OEM should have executed Minimum one (01) assignment of similar nature of providing IT security solutions in any Government / PSU organization.	It should be changed to "Bidder/OEM should be having domain expertise as IT security solution architecture provider. Vendor or OEM should have executed Minimum one (01) assignment of similar nature of providing IT security solutions in any Government / PSU organization."	No Change
5	Page 16, Point 8	(a) The bidder (Company) must be an OEM or its Authorized Vendor and should be a Company registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013. with a minimum of five (05) years into Operation, having relevant experience in providing IT security solutions. (Incorporation/ Registration Certificate required).	It should be changed to "A bidder should be a Company, registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013 with a minimum of 05 years into Operation having experience in providing complete IT security/ IT Infrastructure solutions."	Accepted and may be read as :The bidder (Company) must be an OEM or its Authorized Vendor and should be a Company registered under the Indian Companies Act, 1956/ Revised Companies Act, 2013. with a minimum of five (05) years into Operation, having experience in providing complete IT security / IT Infrastructure solutions.
6	Page 17, Point 8	(c) The bidder (Company)/OEM having expertise as solution provider for IT Security Solutions (supply, installation, commissioning, implementation). It should have a Past Experience of Minimum one (01) assignment of similar nature of providing IT security solutions in Government or and Public Sector (Copy of work order/ Contract of the mentioned assignment/proof of facility required)		
7	Page 53, Point 35	The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, Ransomeware protection, C&C detection, and ability to quarantine and clean the infected files, ability to integrate with Anti APT components and automatically block/Quarantine zero day malwares by sharing Indicators of Compromise.	The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, ransom ware protection, Vulnerability Protection in endpoint, integrated DLP and C&C detection, ability to quarantine and clean the infected files, ability to integrate with Anti APT components and automatically block/Quarantine zero day malwares by sharing Indicators of Compromise.	Accepted and may be read as:- The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, ransom ware protection, Vulnerability Protection in endpoint, integrated DLP and C&C detection, ability to quarantine and clean the infected files, ability to integrate with Anti APT components and automatically block/Quarantine zero day malwares by sharing Indicators of Compromise.
8	Page 87, Point 35			

BIDDER - CISCO SYSTEMS & PROACTIVE DATA SYSTEMS PVT. LTD. (CISCO GOLD PARTNERS)

S.N.	Bidding Document Reference(s) (Clause/Section No/ Page)	Existing Clause in RFP (Content of RFP Requiring Clarification)	Query/ Clarification, Change required /sought	Response by Air India
1	Solution-A, Technical Requirements, Clause 5.4.2	**Basic Criteria**		
		a) OEM should attain ISO 27001 certification as well as should attain ISO for its Support Services		Accepted and Clause Removed
		b) OEM should have support Centre in India.		No Change
		c) Appliance should have ICSA certification for Firewall	Please change the clause to: "The proposed equipment should be ICSA OR EAL4 or NDPP or NSS certified firewall.	No Change
		d) The proposed solution should support High Availability Active-Active mode	Please change the cluase to- The proposed solution should support High Availability Active-Active or Active -Standby mode	No Change
		e) Appliance Throughput	Please change the Clause as -	
		f) Firewall throughput of 100,000 Gbps	Should support Raw Firewall throughput of atleast 30 Gbps	May be read as :- Firewall throughput of 100 Gbps
		g) Minimum 17 Gbps of Antivirus Throughput	Please confirm whether bidder can quote better technology like Anti-APT instead of Gateway Antivirus.	No Change
		h) Minimum 30,000,000 Concurrent sessions	NG Firewall should support atleast 8,500,000 concurrent sessions	No Change
		i) Minimum 22 Gbps of IPS throughput	Minimum 7 Gbps of IPS Throughput	No Change
		j) Minimum 300,000 New Sessions/second	Next Generation Firewall should support atleast 65,000 connections per second with Application visibility	No Change

		k) Minimum 11 Gbps of IPsec VPN throughput	Miminum 5 Gbps of IPSec VPN throughput.	No Change
		m) Minimum of 8 x GBE Interfaces and 2 x GE SFP and 4 x 10 GE SFPwith expansion slot to accommodate more ports if required.	The appliance should support atleast 8 * 10G ports from Day one and should have 2 empty slot for network module for future enhancement. Required module can support 16 x 10 G or 4 * 40G ports in future	No Change
		n) Should have minimum of 500 GB SSD drives in RAID	Minimum 200GB of Storage	No Change
2		**General Features**		
		d) Gateway Anti-virus	Please confirm whether bidder can quote better technology like Anti-APT instead of Gateway Antivirus.	No Change
		e) Gateway Anti-spam with DLP functionality	Please remove this clause	No Change
		g) Web Application Firewall	Pls remove this clause	No Change
		h) Bandwidth Management	Pls remove this clause	No Change
		i) Inbuilt-on Appliance Reporting	Please remove this clause	No Change
		j) High Availability (Active-Active & Active-Passive)	High Availability (Active-Active or Active-Passive)	No Change
		k) Network: OSPF, Round Robin load balance, RIPv2, BGP, equal & unequal cost load balance, High Availability, QoS, etc. Round Robin Balance, Server Load Balancing.	Network: OSPF, RIPv2, BGP, equal & unequal cost load balance, High Availability, QoS, etc.	No Change
		l) Support for user authentication over SMS.	Please remove this clause	No Change
		n) 4 Eye Authentication feature for data integrity.	Request to remove this clause	Accepted and clause removed
		o) Should have an integrated wireless controller and should be able to manage multiple wireless access points centrally from web admin console.	Request to remove this clause	No chnages
3		**Gateway Antivirus, Anti-Spyware and Anti-Spam**		
		Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area. Should have dual AV engine, Email Encryption, **Recipient self-registration SPX password management,** DLP engine with automatic scanning of emails and attachments for sensitive data	Request to remove the clause	May be read as :- Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Should have dual AV engine, Email Encryption, Recipient self-registration, SPX password management, data protection engine with automatic scanning of emails and attachments for sensitive data.
4		**Web and Application Filtering:**		
		The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS.	Request to remove the clause	No Change
5		**Wireless Security and Control:**		
		Should act as a wireless controller, Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center, Central monitor and manage all APs and wireless clients through the built-in wireless controller, Support for IEEE 802.1X (RADIUS authentication), Wireless repeating and bridging meshed network mode with supported Aps	Request to remove the clause	No Change
6		**Security Features**		
		Intrusion Prevention System (IPS): For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (5000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection	Please remove - DDOS Attack ,Automatic real-time updates from CR Protect networks	May be read as :- Intrusion Prevention System (IPS): For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack. Signatures: Default (5000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates, Protocol Anomaly Detection
7		**Web Application Firewall (WAF):**		
		Should have an option of WAF with Positive Protection Module, Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Reverse Proxy, Dual AV Engine, Extensive Logging and reporting. If external, then has to be quoted separately.	Request to remove the clause	No changes
8		**Advance Threat Protection:**		
9		**VPN:**		
		IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal.	Ipsec and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal.	No changes
10		**Load Balance:**		
		For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.	For Automated Failover/Failback, Multi-WAN failover, High availability: Active-Active/Active-Standby. QoS, OSPF, RIPv2, BGP, Policy routing based on Application	No changes

Response to Pre-Bid Queries - IT Security solutions at Air India

11	**Bandwidth Management:**		
	Application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Group, Firewall Rule, URL and Applications.	Please remove the clause	No changes
12	**Monitoring and Reporting System:**		
	a) · Includes Integrated Web Based reporting,, Monitoring & Logging, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. IPS, Web filter, Antivirus, Anti-spam system reports. IP and User basis report, 45+ Compliance reports and 1200+ drilled down reports on the appliance.	The management and reporting platform must provide complete visibility of the network and Real time Threat management, automatic correlation of security events with the vulnerabilities in your environment to identify attacks	No changes
	b) · Should provide User Threat Quotient (UTQ) report for actionable security intelligence, helping Administrators identify risky users with ease within the organization's network.	Please remove this clause	Accepted and clause removed
	c) License for UTM (Unified Threat Management)	License for IPS, URL and AntiAPT must be added from Day-1	No changes
	d) · One Year round the clock support for Gate Way Antivirus, spyware, Anti-Spam, WAF, content and application filtering. IPS, reporting and support, Upgrades.	24x7 Support from TAC for Hardware and software included in the solutio and Next Business day Advance Harware replacement.	No changes