Sr. No.	**Required Minimum Specifications "Annexure 11 A – Firewall - 1" (Qty - 4) Make & Model: ____________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
A	General Requirements:		
1	The Firewall must be appliance based and should facilitate multi-application environment which should support current network traffic as well as future growth		
2	The platform should be based on security-hardened, purpose built operating system architecture that is optimized for packet and application level content processing		
3	Be proprietary to prevent inheriting common OS vulnerabilities		
4	Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance		
5	The proposed system should be able to facilitate administration audit by logging detailed activities to event log for management, configuration changes, updates which also enable Admin to boot firmware on the earlier revision / configuration in case of any errors		
6	The administrator authentication shall be facilitated by local database, PKI & remote server such as Radius, LDAP, AD and TACS+		
7	The Firewall system should have provision of Web Content Filter, Application Control, Antivirus systems and Intrusion Prevention in the same solution		
8	Be proprietary to prevent inheriting common OS vulnerabilities and should Resided on flash disk/Hard disk		
9	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats		
B	Networking & System Performance Requirements:		
1	Should support atleast 15 Gbps of production performance (http based) / multiprotocol combined, Firewall & IPS throughput		
2	Firewall should support atleast 12,000,000 concurrent sessions with application visibility		
3	Firewall should support atleast 1,20,000 new connections per second		

Sr. No.	Required Minimum Specifications “Annexure 11 A – Firewall - 1” (Qty - 4) Make & Model: ______________________	Bidder's compliance (Yes / No)	Bidder's remarks
4	The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth		
5	Should support automatic ISP failover as well as ISP load sharing		
6	The Firewall should support Static, Policy Base, Identity based, Multicast routing and Dynamic routing for RIP1 & 2, OSPF, OSPFv3, BGP4, RIPing		
7	The Firewall should support Static, Policy Based, and Multicast routing		
9	Each Appliance should have at least 4x40 GE fiber, 12x10GE fiber. All ports should be populated with required transceivers. The networks switches supports 40Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored.		
C	Firewall Requirements		
1	The Firewall should support deployment modes as; “Route Mode” or “Transparent Mode”		
2	The firewall shall be able to handle VoIP traffic securely with “pinhole opening” and support SIP, SCCP, MGCP and H.323 ALGs		
3	The Firewall should support Stateful inspection with optional Policy based NAT (Static OR Dynamic)		
4	The Firewall should support Inbound Port Forwarding with inbound Load Balancing		
5	Should support Ipv6 ACL to implement security Policy for Ipv6 traffic		
6	All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc		
7	Should be able to inspect HTTP and FTP traffic when these are deployed using nonstandard port(i.e when HTTP is not using standard port TCP/80)		
8	Centralized Management Server should be deployed in VM （will be provided by Bank) and all necessary license should be provided from day one.		
9	Firewall Appliance should have a feature of holding multiple OS images to support resilience		

Sr. No.	**Required Minimum Specifications “Annexure 11 A – Firewall - 1” (Qty - 4) Make & Model: ______________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
	& easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
10	**Should provide out of box Categories based on Application types, Security Risk level etc**		
D	High Availability Requirements:		
1	The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.		
2	The HA solution should support both Active/Active and Active/Passive load balancing with statefull Failover		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
E	Network Intrusion Detection & Prevention System Requirements:		
1	Should have a built-in Signature and Anomaly based IPS engine on the same unit and Anomaly based detection should be based on thresholds		
2	Ipv4 and Ipv6 rate-based DOS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)		
3	Administrator shall be able to configure DoS policies that are used to associate DoS settings with traffic that reaches an interface based on defined services, source and destinations IP/Range		
4	Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types		
5	Supports at least 7000+ excluding custom signatures attack signature and should be automatic updates directly over the internet for the newly discovered attacks		

Sr. No.	Required Minimum Specifications “Annexure 11 A – Firewall - 1” (Qty - 4) Make & Model: ______________________	Bidder's compliance (Yes / No)	Bidder's remarks
6	Security check updates do not require reboot of the unit		
7	Supports attack recognition inside Ipv6 encapsulated packets		
8	Supports user-defined signatures with Regular Expressions		
9	The IPS signature updates and intelligence database update on Firewall and IPS should be automatic without any reboot on the appliance		
F	Logging & Reporting		
1	Must integrate with centralized logging & reporting solution of same OEM for better reporting		
2	Also should have feature to integrate with syslog & SNMP server		
G	Centralized Logging & Reporting Virtual Image		
1	Virtual OS must support VMWare ESXi 5.0 or above / MS Hyper-V platform for its deployment.		
2	Or else OS must have inbuilt virtualization to deploy without any platform.		
3	It should not deployed as a software for windows/linux machine.		
4	It should support 250 GB HDD from day 1		
5	There should no limit on assigning CPU & memory to the OS for better performance		
6	It must provide granualar reporting, event management & dashboard for events		
7	It must have drill down dashboard option which can take out as PDF/Word if required.		
8	It must be sql based to design custom queries on it		
H	Licensing Requirement		
1	Solution should have enterprise license without any restrictions.		
2	Solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.		
3	The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM		

Sr. No.	**Required Minimum Specifications "Annexure 11 A – Firewall - 1" (Qty - 4) Make & Model: ______________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance		
H	URL Filtering		
1	Should be able to create policy based on URLs specifying in the rules		
2	Should be able to define URL category based on Risk level		

Sr. No.	**Required Minimum Specifications "Annexure 11 B – Firewall –2& 3"** **Make & Model: (Firewall 2) (Qty-4) ________________** **Make & Model: (Firewall 3) (Qty-4) ________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
A	General Requirements:		
1	Proposed solution should be Next Generation Firewall with Application Layer Security Controls and Threat Prevention framework		
2	Proposed solution should have Multi-Layer Threat Prevention Suite with following controls embedded: a. Prevention against Malware b. Prevention against Bot & Botnets, c. Prevention against malware hosting URL, Prevention against risky web2.0 apps d. Widgets like anonymizers, TOR, P2P, Bit Torrents, etc.		
3	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
4	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
5	Proposed solution should have a Unified Policy Frame work for application, user, data awareness, etc in a single rule.		
6	Licensing should be a per device and not limited to user/IP based (should support unlimited users)		
7	Firewall Architecture should be on distributed framework – NGFW with Threat Prevention Policy Management, Logging, Reporting, Dashboard and should be managed from a centralised console.		
8	The communication between all the components should be encrypted with SSL or PKI.		
9	Security effectiveness should be recommended/certified by NSS NGFW test report		
10	Proposed Solution framework should have IPSec VPN (Site to Site VPN) functionalities for Secure Remote access to corporate application over the internet		
11	Solution should have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
12	The proposed solution of appliances should support the dynamic routing protocols with		

Sr. No.	Required Minimum Specifications “Annexure 11 B – Firewall –2& 3” Make & Model: (Firewall 2) (Qty-4) ____________________ Make & Model: (Firewall 3) (Qty-4) ____________________	Bidder’s compliance (Yes / No)	Bidder’s remarks
	readiness for BGPv4 & OSPF		
13	Appliance should have a capability to support for more than 500 VLAN.		
14	The communication between all the components of Firewall System (firewall module, logging & policy management server, and the GUI/WebUI Console) should be encrypted with SSL or PKI.		
15	Firewall Appliances should deployed for Active – Active architecture for both Firewall & VPN.		
16	It should support the system authentication with TACACS+, RADIUS.		
17	IPSec VPN should support the Authentication Header Protocols		
18	IPSec ISAKMP methods should support Diffie-Hellman Group 1,2,5,14 & 19, MD5 & SHA Hash, RSA & Manual Key Exchange Authentication, 3DES/AES-256 Encryption of the Key Exchange Material and algorithms like RSA-1024 / 2048		
19	Should be integrated with Privileged Identity Management (PIM) & Security Incident & Event Management (SIEM) Solutions.		
B	Performance Requirement		
1	The proposed solution should have an integrated solution for IPSEC, site to site		
2	Proposed solution should support IPSec functionality		
3	Solution should support minimum 40,000 new sessions per second processing		
4	Firewall should support atleast 3,000,000 concurrent sessions		
C	Hardware and Interface Requirements		
1	Firewall appliance should have Console port and USB Ports		
2	Solution should support VLAN Tagging and Link Aggregation (IEEE 802.3ad) to achieve higher bandwidth		
3	Solution should support Dual Stack with Ipv4 and Ipv6 functionality		
4	Solution should support Ipv6 NAT functionality NAT64 and NAT46		

Sr. No.	**Required Minimum Specifications "Annexure 11 B – Firewall –2& 3"** **Make & Model: (Firewall 2) (Qty-4) ___________________** **Make & Model: (Firewall 3) (Qty-4) ___________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
5	Firewall should have Hardware Sensor Monitoring capabilities.		
6	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
7	Every Gateway Security control (like Firewall or any other feature required to meet above specification) must not have any licensing restriction on number of users		
8	Each Appliance should have at least 12x10 GE fiber, 12x1G RJ-45 Ethernet interface. All ports should be populated with required transceivers. The networks switches supports 10Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored.		
9	Should support atleast 8 Gbps of production performance (http based) / multiprotocol & multipacket combined, Firewall & IPS throughput		
D	Firewall Filtering & Web Control [Application Control +URL Filtering] Requirements		
1	It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports		
2	The Firewall must provide state engine support for all common protocols of the TCP/IP stack		
3	The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type		
4	The Firewall should be able to filter traffic even if the packets are fragmented		
5	The Firewall should support database related filtering and should have support for Oracle, MS-SQL, and Oracle SQL-Net.		
6	The Firewall should provide advanced NAT capabilities, supporting all applications and services		
7	Local access to firewall modules should support role based access		
8	Solution should support Application Detection and Usage Control.		

Sr. No.	Required Minimum Specifications "Annexure 11 B – Firewall –2& 3" Make & Model: (Firewall 2) (Qty-4) ________________ Make & Model: (Firewall 3) (Qty-4) ________________	Bidder's compliance (Yes / No)	Bidder's remarks
9	Application Control Databases should have sizable application and widget control list		
10	Solution should have an option of creating custom categories for URL and Application control.		
11	**Should provide Seamless integration with Active Directory /LDAP (Agent-less deployment is preferable)**		
12	Should be Managed Centrally from Single Dashboard via user friendly interface.		
13	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats		
E	Anti-Malware & Anti-bot		
1	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
2	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
3	The proposed solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family		
4	The proposed solution should be able to detect & Prevent attack types such as spam sending click fraud or self-distribution, that are associated with Bots		
5	The proposed solution should be able to block traffic between infected bot Host & Remote C&C Operator and it should allow the traffic to legitimate destinations		
6	The proposed should inspect HTTP, HTTPS, DNS & SMTP traffic for the detection and prevention of the Bot related activities and Malware activities		
7	The proposed solution should have an option of configuring file type recognition along with following actions i.e. Scan, Block, Pass on detecting the Known Malware		
8	The Malware prevention engine of the proposed solution should be able to detect & prevent the Spyware, Ransomware & Adware for pattern		

Sr. No.	**Required Minimum Specifications “Annexure 11 B – Firewall –2& 3” Make & Model: (Firewall 2) (Qty-4) __________________ Make & Model: (Firewall 3) (Qty-4) __________________**	**Bidder’s compliance (Yes / No)**	**Bidder’s remarks**
	based blocking at the gateways.		
9	Solution should be able to discover the Bot infected machine		
10	Solution should be able to provide with Forensic tools which give details like Infected Users/Device,Malware type,Malware action etc		
11	Anti-virus scanning should supportproactive and stream mode		
12	Solution should be able to create a protection scope for the inspection		
13	Proposed solution should have an option of configuring Exception		
14	Anti-spyware for pattern based blocking at the gateway		
15	The known Malware scanning should not be restricted by the any specific limit on the size of the of the file(s)		
16	**The proposed solution should be able to detect & prevent the malware by scanning of different file types.**		
17	Proposed solution should have configurable option to inspect, bypass or blocked various file-types as per organization need.		
18	The known Malware scanning should be performed by the proposed solution for the traffic flows with the protocols for HTTP, HTTPS, FTP, POP3,& SMTP		
19	The proposed solution should prevent the users to access the malware hosting websites and/or web resources		
20	**The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds in a common threat language called as STIX (Structured Threat Information expression) or any other internationally supported format**		
21	**The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds from other security & SIEM solution deployed at**		

Sr. No.	**Required Minimum Specifications "Annexure 11 B – Firewall –2& 3"** **Make & Model: (Firewall 2) (Qty-4) ____________________** **Make & Model: (Firewall 3) (Qty-4) ____________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
	bank's data center.		
F	Application Visibility and Awareness		
1	Firewall Should support Identity based controls for Granular user, group and machine based visibility and policy enforcement		
2	Firewall should support the Identity based logging, application detection and usage controls		
3	Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc.		
4	Should have Categories like Business Applications, IM, File Storage and Sharing, Mobile Software, Remote Administration, SMS Tools, Search Engine, Virtual Worlds, Webmail etc.		
5	The proposed solution must delineate specific instances of peer2peer traffic (Bit torrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.).		
6	The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.		
7	Identity Access should be able to distinguish between employee and other like guests and contractors.		
8	**Should have provide out of box Categories based on Application types, Security Risk level etc. Should include filtering of application names based on Application types, Security Risk level etc.**		
9	**Application Control Library should covering most of the Web 2.0 application signatures**		
G	Administration, Management and Logging		
1	Management Should support automation & Orchestration using Open REST API Support.		
2	The Firewall must provide a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall.		

Sr. No.	**Required Minimum Specifications “Annexure 11 B – Firewall –2& 3”** **Make & Model: (Firewall 2) (Qty-4) ________________** **Make & Model: (Firewall 3) (Qty-4) ________________**	**Bidder’s compliance (Yes / No)**	**Bidder’s remarks**
3	Solution should be able provide auditing view / report for FW changes, Rule addition/Deletion & other network changes		
4	Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter.		
5	Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
6	The Firewall administration station must provide a means for exporting the firewall rules set and configuration.		
7	Role based administration with multiple administrators & Separation of duties should be supported. Config conflict should be avoided when multiple administrators works together.		
8	Management should provide role based access on policy configuration to cater separation of duties.		
9	Management should have log indexing capability for faster log search & log optimization.		
10	The Firewall administration software must provide a means of viewing, filtering and managing the log data. Monitoring logs in single console per policy will be plus		
11	The Firewall logs must contain information about the firewall policy rule that triggered the log.		
12	Should support for taking immediate action within logging pane in case of any critical DOS, Threat attempt		
13	Management should alert administrator in case if any configuration error or Misconfiguration.		
14	**The centralized management solution should support integration with the Microsoft AD or LDAP, NAC/IDAM.**		
15	The Solution should be able to ingest the Intelligence shared over STIX & TAXII from the SIEM solution		

Sr. No.	**Required Minimum Specifications “Annexure 11 B – Firewall –2& 3”** **Make & Model: (Firewall 2) (Qty-4) ________________** **Make & Model: (Firewall 3) (Qty-4) ________________**	**Bidder’s compliance (Yes / No)**	**Bidder’s remarks**
16	**Management framework and monitoring solution should monitor compliance status of the Threat Prevention devices in the real time. It is expected, the network solution to provide real-time and continuous assessment of configuration framework.**		
17	It should provide clear indications that highlight regulations with serious indications of potential breaches with respect to Access Policies, Intrusion, Malwares, BOT, URL, Applications etc.		
18	It should indicate automatically where improvements are needed and ongoing continuous assessment rather than manual intervention for meeting up compliance.		
19	Management framework should provide details on unused object and rules in the Policy Dashboard along with overlapping rules and supernet rules.		
20	All proposed components NGFW, Logging, Reporting etc. should be managed from centralised management framework and if not then vendor need to provide additional components if any		
21	Vendor should include additional software and licenses for compliance feature framework and need to integrate with the management framework		
22	Detailed Event analysis for Threat Prevention Controls Anti-Malware, Anti-Bot, IPS, Application Control etc. need to be provided with Real-Time and Historical reporting all the components.		
23	IPS signatures should support more than 7000+ excluding custom signatures.		
24	Centralized Management Server should be deployed in VM (VM to be provided by Bank) and all necessary license should be provided from day one.		
H	Licensing Requirement		
1	Solution should have enterprise license without any restrictions.		
2	Solution should be on Distributed Architecture for Threat Prevention along with Dedicated		

Sr. No.	**Required Minimum Specifications “Annexure 11 B – Firewall –2& 3”** **Make & Model: (Firewall 2) (Qty-4) ________________** **Make & Model: (Firewall 3) (Qty-4) ________________**	**Bidder’s compliance (Yes / No)**	**Bidder’s remarks**
	Management, Logging and Reporting Framework.		
3	The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM		
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc. should be provided		
I	High Availability Requirements:		
1	The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.		
2	The HA solution should support Active/Active or Active/Passive load balancing with state full Failover		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
J	Logging & Reporting		
1	Must integrate with centralized logging & reporting solution of same OEM for better reporting		
2	Also should have feature to integrate with syslog & SNMP server		
H	**URL Filtering**		
1	**Should be able to create policy based on URLs specifying in the rules**		
2	**Should be able to define URL category based on Risk level**		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 C – Firewall –4" (Qty-2)** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
A	General Requirements		
1	Proposed solution should be Next Generation Firewall with Application Layer Security Controls and Threat Prevention framework		
2	Proposed solution should have Multi-Layer Threat Prevention Suite with following controls embedded: a. Prevention against Malware b. Prevention against Bot & Botnets, c. Prevention against malware hosting URL, Prevention against risky web2.0 apps d. Widgets like anonymizers, TOR, P2P, Bit Torrents, etc.		
3	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
4	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
5	Proposed solution should have a Unified Policy Frame work for application, user, data awareness, etc in a single rule.		
6	Licensing should be a per device and not limited to user/IP based (should support unlimited users)		
7	Firewall Architecture should be on distributed framework – NGFW with Threat Prevention Policy Management, Logging, Reporting Dashboard and should be managed from a centralised console.		
8	The communication between all the components should be encrypted with SSL or PKI.		
9	Security effectiveness should be recommended/certified by NSS NGFW test report		
10	Proposed Solution framework should have IPSec VPN (Site to Site VPN) functionalities for Secure Remote access to corporate application over the internet		
11	Solution should have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
12	The proposed solution of appliances should support the dynamic routing protocols with readiness for BGPv4 & OSPF		
13	IPS signatures should support more than 7000+ excluding custom signatures.		
B	Performance Requirement		

Sr. No.	**Required Minimum Specifications** **“Annexure 11 C – Firewall –4” (Qty-2)** **Make & Model: ______________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
1	The proposed solution should have an integrated solution for IPSEC, site to site		
2	Proposed solution should support IPSec functionality		
3	Solution should support minimum 20,000 new sessions per second processing		
4	Firewall should support atleast 2,000,000 concurrent sessions		
C	Hardware and Interface Requirements		
1	Firewall appliance should have Console port and USB Ports		
2	Solution should support VLAN Tagging and Link Aggregation (IEEE 802.3ad) to achieve higher bandwidth		
3	Solution should support Dual Stack with IPv4 and Ipv6 functionality		
4	Solution should support Ipv6 NAT functionality NAT64 and NAT46		
5	Firewall should have Hardware Sensor Monitoring capabilities.		
6	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
7	Every Gateway Security control (like Firewall or any other feature required to meet above specification) must not have any licensing restriction on number of users		
8	Each Appliance should have at least 4x10 GE fiber, 12x1G RJ-45 Ethernet interface. All ports should be populated with required transceivers. The networks switches supports 10Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored.		
9	Should support atleast 4 Gbps of production performance (http based)/ multiprotocol & multipacket combined, Firewall & IPS throughput		
D	Anti-Malware & Anti-bot		
1	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
2	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 C – Firewall –4" (Qty-2)** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
3	The proposed solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family		
4	The proposed solution should be able to detect & Prevent attack types such as spam sending click fraud or self-distribution, that are associated with Bots		
5	The proposed solution should be able to block traffic between infected bot Host & Remote C&C Operator and it should allow the traffic to legitimate destinations		
6	The proposed should inspect HTTP, HTTPS, DNS & SMTP traffic for the detection and prevention of the Bot related activities and Malware activities		
7	The proposed solution should have an option of configuring file type recognition along with following actions i.e. Scan, Block, Pass on detecting the Known Malware		
8	The Malware prevention engine of the proposed solution should be able to detect & prevent the Spyware, Ransomware & Adware for pattern based blocking at the gateways.		
9	Solution should be able to discover the Bot infected machine		
10	Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc		
11	Anti-virus scanning should support proactive and stream mode		
12	Solution should be able to create a protection scope for the inspection		
13	Prposed solution should have an option of configuring Exception		
14	Anti-spyware for pattern based blocking at the gateway		
15	The known Malware scanning should not be restricted by the any specific limit on the size of the of the file(s)		
16	**The proposed solution should be able to detect & prevent the malware by scanning of different file types**		
17	Proposed solution should have configurable option to inspect, bypass or blocked various file-types as per organization need.		
18	The known Malware scanning should be performed by the proposed solution for the traffic flows with the protocols for HTTP, HTTPS, FTP, POP3,& SMTP		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 C – Firewall –4" (Qty-2)** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
19	The proposed solution should prevent the users to access the malware hosting websites and/or web resources		
20	The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds in a common threat language called as STIX (Structured Threat Information expression) **or any other internationally supported format**		
21	**The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds from other security & SIEM solution deployed at bank's data centre**		
E	Application Visibility and Awareness		
1	Firewall Should support Identity based controls for Granular user, group and machine based visibility and policy enforcement		
2	Firewall should support the Identity based logging, application detection and usage controls		
3	Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc		
4	The proposed solution must delineate specific instances of peer2peer traffic (Bit torrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultra surf, ghost surf, free gate, etc.).		
5	The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.		
6	Identity Access should be able to distinguish between employee and other like guests and contractors.		
7	**Should provide out of box Categories based on Application types, Security Risk level etc** Should include filtering of application names based on Application types, Security Risk level etc.		
8	**Application Control Library should have covering most of the Web 2.0 application signature**		
F	Administration, Management and Logging		
1	Management Should support automation & Orchestration using Open REST API Support.		
2	The Firewall must provide a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall.		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 C – Firewall –4" (Qty-2)** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
3	Solution should be able provide auditing view / report for FW changes, Rule addition/Deletion & other network changes		
4	Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter.		
5	Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
6	The Firewall administration station must provide a means for exporting the firewall rules set and configuration.		
7	Role based administration with multiple administrators & Separation of duties should be supported. Config conflict should be avoided when multiple administrators works together.		
8	Management should provide role based access on policy configuration to cater separation of duties.		
9	Management should have log indexing capability for faster log search & log optimization.		
10	The Firewall administration software must provide a means of viewing, filtering and managing the log data. Monitoring logs in single console per policy will be plus		
11	The Firewall logs must contain information about the firewall policy rule that triggered the log.		
12	Should support for taking immediate action within logging pane in case of any critical DOS, Threat attempt		
13	Management should alert administrator in case if any configuration error or Misconfiguration.		
14	**The centralized management solution should support integration with the Microsoft AD or LDAP, NAC/IDAM**		
15	The Solution should be able to ingest the Intelligence shared over STIX & TAXII from the SIEM solution		
16	**Management framework and monitoring solution should monitor compliance status of the Threat Prevention devices in the real time. It is expected, the network solution to provide real-time and continuous assessment of configuration framework**		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 C – Firewall –4" (Qty-2)** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
17	It should provide clear indications that highlight regulations with serious indications of potential breaches with respect to Access Policies, Intrusion, Malwares, BOT, URL, Applications etc.		
18	It should indicate automatically where improvements are needed and ongoing continuous assessment rather than manual intervention for meeting up compliance.		
19	Management framework should provide details on unused object and rules in the Policy Dashboard along with overlapping rules and supernet rules.		
20	All proposed components NGFW, Logging, Reporting etc should be managed from centralised management framework and if not then vendor need to provide additional componennts if any		
21	Vendor should include additional software and licenses for compliance feature framework and need to integrate with the management framework		
22	Detailed Event analysis for Threat Prevention Controls Anti-Malware, Anti-Bot, IPS, Application Control etc need to be provided with Real-Time and Historical reporting all the componets.		
23	Centralized Management Server should be deployed in VM (to be provided by Bank) and all necessary license should be provided from day one.		
G	Licensing Requirement		
1	Solution should have enterprise license without any restrictions.		
2	Solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.		
3	The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM		
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc. should be provided		
H	High Availability Requirements:		
1	The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.		

Sr. No.	**Required Minimum Specifications** **“Annexure 11 C – Firewall –4” (Qty-2)** **Make & Model: ______________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
2	The HA solution should support Active/Active or Active/Passive load balancing with state full Failover		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
J	Logging & Reporting		
1	Must integrate with centralized logging & reporting solution of same OEM for better reporting		
2	Also should have feature to integrate with syslog & SNMP server		
H	**URL Filtering**		
1	**Should be able to create policy based on URLs specifying in the rules**		
2	**Should be able to define URL category based on Risk level**		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 D – Firewall –4 A (Qty.-4) "** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
A	General Requirements		
1	Proposed solution should be Next Generation Firewall with Application Layer Security Controls and Threat Prevention framework		
2	Proposed solution should have Multi-Layer Threat Prevention Suite with following controls embedded: a. Prevention against Malware b. Prevention against Bot & Botnets, c. Prevention against malware hosting URL, Prevention against risky web2.0 apps d. Widgets like anonymizers, TOR, P2P, Bit Torrents, etc.		
3	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
4	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
5	Proposed solution should have a Unified Policy Frame work for application, user, data awareness, etc in a single rule.		
6	Licensing should be a per device and not limited to user/IP based (should support unlimited users)		
7	Firewall Architecture should be on distributed framework – NGFW with Threat Prevention Policy Management, Logging, Reporting Dashboard and should be managed from a centralised console.		
8	The communication between all the components should be encrypted with SSL or PKI.		
9	Security effectiveness should be recommended/certified by NSS NGFW test report		
10	Proposed Solution framework should have IPSec VPN (Site to Site VPN) functionalities for Secure Remote access to corporate application over the internet		
11	Solution should have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.		
12	The proposed solution of appliances should support the dynamic routing protocols with readiness for BGPv4 & OSPF		
13	IPS signatures should support more than 7000+ excluding custom signatures.		
B	Performance Requirement		

Sr. No.	**Required Minimum Specifications** **“Annexure 11 D – Firewall –4 A (Qty.-4) ”** **Make & Model: ______________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
1	The proposed solution should have an integrated solution for IPSEC, site to site		
2	Proposed solution should support IPSec functionality		
3	Solution should support minimum 20,000 new sessions per second processing		
4	Firewall should support atleast 2,000,000 concurrent sessions		
C	Hardware and Interface Requirements		
1	Firewall appliance should have Console port and USB Ports		
2	Solution should support VLAN Tagging and Link Aggregation (IEEE 802.3ad) to achieve higher bandwidth		
3	Solution should support Dual Stack with IPv4 and Ipv6 functionality		
4	Solution should support Ipv6 NAT functionality NAT64 and NAT46		
5	Firewall should have Hardware Sensor Monitoring capabilities.		
6	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
7	Every Gateway Security control (like Firewall or any other feature required to meet above specification) must not have any licensing restriction on number of users		
8	Each Appliance should have at least 4x10 GE fiber, 12x1G RJ-45 Ethernet interface. All ports should be populated with required transceivers. The networks switches supports 10Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored.		
9	Should support atleast 4 Gbps of production performance (http based)/ multiprotocol & multipacket combined, Firewall & IPS throughput		
D	IPS Features		
1	IPS Engine should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behavior-based detection, Multi-element correlation.		
2	IPS should activate protection for both Client Protection and Server Protections		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 D – Firewall –4 A (Qty.-4) "** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
3	The IPS should be constantly updated with new defences against emerging threats.		
4	IPS updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time		
5	IPS should provide Protection against Injection Vulnerabilities SQL Injection, Command Injection, LDAP Injection, HTTP Command Injection		
6	Blocking SQL and Command Injection by Keywords traced in form field GET, POST etc		
7	Should have a provision to configure blocking of Distinct and Non-Distinct SQL Commands, Shell Commands etc.		
8	IPS should provide Application layer protections for Cros site scripting, Directory traversal etc		
9	Specifc vulnerabilities keywords that can be used for scripting code, JavaScript and VBScript. Commands, event that can trigger scripting engine, and HTML attributes and tags.		
10	IPS should have advanced capabilities that detect and prevent attacks launched against the Web infrastructure		
11	Protection against Malicious code for Buffer Overflow, Heap overflow and other malicious executable code attacks that target Web servers and other applications without the need of signature		
12	Monitor web communication for potential executable code, confirms the presence of executable code and identifies whether the executable code is malicious		
13	Protections against Information disclosure for Header spoofing enforcement, directory listing prevention, error concealment		
14	HTTP Protocol Inspections for HTTP format size enforcement, ASCII-only request enforcement, ASCII-only response header enforcement, header rejection definitions, HTTP method definitions		
15	Protection for HTTP Clients using IE for COM (Component Object Model) and DOM (Document Object Model.		
16	IPS should have the functionality of Geo Protection to Block the traffic country wise.		
17	Should have flexibility to define newly downloaded protections will be set in Detect or Prevent mode.		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 D – Firewall –4 A (Qty.-4) "** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
18	**The NGFW must integrate with existing APT / Sand box (Fireeye) to learn new threat IOC such as malicious URL and block it in real time.**		
19	IPS Profile should have an option to select or re-select specific signatures that can be activated/de-activated as per Bank's environment		
20	Activation of new protections based on parameters like Performance impact, Confidence index, Threat severity etc.		
21	IPS should also have IPS should have an option to create your own signatures with an open signature language.		
22	Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance		
23	IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Relrease date, Industry Reference etc.		
24	IPS events/protection exclusion rules can be created and view packet data directly from log entries with RAW Packets and if required can be sent to Wireshark for the analysis.		
25	Configuration granularity for Individual servers protected by Web Intelligence attack protections enabled for each sever; for each attack protection, apply to individual servers or inspect all HTTP traffic; customisable profiles associated.		
26	Real time safeguard and defense updates through update service		
27	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats		
E	IPS should have below mentioned DOS/DDOS functionality		
1	IPS should understand Denial of Service tool used to crafts and send multiple HTTP Request that can potentially cause attached system to become temporarily unresponsive		
2	Should have an understanding of DDOS Tool Kit including SYN Flood, UDP Flood, etc.		
3	Should have protection against exploitation of DOS vulnerability in Microsoft IE, Microsoft IIS, Apache, Oracle etc.		

Sr. No.	**Required Minimum Specifications "Annexure 11 D – Firewall –4 A (Qty.-4) " Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
4	Prevent and Block attempts to exploit DOS related vulnerability in applications		
5	Should have prevention against Script DdoS tool that utilizes high bandwidth webservers to generate malicious DdoS traffic.		
F	Anti-Malware & Anti-bot		
1	The proposed solution should be able to detect & Prevent the Bot communication with C&C		
2	The proposed solution should have an Multi-tier engine to i.e. detect & Prevent Command and Control IP/URL and DNS		
3	The proposed solution should be able to detect & Prevent Unique communication patterns used by BOTs i.e. Information about Botnet family		
4	The proposed solution should be able to detect & Prevent attack types such as spam sending click fraud or self-distribution, that are associated with Bots		
5	The proposed solution should be able to block traffic between infected bot Host & Remote C&C Operator and it should allow the traffic to legitimate destinations		
6	The proposed should inspect HTTP, HTTPS, DNS & SMTP traffic for the detection and prevention of the Bot related activities and Malware activities		
7	The proposed solution should have an option of configuring file type recognition along with following actions i.e. Scan, Block, Pass on detecting the Known Malware		
8	The Malware prevention engine of the proposed solution should be able to detect & prevent the Spyware, Ransomware & Adware for pattern based blocking at the gateways.		
9	Solution should be able to discover the Bot infected machine		
10	Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc		
11	Anti-virus scanning should support proactive and stream mode		
12	Solution should be able to create a protection scope for the inspection		
13	Prposed solution should have an option of configuring Exception		
14	Anti-spyware for pattern based blocking at the gateway		

Sr. No.	**Required Minimum Specifications** **“Annexure 11 D – Firewall –4 A (Qty.-4) ”** **Make & Model: ______________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
15	The known Malware scanning should not be restricted by the any specific limit on the size of the of the file(s)		
16	**The proposed solution should be able to detect & prevent the malware by scanning of different file types**		
17	Proposed solution should have configurable option to inspect, bypass or blocked various file-types as per organization need.		
18	The known Malware scanning should be performed by the proposed solution for the traffic flows with the protocols for HTTP, HTTPS, FTP, POP3,& SMTP		
19	The proposed solution should prevent the users to access the malware hosting websites and/or web resources		
20	The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds in a common threat language called as STIX (Structured Threat Information expression) **or any other internationally supported format**		
21	The proposed solution with Malware & Bot Prevention engines should be supplied with the readily available support for the ingestion of threat intelligence feeds from other security & SIEM solution deployed at bank's data centre		
G	Application Visibility and Awareness		
1	Firewall Should support Identity based controls for Granular user, group and machine based visibility and policy enforcement		
2	Firewall should support the Identity based logging, application detection and usage controls		
3	Should enable securities policies to identify, allow, block or limit application regardless of port, protocol etc		
4	The proposed solution must delineate specific instances of peer2peer traffic (Bit torrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultra surf, ghost surf, free gate, etc.).		
5	The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.		
6	Identity Access should be able to distinguish between employee and other like guests and contractors.		

Sr. No.	**Required Minimum Specifications** **“Annexure 11 D – Firewall –4 A (Qty.-4) ”** **Make & Model: ______________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
7	**Should have provide out of box Categories based on Application types, Security Risk level etc** Should include filtering of application names based on Application types, Security Risk level etc.		
8	**Application Control Library should have covering most of the Web 2.0 application signature**		
H	Administration, Management and Logging		
1	Management Should support automation & Orchestration using Open REST API Support.		
2	The Firewall must provide a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall.		
3	Solution should be able provide auditing view / report for FW changes, Rule addition/Deletion & other network changes		
4	Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter.		
5	Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
6	The Firewall administration station must provide a means for exporting the firewall rules set and configuration.		
7	Role based administration with multiple administrators & Separation of duties should be supported. Config conflict should be avoided when multiple administrators works together.		
8	Management should provide role based access on policy configuration to cater separation of duties.		
9	Management should have log indexing capability for faster log search & log optimization.		
10	The Firewall administration software must provide a means of viewing, filtering and managing the log data. Monitoring logs in single console per policy will be plus		
11	The Firewall logs must contain information about the firewall policy rule that triggered the log.		
12	Should support for taking immediate action within logging pane in case of any critical DOS, Threat attempt		
13	Management should alert administrator in case if any configuration error or Misconfiguration.		

Sr. No.	**Required Minimum Specifications** **"Annexure 11 D – Firewall –4 A (Qty.-4) "** **Make & Model: ______________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
14	The centralized management solution should support integration with the Microsoft AD or LDAP, **NAC/IDAM**		
15	The Solution should be able to ingest the Intelligence shared over STIX & TAXII from the SIEM solution		
16	**Management framework and monitoring solution should monitor compliance status of the Threat Prevention devices in the real time. It is expected, the network solution to provide real-time and continuous assessment of configuration framework**		
17	It should provide clear indications that highlight regulations with serious indications of potential breaches with respect to Access Policies, Intrusion, Malwares, BOT, URL, Applications etc.		
18	It should indicate automatically where improvements are needed and ongoing continuous assessment rather than manual intervention for meeting up compliance.		
19	Management framework should provide details on unused object and rules in the Policy Dashboard along with overlapping rules and supernet rules.		
20	All proposed components NGFW, Logging, Reporting etc should be managed from centralised management framework and if not then vendor need to provide additional componennts if any		
21	Vendor should include additional software and licenses for compliance feature framework and need to integrate with the management framework		
22	Detailed Event analysis for Threat Prevention Controls Anti-Malware, Anti-Bot, IPS, Application Control etc need to be provided with Real-Time and Historical reporting all the componets.		
23	Centralized Management Server should be deployed in VM (to be provided by Bank) and all necessary license should be provided from day one.		
H	Licensing Requirement		
1	Solution should have enterprise license without any restrictions.		
2	Solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.		

Sr. No.	**Required Minimum Specifications “Annexure 11 D – Firewall –4 A (Qty.-4) ” Make & Model: ______________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
3	The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM		
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc. should be provided		
I	High Availability Requirements:		
1	The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.		
2	The HA solution should support Active/Active or Active/Passive load balancing with state full Failover		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
J	Logging & Reporting		
1	Must integrate with centralized logging & reporting solution of same OEM for better reporting		
2	Also should have feature to integrate with syslog & SNMP server		
H	URL Filtering		
1	Should be able to create policy based on URLs specifying in the rules		
2	Should be able to define URL category based on Risk level		

Sr. No.	**Required Minimum Specifications “Annexure 11E – Firewall – 5 (Qty- 7)” Make & Model: ____________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
A	Industry Certifications and Evaluations		
1	The proposed vendor must have a track record of continuous improvement in threat detection and must have successfully completed NSS Labs’		
2	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu’s to protect & scale against dynamic latest security threats.		
3	Each Appliance should have at least 16 X GE RJ-45 Ethernet interface & 1 GE Management, & Console Interface. The networks switches supports 1Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored.		
B	Platform Requirement		
1	The detection engine must be capable of operating in both passive (i.e., monitoring) and inline (i.e., blocking) modes.		
2	The device should have functionality of hardware / Software Fail Open		
3	The solution should support Active/Passive load balancing with stateful Failover		
C	Performance & Scalability		
1	Should have minimum Inspected throughput of 2 Gbps for all kinds of real word traffic after enabling the IPS and Application visibility feature		
2	Should support minimum 1 million concurrent connections or more and minimum 12000 new connection per second with Application Visibility and Control.		
3	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
D	URL Filtering		
1	Should be able to create policy based on URLs specifying in the rules		
2	Should be able to define URL category based on Risk level		
E	AMP		
1	Appliance should be capable of working in Inline Blocking mode without depending on other		

Sr. No.	**Required Minimum Specifications "Annexure 11E – Firewall – 5 (Qty- 7)" Make & Model: ____________________**	Bidder's compliance (Yes / No)	Bidder's remarks
	network components like a separate FW, IPS or Web Security Appliance. AMP license should be given from day 1.Solution should be capable of identifying zero days threat and same should be considered from day one.		
2	Solution should be capable of blocking call-backs to CnC Servers		
3	Solution should be capable of blocking threats based on both signatures and behaviour		
4	The anti-APT Solution should be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behaviour of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.		
5	Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.		
6	The solution should be capable to analysis & block TCPand UDP protocols to identify attacks and malware communications. At a minimum, the following protocols are supported for real-time inspection, blocking and control of downloaded files: HTTP, SMTP, POP3, IMAP, Netbios-ssn and FTP.		
7	The solution should be capable of protecting against spear phishing attacks		
8	The solution should be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.		
9	**The solution should detect and classify mobile devices as mobile devices. For example: iPad, iPhone and Blackberry devices. These devices should be discovered and related back to the user, applications, and possible services they offer**		
10	The solution should be capable of whitelisting trusted applications from being inspected and not an entire segment to avoid business applications from being affected & in turn productivity		

Sr. No.	**Required Minimum Specifications “Annexure 11E – Firewall – 5 (Qty- 7)” Make & Model: __________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
11	The solution should be capable of blocking traffic based on geo locations to reduce the attack landscape and to protect communication to unwanted destinations based on geography		
12	The solution shall be able to detect attacks on 64-bit operating systems		
13	All the devices shall be managed centrally and should be capable of • Centralized, life cycle management for all sensors • Aggregating all events and centralized, real-time monitoring and forensic analysis of detected events • Must provide a highly customizable dashboard		
14	**The proposed solution must be capable of passively gathering information (without active scanning) about network hosts and their activities**		
15	The proposed solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.		
16	The proposed solution must be capable of passively detecting pre-defined services, such as FTP, HTTP, POP3, Telnet, etc., as well as custom services.		
17	The proposed solution must be capable of storing user-defined host attributes, such as host criticality or administrator contact information, to assist with compliance monitoring.		
18	The proposed solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.		
19	The proposed solution must have a granular rule mechanism that allows specifying what type of traffic and transfer context will be subject to the process of analysis and prevention of advanced malware in real time.		
20	The proposed solution must Detect, control access and inspect for malware at least the following file types: Microsoft Office files, executables, multimedia, compressed documents, Windows dump files, pdf, jarpack,		

Sr. No.	Required Minimum Specifications **“Annexure 11E – Firewall – 5 (Qty- 7)”** **Make & Model:** ______________________________	Bidder’s compliance (Yes / No)	Bidder’s remarks
	install shield.		
21	The proposed solution must have capability to Analysis of APTs and malwares must be performed in real-time using hybrid analysis capabilities, using various analysis and control strategies, including simultaneously, whether the local, remote or hybrid execution technology for the determination of advanced malware.		
22	The proposed solution must allow granular definition of the type of compressed files to be analysed, including traffic control options and their access to preventive actions.		
23	The NBA capability must provide the ability to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
24	**Should provide out of box Categories based on Application types, Security Risk level etc**		
F	Management		
1	The management platform must be available in virtual form factor.		
2	The management platform must be accessible via a web-based interface and ideally with no need for additional client software		
3	The management platform must provide a highly customizable dashboard.		
4	The management appliance should be able to support 25 appliance if required in future		
5	The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.		
6	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward		
7	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their		

Sr. No.	**Required Minimum Specifications “Annexure 11E – Firewall – 5 (Qty- 7)” Make & Model: ______________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
	authentication.		
8	Should support REST API for monitoring and config programmability		
9	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
10	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
11	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
12	The management platform must risk reports like advanced malware, attacks and network		
13	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
14	Centralized Management Server should be deployed in VM (to be provided by Bank) and all necessary license should be provided from day one.		
G	Licensing Requirement		
1	Solution should have enterprise license without any restrictions.		
2	Solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.		
3	The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM		
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance		
H	High Availability Requirements:		

Sr. No.	**Required Minimum Specifications "Annexure 11E – Firewall – 5 (Qty- 7)" Make & Model: _______________________**	Bidder's compliance (Yes / No)	Bidder's remarks
1	The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.		
2	The HA solution should support Active/Active or Active/Passive load balancing with state full Failover		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
I	Logging & Reporting		
1	Must integrate with centralized logging & reporting solution of same OEM for better reporting		
2	Also should have feature to integrate with syslog & SNMP server		

Sr. No.	**Required Minimum Specifications “Annexure 11 F – NIPS (Qty- 8)” Make & Model: ____________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
A	Solution Requirement		
1	Should be propose built dedicated appliance from the NIPS OEM and provide Intrusion Prevention System, Anti Malware, Anti BOT, Application control capabilities.		
2	The communication between all the components of solution (IPS module, logging & policy and Web GUI Console) should be encrypted with SSL or PKI		
3	**Solution should provide seamless failover among devices for all components and should be completely automatic**		
4	Solution Should provide protection against various types of cyber-attacks evasive attacks, scripting attacks etc		
5	Solution should have capability to store Logs and configuration of all devices, centrally in the solution and should also have capability to send logs of all devices to the generic central log collection servers		
6	Solution must support the complete STACK of IP V4 and IP V6 services		
7	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).		
8	The device must be capable of dynamically tuning IPS sensors (Like: selecting rules/signatures, configuring policies, updating policies, etc.) with minimal human intervention		
B	Hardware and Interface Requirement		
1	All ports should be populated with required transceivers. Apart from each appliance should have additional ports for sync, HA and other functionalities.		
2	**NIPS should have Console port**		
3	should have management interface for Out of Band Management		
4	The appliance should have separate dedicated 1xG Ethernet interface for management console. None of the monitoring ports should be used for this purpose.		

Sr. No.	**Required Minimum Specifications "Annexure 11 F – NIPS (Qty- 8)" Make & Model: ________________**	Bidder's compliance (Yes / No)	Bidder's remarks
5	NIPS should be rack mountable and support side rails if required		
6	NIPS should have hot swappable redundant power supplies (atleast dual)		
7	NIPS should have hardware health monitoring capabilities and should provide different parameters through SNMP		
8	Solution should support VLAN tagging (IEEE 802.1q)		
9	Solution should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy		
10	Each appliance in the Solution should support and not limited to:		
11	**This device must support active-active OR Active-Standby High Availability without session loss. The HA should be out of the box solution and should not require any third party or additional software/hardware for the same**		
12	Solution should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc		
13	Centralized Management Solution should provide high availability at site level for enabling DR deployment		
14	It should be possible to manage the entire solution from Primary & Secondary management server/appliance placed at DC and DR. Management solution should have the capability to be deployed in geographically different location enabling DR deployment		
15	The NIPS system should have adequate local storage in order to keep the various logs		
16	NIPS should be able to perform entire packet capture of the infected traffic and sent to the other application for analysis		
17	Each Appliance should have at least 4x10 GE fiber, 12x1G RJ-45 Ethernet interface. All ports should be populated with required transceivers. The networks switches supports 10Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored		
18	Centralized Management Server should be deployed in VM (to be provided by Bank) and all		

Sr. No.	**Required Minimum Specifications "Annexure 11 F – NIPS (Qty- 8)" Make & Model: ______________________**	Bidder's compliance (Yes / No)	Bidder's remarks
	necessary license should be provided from day one.		
19	**Proposed solution should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats**		
C	Performance Requirement		
1	NIPS systems should be manageable from the centralised management framework from DC and DR with support for managing MIN 4 NIPS systems		
2	Each appliance in the Solution should be properly sized for following given parameters, with all features enabled at the same time:		
3	**IPS Inspected Throughput (HTTP Based) of 8 Gbps should be minimum 8 Gbps and should be scalable upto 20 Gbps**		
4	Running all internet protocols etc, traffic flowing through different zones in the solution with all the features enabled and running		
5	**Can use multiple pairs of IPSs in Active/Failover mode for factoring the full capacity.**		
6	**Solution should support minimum 10 million concurrent connections**		
7	**Solution should support minimum 200,000 new sessions per second processing**		
8	Maximum permissible latency of solution is less than 200 microseconds with all the services enabled together.		
9	IPS signatures should support more than 7000+ excluding custom signatures.		
D	Feature Requirement		
1	Solution should have capability to keep track the network connections, identify the threats, detect and prevent the threat and relate the threat with corresponding end points (IP address, user, software program etc		
2	Solution should be providing flow information details (Netflow,Jflow, Sflow or similar) for a specific host for given time interval		
3	Solution should able to get enterprise visibility of internet access like URL access, Malicious website visits etc.		

Sr. No.	**Required Minimum Specifications** **“Annexure 11 F – NIPS (Qty- 8)”** **Make & Model:** **__________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
4	Solution should able to get enterprise visibility of internet access – malicious server visits, country details		
5	**Should support application layer controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.**		
6	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location		
7	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Identify and explain each type of detection mechanism supported.		
8	The solution should allow Custom IPS Signatures creation		
E	Detection and Prevention Requirement		
1	NIPS should support different mode of deployment in following modes: a) IDS b) TAP Mode c) Inline		
2	NIPS should accurately detect intrusion attempts and discern between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, hybrids, and zero-day attacks, Worm, Phishing, Spyware, Virus, Trojan, P2P, VoIP, Backdoor, Reconnaissance, Bandwidth Hijacking, Cross-site scripting, SQL Injection etc.		
3	**NIPS should employ all seven-layer (of OSI model) protocol analysis.**		
4	Should support vulnerability based and not exploit based signatures. Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability)		
5	Should support a wide variety of techniques to perform traffic inspection including (a) TCP stream reassembly, b) Does IP defragmentation, c) Bi- directional inspection, d) Protocol Anomaly		

Sr. No.	**Required Minimum Specifications “Annexure 11 F – NIPS (Qty- 8)” Make & Model: ____________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
	Detection, e) Protocol tunneling, f) Signatures g) Behavior anomaly h) Reputation		
6	NIPS should have the ability to identify application traversing on the network and allow or block specific application on the network.		
7	NIPS should support source reputation based analysis. NIPS should obtain through the cloud the reputation for each host involved in an attack and uses the reputation score of the source host as one of the factor for blocking the host		
8	Solution should support malware protection by performing file reputation analysis of malicious files		
9	Solution should have the ability to inspect traffic in the virtual environment and if any additional hardware are required to achieve it, should be provided		
10	NIPS should support provide advanced botnet protection using heuristic detection methods		
11	NIPS should provide advanced botnet protection using multi event behaviour based detection mechanism.		
12	Should protect against DOS/DDOS attacks. Should have —self-learning” capability to monitor the network traffic and develops a baseline profile. It should have the ability to constantly update this profile to keep an updated view of the network		
13	Should support the ability to limit the number of TCP/UDP/ICMP active connections or connection rate from a host		
14	NIPS should support active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done, i.e. before compromise occurs		
15	NIPS should have the ability to control traffic based on geographical locations. For e.g. a policy can be created to block traffic coming or going to a particular country		
16	NIPS should have the ability to block connection from outside based on the reputation of the IP address that is trying to communicate with the network		
17	Should protect against evasion techniques		

Sr. No.	**Required Minimum Specifications “Annexure 11 F – NIPS (Qty- 8)” Make & Model: ____________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
18	Should support a wide range of response actions as a) Block traffic, b) Ignore, c) TCP reset, e) Log traffic, f) Packet capture, g) User defined scripts, h) Email alert, i) SNMP alert, j) syslog alert		
19	The device should accurately detect the following Attack categories:		
20	Malformed traffic, Invalid Headers		
21	Vulnerability exploitation		
22	URL obfuscation		
23	The device must support vulnerability based and exploit based signatures. It should detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability)		
24	Solution should get Signatures, Patches & updates being received from OEM should be from trusted sites		
25	The device should handle following traffic inspection & support following:		
26	Ipv6, Ipv4, Tunneled: 4in6, 6in4, 6to4		
27	Bi- directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection		
28	Application Anomalies, P2P attacks, TCP segmentation and IP fragmentation		
29	Rate-based threats, Statistical anomalies		
30	The device should have the ability to identify/block individual applications (eg. Facebook or skype) running on one protocol (eg HTTP or HTTPs)		
31	IPS should have application intelligence for commonly used TCP/IP protocols, not limited to telnet, ftp, http, https etc		

Sr. No.	**Required Minimum Specifications “Annexure 11 F – NIPS (Qty- 8)” Make & Model: ______________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
32	The device should support Block attacks based on IP reputation, DNS Inspection and Sink-Holing, Geo-location, URL Inspection / intelligence		
33	The device should have the feature for importing SNORT signatures.		
34	Should support basic attack protection features listed below but not limited to :		
35	Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite		
36	It should enable rapid detection of network attacks		
37	TCP reassembly for fragmented packet protection		
38	SYN cookie protection , SYN Flood, Half Open Connections and NUL Packets etc		
39	Protection against IP spoofing		
40	Malformed packet protection		
41	It should be able to block Instant Messaging like Yahoo, MSN, ICQ, Skype (SSL and HTTP tunneled) etc		
42	The Solution should provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and detecting Advanced Malware related DoS & DdoS activity from within the network		
43	Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.		
44	The solution should be capable of whitelisting trusted applications from being inspected and not an entire segment to avoid business applications from being affected & in turn productivity		
F	Administration and Management and Logging Functionality Feature Requirement		
1	Solution Real-Time Monitoring, Management & Log Collection (with storage) should not be distributed to more than ONE server/appliance		
2	A centralized monitoring and management system with multiple administrators who have administrative rights based on their roles, should		

Sr. No.	**Required Minimum Specifications "Annexure 11 F – NIPS (Qty- 8)" Make & Model: __________________________________**	Bidder's compliance (Yes / No)	Bidder's remarks
	provide Audit Trail of the Changes etc		
3	Secondary (SLAVE) Management Server should support the MASTER role once the Disaster recovery is triggered for any or multiple management domains in the Management Server		
4	Solution should be able to support large scale WAN deployment with following important Criteria for Real-Time Monitoring, Management & Log Collection etc		
5	Implementation team has to migrate existing policies and create policies as per Bank's IT & IS.		
6	To ensure business continuity all the solutions/hardware proposed should be in HA		
7	Any changes or commands issued by an authenticated user should be logged to a database of the management system		
8	Any changes or commands issued by an authenticated user should be logged to a database of the management system		
9	It should support SNMP (Simple Network Management Protocol) v 3.0 with all new versions of present and future release		
10	IPS must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.		
11	The management platform must provide a highly customizable dashboard.		
12	The IPS must provide simplified provisioning for addition of new IPSs where by a standard IPS policy could be pushed into the new IPS		
13	The IPS administration station must provide a means for exporting the IPS rules set and configuration		
14	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward		
15	NIPS Management console should be capable of producing extensive graphics metric for		

Sr. No.	**Required Minimum Specifications “Annexure 11 F – NIPS (Qty- 8)” Make & Model: ____________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
	analysis. Further, users should be able to drill down into these graphical reports to view pertinent details.		
16	Support for role based administration of IPS		
17	NIPS should support granular management. Should allow policy to be assigned per device, port, VLAN tag, IP address/range		
18	The IPS administration software must provide a means of viewing, filtering and managing the log data		
19	The IPS logs must contain information about the IPS policy rule that triggered the log		
20	Should support to enable/disable each individual signature. Each signature should allow granular tuning		
21	Centralized Security Management should include for all the proposed security controls but not limited to:		
22	Real Time Security Monitoring		
23	Logging		
24	Reporting functions based on 1. Security event risk level, 2. Date/time, 3. Event name 4. Source IP 5. Destination IP 6. Response Taken 7. Sensor Identity 8. Severity, etc		
25	The solution must provide a minimum basic statistics about the health of the IPS and the amount of traffic traversing the IPS		
26	Solution should support for configuration rollback		
27	Solution should support Real time traffic statistics & Historical report with		
28	Attacks and threat reports, etc.		
29	Customized reports on HTML, CSV and PDF format etc		
30	Solution Audit Trail should contain at a minimum:		
31	The name of the administrator making the change		
32	The change made		
33	Time of change made		

Sr. No.	Required Minimum Specifications “Annexure 11 F – NIPS (Qty- 8)” Make & Model: ____________________	Bidder’s compliance (Yes / No)	Bidder’s remarks
34	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
35	Management system should provide detailed Event analysis for IPS and also should provide Syslog output to integrate with other major SIEM tools and specifically should support RSA SIEM tool current and future versions		
36	Solution should support for real time analysis of all traffic the IPS may encounter (all possible SOURCE, DEST, SERVICE, including groups) etc		
37	Solution should manage the NIPS appliances from a central management console		
38	Management platform supports policy configuration, command, control, and event management functions for the NIPS appliances		
39	Management console should support Radius and LDAP authentication in addition to the local user authentication		
40	F3 Management console should have the ability to allow access to specific hosts by enabling GUI Access and defining the list of authorized hosts/networks		
41	The IPS signature updates and intelligence database update on NIPS and IPS should be automatic without any reboot on the appliance		
42	**The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows**		
G	Licensing Requirement		
1	Solution should have enterprise license without any restrictions. If during the contract, solution is not performing as per specifications in this RFP, bidder has to upgrade/enhance the devices or place additional devices and reconfigure the system without any cost to bank		
2	Solution should be able to achieve all the features and functionalities mentioned in the RFP and accordingly, all the required licenses should be provided as part of solution.		
3	The offered product part codes have to be General Availability Part codes and not custom built Part Code for customer. There should be		

Sr. No.	**Required Minimum Specifications “Annexure 11 F – NIPS (Qty- 8)” Make & Model: ______________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
	cross reference to the public website of the OEM		
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance and necessary hardware, database and other relevant software or hardware etc should be provided		
H	Other		
1	The proposed solutions should must identify network related malicious activity, log information about such activity, report it to SIEM dashboard and attempt to block or stop it.		
2	Should have Intrusion prevention sensors delivering context-aware, IPS device should perform stateful pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.		
3	Must perform protocol decoding and validation for network traffic including: IP, TCB UDP, and ICMP.		
4	Should identify attacks based on observed deviations in the normal RFC behaviour of a protocol or service.		
5	Should identify attacks running inside of these tunnelling protocols such as GRE, IP-in-IP, MPLS, and Ipv4/Ipv6.		
6	Ability to setup exceptions to filter out, fine-tune or adjust the actions for specific attacker or destination IP on a per signature basis.		
7	**Capable to detect device failure link failure.**		
8	Should have an option to add exceptions for network and services.		
9	Should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, performance impact, Release date, Industry Reference, Confidence level etc.		
10	Should be integrated with Privileged Identity Management (PIM) & Security Incident & Event Management (SIEM) Solutions.		
11	**Should have Categories based on Application types, Security Risk level etc**		

Sr. No.	**Required Minimum Specifications “Annexure 11 F – NIPS (Qty- 8)” Make & Model: ________________________**	Bidder’s compliance (Yes / No)	Bidder’s remarks
I	High Availability Requirements:		
1	**This device must support active-active OR Active-Standby High Availability without session loss. The HA should be out of the box solution and should not require any third party or additional software/hardware for the same**		
2	**Solution should provide seamless failover among devices for all components and should be completely automatic without any sort of manual intervention**		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
6	**All components of the appliance should be in HA**		

Sr. No.	**Required Minimum Specifications “Annexure 11G –Router (Qty- 2)” Make & Model: ____________________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
A	The following are the functional requirements to be met by the access router:-		
1	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
2	The router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multi-processor based for enhanced performance.		
3	The router must support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities.		
4	The Core router must have onboard support for intelligent traffic measurement and analysis. The router must support flow based traffic analysis feature.		
5	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.		
6	Rack mounting kit for securing the router in standard rack are to be provided.		
7	The proposed model should be compatible with Cisco Ace router		
8	Router shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one		
B	Router Architecture		
1	Architecture: The architecture of the router must be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 6 Gbps on Day 1 and should be scalable to 20 Gbps in future.		
2	Number of Slots: The router must be chassis based and should accommodate 1 nos. interface slots.		
3	The router must have redundant power supply module. The router must support 220V AC or -48V DC power supply module. There should not be any impact on the router performance in case of one power supply fails. Router should be proposed with AC power supply.		
4	Power Supply: The router must have redundant power supply module. The router must support		

Sr. No.	Required Minimum Specifications “Annexure 11G –Router (Qty- 2)” Make & Model: ______________________	Bidder's compliance (Yes / No)	Bidder's remarks
	220V AC power supply module. There should not be any impact on the router performance in case of one power supply fails.		
5	Router Processor Architecture: The router processor architecture must be multi-processor / Multi-core based and should support hardware accelerated, parallelised and programmable IP forwarding and switching.		
6	Redundancy Feature: The router must support Operating System (OS) redundancy or dual control module in 1:1 mode to ensure high-availability of the system. The router in the event of failure of any one OS or control module should switchover to the redundant OS or redundant control module without dropping any traffic flow. There should not be any impact on the performance in the event of active processing engine failure.		
7	Hot Swapability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way.		
8	Clock: The router must derive clock from the hired links. The hired links will provide Stratum II/III Clock. The router must sync to the Network Time Protocol (NTP) server.		
9	The router must have support for flash memory for configuration and OS backup.		
10	The Proposed VPN headend router should be supplied & supported in at least one commercial Bank / Financial Institutions / Govt Organization in India with supporting minimum 5000 tunnels.		
C	Router Performance Parameter:		
1	Routing Table Size: The router must support minimum 2,000,000 IPv4 or 2,000,000 IPv6 routes entries in the routing table and should be scalable.		
2	The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.		
3	Router must support 6 Gbps of Crypto throughput (IMIX) for IPSEC performance and 8000 IPSEC tunnels from day 1		

Sr. No.	**Required Minimum Specifications “Annexure 11G –Router (Qty- 2)” Make & Model: ____________________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
	(internal/external).In case of an external box, The vpn concentrator must have redundant power supply & at least 6 x 1GE interfaces from Day 1.		
4	The Router solution must be a enterprise grade Equipment supporting the following:		
a.	In-band and out-band management		
b.	Software rollback feature		
c.	Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.		
8	The proposed router should support modular OS and simply the changes through In-Service OS upgrade mechanism		
9	The router should be able to select a WAN/LAN path based on interface parameters such as reachability, load, throughput, and link cost of using a path		
D	Physical Parameters:		
1	The router must have the following interface as defined in the IEEE, ITU-T:		
2	6 x 1 GE Copper ports from day one and support for atleast 3 nos. of 10Gbps of ports in future		
3	**The router card must support following interface:** **Fast Ethernet, Gigabit Ethernet, Channelized STM1, Channelized STM16, STM 64 , 10G Ethernet, POS, ATM, E1, Chn E1 Ports.**		
E	Layer 3 Routing Protocols		
1	The router must support the IPv4 and IPv6 stack in hardware and software. It must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains.		
2	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.		
3	The router should support minimum 7000 VRF instances from day one		
4	MPLS OAM - LSP Ping/Trace route for MPLS core		
5	Multicast VPN (mVPN)		
6	The Router should have at-least 4 GB of DRAM from day one		

Sr. No.	**Required Minimum Specifications “Annexure 11G –Router (Qty- 2)” Make & Model: ______________________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
F	IPv6 Support		
1	Should support IP version 6 in hardware.		
2	Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
3	The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunnelling, IPv6 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, SSH over IPv6, MPLS Support for IPv6 - IPv6 VPN over MPLS (6VPE) Inter-AS options, IPv6 VPN over MPLS (6VPE), IPv6 transport over MPLS (6PE)		
4	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
5	The router should support for IPv6 Multicast.		
6	Should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
7	Should support IPv6 Quality of Service		
8	Should support IPv6 dual stack		
9	Should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
10	Should support SNMP over IPv6 for management.		
11	The router must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
12	The router must support router redundancy protocol like VRRP.		
13	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
G	Multicast		
1	The router must support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).		
2	The multicast implementation must support Rendezvous Points on both leaf and non-leaf nodes.		

Sr. No.	Required Minimum Specifications “Annexure 11G –Router (Qty- 2)” Make & Model: ____________________	Bidder's compliance (Yes / No)	Bidder's remarks
3	The multicast implementation must support source specific multicast.		
4	The router must support multiprotocol BGP extensions for multicast.		
5	The router must support multicast load balancing traffic across multiple interfaces.		
6	The router must support RFC 3618 Multicast Source Discovery Protocol (MSDP).		
7	The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP) as defined in RFC 3446.		
H	Quality of Service		
1	The router must be capable of doing Layer 3 classification and setting ToS/Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting.		
2	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP and by some well-known application types through Application Recognition techniques.		
3	The router shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter.		
4	The QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue.		
5	The router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP.		
6	The router should have support for minimum 8 queues per port		
7	Scheduling should allow for round robin and weighted round robin.		
8	The scheduling mechanism must allow for expedited or strict priority routing for all high		

Sr. No.	Required Minimum Specifications “Annexure 11G –Router (Qty- 2)” Make & Model: ______________________________	Bidder's compliance (Yes / No)	Bidder's remarks
	priority traffic.		
9	The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues.		
10	All network based keep alives (PPP keep alives, OSPF LSAs, BGP updates etc) must be given the highest priority and route before any traffic type		
11	The traffic must be able to be prioritized into 8 class types. Class types must be able to be mapped into 1 of 8 bandwidth constraints. Bandwidth Constraints should be assignable to in individual hardware queues. Oversubscription rates for bandwidth constraints should have local significance only.		
12	The router shall support at least180k queues to offer granular QoS, policing and shaping capabilities.		
13	Queuing and Scheduling must be able to be configured on a per physical port or logical port		
14	IPSec packets should be marked with QoS		
I	Security Feature		
1	The router shall meet the following requirements for security –		
2	The router shall support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc.		
3	The router shall support time based ACL to reflect time based security and QoS policy.		
4	The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
5	The router shall support firewall service in hardware on all interfaces.		
6	The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.		
7	The router shall support AAA features through RADIUS or TACACS+.		

Sr. No.	**Required Minimum Specifications “Annexure 11G –Router (Qty- 2)” Make & Model: ____________________________**	**Bidder's compliance (Yes / No)**	**Bidder's remarks**
8	The router shall support Control Plane Policing to protect the router CPU from attacks.		
9	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP and MPLS routing protocols.		
10	The proposed router should have embedded support for 8000 IPsec tunnels from day one, which should be activated from day 1.		
J	System Management and Administration		
1	Routers should support Configuration rollback		
2	Support for accounting of traffic flows for Network planning and Security purposes		
3	Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP		
4	Routers should support Software upgrades		
5	Routers should support SNMPv2 and SNMPv3		
6	Device should have Console, Telnet, SSH1 and SSH2 support for management		
K	Built-in trouble shooting		
1	Extensive debugs on all protocols		
2	Shall support Secure Shell for secure connectivity		
3	Should have to support Out of band management through Console and an external modem for remote management		
4	Pre-planned scheduled Reboot Facility		
5	Real Time Performance Monitor – service-level agreement verification probes/alert		
L	Certifications		
1	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
2	The proposed router should be NDPP/EAL4 certified		

Sr. No.	**Required Minimum specifications "Annexure 11H – Switch (Qty-8)" Make and Model:_ ______________________**	**Bidder's Compliance (Yes/No)**	**Bidder's Remarks**
A	Required Minimum Specifications		
1	Minimum of 48 port 10 Gb SFP + port + 6 nos. 40 Gbps ports, with minimum 1280 Gbps switching backplane		
2	10G SFP+LC SR Transreceiver - 46 Nos		
3	40GbE QSFP+ uplink ports - 2 Nos		
4	QSFP+ to QSFP+ 3 mts DAC cable		
5	SFP+ to SFP+ 3 mts DAC cable		
6	Full-Duplex Operation on GbE		
7	Multiple Load Sharing Trunks		
8	Minimum of 2 GB SDRAM and 512MB Flash memory, packet buffer size: 9 MB		
9	650W AC Power Supply - 2 Nos (port side intake)		
10	Fan Tray - 2 Nos		
11	1 RJ-45 serial console port 1 RJ-45 out-of-band management port 1 USB 2.0 port		
12	Minimum throughput of 250 million pps (64-byte packets)		
13	Minimum routing/switching capacity should be 336 Gb/s		
14	10 Gb/s latency should be <1.5 microsec (64-byte packets)		
15	Support for minimum of 128000 MAC addresses		

Sr. No.	**Required Minimum specifications “Annexure 11H – Switch (Qty-8)”** **Make and Model:_ ______________________**	**Bidder’s Compliance (Yes/No)**	**Bidder’s Remarks**
16	RFC 1027 Proxy ARP RFC 1058 RIPv1 RFC 1091 Telnet Terminal-Type Option RFC 1141 Incremental updating of the Internet checksum RFC 1142 OSI IS-IS Intra-domain Routing Protocol RFC 1191 Path MTU discovery RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1253 (OSPFv2) RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1534 DHCP/BOOTP Interoperation RFC 1541 DHCP RFC 1591 DNS (client only) RFC 1624 Incremental Internet Checksum RFC 1723 RIPv2 RFC 1812 IPv4 Routing RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2131 DHCP RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2453 RIPv2		
17	TACACS/TACACS+		
18	High MTBF Support		
19	The Switches must be able to generate Syslog Messages with timestamp and Severity codes, which can be exported to a Syslog Server.		
20	The Switches must be able to Build up its own inventory (like Device Name, Chassis Type, Memory, Flash, Software ver. Etc or equivalent fields)		
21	Rack mounting kit for securing the switch in standard rack are to be provided.		
B	Layer 3 Features		
1	RFC 2918 Route Refresh Capability RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4)		

Sr. No.	**Required Minimum specifications “Annexure 11H – Switch (Qty-8)”** **Make and Model:_ ______________________**	**Bidder’s Compliance (Yes/No)**	**Bidder’s Remarks**
2	RFC 2573 SNMP-Target MIB RFC 2574 SNMP USM MIB RFC 2737 Entity MIB (Version 2) RFC 3414 SNMP-user based-SM MIB RFC 3415 SNMP-view based-ACM MIB		
3	RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2473 Generic Packet Tunneling in IPv6 RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2563 ICMPv6 RFC 2711 IPv6 Router Alert Option RFC 2740 OSPFv3 for IPv6		
4	RFC 3623 Graceful OSPF Restart RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)		
5	ACL - SSHv2 Secure Shell		
C	QoS Features:-		
1	RFC 3260		
D	Security Features:-		
1	Support for External RADIUS for console access restriction and authentication		
2	Multi-Level access security on switch console to prevent unauthorized users		
3	Support for 802.1x port based authentication		
4	Support for IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN.		
5	Configuration Change Tracking		
6	System Event Logging		
7	Syslog		
8	SNMP v1, v2c, v3 compatible		
9	Support for Secured ports which restrict a port to a user-defined group of authorized stations. When secure addresses are assigned to a secure port, the switch should not forward any packets with source addresses outside the defined group of addresses		
E	Other Features:		
1	The switch should have its own management software, which can be used remotely (through secured Web interface) to monitor, troubleshoot & manage the switch.		

Sr. No.	Required Minimum specifications “Annexure 11H – Switch (Qty-8)” Make and Model:_ ______________________	Bidder’s Compliance (Yes/No)	Bidder’s Remarks
2	The management software should integrate with any EMS product suite.		
3	The Switch should seamlessly integrate with existing network equipments		
4	**Layer 2 / layer 3 traceroute to ease troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.**		
5	Should support Link layer Discovery Protocol		
6	Should Support DNS		
7	Secure access to switch management, limiting management applications from specifc hosts only		
8	Should support BPDU guard to avoid topology loop.		
9	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
10	Support for MAC address notification allows administrators to be notified of users added to or removed from the network.		
11	The operating system should have a self healing mechanism for the automatic recovery of the switch when a specified event occurs		
12	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
13	Support Bidirectional data support on the SPAN port allows the Intrusion Detection System (IDS) to take action when an intruder is detected.		
14	IPv6 support with full L2/L3 features		
F	Network Management (Management Feature) :-		
1	Embedded support for Web based management using standard secured web browser.		
2	RFC 1908 (SNMPv1/2 Coexistence) RFC 2573 (SNMPv3 Applications) RFC 2576 (Coexistence between SNMPv1, v2, and v3)		
3	Support for TFTP based software download		
4	Support for port mirroring measurement using a network analyzer or RMON probe.		
5	RMON: 4 Group (Statistics, Alarm, Events, History), on every port, no impact to		

Sr. No.	**Required Minimum specifications “Annexure 11H – Switch (Qty-8)”** **Make and Model:_ ______________________**	**Bidder’s Compliance (Yes/No)**	**Bidder’s Remarks**
	performance		
6	Switch must be remotely managed via one telnet session for all module configuration		
7	Should have functionality to add new features like IOS/Firmware upgrades from central location, etc.		
8	Provisioned and Dynamic Policies at Layers 1-4 for QoS and Security		
9	Support for Dynamic VLAN assignment or equivalent feature is supported through implementation of VLAN Membership Policy Server (VMPS) client functions to provide flexibility in assigning ports to VLANs. Dynamic VLAN or equivalent feature helps enable the fast assignment of IP addresses.		
10	Real Time Multi-Port Statistics		
11	Mac/IP Address Finder or equivalent feature		
12	Device and Port Groupings for Navigation and Policy Management		
13	Radius or TACACS+ server Support		
14	Private and Enterprise MIB / MIB		
15	Administrative Access Right		
16	Traffic Volume/Error/Congestion Monitoring		
17	TFTP Download/Upload Software		
18	The Switch should be able to discover the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.		
G	IEEE Standard Compliance: -		
1	802.1Q VLAN tagging		
2	802.1p Priority		
3	802.1D Spanning Tree		
4	802.3u Fast Ethernet		
5	802.3x Flow Control		
6	802.1x Authentication		
7	802.3ab Gigabit Interface		
H	RFC (Request for Comment) Support: -		
1	768 UDP		
2	783 TFTP		
3	791 IP		
4	792 ICMP		

Sr. No.	**Required Minimum specifications “Annexure 11H – Switch (Qty-8)”** **Make and Model:_ ______________________**	**Bidder’s Compliance (Yes/No)**	**Bidder’s Remarks**
5	826 ARP		
6	854 Telnet		
7	1122 Host Requirements / ICMP		
8	1542 BootP		
9	2068 HTTP or equivalent		
10	2236 IGMP		
11	SNTP – RFC1769 or equivalent		

ANNEXURE 11I **Structured Cable**		**Bidder’s Compliance (Yes/No)**	**Bidder’s Remarks**
S/N	**Required Minimum Specifications**		
1	All passive component, accessories and cables supplied under this contract shall be in accordance with the latest applicable recommendations, regulations and standards of: - CCITT / ITU - ANSI - IEC 60364 - IEEE Standard 1100 - IETF - TIA 942 - IS 3043 - EIA / TIA 568 Standards - NFPA 72 and NFPA 318 International Electro-technical Commission (IEC)		
2	Quality Control: The horizontal cable shall have a unique print string on the cable jacket. This unique identifier shall also be used for on-line reference to a full set of factory tests that were performed on a sample from the same mater reel. The on-line reference must be available on the SCS vendor public website, such that it can be accessed at any time.		
3	Cabling Solution should be a high density LSZH system solution with reduced installation time.		
4	All Passive Components should be RoHS (Restriction of Certain Hazardous Substances) complied. Declaration –RoHS Compliant should clearly be mentioned on datasheets of each Passive Components.		
5	OEM shall submit the certificate stating bend insensitive glass is supplied for this project and also attenuation report of fiber used.		

ANNEXURE 11J		**Bidder's Compliance (Yes/No)**	**Bidder's Remarks**
CAT 6A Cable			
S/N	**Required Minimum Specifications**		
1	The Cable should meet ANSI/TIA 568C.2 Category 6A Specifications		
2	The Conductors should be twisted in pairs with four pairs contained in a flame retardant LSZH jacket separated by a divider and conductor size should be 23 AWG.		
3	The cable should support the installation temperature: 0 to 60 0 C		
4	The Cable should support Operating temperature of -20 to 60 0 C		
5	The Category 6A/ Class EA STP Structured Cabling System(SCS) shall comply with the standards ISO/IEC 11801:2010,EN 50173 Part 1 through Part 5:2010 and 2011, ANSI/TIA-568-C IEC 60603-7-4,IEEE 802.3 applications as outlined in section 2 & Local/National Codes and Regulations.		
6	The Category 6A/ Class EA UTP system should support IEEE Ethernet applications: 802.3e - 1BASE5, 802.3i – 10GBASE-T , 802.3u - 100BASE-TX, 100BASE-T4, 802.3y - 100BASE-T2, 802.3z - 1000BASE-X, 8023ab - 1000BASE-T,802.af - Power Over Ethernet (15.4W),802.3at - Power Over Ethernet Enhancements (25.5W),802.3az - Energy Efficient Ethernet.		
7	The SCS must be tested by a 3rd Party test facility to EIA/TIA 568C, ISO/IEC 11801 Amendment 1 and for the channel testing ,the certificate for the same must be provided as part of the bid response.		
8	Each patch cord should be 100% factory made and performance tested.		

ANNEXURE 11K		**Bidder's Compliance (Yes/No)**	**Bidder's Remarks**
Fibre Cables (OM3/OM4)			
S/N	**Required Minimum Specifications**		
1	The 50/125 mm fiber channel shall support single-channel serial transmission, 10 gigabits per second (Gb/s) for a distance of 300 meters, 40Gbps up to a distance of 100-150 meters		

ANNEXURE 11K		**Bidder's Compliance (Yes/No)**	**Bidder's Remarks**
Fibre Cables (OM3/OM4)			
S/N	**Required Minimum Specifications**		
2	The channel shall support 10 Gb/s short wavelength (850 nm) emerging technology applications using vertical cavity surface emitting lasers (VCSELs) and low bit rate LED applications for legacy systems.		
3	The 50 micron fiber shall be optimized to control differential mode delay (DMD) or equivalent standard, so that "pulse splitting" at 10 Gb/s is eliminated.		
4	The high performance fiber shall use the same termination and test procedures that are currently used for the existing industry's lower performance 50 mm fiber. Fibers shall be manufactured with dual acryl ate coating for maximum color retention and protection.		
5	The 50 mm fiber cable, 50 mm fiber connectors, 50 mm patch cords and apparatus, which comprise the channel shall be manufactured from a single manufacturer		
6	The 50 micron fiber shall meet or exceed the following standards, as applicable, for OSP or Plenum cables: ICEA S-83-596, ISO/IEC-794, GR-409, TIA/EIA455, TIA/EIA492, TIA/EIA568-B, ANSI-FDDI, IEEE 802, UL 910 or equivalent, OFNP classification as described in the National Electric Code (NEC2), OFN-LS Low Smoke Cables, CSA Certified (OFN FT4/FT6) or equivalent and approved component industry standards.		
7	Multimode fiber cable should be Bend - Insensitive multi-mode fiber (BIMMF) to significantly reduce macro bend losses even in the most challenging bend scenarios.		
8	The cable should be able to withstand bending radius of 3 times the outer diameter. Maximum insertion loss in MTP connector should be <=0.35 dB		
9	Maximum reflectance loss in MTP connector should be <-35 dB		

ANNEXURE 11K		**Bidder's Compliance (Yes/No)**	**Bidder's Remarks**
Fibre Cables (OM3/OM4)			
S/N	**Required Minimum Specifications**		
10	Trunks cable shall be manufactured with ultra-bendable fiber and meet the fiber performance: (@ 850 nm wavelength) - (a) Max. Attenuation, Loose Tube Cable - 3.0 dB/km (b) Max. Attenuation, Tight Buffer Cable - 3.0 dB/km (@ 1300 nm wavelength) - (a) Max. Attenuation, Loose Tube Cable - 1.0 dB/km (b) Max. Attenuation, Tight Buffer Cable - 1.0 dB/km		
11	Flame Test Specifications : Flame Test Listing NEC OFNRLS (ETL) and c(ETL) or equivalent		
12	The OM3/OM4 fibre should be bidirectional mode		

ANNEXURE 11L		**Bidder's Compliance (Yes/No)**	**Bidder's Remarks**
CAT 6A/ Fiber Optic Patch Chord/Panel			
S/N			
1	The ganged adapter style patch panel will utilise increments of six RJ-45 style jacks in a common molded component.		
2	The ganged adapters shall have RJ45 jack in the front and Insulation Displacement Connector (IDC) at the rear of the module.		
3	The panel shall have horizontal cord organizers available as to improve patch cord management		
4	The patch panel type shall be a 1U panel capable of supporting 24 Port (copper) configuration compliant with IEC 60603-7-4 while meeting the Channel Performance as specified in Amendment 1 to ISO/IEC 11801:2002		
5	The panel shall be equipped with a removable rear mounted cable management bar and front and rear labels		

ANNEXURE 11M		**Bidder's Compliance (Yes/No)**	**Bidder's Remarks**
Fiber LIU/Casette			
S/N			
1	Fiber shelf should have High Density Enclosure which can cater 144 Core in 1U Rack Size for Server Rack, however there should be minimum 24 core to start with, OM3/OM4 MM with Accessories with LC or MPO Sockets,.		
2	Each 1U Tray shall have patch cord routing guides that allow a transition and jumper management point.		
3	The connector housings shall have a labeling scheme that complies with ANSI/TIA/EIA-606.		
4	MPO cassette shall have dust cover. The shutter adapter shall be VFL compatible.		
5	Fiber LIU tray should be able to support both LC and MPO cassette for (10/40/100G) requirement		
6	Each MTP cassette shall have 6 LC duplex port in front and 1 MTP connector at rear side.		