Next Generation Firewall- Technical Specifications - OEM 1			
S.N.	**Minimum Technical Specifications**	**Bidder Compliance (YES/NO)**	**Remark**
A	**General Features**		
1	The appliance based security platform should be capable of providing firewall, IPS ,IPSec VPN , Application control , Anti Virus , Anti Bot and Threat-prevention functionality on a single appliance		
2	The Management Server must be a physical appliance with same support duration as Gateway Firewall		
3	The appliance should support at least 8*1 G Copper Ports & 4 * 10 G SFP+ ports from day-1 and should be expandable to 2 * 40 G ports for future use . The appliance should have a dedicated Console and at least 1 USB ports.		
4	FW should have at least One Out of Band remote Management Port to enable remote management to start , restart , diagnosis , IOS installation via its web interface		
5	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory		
6	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.		
7	Firewall should have hot swappable dual power supplies, hot swappable hard disk & cooling fans		
8	Firewall must support both Active/Active and Active/Standby architecture in production for high availability and clustering		
9	The OEM should have a Recommended Overall rating in latest NSS Lab Reports for NGFW Comparative report in Security Effectiveness		
B	**Performance & Scalability**		
1	All Performance threshold are to be considered in real time and UDP traffic measurements are not Valid		
2	NGFW should support firewall performance throughput of atleast 10 Gbps		
3	NGFW should support atleast 8 Gbps of throughput with Firewall + IPS features		
4	NGFW should support atleast 6 Gbps of NGFW throughput with Firewall + IPS + Application Control		
5	NGFW should support atleast 4 Gbps with all features of NGFW and all threat prevention features enabled , which includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot , Anti APT , SandBox , Zero-Day Protection Software		
6	NGFW should support atleast 8 million concurrent sessions		
7	NGFW should support atleast 65000 new connections per second		
8	NGFW should support 5 Gbps of IPSec VPN throughput		
9	NGFW should support atleast 1000 VLANs		
10	All features of individual blade of appliance must work smoothly for both IPv4 and IPv6 without any additional purachase of License		

11	Hardware should be capable of sustaining the given performance parameters anytime whenever the license is enabled and should not include any separate license purchase for any stated points		
12	Penalty as per the RFP terms will be applied in case Performance parameters are not met in Production anytime during the Service Period		
C	**Firewall**		
1	The Firewall should support all routing Protocols like Static, Policy Based Routing, Identity based, Dynamic routing like RIP1 & 2, OSPF, OSPFv3, BGP4, MPLS routing		
2	Firewall should provide application detection for DHCP , DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SQLNET, TFTP, H.323, SNMP v2 , SNMP v3 , TELNET		
3	Firewall must support Inter VLAN routing / VLAN tagging		
4	Firewall must support all IPSec VPNs like Site to Site , Remote Site		
5	Firewall must support all standard and latest Hashing and Encryption techniques and algorithms of SHA/DES/RSA/AES/MD5 like SHA 256 /3DES /RSA 2048		
6	Firewall should support access-rules with IPv4 & IPv6 objects simultaneously		
7	Firewall should support operating in routed & transparent mode		
8	Firewall must support all listed NAT functionality both Hardware and Software wise , Manual NAT , PAT , Auto-NAT, static nat, dynamic nat, dynamic pat		
9	Firewall should support Multicast protocols like IGMP, PIM, etc both in IPv4 and IPv6		
10	Should support Security Policies based on Group wise /User wise in Source and Destination or both field		
11	Should support capability to limit bandwidth on basis of apps / User/groups, Networks etc		
12	The Firewall should support authentication protocols like LDAP, RADIUS and have support for firewall passwords, & token-based products like SecureID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.		
13	Firewall should support 802.3ad Etherchannel functionality to increase the bandwidth for a segment.		
14	Firewall should support redundant interfaces to provide interface level redundancy before device failover		
15	Firewall should have a minimum 200 Gb storage		
16	The Firewall should be able to filter traffic even if the packets are fragmented		
17	The firewall shall be able to handle VoIP traffic securely with "pinhole opening" and support SIP, SCCP, MGCP and H.323 ALGs		
18	Firewall should be capable of QoS configuration .QoS Support Guaranteed bandwidth, Maximum bandwidth, Priority bandwidth utilization, QOS weighted priorities, QOS guarantees, QOS limits and QOS VPN] in both IPv4/IPv6		
D	**Next Generation IPS and URL Filtering**		

1	The IPS should have 20,000+ signature and it should have a extreme database for higher threat efficacy		
2	Url Filtering should be capable of blocking and allowing urls based on categories in-build and customized ones , allow and block must be available on IP/Port/Services/Application/Usage		
3	Should have the capability of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		
4	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
5	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over all standard and non-standard communications ports.		
6	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.		
7	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor		
8	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.		
9	Should support more than 3000 application detection signatures and risk-based controls for application detection & control. Signatures should be periodically updated for latest application support.		
10	The Appliance OEM must have its own threat intelligence analysis centre and must use the global footprint of security deployments for more comprehensive network protection and incorporate same in our Network		
11	The IPS 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, HTML Obfuscation etc.).		
12	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location		
13	The detection engine should support the capability of detecting variants of known threats, as well as new threats		
14	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.		

15	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications signature quickly		
16	IPS should understand and take action on Denial of Service /DDOS used to crafts and send multiple communication Request that can potentially cause attached system to become temporarily unresponsive. It Should have prevention against Script DDoS tool that utilizes high bandwidth web servers to generate malicious DDoS traffic.		
17	IPS Should be able to detect and prevent Worms , Trojan, Zero day attacks ,Unknown Threat Protections , Protection against Backdoor , SQL Injection , Cross Site Scripting, Phishing , IP Spoofing , TCP SYN Flood ,		
18	System should be intelligent enough to minimize the false positives in logs/alerts		
19	The IPS updates should be able to be downloaded manually and automatically with the scheduler option to download the same on specific days and time		
20	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 60 categories.		
21	Solution must be able to inspect the SSL traffic		
22	Solution must be able to detect and protect protocol misuse , tunnelling attempts ,malware communications without predefined signatures		
23	The Reports/Alerts/Logs should be in detail , with all flow of data , and should be able to be exported in proper formats like pdf or csv		
24	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
25	IPS/Application control must be able to detect and block peer to peer traffic		
26	IPS/Application control must be able to detect and block remote control applications		
E	**IPv6 Support**		
1	Solution must support Dual Stack Configuration on the physical interface or on the sub interface		
2	Solution must support IPv6 Traffic on FW , IPS , Application Control , URL filtering , AV , AB , Threat Prevention for all stated features		
3	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) functionality , 6 to 4 Tunnel , NAT46		
4	Solution must support AD/LDAP/TACAS+ integration in IPv6		
5	Solution must support ICMP , SNMP , All Routing Protocols , MPLS Routing , Multicast in IPv6		
6	Should be capable of detecting and blocking IPv6 attacks like DDOS , TCP SYN Flood		
7	NGFW should support Active/Active model in IPv6 also		
8	All other features as stated above in Appliance must support in IPV6		
F	**Advance Malware Protection**		
1	Appliance should work in inline mode		

2	Appliance should be capable of blocking callbacks to C&C 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	Administrator should be able to create their own threat prevention rules and customize any vendor provided rules		
6	The solution should be capable to analysis & block TCP and 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, HTTP(s),POP3 , IMAP, Netbios, FTP SMTP, SMB, CIFS etc.		
7	Must be capable of providing network-based detection of malware by checking the Threat signatures of known files and capability to do dynamic analysis unknown files on-premise on purpose built-appliance		
8	Sandbox should provides safe and highly secure on-premises static and dynamic malware analysis to maintain the confidentiality ofdata. Its should easily integrate with existing security infrastructure and should also provide safe on-premises storage of malware analysis results.		
9	Sandbox appliance Integrated redundant power supply and 4*1 G interface support		
10	Sandbox appliance should deliver dynamic and static analysis engines that provide a full understanding of malware behaviour		
11	Sandbox appliance should provide detailed analysis reports of all malware sample activities, including network traffic		
12	The solution should be capable of protecting against spear phishing attacks		
13	NGFW 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 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.		
15	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, install shield.		
16	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.		

17	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.		
18	The proposed should be able to detect and prevent the malware by scanning 50 different file types/day		
E	**Anti Virus and Anti Bot**		
1	AV/AB should be integrated on the NGFW		
2	The solution must be able to scan and detect and stop any suspicious abnormal NW behaviour		
3	The solution should detect and prevent the Trojans , Worms , Viruses, Ransomwares, Phising, Spear Phising , DNS attacks		
4	The solution must prevent access to malicious websites and incoming malicious files		
5	Anti Bot solution must be able to scan for bot and botnets actions		
6	AV must be able to inspect SSL traffic		
7	AV and AB must have be managed and administered centrally		
8	AV should scan the links in mails and protect the user accordingly		
F	**Management**		
1	One Management Device of each OEM at each site (DC and DR)		
2	Each Management device should be capable of handling at least 5 appliances		
3	The management platform must be available in physical appliance and should have dual power supplies.		
4	The management platform must be accessible via a CLI and web-based interface or with secure software agent based console with no additional purchase and should be easy to use and comprehensive		
5	The transfer of Logs/alerts or any other transfer of data between all the components of NGFW or from NGFW to any Log Server must be encrypted and authenticated		
6	The Dashboard should be detailed , separate Blade wise and should be able to customize.		
7	The management should not have any restriction deviated to log licensing		
8	The management platform must have minimum 32Gb of RAM, 900 Gb event storage hardware configuration		
9	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.		
10	The management appliance should be able to manage the Sandbox server also , or provide management of the same with the features as defined without any additional purchase		
11	The management platform must support 10 million of IPS events		

12	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		
13	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.		
14	Should support REST API for monitoring and config programmability		
15	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV		
16	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
17	The management platform must provide robust & advance reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. If not available in centralized Mgmt. Vendor should provide additional advance logging & reporting solution with no additional expense		
18	The management platform must provide risk reports like advanced malware, network and application layer attacks		
19	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), log management tools , PIM etc		
20	The solution should have enterprise license without any restrictions on number of users for all the components		
21	Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard e.g CPU & memory utilization, state table, total number of concurrent connections the connections per second , traffic data, dropped traffic data , Top IPs and Services , Top Source and Destination IPs		
22	Server must provide detailed information in reports like Top IP/Ports , Top VPN users and longest duration connections , Top Rules , Top Security attacks , their Ips and Ports , Web Activity like most visited sites, Blocked connections their Ips and ports , Modification in rules like audit reports		
23	The Firewall Management must provide a means for exporting the firewall rules set and configuration.		
24	All appliances will be taken for 3 years Warranty and 4 years of AMC		
25	All appliances and its components should not be End of Support for the next 7 years from the date of issuance of this RFP.		

Next Generation Firewall- Technical Specifications - OEM 2			
S.N.	**Minimum Technical Specifications**	**Bidder Compliance (YES/NO)**	**Remark**
1	The appliance based security platform should be capable of providing firewall, IPS ,IPSec VPN , Application control , Anti Virus , Anti Bot, and Threat-prevention functionality on a single appliance		
2	The Management Server must be a physical appliance with same support duration as Gateway Firewall		
3	The appliance should support at least 8*1 GbE Copper Ports & 4 * 10 Gb SFP+ ports from day-1 and should be expandable to 2 * 40 G ports for future use . The appliance should have a dedicated Console and at least 1 USB ports.		
4	FW should have at least One Out of Band remote Management Port to enable remote management to start , restart , diagnosis , IOS installation via its web interface		
5	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory		
6	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.		
7	Firewall should have hot swappable dual power supplies, hot swappable hard disk & cooling fans		
8	Firewall must support both Active/Active and Active/Standby architecture in production for high availability and clustering		
9	The OEM should have a Recommended Overall rating in latest NSS Lab Reports for NGFW Comparative report in Security Effectiveness		
B	**Performance & Scalability**		
1	All Performance threshold are to be considered in real time and UDP traffic measurements are not Valid		
2	NGFW should support firewall performance throughput of atleast 6 Gbps		
3	NGFW must support atleast 4 Gbps of throughput with Firewall + IPS features		
4	NGFW must support atleast 2.5 Gbps of NGFW performance throughput with combined FW+ IPS+Application visibility functionality		
5	NGFW must support atleast 1.5 Gbps with all features of NGFW and all threat prevention features enabled, which includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot , Anti APT , SandBox and Zero-Day Protection Software		
6	NGFW should support atleast 5 million concurrent sessions		
7	NGFW should support atleast 50000 new connections per second		
8	NGFW should support 2 Gbps of IPSec VPN throughput		
9	NGFW should support atleast 1000 VLANs		
10	All features of individual blade of appliance must work smoothly for both IPv4 and IPv6 without any additional purachase of License		
11	Hardware should be capable of sustaining the given performance parameters anytime whenever the license is enabled and should not include any separate license purchase for any stated points		
12	Penalty as per the RFP terms will be applied in case Performance parameters are not met in Production anytime during the Service Period		
C	**Firewall**		
1	The Firewall should support all routing Protocols like Static, Policy Based, Identity based, Dynamic routing like RIP1 & 2, OSPF, OSPFv3, BGP4, MPLS routing		

2	Firewall should provide application detection for DHCP , DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SQLNET, TFTP, H.323, SNMP v2 , SNMP v3 , TELNET		
3	Firewall must support Inter VLAN routing / VLAN tagging		
4	Firewall must support all IPSec VPNs like Site to Site , Remote Site		
5	Firewall must support all standard and latest Hashing and Encryption techniques and algorithms of SHA/DES/RSA/AES/MD5 like SHA 256 /3DES /RSA 2048		
6	Firewall should support access-rules with IPv4 & IPv6 objects simultaneously		
7	Firewall should support operating in routed & transparent mode		
8	Firewall must support all listed NAT functionality both Hardware and Software wise Manual NAT and Auto-NAT, static nat, dynamic nat , dynamic pat		
9	Firewall should support Multicast protocols like IGMP, PIM, etc both in IPv4 and IPv6		
10	Should support Security Policies based on Group wise /User wise in Source and Destination or both field		
11	Should support capability to limit bandwidth on basis of apps / User/groups, Networks etc		
12	The Firewall should support authentication protocols like LDAP, RADIUS and have support for firewall passwords, & token-based products like SecureID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.		
13	Firewall should support 802.3ad Etherchannel functionality to increase the bandwidth for a segment.		
14	Firewall should support redundant interfaces to provide interface level redundancy before device failover		
15	Firewall should have a minimum 200 Gb storage		
16	The Firewall should be able to filter traffic even if the packets are fragmented		
17	The firewall shall be able to handle VoIP traffic securely with "pinhole opening" and support SIP, SCCP, MGCP and H.323 ALGs		
18	QoS Support [Guaranteed bandwidth, Maximum bandwidth, Priority bandwidth utilization, QOS weighted priorities, QOS guarantees, QOS limits and QOS VPN]		
D	**Next Generation IPS and URL Filtering**		
1	The IPS should have 5000+ signature and it should have a extreme database for higher threat efficacy		
2	Url Filtering should be capable of blocking and allowing urls based on categories in-build and customized ones , allow and block must be available on IP/Port/Services/Application/Usage		
3	Should have the capability of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		
4	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
5	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over all standard and non-standard communications ports.		
6	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.		

7	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor		
8	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.		
9	Should support more than 3000 application detection signatures and risk-based controls for application detection & control. Signatures should be periodically updated for latest application support.		
10	The Appliance OEM must have its own threat intelligence analysis centre and must use the global footprint of security deployments for more comprehensive network protection and incorporate same in our Network		
11	The IPS 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, HTML Obfuscation etc.).		
12	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location		
13	The detection engine should support the capability of detecting variants of known threats, as well as new threats		
14	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.		
15	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications signature quickly		
16	IPS should understand and take action on Denial of Service /DDOS used to crafts and send multiple communication Request that can potentially cause attached system to become temporarily unresponsive. It Should have prevention against Script DDoS tool that utilizes high bandwidth web servers to generate malicious DDoS traffic.		
17	IPS Should be able to detect and prevent Worms, Trojan, Zero day attacks, Unknown Threat Protections, Protection against Backdoor, SQL Injection, Cross Site Scripting, Phishing, IP Spoofing , TCP SYN Flood		
18	System should be intelligent enough to minimize the false positives in logs/alerts		
19	The IPS updates should be able to be downloaded manually and automatically with the scheduler option to download the same on specific days and time		
20	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 60 categories.		
21	Solution must be able to inspect the SSL traffic		
22	Solution must be able to detect and protect protocol misuse , tunnelling attempts ,malware communications without predefined signatures		
23	The Reports/Alerts/Logs should be in detail , with all flow of data , and should be able to be exported in proper formats like pdf or csv		
24	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
25	IPS/Application control must be able to detect and block peer to peer traffic		
26	IPS/Application control must be able to detect and block remote control applications		
E	**IPv6 Support**		
1	Solution must support Dual Stack Configuration on the physical interface or on the sub interface		

2	Solution must support IPv6 Traffic on FW , IPS , Application Control , URL filtering , AV , AB , Threat Prevention for all stated features		
3	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) functionality , 6 to 4 Tunnel, NAT46		
4	Solution must support AD/LDAP/TACAS+ integration in IPv6		
5	Solution must support ICMP , SNMP , All Routing Protocols , MPLS Routing , Multicast in IPv6		
6	Should be capable of detecting and blocking IPv6 attacks like DDOS , TCP SYN Flood		
7	NGFW should support Active/Active model in IPv6 also		
8	All other features as stated above in Appliance must support in IPV6		
F	**Advance Malware Protection**		
1	Appliance should work in inline mode		
2	Appliance should be capable of blocking callbacks to C&C 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	Administrator should be able to create their own threat prevention rules and customize any vendor provided rules		
6	The solution should be capable to analysis & block TCP and 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, HTTP(s),POP3 , IMAP, Netbios, FTP SMTP, SMB, CIFS etc.		
7	Must be capable of providing network-based detection of malware by checking the Threat signatures of known files and capability to do dynamic analysis unknown files on-premise on purpose built-appliance		
8	Sandbox should provides safe and highly secure on-premises static and dynamic malware analysis to maintain the confidentiality of data. Its should easily integrate with existing security infrastructure and should also provide safe on-premises storage of malware analysis results.		
9	Sandbox appliance Integrated redundant power supply and 4*1 G interface support		
10	Sandbox appliance should deliver dynamic and static analysis engines that provide a full understanding of malware behaviour		
11	Sandbox appliance should provide detailed analysis reports of all malware sample activities, including network traffic		
12	The solution should be capable of protecting against spear phishing attacks		
13	NGFW 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 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.		
15	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, install shield.		

16	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.		
17	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.		
18	The proposed should be able to detect and prevent the malware by scanning 50 different file types/day		
E	**Anti Virus and Anti Bot**		
1	AV/AB should be integrated on the NGFW		
2	AB must be able to scan and detect and stop any suspicious abnormal NW behaviour		
3	The solution should detect and prevent the Trojans , Worms , Viruses, Ransomwares ,Phishing , Spear Phishing , DNS attacks		
4	The solution must prevent access to malicious websites and incoming malicious files		
5	Anti Bot solution must be able to scan for bot and botnets actions		
6	AV must be able to inspect SSL traffic		
7	AV and AB must have a managed and administered centrally		
8	AV should scan the links in mails and protect the user accordingly		
F	**Management**		
1	One Management Device of each OEM at each site (DC and DR)		
2	Each Mangement device should be capable of handling at least 5 appliances		
3	The management platform must be available in physical appliance or Software and should have dual power supplies.		
4	The management platform must be accessible via a CLI and web-based interface or with secure software agent based console with no additional purchase and should be easy to use and comprehensive		
5	The transfer of Logs/alerts or any other transfer of data between all the components of NGFW or from NGFW to any Log Server must be encrypted and authenticated		
6	The Dashboard should be detailed , separate Blade wise and should be able to customize.		
7	The management should not have any restriction deviated to log licensing		
8	The management platform must have minimum 32GB of RAM, 900 Mb event storage hardware configuration		
9	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.		
10	The management appliance/software should be able to manage the Sandbox server also , or provide management of the same with the features as defined without any additional purchase		
11	The management platform must support 10 million of IPS events		
12	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		
13	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.		
14	Should support REST API for monitoring and config programmability		

15	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV		
16	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
17	The management platform must provide robust & advance reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. If not available in centralized Mgmt. vendor should provide additional advance logging & reporting solution with no additional expense		
18	The management platform must provide risk reports like advanced malware, network and application layer attacks		
19	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.		
20	The solution should have enterprise license without any restrictions on number of users for all the components		
21	Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard e.g CPU & memory utilization, state table, total number of concurrent connections the connections per second , traffic data, dropped traffic data , Top IPs and Services , Top Source and Destination IPs		
22	Server must provide detailed information in reports like Top IP/Ports , Top VPN users and longest duration connections , Top Rules , Top Security attacks , their Ips and Ports , Web Activity like most visited sites, Blocked connections their Ips and ports , Modification in rules like audit reports		
23	The Firewall Management must provide a means for exporting the firewall rules set and configuration.		
24	All appliances will be taken for 3 years Warranty and 4 years of AMC		
25	All appliances and its components should not be End of Support for the next 7 years, from the date of issuance of this RFP.		

Core Router - Technical Specifications			
S.N.	**Minimum Technical Specifications**	**Bidder Compliance (YES/NO)**	**Remark**
A	**Router Architecture:**		
1	The 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. The router in the event of failure of any one OS or control module should switch over to the redundant OS or redundant control module without dropping any traffic flow		
2	The architecture of The Router should be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor		
3	The Router should have a Modular hardware architecture of the chassis		
4	The Router should be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multi processor based and should support hardware acceleration for enhanced performance		
5	The Router should support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities		
6	The Router should have onboard support for intelligent traffic measurement and analysis. The Router should support flow based traffic analysis feature		
7	The Router should 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	Rack mounting kit for securing the router in standard rack are to be provided		
B	**Router Performance Parameter:**		
1	The Router should support minimum 2,000,000 IPv4 or 2,000,000 IPv6 routes entries in the routing table and should be scalable.		
2	The Router solution must be a carrier-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.		
3	The router should have modular OS		
4	The Router should be able to select a WAN/LAN path based on interface parameters such as reachability, load, throughput, and link cost/metric of using a path		
5	The Router or system must have support for Application level Visibility using Deep Packet Inspection Technology to identify the non-critical traffic and set the lowest priority or drop the traffic and prioritize the legitimate critical applications traffic using QOS from day one		
6	The Router should support of granularly identify applications in the enterprise (For e.g. Oracle, SAP, WebEx etc.) from day one		
7	The Router should support of identify L3, L4 and L7 applications from day one		
8	The Router should identify encrypted applications (for e.g. SSL/TLS based)		

9	The Router should classify applications based on the category they belong to (For e.g. file sharing, voice, video- conferencing, business-tools etc.) from day one		
10	The Router should support of a custom application be defined based on multiple criteria: Port numbers, payload analysis or URL/URI from day one		
11	The Router should help to identify distinctly the voice and video streams in the network from day one		
12	The Router should support the export of the learnt application information to third party management The Routers from day one		
13	The Router should support DHCP Server , Relay, Client		
14	The Router should have hardware assisted Network Address Translation (NAT) and Port Address Translation (PAT) capability		
15	The Router should support Virtual Private LAN Service (VPLS)		
C	**Physical Parameters:**		
1	The Router throughput should be at least 2.5 Gbps from Day 1 and should be scalable to 10 Gbps in future		
2	The Router should have at-least 4 GB of DRAM from day one		
3	The Router should have support for 1 Gb flash memory for configuration and OS backup.		
4	The Router should have the following interface as defined in the IEEE, ITU-T: 10 x 1 /10 GbE Copper ports from day one and support for atleast 2 more Slots including 2 nos. of 10GbE SFP+ of ports in future		
5	The Router card must support following interface:Fast Ethernet, Gigabit Ethernet, Channelized STM1, Channelized STM16, STM 64 , 10G Ethernet, POS, ATM, V.35,Serial Ports, E1, Chn E1 Ports.		
6	The Router should 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.		
7	The Router should support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol , Policy Based Routing both in IPv4 and IPv6		
8	The Router should support minimum 5000 VRF/VPN instances from day one		
9	The Router should support MPLS OAM - LSP Ping/Trace route for MPLS core		
D	**IPv6 Support**		
1	The Router should support IPV6 in hardware. The Router The Router should support IPv6 static route, OSPFv3, IS-IS support for IPv6,Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
2	The Router should identify native IPv6 applications granularly		
3	The Router should identify IPv6 applications tunnelled in IPv4 granularly(Advance)		

4	The Router should 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, IPv6 Firewall, 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)		
5	The Router should support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6		
6	The Router should support for IPv6 Multicast		
7	The Router should support IPv6 stateless auto- configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection		
8	The Router should support IPv6 Quality of Service		
9	The Router should support IPv6 dual stack		
10	The Router should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
11	The Router should support SNMP over IPv6 for management.		
12	The Router should perform Hardware assisted GRE tunnelling and VTI Tunnelling		
13	The Router should support a router redundancy protocol like VRRP		
14	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
E	**Multicast**		
1	The Router should 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.		
3	The Router should support Multicast VPN (mVPN)		
4	The multicast implementation must support source specific multicast.		
5	The Router should support multiprotocol BGP extensions for multicast		
6	The Router should support multicast load balancing traffic across multiple interfaces.		
7	The Router should support Multicast Source Discovery Protocol (MSDP).		
8	The Router should support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP)		
9	Router should support Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping		
F	**Quality of Service:**		
1	The Router should 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 on separate queues with minimum delay and jitter		
4	The Router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP		
5	The Router shall support cRTP for VoIP		
6	The Router should have support for minimum 8 queues per port		
7	The Scheduling should allow for round robin and weighted round robin		
8	The Router Should be able to identify approx 1000+ applications natively at layer7 and it should be possible to define QoS based on application		
9	The Router should support Committed Access Rate (CAR) and line rate		
G	**Security Feature**		
1	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.		
2	The Router should support Application layer protocol inspection, Transport layer protocol inspection, ICMP error message check, and TCP SYN check. Support more L4 and L7 protocols like TCP, UDP, UDP-Lite, ICMPv4/ICMPv6, SCTP, DCCP, RAWIP, HTTP, FTP, SMTP, DNS, SIP, H.323, SCC		
3	The Router should support time based ACL to reflect time based security and QoS policy.		
4	The Router should support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
5	The Router should support firewall service in hardware on all interfaces.		
6	The Router should support AAA features through RADIUS or TACACS+.		
7	The Router should support Control Plane Policing to protect The Router CPU from attacks.		
8	The Router should support DES, 3DES, and AES 128/192/256 encryption, and MD5 and SHA		
H	**System Management and Administration**		
1	The Router should restrict access to critical configuration commands to offer multiple privilege levels with password protection		
2	The Router should support Configuration rollback		
3	The Router should support for accounting of traffic flows for Network planning and Security purposes		
4	The Router should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, cRTP		
5	The Router should support SNMPv2 and SNMPv3		
6	Device should have Console, Telnet, SSH1 and SSH2 support for management		
7	The Router should have options for Extensive debugs on all protocols		
8	The Router should support Secure Shell for secure connectivity		

9	The Router should support Out of band management through Console and an external modem for remote management		
10	The Router should support Network Time Protocol (NTP)		
11	The Router should support ping and traceroute for both IPv4 and IPv6		
I	**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 certified		

VPN Router - Technical Specifications			
S.N.	**Minimum Technical Specifications**	**Bidder Compliance (YES/NO)**	**Remark**
A	**Router Architecture:**		
1	The 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 .The router in the event of failure of any one OS or control module should switch over to the redundant OS or redundant control module without dropping any traffic flow		
2	The architecture of The Router should be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor		
3	The Router should have a Modular hardware architecture of the chassis		
4	The Router should be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multi processor based and should support hardware acceleration for enhanced performance		
5	The Router should support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities		
6	The Router should have onboard support for intelligent traffic measurement and analysis. The Router should support flow based traffic analysis feature		
7	The Router should 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	Rack mounting kit for securing the router in standard rack are to be provided		
B	**Router Performance Parameter:**		
1	The Router should 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 6 Gbps of Crypto throughput for IPSEC performance and 8000 IPSEC tunnels (internal/external).		
3	The Router solution must be a carrier-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.		
4	The router should have modular OS		
5	The Router should be able to select a WAN/LAN path based on interface parameters such as reachability, load, throughput, and link cost/metric of using a path		
6	The Router or system must have support for Application level Visibility using Deep Packet Inspection Technology to identify the non-critical traffic and set the lowest priority or drop the traffic and prioritize the legitimate critical applications traffic using QOS from day one		
7	The Router should support of granularly identify applications in the enterprise (For e.g. Oracle, SAP, WebEx etc.) from day one		
8	The Router should support of identify L3, L4 and L7 applications from day one		
9	The Router should identify encrypted applications (for e.g. SSL/TLS based)		

10	The Router should classify applications based on the category they belong to (For e.g. file sharing, voice, video-conferencing, business-tools etc.) from day one		
11	The Router should support of a custom application be defined based on multiple criteria: Port numbers, payload analysis or URL/URI from day one		
12	The Router should help to identify distinctly the voice and video streams in the network from day one		
13	The Router should support the export of the learnt application information to third party management The Routers from day one		
14	The Router should support DHCP Server , Relay, Client		
15	The Router should have hardware assisted Network Address Translation (NAT) and Port Address Translation (PAT) capability		
16	The Router should support Virtual Private LAN Service (VPLS)		
C	**Physical Parameters:**		
1	The Router throughput should be at least 2.5 Gbps from Day 1 and should be scalable to 10 Gbps in future		
2	The Router should have at-least 4 GB of DRAM from day one		
3	The Router should have support for 1 Gb flash memory for configuration and OS backup.		
4	The Router should have the following interface as defined in the IEEE, ITU-T: 10 x 1 /10 GbE Copper ports from day one and support for atleast 2 more Slots including 2 nos. of 10GbE SFP+ of ports in future		
5	The Router card must support following interface:Fast Ethernet, Gigabit Ethernet, Channelized STM1, Channelized STM16, STM 64 , 10G Ethernet, POS, ATM, V.35,Serial Ports, E1, Chn E1 Ports.		
6	The Router should 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.		
7	The Router should support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol , Policy Based Routing both in IPv4 and IPv6		
8	The Router should support minimum 5000 VRF/VPN instances from day one		
9	The Router should support MPLS OAM - LSP Ping/Trace route for MPLS core		
D	**IPv6 Support**		
1	The Router should support IPV6 in hardware. The Router The Router should support IPv6 static route, OSPFv3, IS-IS support for IPv6,Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
2	The Router should identify native IPv6 applications granularly		
3	The Router should identify IPv6 applications tunnelled in IPv4 granularly(Advance)		

4	The Router should 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, IPv6 Firewall, 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)		
5	The Router should support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6		
6	The Router should support for IPv6 Multicast		
7	The Router should support IPv6 stateless auto- configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection		
8	The Router should support IPv6 Quality of Service		
9	The Router should support IPv6 dual stack		
10	The Router should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
11	The Router should support SNMP over IPv6 for management.		
12	The Router should perform Hardware assisted GRE tunnelling and VTI Tunnelling		
13	The Router should support a router redundancy protocol like VRRP		
14	The proposed router should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
E	**Multicast**		
1	The Router should 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.		
3	The Router should support Multicast VPN (mVPN)		
4	The multicast implementation must support source specific multicast.		
5	The Router should support multiprotocol BGP extensions for multicast		
6	The Router should support multicast load balancing traffic across multiple interfaces.		
7	The Router should support Multicast Source Discovery Protocol (MSDP).		
8	The Router should support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP)		
9	Router should support Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping		
F	**Quality of Service:**		
1	The Router should 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 on separate queues with minimum delay and jitter		
4	The Router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP		
5	The Router shall support cRTP for VoIP		
6	The Router should have support for minimum 8 queues per port		
7	The Scheduling should allow for round robin and weighted round robin		
8	The Router Should be able to identify approx 1000+ applications natively at layer7 and it should be possible to define QoS based on application		
9	The Router should support Committed Access Rate (CAR) and line rate		
G	**Security Feature**		
1	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.		
2	The Router should support Application layer protocol inspection, Transport layer protocol inspection, ICMP error message check, and TCP SYN check. Support more L4 and L7 protocols like TCP, UDP, UDP-Lite, ICMPv4/ICMPv6, SCTP, DCCP, RAWIP, HTTP, FTP, SMTP, DNS, SIP, H.323, SCC		
3	The Router should support time based ACL to reflect time based security and QoS policy.		
4	The Router should support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
5	The Router should support firewall service in hardware on all interfaces.		
6	The Router should support AAA features through RADIUS or TACACS+.		
7	The Router should support Control Plane Policing to protect The Router CPU from attacks.		
8	The Router should support DES, 3DES, and AES 128/192/256 encryption, and MD5 and SHA		
H	**System Management and Administration**		
1	The Router should restrict access to critical configuration commands to offer multiple privilege levels with password protection		
2	The Router should support Configuration rollback		
3	The Router should support for accounting of traffic flows for Network planning and Security purposes		
4	The Router should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, cRTP		
5	The Router should support SNMPv2 and SNMPv3		
6	Device should have Console, Telnet, SSH1 and SSH2 support for management		
7	The Router should have options for Extensive debugs on all protocols		
8	The Router should support Secure Shell for secure connectivity		

9	The Router should support Out of band management through Console and an external modem for remote management		
10	The Router should support Network Time Protocol (NTP)		
11	The Router should support ping and traceroute for both IPv4 and IPv6		
I	**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 certified		
Other Router - Technical Specifications			
S.N.	**Minimum Technical Specifications**	**Bidder Compliance (YES/NO)**	**Remark**
A	**Router Architecture requirements**		
1	The architecture of The Router should be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor.		
2	The Router should have a Modular hardware architecture of the chassis		
3	The router should have 4 10/100/1000 Mbps Ethernet Routed WAN ports from day 1 and expandable to 3 more ethernet interfaces in Future		
4	The router card should support following interfaces :LAN/WAN/Voice interface cards - Ethernet, V.35, ISDN, E1, FXS/FXO, 3G Module etc.The Router shall provide a traditional link with E1, T1, ADSL, ADSL2, ADSL2+, G.SHDSL,Serial, ISDN/AM backup		
5	The Router should support Virtual Private LAN Service (VPLS)		
6	The router's aggregate performance should be 100 Mbps and scalable to 400 Mbps		
7	The Router DRAM should be minimum 2 GB from day one and scalable to 10 GB		
8	The Router Flash memory should be minimum 512 Mb from day one		
9	Router should support atleast 750000 routes or higher in routing table from day1		
10	The Router card should support following interface:Fast Ethernet, Gigabit Ethernet, Channelized STM1, Channelized STM16, STM 64 , 10G Ethernet, POS, ATM, V.35,Serial Ports, E1, Chn E1 Ports.		
B	**Features**		
1	The Router should support GRE and IP Sec 3DES/AES and complex suit of crypto for configuration of VPN tunnels		
2	The Router should support for IPSEC Site-to-Site and Remote Access VPNs. System Should provide hardware assisted IPSec acceleration		
3	Router should be able to support up to 1500 IPSec tunnels		
4	The Router should support Dynamic/Automatic tunnel-less VPN, IPSec VPN etc.		
5	The Router should support IKEv2 support and IPv6- IKEv2, IPSec		
6	The Router should support MD5, SHA-1, SHA-2 , SHA256 Authentication		
7	The Router should support PKI (CA certificate) infrastructure support		

8	The Router should have hardware assisted Network Address Translation (NAT) and Port Address Translation (PAT) capability		
9	The Router should support AAA features through RADIUS or TACACS+.		
10	The Router should support for Standard, Advanced, time based Access Lists to provide supervision and control.		
11	The Router should support DNS, DHCP, DNS spoofing		
12	The router should support DHCP Server , Relay, Client		
13	The Router should be able to support zone based firewall, IPS as and when required		
14	Router should have capability to support WAN optimization i.e. TCP optimization with DRE and TFO, LZ compression and SSL accelerator feature built in to the router either through software / hardware and support for minimum 750 TCP optimized concurrent connections as and when required.		
15	The Router should support all major routing protocols :Static Routes , RIPv1, RIPv2, RIPng, EIGRP, OSPFv2 and v3 , BGP , BGP+, mlps routing, IS-IS , Policy based routing for both IPv4 and IPv6		
16	The Router should support failover and load balancing via VRRP or any other for IPv4 and IPv6		
17	The Router should support all features in IPv6 also with no additional cost		
18	MPLS Layer 2 VPN, MPLS Layer 3 , RFC 2702 Requirements for Traffic Engineering Over MPLS, RFC 3032 MPLS Label Stack Encoding, MPLS Loop Prevention Mechanism.		
C	**QOS**		
1	The Router Should be able to identify approx 1000+ applications natively at layer7 and it should be possible to define QoS based on application.		
2	The Router should support Committed Access Rate (CAR) and line rate		
3	The Router should support FIFO, PQ, CQ, WFQ, CBQ, and RTPQ Congestion management		
4	The Router should support Weighted random early detection (WRED)/random early detection (RED) congestion avoidance capabilities through the use of queue management algorithms		
5	The Router should support traffic shaping, FR QoS, MPLS QoS, and MP QoS/LFI		
6	Router should support IPv6 Packet classification & Marking, IPv6 Policing & Shaping, IPv6 Queuing		
D	**Multicasting**		
1	The Router should support traffic shaping, FR QoS, MPLS QoS, and MP QoS/LFI		
2	The Router should support Internet Group Management Protocol (IGMP). The Router should support Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks and should support IGMPv1, v2, and v3		

3	The Router should support IPv4 and IPv6 multicasting to allow one-to-many and many-to- many transmission of information and support PIM Dense Mode (DM), Sparse Mode (SM), and Source-Specific Mode (SSM)		
4	The Router should support Multicast Source Discovery Protocol (MSDP)		
5	The Router should support Multicast Border Gateway Protocol (MBGP)		
6	The Router should support Multicast over GRE Tunnels		
7	The Router should support traffic distribution using powerful scheduling algorithms, including Layer 4 to 7 services and monitor the health status of servers and firewalls		
8	The Router should 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, IPv6 Firewall, 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)		
E	**Security Feature**		
1	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.		
2	The Router should support Application layer protocol inspection, Transport layer protocol inspection, ICMP error message check, and TCP SYN check. Support more L4 and L7 protocols like TCP, UDP, UDP-Lite, ICMPv4/ICMPv6, SCTP, DCCP, RAWIP, HTTP, FTP, SMTP, DNS, SIP, H.323, SCC		
3	The Router should support time based ACL to reflect time based security and QoS policy.		
4	The Router should support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.		
5	The Router should support firewall service in hardware on all interfaces.		
6	The Router should support AAA features through RADIUS or TACACS+.		
7	The Router should support Control Plane Policing to protect The Router CPU from attacks.		
8	The Router should support DES, 3DES, and AES 128/192/256 encryption, and MD5 and SHA		
F	**Management**		
1	The Router should restrict access to critical configuration commands to offer multiple privilege levels with password protection		
2	The Router should support Configuration rollback		
3	The Router should support for accounting of traffic flows for Network planning and Security purposes		
4	The Router should support SNMPv2 and SNMPv3		
5	Device should have Console, Telnet, SSH1 and SSH2 support for management		

6	The Router should have options for Extensive debugs on all protocols		
7	The Router should support Secure Shell for secure connectivity		
8	The Router should support Out of band management through Console and an external modem for remote management		
9	The Router should support Network Time Protocol (NTP)		
10	The Router should support ping and traceroute for both IPv4 and IPv6		
G	**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 certified		