6.2.2.69 GTP of WAN Switch

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

WAN Switch			
S/N	Product Names/Items	Description of requirements	Bidder's Responses
1	Brand	To be mentioned by the bidder	
2	Model	To be mentioned by the bidder	
3	Country of Origin	To be mentioned by the bidder	
4	Country of Manufacturer	To be mentioned by the bidder	
5	Quantity	Four	
6	Industry Recommendations	The OEM must be recognized as a Leader in 2024 & 2025 Gartner Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure.	
7		Proposed switch must be FCC, CE, RCM, VCCI, BSMI, UL, CB and RoHS2 certified	
8	Architecture	Switch proposed should have minimum 24 x 1GE/5GE copper downlink & 4 x 10GE/25GE SFP/SFP+/SFP28 ports uplink ports from day one. Bidder should quote 4 x 10G SFP+ SR module for each appliance.	
9		Switch should support non-blocking, store-n-forward architecture	
10		Switch should have a RJ-45 Serial console port	
11		Switch should have a dedicated MGMT port	
12		The form factor of the proposed switch should be 1 RU Rack-Mount Appliance	
13		Proposed Switch should support minimum 64K MAC address storage	
14		Propsoed switch should support minimum 8 MB Packet Buffers	
15		Proposed switch should support 4000 VLANs	
16		Network Latency: Less than 1µs	
17		Should support DRAM 4GB or higher	
18		Mean Time Between Failures : Minimum 10 years	
19		Redundant Power : Redundant AC	
20		Operating Temperature: 32°–113°F (0°–45°C)	
21		Humidity: 5%–95% non-condensing	
22		Air-Flow Direction: side-to-back	
23	Switching Performance	Switching capacity ((Duplex)) of the proposed switch should be minimum 400 Gbps	
24		Packet per second capacity ((Duplex)) of the switch should be minimum 200 Mpps or higher	
25	Switch Layer 2 Services	Switch must support Jumbo frames and link auto-negotiation	
26		Should support Spanning Tree Protocol MSTP native, and backwards compatible with RTSP and STP	
27		Should support Edge Port / Port Fast	
28		Should support IEEE 802.1p Mapping to priority queue	
29		Should support IEEE 802.1q VLAN tagging, Private VLAN	

30		Should support IEEE 802.3ad Link Aggregation with LACP with maximum 8 Link Aggregation Group size	
31	Authentication Services	Switch should support LLDP, LLDP-MED	
32		Switch should support MAC based, IP based, protocol based VLAN assignment	
33		Switch should support 802.1x port-based authentication	
34		Switch should support 802.1x authentication via certificate EAP-TLS and EAP-TTLS	
35		Switch should support 802.1x guest VLAN assignment	
36		Switch should support 802.1x authentication fail VLAN for unauthenticated users	
37		Switch should support LDAP, RADIUS, TACACS+	
38	Security Features	Switch should support minimum 1,000 Access control list (ACL) with Schedule features	
39		Switch should support Storm Control, LoopGuard	
40		Should support IGMP snooping, DHCP snooping, DHCP relay	
41		Should support Port mirroring, sFlow/Netflow/jFlow	
42		Should support port MAC limit, MAC-IP binding, Per-port and per-VLAN MAC learning limit	
43		Switch should support ACL with classifier(src-mac, dst-mac, ether-type, src-prefix, dst-prefix, service-id, vlan-id)	
44	QoS	Switch should support support QoS to provide packet classification, packet marking, packet queuing	
45		Switch should support 4 queues per port	
46		Switch should support CoS and DSCP marking to indicate the priority of outgoing packets	
47		Switch should support Strict Scheduling, Simple Round Robin (RR), and Weighted Round Robin (WRR) scheduling modes for queuing	
48	Management Features	Switch must support central management system though offered router/firewall to built up a software define network architecture from day one. Bidder may quote additional hardware/software for central switching mangement	
49		Switch must support Telnet/SSH, HTTP/HTTPS...etc.	
50		Switch should support SNMP v1, v2c and v3	
51		switch must log all authentication events: locally and via syslog	
52		Switch should support Packet Capture and diagnose features in CLI offer similar packet capture capabilities like tcpdump.	
53		Switch should support Dual Firmware	
54		Switch must support SPAN, RSPAN, and ERSPAN	
55		Switch must support software download/upload via TFTP/FTP/GUI	
56		Support for HTTP REST APIs for Configuration and Monitoring	
57	Manufacturer authorization	Bidder must be submitted Manufacturer Authorization form (MAF) from the OEM	
58	License	Bidder should quote necessary license to meet the all the requirements. The license period shall have at least 03 years and will be calculated from the first day of system handover.	
59	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty for OEM technical solution support, Patch, New Software Upgrade and RMA replacement	

60		The Original Equipment Manufacturer (OEM) must have 24x7x365 Global TAC support and toll-free number for after sales service	
61	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network Functional and shall provide respective documentation to IT Division.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer

6.2.2.70 GTP of Core Router

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Core Router			
S/N	Product Names/Items	Description of requirements	Bidder's Responses
1	Brand	To be mentioned by the bidder	
2	Model	To be mentioned by the bidder	
3	Country of Origin	To be mentioned by the bidder	
4	Qty	Two	
5	Compliance Certification	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
6	Enclosure Type	Rack mountable maximum 2 RU	
7	Industry Certifications and Evaluations	Proposed solution must be in Leader for WAN Edge Infrastructure segment in Gartner MQ-2022/2023/2024	
8	Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
9	Router Processor Type	High-performance dedicated ASIC based network processors to deliver unmatched performance and scalability for critical network functions	
10		• WAN architecture should have centralized control plane architecture.	
11		• It should provide transport layer independence and will allow to use any transport like MPLS, internet, point to point links between locations.	
12		• It should support various last mile connectivity i.e., ethernet, 4G LTE.	
13		• It should build secure overlay network on any transport and will allow to create various topology like Hub & spoke, full mesh, partial mesh.	
14		• WAN edge device should perform actual data forwarding based on control communication from centralize controller.	
15	Router Processor Type	• It should build secure IPsec network between locations for secure communication and allow various last mile connectivity.	
16	DRAM and Flash	Min. DRAM 16GB and Min. Flash 30GB from day one.	
17	Power Supply	Redundant power Supply from day 1	
18	Hardware Capacity	Router should support in SD-WAN mode min. 20 Gb from day 1 and scale up to 50 Gbps	
19		Router should support minimum 10 Gbps encrypted traffic for deep packet inspection	
20	Interfaces	Router should have Min. 8 x 1/10GE SFP+, and 8 x 1GE Copper port from day one. Bidder should quote 8 x 10G SFP+ SR module for each appliance.	
21		Management: 1 x console and 1 x Gigabit Ethernet port for device management (OOB)	
22	SD-WAN requirements	Should support granular application policies, application SLA based path selection, dynamic bandwidth measurement of SD-WAN paths, active/active and active/standby forwarding, overlay support for encrypted transport, Application session-based steering and probe-based SLA measurements	
23		SDWAN solution should support minimum BGP and Static routing	

24		SDWAN solution should support performance SLA based on latency , packet loss , jitter or all 3 combined	
25		SDWAN edge devices should support 802.1Q, sub interface, Inter VLAN routing	
26		SDWAN solution should support rule based routing based on Application, user, user group, source , destination or combination of any of them	
27		SDWAN Solution should support rule creation based on Application or source address or destination address and each rule should have option to use different performance SLA	
28		SDWAN should support QoS based on application	
29		SDWAN should support FEC (Forward Error correction) and DSCP matching	
30		SDWAN must support BGP additional path support and route-map	
31		SDWAN solution must support Auto-Discovery VPN	
32		Should support stateful Firewall, transparent firewall, advance application inspection and control for HTTP, ACL bypass and VRF aware Firewall features	
33		Should have up to 20 Gbps of IPsec throughput in SDWAN mode min. Number of ACL 10,000, Number of Firewall session 4 Million from day 1.	
34		Router should support Site-to-site dynamic VPN tunnels, policy-based VPN, IKEv1, IKEv2, DPD, PFS, ESP and ESPHMAC support, symmetric cipher support (IKE/ESP): AES-128 and AES-256 modes: CBC, CNTR, XCBC,GCM, Pre-shared and PKI authentication with RSA certificates, Diffie-Hellman key exchange (Group 1, 2, 5,14 through 21 and 27 through 32), MD5, and SHA-based HMAC.	
35		WAN should support end to end segmentation with different routing table per segment and it should be possible to create per segment topology on WAN like HUB & Spoke, full mesh, partial mesh, point to point.	
36		It should be possible to create minimum 8 segments from day 1	
37		Solution should support security features Like IPS, AV, Sandboxing which can be utilized for future if required.	
38	Security & VPN	Should support ACL for IPv4 and IPv6, Time based ACL,	
39	Routing Features	Static routing, Internal Gateway (iBGP, OSPF v2/v3 , RIP v2), External Gateway(eBGP), VRF, route redistribution, route leaking, BGP confederation, router reflectors, summarization and route-aggregation, route asymmetry	
40	QOS Features	Traffic shaping based on bandwidth limits per application and WAN link, rate limits per application and WAN link, prioritize application traffic per WAN link, mark/remark DSCP bits for influencing traffic QoS on egress devices, application steering based on ToS marking	
41		The router should support complete GUI and CLI, HTTPS, SSH, Console, SNMP, API, Central Management from day one	
42	Management	The router should have private & public multi-cloud support for AWS, Microsoft Azure, GCP, OCI, AliCloud, VMware ESXi, NSX, OpenStack, Cisco ACI and Nuage Virtualized Service Platforms	

43		The router should have in-built CLI option in Graphical Interface for easy access in troubleshooting & configuration	
44		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.	
45		Bidder must submit the required performance document and compliance reference document for the proposed device.	
46	Manufacturer authorization	Bidder must submit Manufacturer Authorization from the OEM	
47	Warranty	Bidder should propose all the necessary hardware for Central Management, software & license and the entire solution should be offered from OEM.	
48		The Original Equipment Manufacturer (OEM) must have 24x7x365 Global TAC support and toll-free number for after sales service	
49		Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty for OEM technical solution support, Patch, New Software Upgrade and RMA replacement	
50	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. In consultation with the customer IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network Functional and shall provide respective documentation to IT Division.	
51	License	The license period shall have at least 03 years and will be calculated from the first day of system handover.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer

6.2.2.71 GTP of Core Firewall

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Core Router			
S/N	Product Names/Items	Description of requirements	Bidder's Responses
1	Brand	To be mentioned by the bidder	
2	Model	To be mentioned by the bidder	
3	Country of Origin	To be mentioned by the bidder	
4	Qty	Two	
5	Compliance Certification	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
6	Enclosure Type	Rack mountable maximum 2 RU	
7	Industry Certifications and Evaluations	Proposed solution must be in Leader for WAN Edge Infrastructure segment in Gartner MQ-2022/2023/2024	
8	Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
9	Router Processor Type	High-performance dedicated ASIC based network processors to deliver unmatched performance and scalability for critical network functions	
10		• WAN architecture should have centralized control plane architecture.	
11		• It should provide transport layer independence and will allow to use any transport like MPLS, internet, point to point links between locations.	
12		• It should support various last mile connectivity i.e., ethernet, 4G LTE.	
13		• It should build secure overlay network on any transport and will allow to create various topology like Hub & spoke, full mesh, partial mesh.	
14		• WAN edge device should perform actual data forwarding based on control communication from centralize controller.	
15	Router Processor Type	• It should build secure IPsec network between locations for secure communication and allow various last mile connectivity.	
16	DRAM and Flash	Min. DRAM 16GB and Min. Flash 30GB from day one.	
17	Power Supply	Redundant power Supply from day 1	
18	Hardware Capacity	Router should support in SD-WAN mode min. 20 Gb from day 1 and scale up to 50 Gbps	
19		Router should support minimum 10 Gbps encrypted traffic for deep packet inspection	
20		Router should have Min. 8 x 1/10GE SFP+, and 8 x 1GE Copper port from day one. Bidder should quote 8 x 10G SFP+ SR module for each appliance.	
21	Interfaces	Management: 1 x console and 1 x Gigabit Ethernet port for device management (OOB)	
22	SD-WAN requirements	Should support granular application policies, application SLA based path selection, dynamic bandwidth measurement of SD-WAN paths, active/active and active/standby forwarding, overlay support for encrypted transport, Application session-based steering and probe-based SLA measurements	

23		SDWAN solution should support minimum BGP and Static routing	
24		SDWAN solution should support performance SLA based on latency , packet loss , jitter or all 3 combined	
25		SDWAN edge devices should support 802.1Q, sub interface, Inter VLAN routing	
26		SDWAN solution should support rule based routing based on Application, user, user group, source , destination or combination of any of them	
27		SDWAN Solution should support rule creation based on Application or source address or destination address and each rule should have option to use different performance SLA	
28		SDWAN should support QoS based on application	
29		SDWAN should support FEC (Forward Error correction) and DSCP matching	
30		SDWAN must support BGP additional path support and route-map	
31		SDWAN solution must support Auto-Discovery VPN	
32		Should support stateful Firewall, transparent firewall, advance application inspection and control for HTTP, ACL bypass and VRF aware Firewall features	
33		Should have up to 20 Gbps of IPsec throughput in SDWAN mode min. Number of ACL 10,000, Number of Firewall session 4 Million from day 1.	
34		Router should support Site-to-site dynamic VPN tunnels, policy-based VPN, IKEv1, IKEv2, DPD, PFS, ESP and ESPHMAC support, symmetric cipher support (IKE/ESP): AES-128 and AES-256 modes: CBC, CNTR, XCBC,GCM, Pre-shared and PKI authentication with RSA certificates, Diffie-Hellman key exchange (Group 1, 2, 5,14 through 21 and 27 through 32), MD5, and SHA-based HMAC.	
35		WAN should support end to end segmentation with different routing table per segment and it should be possible to create per segment topology on WAN like HUB & Spoke, full mesh, partial mesh, point to point.	
36		It should be possible to create minimum 8 segments from day 1	
37		Solution should support security features Like IPS, AV, Sandboxing which can be utilized for future if required.	
38	Security & VPN	Should support ACL for IPv4 and IPv6, Time based ACL,	
39	Routing Features	Static routing, Internal Gateway (iBGP, OSPF v2/v3 , RIP v2), External Gateway(eBGP), VRF, route redistribution, route leaking, BGP confederation, router reflectors, summarization and route-aggregation, route asymmetry	
40	QOS Features	Traffic shaping based on bandwidth limits per application and WAN link, rate limits per application and WAN link, prioritize application traffic per WAN link, mark/remark DSCP bits for influencing traffic QoS on egress devices, application steering based on ToS marking	
41		The router should support complete GUI and CLI, HTTPS, SSH, Console, SNMP, API, Central Management from day one	
42	Management	The router should have private & public multi-cloud support for AWS, Microsoft Azure, GCP, OCI, AliCloud, VMware ESXi, NSX, OpenStack, Cisco ACI and Nuage Virtualized Service	

		Platforms	
43		The router should have in-built CLI option in Graphical Interface for easy access in troubleshooting & configuration	
44		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.	
45		Bidder must submit the required performance document and compliance reference document for the proposed device.	
46	Manufacturer authorization	Bidder must submit Manufacturer Authorization from the OEM	
47		Bidder should propose all the necessary hardware for Central Management, software & license and the entire solution should be offered from OEM.	
48	Warranty	The Original Equipment Manufacturer (OEM) must have 24x7x365 Global TAC support and toll-free number for after sales service	
49		Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty for OEM technical solution support, Patch, New Software Upgrade and RMA replacement	
50	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. In consultation with the customer IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network Functional and shall provide respective documentation to IT Division.	
51	License	The license period shall have at least 03 years and will be calculated from the first day of system handover.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer

6.2.2.72 GTP of Internet Firewall

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Internet Firewall			
S/N	**Product Names/Items**	**Description of requirements**	**Bidder's Responses**
1	Brand	To be mentioned by the bidder	
2	Country Of Origin	To be mentioned by the bidder	
3	Country of Manufacture	To be mentioned by the bidder	
4	Model	To be mentioned by the bidder	
5	Compliance Certification	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
6	Enclosure Type	Rack-mountable & Maximum 1U	
7	Quantity	02 (Tow)	
8	Industry Recommendations	The OEM must be recognized as a Leader in 2025 Gartner Magic Quadrant for Hybrid Mash Firewalls.	
9		The OEM must be recognized as a leader in 2024 Q4 Forrester wave report for Enterprise Firewalls	
10	Hardware Architecture	The appliance-based security platform should be capable of providing Next Generation IPS functionality with application visibility, URL Filtering and Malware Protection in a single appliance from day one.	
11		The appliance should have at least 4 x 10G SFP+, 4 x 10GE/25GE SGP+ & 12 x 1G Copper Ethernet ports from day one	
12		The firewall should have dedicated 1GE HA port	
13		The firewall appliance must have dual hot-swappable power supplies.	
14		The firewall appliance should have dedicated service/content processor to detect emerging threats and block malicious content and avoid performance bottleneck	
15		The appliance hardware should be a multicore CPU architecture with a hardened 64 bit (minimum) operating system to support higher memory.	
16	Performance & Scalability	The solution should support at least 50 Gbps of Firewall throughput in 64 byte UDP packet size from day one	
17		The solution should support at least 10 Gbps Threat Protection throughput considering next-generation security feature like Application Visibility , IPS and malware protection	
18		The solution should support at least 8 Gbps or more of SSL inspection (DPI) performance throughput from day 1.	
19		The solution should support at least 8 Milloin concurrent sessions from day one	
20		The solution should support at least 500K connections per second from day one	
21		The solution should support at least 10 Gbps IPSec VPN throughput from day one	
22		The solution should support at least 2,000 IPSec tunnel for Site to Site VPN and 5,000 IPSec tunnel for remote access end-point VPN from day one.	
23		The solution must support minimum 8 Virtual Systems/Domain/ Security Context from day one	

24		The solution should support Active-Active & Active-Passive & Clustering high availability from day one	
25		The solution should support at least 8,000 firewall policy from day one.	
26	Next-Generation Firewall Protection Features	The firewall should support static NAT, dynamic NAT, PAT, NAT64 and NAT46.	
27		The firewall shall support static routing, Internal Gateway (iBGP, OSPF v2/v3 , RIP v2), External Gateway(eBGP) and VRF redistribution, route leaking, router reflectors, summarization, and route-aggregation, route asymmetry for both IPv4 & IPv6	
28		The firewall shall support Site-to-site dynamic VPN tunnels, policy-based VPN, IKEv1, IKEv2, DPD, PFS, ESP and ESPHMAC support, Pre-shared and PKI authentication with RSA certificates and Diffie-Hellman key exchange (Group 1, 2, 5, 14 through 21 and 27 through 32)	
29		The firewall shall allow organizations to implement both flow-based and proxy-based anti-malware concurrently, depending on the network and security needs	
30		The firewall shall provide ability to allow/monitor, block and quarantine attachments or downloads after malware detection	
31		The AV Engine should have AI malware detection model which integrated with regular AV scanning to help detect potentially malicious Windows Portable Executables (PEs) in order to mitigate zero-day attacks.	
32		The firewall shall support stream-based antivirus scanning for FTP, SFTP, and SCP protocols.	
33		The firewall shall support external block lists for domain names, web filtering URLs, IP addresses and malware hashes	
34		The firewall shall support real-time checksums DB of newly detected threats before AV signatures are available	
35		The firewall shall also be able to block graywares and mobile malwares	
36		The firewall shall offer the ability to treat Windows Executable files in Email Attachments as viruses	
37		The antivirus scanning should be supported on various protocols not limited to HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP and CIFS	
38		The firewall shall able to quarantine file and ban infected host	
39		The firewall's IPS database shall have over 11,000 up-to-date signatures	
40		The firewall shall provide configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.	
41		The firewall shall support Allow session, Monitor and log session, Block session, Reset session, Quarantine attacker actions when an IPS attack is detected	
42		The IPS system shall able to scan botnet-connections to block Botnet C&C communication	
43		The firewall must support DPI (Deep packet Inspection) for all types of traffic.	
44		The firewall shall support certificate inspection on port 443, all ports or a specific non-standard port.	
45		The firewall shall able to detect and take action against network traffic depending on the application generating the traffic.	

46		The firewall shall able to analyse network traffic to detect application traffic even if the traffic uses non-standard ports or protocols	
47		The firewall shall supports detection for traffic using HTTP/2 protocol and able to block QUIC traffic so that browser automatically falls back to HTTP/2 + TLS 1.3	
48		The firewall shall support dynamic application filtering by querying real-time cloud-based categorization database over 2500+ application rated by 18 categories.	
49		Application Control filtering engine should support Allow, block, reset session, monitor only and attacker quarantine actions when matched to a category	
50		The firewall shall able to setting threshold value against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination) to protect against DoS attack	
51		OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection.	
52		The firewall shall support subnet, IP, IP range, GeoIP (Geography), FQDN, Dynamic (based on received tags from external systems) and MAC address policy objects	
53		The firewall shall support Seven-day rolling counter for each policy hit & byte count	
54		The firewall shall support policy lookup tool to find out which policy matches specific traffic from a number of policies	
55		The firewall should support RADIUS, TACACS, MFA, SAML and SSO authentication	
56	QoS	The firewall shall support per-user and per-IP based bandwidth management in addition to identifying service, applications, URL category & schedule to ensure the network access experience of key services and users	
57		The firewall must support shared and per-IP policy-based traffic shaping where the traffic priority, guaranteed and maximum bandwidth can be applied for group of IP/users as well as particular IP/user	
58		The firewall must support upload & download bandwidth management.	
59	Management and Reporting	The firewall should support complete GUI and CLI, HTTPS, SSH, Console, SNMP, API from day one	
60		Firewall should be manageable though central management platform. Central management platform should be VM based and VM resource will be provide by the end customer. Bidder should quote every proposed firewall license for central management from day one.	
61		The firewall should have in-built CLI option in Graphical Interface for easy access in troubleshooting & configuration	
62		The solution should have built-in log and reporting module or vendor may offer additional VM based appliance for log and reporting solution with minimum one year log storage capacity	
63		The log & reporting module should be capable of receiving 10GB/day or more log/event	
64		Log & reporting solution should be capable of providing rich reports based on application, users and threats or in any custom combination.	

65		Log & reporting solution should have IOC, SOC subscription, and Outbreak Alert service license from day one	
66		The solution should have IOC package/license to alert on suspicious or infected hosts in the network	
67		The solution should have Outbreak Detection Service to deliver automated content package download for detecting the latest malware, including a summary of outbreaks and kill chain mapping for how the malware works.	
68		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.	
69		The solution should support automation by triggering security/system events like compromised host detection, system status, configuration changes with multiple automatic action not limited to CLI scripts, email notification & API calls	
70		The firewall should have private & public multi-cloud support for AWS, Microsoft Azure, GCP, OCI, AliCloud, VMware ESXi, NSX, OpenStack, Cisco ACI and Nuage Virtualized Service Platforms	
71		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.	
72		The security management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
73	Manufacturer authorization	Bidder must be submitted Manufacturer Authorization form (MAF) from the OEM	
74	Warranty	Bidder should propose all the necessary hardware for Central Management, software & license and the entire solution should be offered from OEM.	
75		The Original Equipment Manufacturer (OEM) must have 24x7x365 Global TAC support and toll-free number for after sales service	
76		Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty for OEM technical solution support, Patch, New Software Upgrade and RMA replacement	
77	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. In consultation with the customer IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network Functional and shall provide respective documentation to IT Division.	
78	License	The license period shall have at least 03 years and will be calculated from the first day of system handover.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer