Dated:30.04.2019

A mini ratna enterprise

RailTel Corporation of India Ltd
(A Government of India Enterprise)

Plot No 143, Sector 44, Institutional Area,
Opposite to Gold Souk Mall,
Gurgaon, Haryana- 122003
Work: 0124-4236083
Fax: 0124-4236084

Website: **www.railtelindia.com**

Corrigendum -II

Sub: Request for proposals for **"Tender document for Supply, Installation, Testing & Commissioning of Security Solution for Data Center (DC & DR) against e-Office Project"**

Ref: i) This office Tender No. RAILTEL/TENDER/OT/CO/DNM/2018-19/ Security Solution for DC & DR /476.

In reference to the above referred tender the following amendment are issued under the Corrigendum-II. The bids may be submitted in consideration of this amendment.

1. Chapter-2, SCHEDULE OF REQUIREMENT may be read as

SOR		ITEM DESCRIPTION	UOM	QTY	Unit Rate (All inclusive) (in Rs.)		Total Cost (in Rs.)	
					In Fig	In word	In Fig	In word
SOR-A-1		Data Centre Router as per technical specification given in Chapter-3A	Nos	04				
SOR-A-2		L3/Leaf Switch with redundant power supply as per technical specification given in Chapter-3A	Nos	04				
SOR-A-3		UTM Solution along with other appliances as per technical specification given in Chapter-3A						
a.		Next Generation Firewall	Nos	04				
b.		Network Behavior Analysis	Nos	02				
c.	i)	Network Access Control & Authentication	Nos	02				
	ii)	NAC End point License (for 2000 End points)	Nos	02				
d.	i)	Anti-Malware Protection for Endpoint	Nos	02				
	ii)	Anti-Malware Protection License (for 1000 End point)	Nos	02				

रेलटेल कॉर्पोरेशन ऑफ इंडिया लिमिटेड (भारत सरकार का उपक्रम)
RailTel Corporation of India Ltd. (A Government of India Undertaking)
CIN : U64202DL2000GOI107905
Corporate Office : 143, Institutional Area, Sector-44, Gurugram - 122 003, NCR (India), T : +91 124 2714000, F +91 124 4236084
Regd. Office : 6th Floor, IIIrd Block, Delhi Technology Park, Shastri Park, Delhi - 110053
Website : www.railtelindia.com

SOR-B-1	Core /Spine Switch as per technical specification given in Chapter-3A							
a.	Fabric Controller	Nos	02					
b.	Core /Spine Switch	Nos	04					
SOR-B-2	Internet Firewall as per technical specification given in Chapter-3A	Nos	04					
Sub Total								
SOR-C	Incremental% AMC cost in addition to 3.5 % mentioned in clause 3.8 of Chapter-3	Years	05					
Grand Total								
Grand Total (In Words)								

2. Chapter-2, Annexure-A, Tax Breakup for SOR may be read as:

Annexure-A

Tax Breakup for SOR

SOR	Description	Total Qty	Basic Unit Price (exclusive of all levies and charges)	Pkg & Forwarding Charges		Freight & Insurance Charges		CGST/SGST /IGST/UTGST etc.		Price Per Unit (all inclusive) for delivery at destination (In Rs.) (4+6+8+10)	
				%	Amt	%	Amt	%	Amt	In Fig	In Word
1	2	3	4	5	6	7	8	9	10	11	12
SOR-A-1											
SOR-A-2											
SOR-A-3-a											
SOR-A-3-b											
SOR-A-3-c-i											
SOR-A-3-c-ii											
SOR-A-3-d-i											
SOR-A-3-d-ii											
SOR-B-1-a											
SOR-B-1-b											
SOR-B-2											

3. Chapter-2, Foot Note No. VII may be read as.

The Bidder should have authorization specific to this tender from respective OEM. Bidder has to quote same OEM for SOR-A-2 and SOR-B-1 (a & b).

4. **Chapter-3-A, Technical Requirement may be read as.**

Chapter-3-A

Technical Requirement

The bidder has to carry out following activities: -

1. Supply, Installation, Configuration, performance Tuning & Integration, Performance Testing, Acceptance Testing, Commissioning and Training of the supplied hardware, software, network equipment and network & security software as per Schedule of Requirements at RailTel Data Center Gurugram and Secunderabad.

2. Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with OEM professional services for the supplied Hardware, Software, Network equipment and Network & Security software for their installation, configuration, fine-tuning, integration with existing components and commissioning to meet the functional requirements. OEMs shall also be responsible for successful implementation and system operations.

3. Comprehensive Warranty support services of all supplied Hardware, Network equipment and Cabling for all the supplied Software and Network & Security software valid for a period of 36 months from the Date of System Commissioning or 40 months from the date of delivery to the site (Only in case the delay in system commissioning is on the part of consignee), whichever is earlier.

A. Scope of Work

- Proposed Secure Data Centre solution should provide integrated protection and dynamic, intelligent control to defend against today's sophisticated attacks.

- Solution should establish a true threat management system to detect threats and mitigate risk.

- Secure Data Centre delivers dynamic security capabilities, reduces complexity, and increases flexibility by coordinating security between Firewall, AAA, Network Behavior Anomaly detection and Endpoint.

- With integrated network access control technology, RailTel should be able to manually or automatically change users' access privileges (quarantine device) when there's suspicious activity, a threat or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications.
- Solution should turn security intelligence and response technologies into an integrated operation to see and stop threats wherever and whenever they occur in network.

- The Data Centre Solution should have "Secure tool" should provide application insights and inventory across DC's using auto generated application discovery and dependency mapping for workloads in various Dev, Test, Pre-Prod, Prod and other DC zones. It should provide an always on application blueprint for ever changing application relationships and inter-dependencies.

- It should generate a whitelist policy based on real-time application behaviour and keep the policies up-to-date as applications evolves and more applications are added and modified. The

tool should enforce the generated application whitelisted policy consistently across bare-metal, virtual and container workloads. It should track policy compliance.

- The tool should have the capability to track every process executed on the server and map behavior deviations instantaneously to malware execution patterns. It should provide high fidelity alters for both system generated and user defined events.

- It should provide accurate inventory of the installed software packages on the workloads to quickly identify any known vulnerabilities and exposures. It should then provide actions to quarantine or restrict communications based on vulnerabilities or vulnerability score.

- It should provide a always-on traffic search and analysis capability for tracking and monitoring application and network performance on a per flow basis between all DC and external endpoints for real time and historic traffic flow.

- The tool should be quoted as an appliance form factor, Scope should include monitoring and display of each and every process, process ID, Process owner, Process mapping running on the server (Physical / VM form factor). Solution must also display the Top 10 providers and consumers on the dashboard. Bidder has to provide secure tool as a part of solution either internal or external or part of NBA.

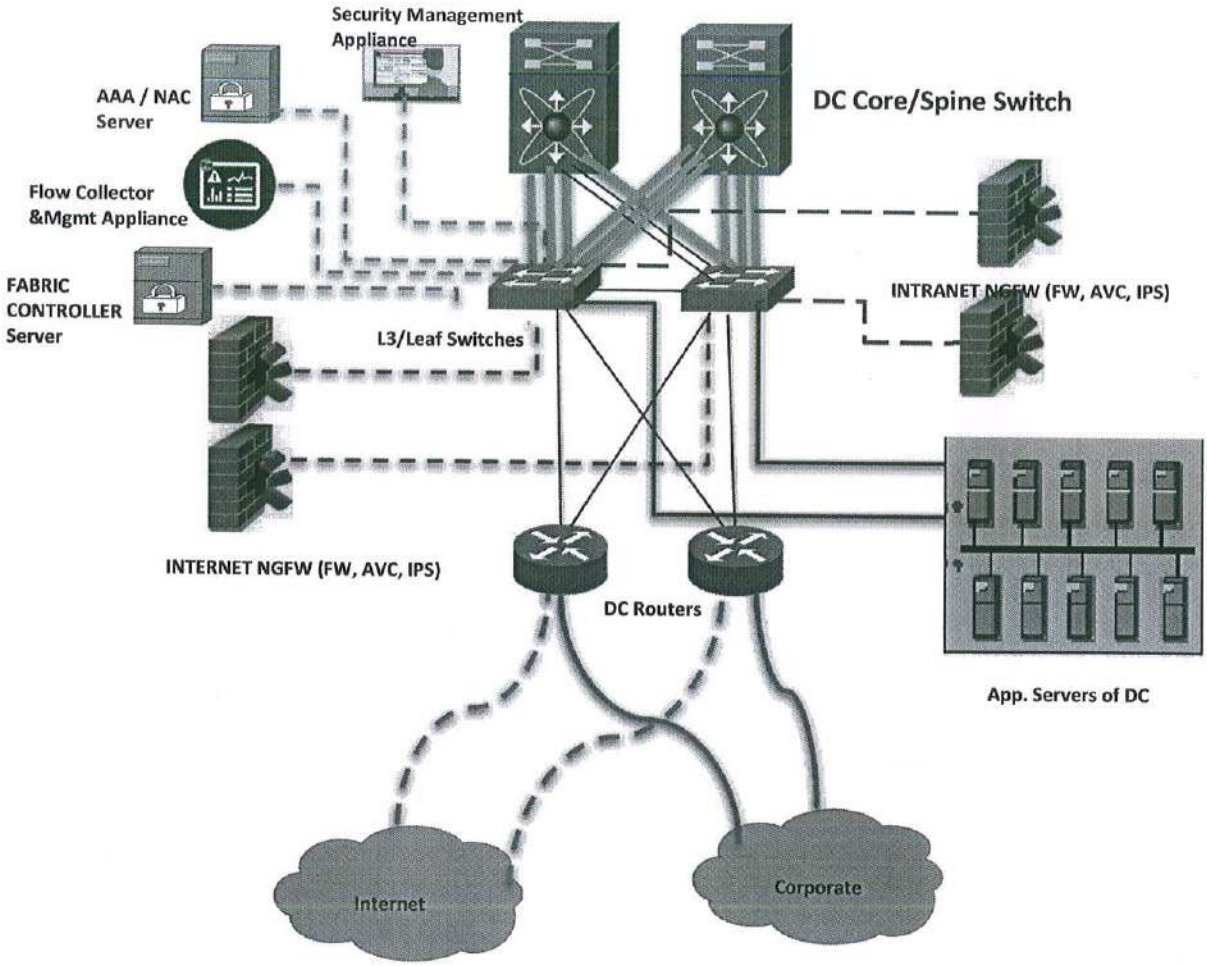
Note 1: It may kindly be noted that in the specification wherever support for a feature has been asked for, it will mean that the feature should be available without RailTel requiring any other hardware/software/licenses. Thus, all hardware/software/licenses required for enabling the support/feature shall be included in the offer.

Note 2: Bidder should submit the vetted BOM from their respective OEMs.

Note 3: The Bidder should have OEM authorization specific for this tender.

Note 4: Bidder has to provide all type of optics (SFP/ SFP+/XFP/QSFP28 etc.) of same OEM offered against SOR and Passive component (Patch Cords & other items) required for Installation and Commissioning of complete solution should be from reputed OEM.

High Level Connectivity Diagram:



CONNECTIVITY TOWARDS BOTH L3 SWITCHES

100G CONNECTIVITY Between Spine and Leaf

SOR-A-1: Data Centre Router:

SN	Functional Requirements:
1	**The following are the functional requirements to be met by the access router:**
1.1	The router shall have control processor (Control plane) and switch fabric (forwarding plane) redundancy, and PSU redundancy
1.2	The Core router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multi-processor based for enhanced performance. The Router should have multi-core Processor.
1.3	The router must support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities.
1.4	The Core router must have onboard support for intelligent traffic measurement and analysis. The router must support flow based traffic analysis feature.
1.5	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.
2	**Router Architecture:**
2.1	Architecture: The architecture of the router must be modular and redundant. Router should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 100 Gbps or more.
2.2	Number of Slots: The router must be chassis based and accommodate at least required physical interfaces in Day-1 and should able to accommodate 2x100GE interfaces in future.
2.3	Router Processor Architecture: The router processor architecture must be multi-processor based and should support hardware accelerated, parallelized and programmable IP forwarding and switching.
2.4	Processor Redundancy Feature: The router must support processor redundancy (both route processor and switch fabric (forwarding plane)) in 1:1 mode to ensure high-availability of the system. The router in the event of failure of any one processor should switch over to the redundant processor without dropping any traffic flow. There should not be any impact on the performance in the event of active processing engine failure.
2.5	Hot Swap-ability: The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way.
2.6	The router clock must sync to the Network Time Protocol (NTP) server of the Service Provider through the WAN links.
2.7	The router should have minimum 8GB flash and 8GB DRAM. It should also support DRAM expandable to 64GB DRAM.
3	**Router Performance Parameter:**
3.1	Routing Table Size: The router must support 20,00,000 IPv4 and 2,00,000 IPv6 routes entries in the routing table from Day-1. Should support at least 50,000 multicast routes/destinations.

3.2	The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.
3.3	Router should support 26 Gbps of IPSEC performance and 6000 tunnels (internal/external).
3.4	The Router solution must be a carrier-grade Equipment supporting the following:
i.	No single point of failure
ii.	In-band and out-band management
iii.	Router should have capability for configuration and software rollback feature and should support at least 10 configuration rollback.
iv.	Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.
3.5	The proposed router should support modular OS and simply the changes through In-Service OS upgrade mechanism
4	**Physical Interface Support:**
4.1	The router line card must support following interface as defined in the IEEE, ITU-T:
4.2	The router should have Short Haul SFP enabled on all ports. The Router should have at least 8 port 1G optical and 8 port 10G optical from day 1. The router should support 2x100GE optical interfaces in the same chassis in future.
4.3	The router should support following interfaces: Channelized E1, Channelized POS STM1, Channelized POS STM16, POS STM 64, Fast Ethernet, Gigabit Ethernet, 10G Ethernet, 40G Ethernet,100G Ethernet.
5	**Layer 3 Routing Protocols**
5.1	The router must support the IPv4 and IPv6 stack in hardware and software. It must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains.
5.2	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.
5.3	The router should support minimum 6000 VRF instances from day one
5.4	The Router should support 5 level of MPLS Labels lookup
5.5	The router should support minimum 64K number of MPLS Labels
5.6	MPLS OAM - LSP Ping/Trace route for MPLS core
5.7	Multicast VPN (mVPN)
5.8	The Router shall support dynamically established spoke-to-spoke VPN capabilities over public networks
5.9	The Router shall support GRE-based IPsec VPN
5.10	The Router shall support L2TP
5.11	The Router shall support for improvement of application performance and availability
6	**IPv6 Support.**
6.1	Should support IP version 6 in hardware.
6.2	Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.

6.3	The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunneling, 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)
6.4	Support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.
6.5	The router should support for IPv6 Multicast.
6.6	Should support IPv6 stateless auto-configuration, IPv6 neighbor discovery and, Neighbor Discovery Duplicate Address Detection.
6.7	Should support IPv6 Quality of Service
6.8	Should support IPv6 dual stack
6.9	Should perform IPv6 transport over IPv4 network (6to4 tunneling).
6.10	Should support SNMP over IPv6 for management.
6.11	The router must perform Hardware assisted GRE tunneling as per RFC 1701 and RFC 1702.
6.12	The router must support router redundancy protocol like VRRP.
7	**Multicast**
7.1	The router must support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).
7.2	The multicast implementation must support Rendezvous Points on both leaf and non-leaf nodes.
7.3	The multicast implementation must support source specific multicast.
7.4	The router must support multiprotocol BGP extensions for multicast.
7.5	The router must support multicast load balancing traffic across multiple interfaces.
7.6	The router must support RFC 3618 Multicast Source Discovery Protocol (MSDP).
7.7	The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP) as defined in RFC 3446.
8	**Quality of Service:**
8.1	The router must be capable of doing Layer 3 classification and setting ToS/Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting.
8.2	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 and DSCP.
8.3	The router shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter.
8.4	The QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue.
8.5	The router shall support congestion avoidance through WRED and selective packet discard using WRED through IP Precedence and DSCP.
8.6	The router should have support for minimum 8 queues per port
8.7	The scheduling mechanism must allow for expedited or strict priority routing for all high priority traffic.

8.8	The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues.
8.9	All network based keep alives (PPP keep alives, OSPF LSAs, BGP updates etc) must be given the highest priority and route before any traffic type
8.1	The traffic must be able to be prioritized into 8 class types. Class types must be able to be mapped into 1 of 8 bandwidth constraints. Bandwidth Constraints should be assignable to in individual hardware queues. Oversubscription rates for bandwidth constraints should have local significance only.
8.11	The router shall support 200k queues to offer granular QoS, policing and shaping capabilities.
8.12	Queuing and Scheduling must be able to be configured on a per physical port or logical port
9	**Security Feature**
	The router shall meet the following requirements for security –
9.1	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.
9.2	The router shall support time based ACL to reflect time based security and QoS policy.
9.3	The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.
9.4	The router shall provide Firewall Services that are required for routing purposes for enhanced security to protect the WAN backbone from malicious activities. (Internal or external)
9.5	The router should have support for Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.
9.6	The router shall support AAA features through RADIUS or TACACS+.
9.7	The router shall support Control Plane Policing to protect the router CPU from attacks.
9.8	The router shall provide MD5 hash authentication mechanism for RIPv2, OSPF, IS-IS, BGP and MPLS routing protocols.
9.9	The Router shall support IKEv1 and IKEv2 (RFC 5996)
9.10	The Router shall support Suite B Cryptographic Suites for Ipsec (RFC 4869)
10	**System Management and Administration**
10.1	Routers should support Configuration rollback
10.2	Support for accounting of traffic flows for Network planning and Security purposes
10.3	Should support extensive support for SLA monitoring for metrics like delay, latency, jitter and packet loss
10.4	Routers should support Software upgrades
10.5	Routers should support SNMPv2 and SNMPv3
10.6	Device should have Console, Telnet, SSH1 and SSH2 support for management
11	**Built-in trouble shooting**
11.1	Extensive debugs on all protocols
11.2	Shall support Secure Shell for secure connectivity

11.3	Should have to support Out of band management through Console and an external modem for remote management
11.4	Pre-planned scheduled Reboot Facility
11.5	Real Time Performance Monitor – service-level agreement verification probes/alert
12	**Certifications**
12.1	The proposed router should have IPv6 ready from day 1.
12.2	The proposed router should be Common Criteria Certified such as EAL3 / NDPP or above.
12.3	Safety certifications UL 60950-1
12.4	EMC certifications FCC Class A. IEC/EN61000-4-2 to 4-6, 4-8, 4-11 and EN55022 & EN55024

SOR-A-2: L-3/ Leaf Switch:

SN	Technical Specification
1	**Solution Requirement**
1.1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing
1.2	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy
1.3	Switch should support the complete STACK of IPv4 and IPv6 services.
1.4	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied
1.5	The switch quoted should be part of latest Gartner's Leader Quadrant for Data Center networking
2	**Hardware and Interface Requirement**
2.1	Switch should have the following interfaces:
2.2	48 x 1G/10G/25G Multi Mode Fiber Interface fully populated with 48*10G multi-mode Transceivers
2.3	6 x 40G /100G ports fully populated using multimode 100G SR Transceivers for uplink connectivity
2.4	Switch should have console port
2.5	Switch should have management interface for Out of Band Management
2.6	Switch should be rack mountable and support side rails if required
2.7	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant
2.8	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP
2.9	Switch should have a minimum 32MB buffer of more.
2.10	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.
2.11	Switch should support VLAN tagging (IEEE 802.1q)
2.12	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy
2.13	Switch should support Configuration roll-back and check point

2.14	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc
3	**Performance Requirement**
3.1	Switch should support Graceful Restart for OSPF, BGP etc.
3.2	Switch should support minimum 512 VRF instances
3.3	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure
3.4	The switch should support hardware based load balancing at wire speed using LACP and multi chassis etherchannel/LAG
3.5	Switch should support minimum 3.6 Tbps non blocking switching capacity including the services:
	a. Switching
	b. IP Routing (Static/Dynamic)
	c. IP Forwarding
	d. Policy Based Routing
	e. QoS
	f. ACL and Other IP Services
	g. IPv6 host and IPv6 routing
4	**Advance Features**
4.1	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN /NVGRE
4.2	Switch should support VXLAN and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center
4.3	Switch should support Open Flow/Open Day light/Open Stack controller
4.4	Switch should support VXLAN routing (single pass without any re-circulation)
4.5	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.
5	**Layer2 Features**
5.1	Spanning Tree Protocol (IEEE 801.D, 802.1W, 802.1S)
5.2	Switch should support VLAN Trunking (802.1q) and should support 3900 VLAN
5.3	Switch should support basic Multicast IGMP v1, v2, v3
5.4	Switch should support minimum 64K no. of MAC addresses
5.5	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch
5.6	Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.
5.7	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server
5.8	Switch should support Jumbo Frames up to 9K Bytes on all available Ports
5.9	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
5.10	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures

5.11	Switch platform should support MAC Sec in hardware
6	**Layer3 Features**
6.1	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
6.2	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing
6.3	Switch should support MPLS segment routing and VRF route leaking functionality from day 1
6.4	Switch should provide multicast traffic reachable using:
	a. PIM-SM
	b. PIM-SSM
	c. IGMP v1, v2 and v3
7	**Availability**
7.1	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
7.2	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/VRRP
7.3	Switch should support for BFD for Fast Failure Detection as per RFC 5880
7.4	**Quality of Service**
7.5	Switch system should support 802.1P classification and marking of packet using:
	a. CoS (Class of Service)
	b. DSCP (Differentiated Services Code Point)
	c. Source physical interfaces
	d. Source/destination IP subnet
	e. Protocol types (IP/TCP/UDP)
	f. Source/destination TCP/UDP ports
7.6	Switch should support methods for identifying different types of traffic for better management and resilience
7.8	Switch should support for different type of QoS features for ream time traffic differential treatment using
	a. Weighted Random Early Detection
	b. Strict Priority Queuing
7.9	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
7.10	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic
8	**Security**
8.1	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
8.2	Switch should support control plane i.e. processor and memory protection from unnecessary or DoS traffic by control plane protection policy
8.3	Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4
8.4	Switch should support for external database for AAA using:

	a. TACACS+
	b. RADIUS
8.5	Switch should support DHCP Snooping
8.6	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol
8.7	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes
8.8	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
8.9	Switch should support Spanning tree BPDU protection
9	**Manageability**
9.1	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail
9.2	Switch should provide remote login for administration using:
	a. Telnet
	b. SSH v2
9.3	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures
9.4	Switch should support for management and monitoring status using different type of Industry standard NMS using:
	a. SNMP v1 and v2
	b. SNMP v3 with encryption
	c. Filtration of SNMP using Access list
	d. SNMP MIB support for QoS
9.5	Switch should support for basic administrative tools like:
	a. Ping
	b. Traceroute
9.6	Switch should support central time server synchronization using Network Time Protocol NTP v4
9.7	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces
9.8	Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management
9.9	Switch should provide different privilege for login in to the system for monitoring and management
9.10	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding
10	**IPv6 features**
10.1	Switch should support for IPv6 connectivity and routing required for network reachability using different routing protocols such
	a. OSPF v3
	b. BGP with IPv6
	c. IPv6 Policy based routing
	d. IPv6 Dual Stack etc

	e. IPv6 Static Route
	f. IPv6 Default route
	g. Should support route redistribution between these protocols
10.2	Switch should support multicast routing in IPv6 network using PIMv2 Sparse Mode
10.3	Switch should support for QoS in IPv6 network connectivity
10.4	Switch should support for monitoring and management using different versions of SNMP in IPv6 environment such as:
	a. SNMPv1, SNMPv2c, SNMPv3
	b. SNMP over IPv6 with encryption support for SNMP Version 3
10.5	Switch should support syslog for sending system log messages to centralized log server in IPv6 environment
10.6	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events
10.7	Switch should support for IP V.6 different types of tools for administration and management such as:
	a. Ping
	b. Traceroute
	c. SSH
10.8	All relevant licenses for all the above features and scale should be quoted along with switch
10.9	Switch and optics should be from the same OEM

SOR-A-3: UTM:

SOR-A-3-a: Technical Specification for Next Generation Firewall:

SN	Feature	Technical Specification
1	Industry recommendations	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years.
2	Hardware Architecture	Chassis based security appliance should provide firewall, AVC and IPS functionality from day one.
		Chassis platform should support at least 8 * 10G Gigabit ports along with SR Optics from day 1 and should be scalable to additional 4 * 40G or 2*100G in future.
		The appliance hardware should be a multicore CPU architecture with a hardened 64bit operating system to support higher memory and should support minimum of 256 GB of RAM
		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.
		The proposed solution shouldn't use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet.

3	Performance & Scalability	Should support 40 Gbps of NGFW (FW, AVC and IPS) real-world / production performance and should be scalable to 80 Gbps in future without replacing hardware.
		Firewall should support at least 25,000,000 concurrent sessions and should be scalable to 50,000,000 in future.
		Firewall should support at least 300,000 connections per second and should be scalable to 600,000 in future.
		Firewall should have integrated redundant hot-swappable power supply
		Firewall should have integrated redundant hot-swappable fan tray / modules
4	NG Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc. Firewall should support Next-Gen IPS (NGIPS) from day one. The same Firewall should have Anti Malware Protection for Networks, and URL Filtering. No file should be submitted in cloud for sandboxing. Bidder to include on-premise appliances for sandboxing.
		Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat
		Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
		Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6
		Should support Multicast protocols like IGMP, PIM, etc
		Should support capability to integrate with other security solutions (AAA) to receive contextual information like security group tags/names
		Should have the capability of passively gathering information about virtual machine traffic, 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. This feature can be part of solution either internal or external or part of NBA
		Should have the capability of passively gathering information about virtual machine traffic, 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. This feature can be part of solution either internal or external or part of NBA.
		Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware. This feature can be part of solution either internal or external or part of NBA.

		Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency
		Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
		Should support more than 10,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy.
		Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
		Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
		Should be capable of detecting and blocking IPv6 attacks.
		The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box
		Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control
		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. This feature can be part of solution either internal or external or part of NBA.
		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
		Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist
		Should have DNS threat intelligence feeds to protect against threats
		The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.
		The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/ reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
		Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location
		The detection engine should support the capability of detecting variants of known threats, as well as new threats

		The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.
		Should support custom based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
5	URL Filtering Features	Should support URL threat intelligence feeds to protect against threats
		Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 200 million of URLs in more than 60 categories.
		Should support safe search enforcement.
6	Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software
		The management platform must be a dedicated OEM appliance and VM running on server will not be accepted
		The management appliance should have 2 x 10G port and integrated redundant power supply from day one
		The management platform must be able to store record of 15000 user or more
		The management platform must provide a highly customizable dashboard.
		The management platform must domain multi-domain management
		The management platform must provide centralized logging and reporting functionality
		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
		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.
		Should support troubleshooting techniques like Packet tracer and capture
		Should support REST API for monitoring and config programmability
		The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
		The centralized management platform must not have any limit in terms of handling logs per day. Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one

		The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
		The management platform support running on-demand and scheduled reports
		The management platform must risk reports like advanced malware, attacks and network
		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.
7.	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement	

SOR-A-3-b: Technical Requirement for Network Behavior Analysis:	
SN	**Minimum Requirement Specification**
1	Solution should provide a full-featured Network threat analyzer capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish "normal" traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.
2	Should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.
3	Should capture signature / heuristics based alerts and block the same
4	Should Identify the source of an attack and should not block legitimate users
5	Should identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities
6	The solution should be capable of detecting denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types (ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc.), identify the presence of botnets in the network, identify DNS spoofing attack etc.
7	Solution should detect common events like Scanning, Worms, Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc.
8	Solution should provide application insights and inventory across data center using auto generated application discovery and dependency mapping for workloads in various environments like dev, test, Pre-Prod, Prod and other zones in datacenter. It should provide an always-on application blueprint for ever changing application relationships and inter-dependencies.

9	Solution should generate a whitelist policy based on real-time application behavior and keep the policies up-to-date as applications evolves and more applications are added and modified. It should enforce the generated application whitelisted policy consistently across bare-metal, virtual and container workloads. It should track policy compliance.
10	Should utilize Anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration.
11	Solution should Integrates with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provides full historical mapping of User Name to IP address logins in a searchable format
12	Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantine VLANS
13	Should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue
14	The system should be able to monitor flow data between various VLANS
15	Should support the capability to identify network traffic from high risk applications such as file sharing, peer-to-peer, etc.
16	Should support the capability to link usernames to IP addresses for suspected security events.
17	Should support the capability to extract user defined fields (including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, no. of packets and no. of bytes transmitted in a session, timestamps for start and end of session etc.) from captured packet data and then utilize fields in correlation rules.
18	Should support the capability Application profiling in the system and should also support custom applications present or acquired by the bank/customer
19	Solution should be compatible with a virtual environment.
20	Solution should support capability to quarantine / remediate endpoint
21	Solution should be able to identify potential DDOS attacks originating from behind proxies.
22	Solution should be able to identify anomalies related to VOIP protocols over data network
23	Solution should have the capability to track every process executed on the server and map behavior deviations instantaneously to malware execution patterns. It should provide high fidelity alters for both systems generated and user defined events.
24	Solution should provide accurate inventory of the installed software packages on the workloads in real time to quickly identify any known vulnerabilities and exposures. It should then provide actions to quarantine or restrict communications based on vulnerabilities or vulnerability score.

25	It should provide a always-on traffic search and analysis capability for tracking and monitoring application and network performance on a per flow basis between all DC and external endpoints for real time and historic traffic flow.
26	Solution should be dedicated network behaviour analysis solution and not a subset of SIEM or Forensic analysis
27	Solution should support built-in firewalling support, rejecting all packets by default (transparent to pings and port scans)
28	Dashboard should have the facility to be configured according to user profile
29	System should support event forwarding for SMTP, SYSLOG & SNMP for high risk issues
30	The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc.
31	Solution should be able to track user's activities locally and remote network sites and should be able to report usage behaviour across the entire network.
32	The solution should support the identification of applications tunneling on other ports
33	Solution should be able to collect security and network information of servers and clients without the usage of agents
34	Solution include capability to monitor and display of each and every process, process ID, Process owner, Process mapping running on the server (Physical / VM form factor).
35	Solution should be capable of simulating "what if" scenario with existing policy in data center workload on past traffic or new policy on current / old traffic and validate the result before applying the policy on the production network.
36	Solution should provide contextual search capability with actionable insight for faster troubleshooting and anomaly detection
37	The solution should be able to conduct de-duplication of redundant flow identified in the network to improve performance
38	The solution should have the ability to statefully reassemble uni-directional flows into bi-directional conversations; handling de-duplication of data and asymmetry
39	The solution should support all forms of flows including but not limited to cisco netflow, juniper jflow, sflow, ipfix for udp etc.
40	The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall that are associated with a single conversation and present them as a single bi-directional flow record
41	The solution should be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address
42	The solution should be able to leverage external threat feeds for information about known detection methods/fingerprints for Phishing, Botnets, Malware, Spyware, Connections to bad reputation Nations and Dark IP
43	Solution should support detection methods/fingerprints for Web crawler identification, location-based threats & GEO IP based threats
44	The solution should be able to integrate with various SIEMs available in the market like RSA, Splunk, HP, etc

45	Solution should collect telemetry information from every packet in the data center without sampling along with support of long term data retention.
46	Solution should analysis each and every flow in different dimension i.e. location, time of transaction, network and application latency, source and destination ports and IP, Session duration etc to find out application anomaly in data center
Network performance	
47	Solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.
48	Dashboard should have the facility to be configured according to user profile
49	Solution should probe the network in a manner so that impact on network performance is minimal.
50	Should support both in line and/or offline modes.
51	The tool should have a system for interactive event identification and rule creation
52	Devices / applications those do not support flows, the solution should be capable to generate its own flows for monitoring.
53	Solution should have facility to assign risk and credibility rating to events.
54	Solution should include 100 license for Data Center workload for monitoring and policy enforcement
55	Solution should support traffic rate at least 10 Gbps
56	Proposed flow collectors should have at least 5000 flows per second from day 1 and should have ability to scale from 5000 flows per second to 80000 flows per second in future.
57	Proposed solution should be a dedicated appliance-based solution
SOR-A-3-c- i & ii: Technical Requirement for Network Access Control & Authentication:	
SN	**Minimum Requirement Specification**
1	The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); profiling; posture/health check; and guest management services on a single platform.
2	Solution should have concurrent capacity for 2000 endpoints out of 50000 endpoint from day one with scaling upto 50000 concurrent end points. Bidder should quote the required appliance for 50,000 end points.
3	It should allow organisations to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise
4	Solution should enable administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, greatly simplifying administration by providing consistency in managing all these services.
5	Provides complete guest lifecycle management by empowering sponsors to on-board guests
6	Should help organisations to identify the number of endpoints that have a specified application installed and these applications should be classified into 13 categories
7	Offered solution should be dedicated appliance based.
8	Proposed appliances should be configured in Active/Standby or Active/Active across DC & DR.

9	Should support consistent policy in centralized and distributed deployments that allows services to be delivered where ever required
10	Solution should deliver customizable self service portals as well as the ability to host custom web pages to ease device and guest on-boarding, automate endpoint secure access and service provisioning, and enhance the overall end-user experience inside business-defined workflows
11	Should enforces security policies by blocking, isolating, and repairing non-compliant machines in a quarantine area without requiring administrator attention
12	Should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases: Internal Users, Internal Endpoints, Active Directory, LDAP, RSA, RADIUS Token Servers, Certificate Authentication Profiles
13	Support password settings for internal users and admin users, option should be available to choose if the password can contain any dictionary word or its characters in reverse order
14	Support allows Organisation to configure the AD and LDAP server with IPv4 or IPv6 address
15	Should utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA).
16	Supports a wide range of 802.1x authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS).
17	Solution should support TACACS+ to simplify device administration and enhance security through flexible, granular control of access to network devices
18	TACACS+ device administration should support: i. Role-based access control ii. Flow-based user experience iii. Per Command level authorization with detailed logs for auditing
19	Solution should support capability to customize TACACS+ Services by specifying customer TACACS+ port number
20	Solution should support capability to create different network device groups so that administrator can create: i. Different policy sets for IOS/OS or wireless controller OS ii. Different for firewall iii. Differentiate base on location of device
21	Solution should be able to create TACACS+ profile like Monitor, Priviledge level, default, etc to control the initial login session of device administrator.
22	solution should be able to create TACACS+ authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive, ? (any character), * (matches any), etc and support stacking as well
23	Solution must support TACACS+ in IPV4 & IPv6 network
24	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect

25	Solution should be able to integrate with MDM vendors like: Airwatch, Good, Mobileiron, Zenprise,etc
26	Should support full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Should include guest portal customize from day one
27	Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.
28	Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.
29	Solution should have profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors: * Profiling using MAC OUIs * Profiling using DHCP information * Profiling using RADIUS information * Profiling using HTTP information * Profiling using DNS information / Nessus * Profiling using NetFlow information / Onguard Agent * Profiling using SPAN/Mirrored traffic
30	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets.
31	Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database.
32	Solution should support the following endpoint checks for compliance for windows endpoints: Check process, registry, file & application Check operating system/service packs/hotfixes Check firewall product is running check for Antivirus installation/Version/ Antivirus Definition Date check for Antispyware installation/Version/ Antispyware Definition Date Check for windows update running & configuration
33	Should be a persistent client-based agent or clientless to validate that an endpoint is conforming to a company's posture policies.
34	Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network.
35	Should support integration with 3rd party vulnerability assessment tools like Rapid7, Tenable/Nessus, etc
36	Should allows to create read-only administrative users who can view the configurations on GUI, but cannot create, update, or delete data
37	Should allow viewing the summary of the reports that are exported by the users in the last 48 hours along with the status.
38	Should support troubleshooting & Monitoring Tools
39	Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.

SOR-A-3-d- i & ii: Anti-Malware Protection for Endpoint Specification	
1	**Minimum Requirement Specification**
2	The bidder shall propose dedicated endpoint based solution to protect systems Advanced Targeted Attacks and APT's.
3	The proposed solution shall work on a signature-less mechanism to stop threats without relying on a database to be present at the endpoint
4	The proposed solution shall work as an independent module without relying on other endpoint and network systems for any of its functionality
5	The proposed solution shall be capable of working along with all leading endpoint AV vendors without needing to replace them
6	The proposed solution shall utilize layered and defense in depth approach, wherein the solution cannot be of the same make as existing endpoint AV
7	The proposed endpoint solution should support detecting of all malware types, both known and unknown. The movement of all known and unknown malware should be tracked and reported across the endpoints.
8	The proposed endpoint solution should be able to support continuous and root cause analysis to help in triaging of security incidents.
9	Security vendor should have a dedicated research organization that is focus on vulnerability research and should actively contribute to discoveries of new vulnerabilities exploited in the wild.
10	Software footprint should be small <50MB and should support interactive and/or silent install. Total of 2000 Licenses should be factored for this End Points from day 1. Proposed appliance should support 100000 concurrent endpoints from day 1 by purchasing additional licenses in future.
11	Endpoint software should be easy to deploy and support (not limited to) deployment through 3rd party systems management tools
12	Root cause analysis on a suspected machines should include the following capability:
13	- Sequential and chronological trace of events with details including host, username, IP, client application involved
14	- Details should highlight which file/process/services that affected
15	Proposed endpoint software should support malware tracking and provide visualization at the network level: systems and users affected, patient zero, and method/point of entry.
16	Proposed system should support continuous and persistent monitoring of files to detect polymorphic and time bound malware whenever they start turning bad and shall not be only an on-demand scan mechanism
17	Proposed endpoint software should be capable to block CnC communications and dropper activity and contain the spread of malware
18	Remediation at endpoints for incident response should include (and not limited to):
	- Track and capture files on suspected machine with option for lookups on suspected devices
	- Block of files / process / services that are showing malicious behaviours

	- Dropper detection and blocking of downloads via URL / sites
	- Submit suspected malicious files for further analysis
19	The proposed solution shall have the capability to quarantine the malicious application/program/file automatically without quarantining the entire user machine from network which would affect business productivity of the user
20	The proposed solution shall have the capability to work with Indicators of Compromise (IOC's)
21	The proposed solution shall provide the capability to write/upload custom IOC's
22	The proposed solution shall provide details to enable forensic analysis of incidents
23	The solution shall be capable of working in Windows, Windows Server &Linux operating systems
24	The endpoint solution shall be able to pinpoint vulnerable versions of popular applications installed in Endpoints
25	The proposed solution shall be able to identify the threat root cause of incidents, child processes of malwares and parent file disposition
26	The proposed solution should not be dependent on a network sandbox for its detection as it takes up bandwidth and affects productivity and shall provide the option of choosing which files to be submitted for sandboxing, to administrator.
27	The proposed solution should be able to do a threat hunting across all endpoints and quarantine the specific malicious file
28	The proposed endpoint solution should run as is and not require any system changes at OS level like enabling Volume Shadow copy Service, disabling admin access or any other user level change
29	Solution should allow Users to choose to preview the new Policy UI.

SOR-B-1-a: Fabric Controller:

SN	Feature Set
1	**Fabric Definition**
1.1	Proposed fabric must be the Clos architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol
1.2	Fabric should have achieved following functionalities:
i.	**Flexibility:** Should allow workload mobility anywhere in the DC, across the DC
ii.	**Robustness:** while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone
iii.	**Performance:** full cross sectional bandwidth (any-to-any) – all possible equal paths between two endpoints are active
iv.	**Deterministic Latency:** fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale
v.	**Multi-site design:** The fabric should support a Multi-Site/Multi-Fabric design to interconnect separate availability zones (fabrics), each deployed either as a single pod or multiple pods (a Multi-Pod design)

vi.	**Business Continuance:** The fabric should be able to deploy applications across data center fabrics representing separate availability zones, to ensure that any network-level failures or configuration or policy definition errors that occur in one availability zone will not ever be propagated to the application's workloads running in a separate availability zone
vii.	**Scalability:** add as much Leaf as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric.
2	**Hardware and Interface Requirement**
2.1	Fabric Connectivity should have the following properties:
i.	Leaf switches to Spine connectivity should use uplink port using line rate 40G/100G .
ii.	All switches including Spine and leafs should be of line rate including access and uplink ports non-blocking
iii.	Fabric controller should connect to leaf switch with multiple 10G connectivity.
3	**Fabric Features**
3.1	Fabric must support various Hypervisor encapsulation including VXLAN natively without any additional hardware/software or design change.
3.2	Fabric must be created based on hardware based VXLAN + ISIS or VXLAN + EVPN architecture.
3.3	Fabric must auto discover all the hardware and auto provision the fabric based on the policy.
3.4	The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing.
3.5	Fabric must provide open programmable interface using python SDK/JSon SDK/XMLS or COBRA etc. from the Central Management appliance / SDN Controller for programming/configuring the entire fabric.
3.6	Fabric must provide open scripting interface using Bash / powershell / NetConf/YANG from the central management appliance / SDN Controller for configuring the entire fabric.
3.7	Fabric must support Role Based Access Control in order to support Multi - Tenant environment.
3.8	Fabric must integrate with different virtual machine manager viz. Vmware vCenter, Microsoft Hyper-V with System Center and manage virtualize networking from the single pane of Glass - Fabric Controller/SDN Controller
3.9	Fabric must support provide default gateway redundancy
3.10	Fabric must integrate with best of breed L4 - L7 Physical and virtual appliances and manage using single pane of glass - Fabric Controller / SDN Controller
3.11	Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between any two endpoints on the fabric
3.12	Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc. Security feature should be included in fabric created with Spine and Leaf architecture
3.13	Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software.
4	**Fabric Layer 2, Layer 3 and Misc. Features**

4.1	Fabric must support Layer 2 features like LACP, STP /RSTP /MSTP, VLAN Trunking, LLDP etc.
4.2	Fabric must support multi chassis ether channel/MLAG i.e. Host connects to two different Leaf switches and form ether channel using LACP/NIC Teaming on Host
4.3	Fabric must support Jumbo Frame up to 9K Bytes on 1G/10G/25G/40G/100G ports
4.4	Fabric must support Layer 2 Multicast i.e. IGMP v1, v2 and v3
4.5	Fabric must support IP v4 and IP v6 FHRP using HSRP or VRRP
4.6	Fabric Must support IP v4 and IP v6 Layer 3 routing protocol OSPF and BGP
4.7	Fabric must support IP v6 dual stack
4.8	Fabric must support traffic redistribution between different routing protocol
4.9	Fabric must support IP v4 and IP v6 management tools like - Ping, Traceroute, SSH
4.10	Fabric must support IP v4 and IP v6 SNMP V1 / V2 / V3
4.11	Fabric must support integration with the centralized Syslog server for monitoring and audit trail
4.12	Fabric must support NTP
5	**Fabric Security Features**
5.1	Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service
5.2	Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD
5.3	Fabric must support VM attribute based zoning and policy.
5.4	Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment
5.5	Fabric must support true multi - tenancy
5.6	Fabric must be accessible using CLI over SSH and GUI using HTTP/HTTPS
5.7	Fabric must support SNMP v2/3 with HMAC-MD5 or HMAC-SHA authentication and DES encryption.
5.8	Fabric must act as a State-less distributed firewall with the logging capability. Security feature should be included in fabric created with Spine and Leaf architecture
5.9	Fabric must be capable to provide services of L 4 - L7 services using physical or virtual appliances i.e. Firewall, ADC, IPS etc.
6	**Fabric Scale and Performance**
6.1	Fabric should support scale up and scale out without any service disruption
6.2	Fabric must support for 512 VRF/Private network/tenants without any additional component or upgrade or design change
6.3	Fabric must integrate with minimum 3 Virtual Machine Manager (i.e. vCenter, SCVMM, OpenStack etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without common orchestrator
6.4	Fabric must be capable of connecting up to 200 physical servers.
6.5	Fabric must be capable of integrating minimum of 8 nos. of L4 - L7 services physical or virtual appliances (i.e. Firewall, ADC, IPS etc.) and scale up to 16 nos. of L4 - L7 Services appliances.

7	**Fabric management**
7.1	Fabric must provide Centralized Management Appliance or SDN Controller - Single pane of glass for managing, monitoring and provisioning the entire Fabric.
7.2	Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralized Management appliance or SDN Controller.
7.3	Centralized management appliance or SDN Controller must manages and provision rules on L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager.
7.4	Centralized management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric.
7.5	Centralized management appliance or SDN Controller must provide necessary report for compliance and audit.
7.6	Centralized management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX / OPENFLOW / OVSDB etc. or using Device APIs.
7.7	Centralized management appliance or SDN Controller communication with the south bound devices must be encrypted
7.8	Centralized management appliance or SDN Controller must communicate with the south bound devices using more than one path i.e. in-path connectivity and out of band management connectivity
7.9	Centralized management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.
7.10	Centralized management appliance or SDN Controller must run in "N + 1" redundancy to provide availability as well as function during the split brain scenario
7.11	In Event of all Centralized management appliances or SDN Controllers fails, the fabric must function without any performance degradation and with the current configuration.
7.12	Centralized management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management.
7.13	Centralized management appliance or SDN Controller must support TACACS+, RADIUS, LDAP or Local Authentication. It must also provide an integration with the Syslog servers.
7.14	The proposed solution must be able to analyze real time data about the network which includes any metadata, configurations, policies, device states or protocol states and then run automated checks to identify potential errors, misconfigurations and network misbehaviors.
7.15	The proposed solution must be able to verify configurations before been committed to be adherent to configuration best practices and if any check/verification failure occurs then system must notify it to the admin via a suitable mechanism
7.16	The proposed solution must be able to analyse configuration/policies across all devices in the fabric and then verify information such as Two endpoints will be able to communicate with each other with the defined configuration/policies. a. Two different sets of endpoints will be able to communicate with each other with the defined configuration/policies.

	b. Tenants defined are indeed isolated as per configuration/policy across the entire fabric
SOR-B-1-b: Technical requirement for Core/Spine Switch:	
SN	**Item Description**
1	**Solution Requirement - Spine Switch**
1.1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing
1.2	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy
1.3	Switch should support the complete STACK of IPv4 and IPv6 services.
1.4	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied
1.5	The switch quoted should be part of latest Gartner's Leader Quadrant for Data Center networking
2	**Hardware and Interface Requirement**
2.1	Spine Switch should have Minimum 36 numbers of 40/100 Gbps QSFP28 ports. 16 nos of 100G short haul optics should be offered from Day-1 in each Spine Switch
2.2	Switch should have console port
2.3	Switch should have management interface for Out of Band Management
2.4	Switch should be rack mountable and support side rails if required
2.5	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant
2.6	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP
2.7	Switch should have a minimum 40MB buffer of more.
2.8	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically priorities short lived flows during congestion to avoid packet drop of mission critical traffic. In case of such classification not being supported then the OEM must supply a deep buffer (4GB or higher) switch.
2.9	Switch should support VLAN tagging (IEEE 802.1q)
2.10	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy
2.11	Switch should support Configuration roll-back and check point
2.12	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc
3	**Performance Requirement**
3.1	Switch should support Graceful Restart for OSPF, BGP etc.
3.2	Switch should support minimum 512 VRF instances
3.3	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure
3.4	The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether-channel/LAG
3.5	Switch should have minimum 7.2 Tbps non-blocking switching capacity including the services:
	a. Switching
	b. IP Routing (Static/Dynamic)

	c. IP Forwarding
	d. Policy Based Routing
	e. QoS
	f. ACL and Other IP Services
	g. IPv6 host and IPv6 routing
4	**Advance Features**
4.1	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN /NVGRE
4.2	Switch should support VXLAN and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center
4.3	Switch should support OpenFlow/Open Day light/Open Stack controller
4.4	Switch should support VXLAN routing (single pass without any re-circulation)
4.6	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.
5	**Layer2 Features**
5.1	Spanning Tree Protocol (IEEE 801.D, 802.1W, 802.1S)
5.2	Switch should support VLAN Trunking (802.1q) and should support 3900 VLAN
5.3	Switch should support basic Multicast IGMP v1, v2, v3
5.4	Switch should support minimum 64K no. of MAC addresses
5.5	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch
5.6	Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.
5.7	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server
5.8	Switch should support Jumbo Frames up to 9K Bytes on all available Ports
5.9	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
5.10	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
5.11	Switch platform should support MAC Sec in hardware
6	**Layer3 Features**
6.1	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
6.2	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing
6.3	Switch should support MPLS segment routing and VRF route leaking functionality from day 1
6.4	Switch should provide multicast traffic reachable using:
	a. PIM-SM
	b. PIM-SSM
	c. IGMP v1, v2 and v3
7	**Availability**

7.1	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
7.2	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/VRRP
7.3	Switch should support for BFD for Fast Failure Detection as per RFC 5880
8	**Quality of Service**
8.1	Switch system should support 802.1P classification and marking of packet using:
	a. CoS (Class of Service)
	b. DSCP (Differentiated Services Code Point)
	c. Source physical interfaces
	d. Source/destination IP subnet
	e. Protocol types (IP/TCP/UDP)
	f. Source/destination TCP/UDP ports
8.2	Switch should support methods for identifying different types of traffic for better management and resilience
8.3	Switch should support for different type of QoS features for ream time traffic differential treatment using
	a. Weighted Random Early Detection
	b. Strict Priority Queuing
8.4	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
8.5	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic
9	**Security**
9.1	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
9.2	Switch should support control plane i.e. processor and memory protection from unnecessary or DoS traffic by control plane protection policy
9.3	Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4
9.4	Switch should support for external database for AAA using:
	a. TACACS+
	b. RADIUS
9.7	Switch should support DHCP Snooping
9.8	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol
9.11	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes
9.12	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
9.13	Switch should support Spanning tree BPDU protection
10	**Manageability**
10.1	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail

10.2	Switch should provide remote login for administration using:
10.3	a. Telnet
	b. SSH v2
10.3	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures
10.4	Switch should support for management and monitoring status using different type of Industry standard NMS using:
	a. SNMP v1 and v2
	b. SNMP v3 with encryption
	c. Filtration of SNMP using Access list
	d. SNMP MIB support for QoS
10.5	Switch should support for basic administrative tools like:
	a. Ping
	b. Traceroute
10.6	Switch should support central time server synchronization using Network Time Protocol NTP v4
10.7	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces
10.8	Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management
10.9	Switch should provide different privilege for login in to the system for monitoring and management
10.10	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding
11	**IPv6 features**
11.1	Switch should support for IPv6 connectivity and routing required for network reachability using different routing protocols such
	a. OSPF v3
	b. BGP with IPv6
	c. IPv6 Policy based routing
	d. IPv6 Dual Stack etc
	e. IPv6 Static Route
	f. IPv6 Default route
	g. Should support route redistribution between these protocols
11.2	Switch should support for QoS in IPv6 network connectivity
11.3	Switch should support for monitoring and management using different versions of SNMP in IPv6 environment such as:
	a. SNMPv1, SNMPv2c, SNMPv3
	b. SNMP over IPv6 with encryption support for SNMP Version 3
11.4	Switch should support syslog for sending system log messages to centralized log server in IPv6 environment
11.5	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events

11.6	Switch should support for IP V.6 different types of tools for administration and management such as:
	a. Ping
	b. Traceroute
	c. SSH
	d. SSH
11.8	All relevant licenses for all the above features and scale should be quoted along with switch
11.9	Switch and optics should be from the same OEM

SOR-B-2: Internet Firewall:

SN.	Specifications
1	**Industry Certifications and Evaluations**
1.1	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years
2	**Hardware Architecture**
2.1	The appliance based security platform should be capable of providing firewall, application visibility, and IPS functionality in a single appliance
2.2	The appliance should have at least 8*1G electrical and 8*10G SFP+ ports with SR optics from day-1
2.3	The appliance hardware should be a multicore CPU architecture with a hardened operating system
3	**Performance & Scalability**
3.1	Should support at least 10 Gbps of NGFW Real world performance (includes FW, Application Visibility and IPS) from day one.
3.2	NG Firewall should support at least 40,00,000 concurrent sessions
3.3	NG Firewall should support at least 50000 connections per second
3.4	NG Firewall should support at least 1024 VLANs
4	**High-Availability Features**
4.1	Firewall should support Active/Standby or Active/Active failover
4.2	Firewall should support 802.3ad functionality for the failover control & date interfaces for provide additional level of redundancy
4.3	Firewall should support redundant interfaces to provide interface level redundancy before device failover
4.4	Firewall should support 802.3ad functionality to increase the bandwidth for a segment.
4.5	Firewall should have integrated redundant power supply without any external adaptors
5.	**Firewall Features**
5.1	Solution must be capable 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. This feature can be part of solution either internal or external or part of NBA.
5.2	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously
5.3	Firewall should support operating in routed & transparent mode

5.4	Should support Static, RIP, OSPF, OSPFv3 and BGP/BGPv6
5.5	Firewall should support manual NAT and Auto-NAT, static NAT, dynamic NAT, dynamic pat
5.6	Firewall should support NAT66 (IPv6-to-IPv6), NAT44 (IPv4 to IPv4) and NAT64(IPv6 to IPv4) and NAT46(IPv4 to IPv6) for IP address translation/tunneling functionality.
5.7	Firewall should support Multicast protocols like IGMP, PIM, etc.
5.8	Should support security policies based on security group in source or destination fields or both
5.9	Should support capability to receive contextual user information like username, IP address, authentication status, location and device information from 3rd party vendors
5.10	Should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc.
5.11	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.).
5.12	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
5.13	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
5.14	Should be capable of detecting and blocking IPv6 attacks.
5.15	Deleted.
5.16	Solution should support the capability to configure the access policy on the basis of IP Address, User ID/Group, VLAN, Network, Objects, Device type, Location, Ports, Protocols, etc.
5.17	Solution must provide IP reputation feed that comprised of several regularly updated collections of poor reparation of IP addresses determined by the proposed security vendor
5.18	Solution must support IP reputation intelligence feeds from in-house/third party and custom lists of IP addresses including a global blacklist.
5.19	Should support URL and DNS threat intelligence feeds to protect against threats
5.20	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic.
5.21	Deleted.
5.22	Should support more than 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.
5.23	Should support the capability (by purchasing license) of providing network-based detection of malware by checking the disposition of unknown files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on premise (if required in future) on purpose built-appliance
5.24	NGFW OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.
5.25	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
5.26	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location

5.27	The detection engine should support the capability of detecting variants of known threats, as well as new threats
5.28	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.
6.	**VPN features**
6.1	Firewall should support RFC 6379 based Suite-B Cryptography Suites/algorithms like AES-GCM/GMAC support (128-, 192-, and 256-bit keys)
6.2	Firewall should support latest IKEv2 standards.
6.3	Should support pre-shared keys & Digital Certificates for VPN peer authentication
6.4	Should support perfect forward secrecy & dead peer detection functionality
6.5	Should support Nat-T for IPsec VPN
7.	**Regulatory Compliance**
7.1	Firewall shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.
7.2	Firewall shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.
8.	**Evaluation Compliance**
8.1	Firewall/ Firewall's Operating System should be tested and certified for EAL 4/NDPP or above under Common Criteria Certification or FIPS Level 2 Certifications
8.2	Firewall/ Firewall's Operating System should be USGv6/IPv6 Certified/IPv6 logo ready
9	**Management**
9.1	The management platform must be accessible via a web-based interface and ideally with no need for additional client software
9.2	The management platform must provide a highly customizable dashboard.
9.3	Deleted.
9.4	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.
9.5	Should support REST API for monitoring and config. programmability
9.6	Should support troubleshooting techniques like Ping, Trace route, etc.
9.7	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
9.8	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
9.9	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
9.10	The management platform should support risk reports like advanced malware, attacks and network
9.11	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.

5. Added New clause 44 in Chapter-4 (Integrity Pact):

Integrity Pact Program

a) RailTel has adopted Integrity Pact Program and for implementation thereof all tenders relating to procurement of OFC, quad cable, pre-fab shelters, electronic equipments and its installation and/or commissioning etc and other item(s) or activity/activities proposed to be carried out or required by the Company for the value exceeding Rs. 15 crores at a time including for repair and maintenance of cable/network and any other items required for special works assigned to RailTel will be covered under the Integrity Pact Program and the vendors are required to sign the IP document and submit the same to RailTel before or along with the bids.

b) Only those vendors who have purchased the tender document and signed the IP document can send their grievances, if any, to the Independent External Monitors (IEMNs) through the nodal officer.

Name of IEMs and contact details:

a)	Sh. Ashok Kumar Garg, New Delhi	e-mail: akgarg1654@gmail.com
b)	Sh. Jayanta Kumar Roy, Kolkata	e-mail: jkroy.its@gmail.com

c) If the order, with total value equal to or more than the threshold value, is split to more than one vendor and even if the value of PO placed on any/each vendor(s) is less than the threshold value, IP document having been signed by the vendors at bid stage itself, the Pact shall continue to be applicable.

d) Bidder of Indian origin shall submit the Integrity Pact (in 2 copies) on a non-judicial stamp paper of Rs. 100/- duly signed by the person signing the bid. If the bidder is a partnership or a consortium, the Integrity Pact shall be signed by all the partners or consortium members.

e) Bidder of foreign origin may submit the Integrity Pact on its company's letterhead, duly signed by the person signing the bid.

f) The 'Integrity Pact' shall be submitted by the Bidder duly signed in all pages along with the Bid in a separate envelope, duly superscripted with 'Integrity Pact'. Tender received without signed copy of the Integrity Pact document will be liable to be rejected. Proforma for signing the Integrity Pact is available in Chapter-6 of this tender document (Form No. 5).

g) One copy of the Integrity Pact shall be retained by RailTel and the 2nd copy will be issued to the representative of the bidders during bid opening. If the Bidders representative is not present during the Bid opening, the 2nd copy shall be sent to the bidder by post/courier.

Chapter-6

Form No.-5

PROFORMA FOR SIGNING THE INTEGRITY PACT

RailTel Corporation of India Limited, hereinafter referred to as "The Principal".

And

....., hereinafter referred to as "The Bidder/ Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for .....The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relations with its Bidder(s) and /or Contractor(s).

In order to achieve these goals, the Principal will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1- Commitments of the Principal

1. The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

    a. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

    b. The Principal will during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the process or the contract execution.

    c. The Principal will exclude from the process all known prejudiced persons.

2. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2- Commitments of the Bidder(s) / Contractor(s)

1. The Bidder(s)/Contractor(s) commit himself to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

    a. The Bidder(s)/contractor(s) will not, directly or through any other persons or firm, offer promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage during tender process or during the execution of the contract.

b. The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s)/Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s) /Contractors will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the bidder(s)/contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers' as annexed and marked as Annexure A.

e. The Bidder(s)/Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

2. The Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3: Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings". Copy of the "Guidelines on Banning of business dealings" is annexed and marked as Annex-"B".

Section 4: Compensation for Damages

1. If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/Bid Security.

2. If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to be terminated the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5: Previous Transgression

1. The Bidder declares that no previous transgressions occurred in the last three years with any other company in any country conforming to the anti corruption approach or with any other public sector enterprise in India that could justify his exclusion from the tender process.

2. If the bidder makes incorrect statement on this subject, he can be disqualified from the

tender process for action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6: Equal treatment of all Bidders / Contractors/Subcontractors.

1. The Bidder(s)/Contractor(s) undertake(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact, and to submit it to the Principal before contract signing.

2. The Principal will enter into agreements with identical conditions as this one with all bidders, contractors and subcontractors.

3. The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7: Criminal charges against violation by Bidder(s) / Contractor(s) / Sub contractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8: Independent External Monitor / Monitors

1. The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the CMD, RailTel.

3. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/Subcontractor(s) with confidentiality.

4. The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

6. The Monitor will submit a written report to the CMD, RailTel within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

7. Monitor shall be entitled to compensation on the same terms as being extended to provided to Independent Directors on the RailTel Board.

8. If the Monitor has reported to the CMD, RailTel, a substantiated suspicion of an offence under relevant IPC/PC Act, and the CMD, RailTel has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

9. The word 'Monitor' would include both singular and plural.

Section 9: Pact Duration

This pact begins when both parties have legally signed it. It expires for the Contractor 10 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made / lodged by either party during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by CMD of RailTel.

Section 10: Other Provisions

1. This agreement is subject to Indian Law, Place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.

2. Changes and supplements as well as termination notices need to be made in writing.

3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

4. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(For & on behalf of the Principal)
(Office Seal)

(For & On behalf of Bidder/Contractor)
(Office Seal)

Place _____

Date _____

Witness 1:
(Name & Address)

_____

_____

Witness 2:
(Name & Address)

_____

_____

The last date of submission of bids is extended from 03.05.2019 to 10.05.2019 up to 15.00 Hrs. Tender will be opened at 15:30 Hrs. on 10.05.2019

All other term & conditions will remain same.

30/4/19

(A.K. Sablania)
Executive Director/DNM