UCO BANK

Department of Information Technology

Request for Proposal (RFP) for Supply, Delivery, Installation and Maintenance of Network Devices

RFP Ref. No: DIT/BPR & BTD/OA/4412/2019-20 Date: 02/12/2019

Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s), Amendments, Addendums and Corrigendum's

Sl. No	Page No	Clause No	Clause as per RFP	Description of Query/ Clarification sought by Bidder	Bank Response
1.	33	SCOPE OF THE WORK	Bank existing servers will be connected with leaf switch (copper) with 1G port	Since old servers with 1G network connectivity will be used in the leaf switch (copper), requesting to consider 6 x 40G uplinks to the Spine Switch for leaf switch (copper) instead of or in addition to 2 x 100G uplinks.	Clause stands as per RFP
2.	30	SCOPE OF THE WORK	Interconnection between spine and leaf switches through Direct Attach Cables (DAC) provided by OEM or through 100G fiber cables is the scope of the bidder without any additional cost to the bank.		Clause stands as per RFP
3.	34	SCOPE OF THE WORK - Spine & Leaf switches in brief: Leaf switch (Copper)	Switch should have minimum 2 fiber uplinks of 100G ports with the spine switch.		Clause stands as per RFP
4.	35	SCOPE OF THE WORK - The requireme	VPN concentrator must support 6 Gbps of Crypto throughput for IPSEC performance and 10000 IPSEC tunnels from day 1. In case	As per tender specification the VPN concentrator need to support at least 10,000 VPN tunnels and crypto throughput is only 6 Gbps. So per	Clause modified as under: VPN concentrator must support 10 Gbps of Crypto throughput for

		nt of Spine & Leaf switches in brief: VPN concentrator	of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 4 no. of 10 G interface (SFP) from Day1.	tunnel throughput is only around 600 Kbps, which would be limiting factor for smooth operation of the branch. So we request you to revisit the crypto throughput requirement and we believe it should be at least 50 Gbps for large frame so that each tunnel can deliver 5 Mbps of throughput. Since the VPN concentrator would be connected to high speed backbone, please revisit the interface requirement (6 x 1 GigE and 4 x 10 GigE) to 8 x 10G and 2 x 40G	IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any point of time (at start, re-start or throughout the day)
5.	83	Spine Switch Requirements	Spine Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 100 G ports connectivity i.e. Each Spine must have 200 nos. of line rate 40G/100G ports scalable to 128 nos. with consideration of leaf to SPINE over subscription ration of 6:1	200 nos. of 40G/100G ports looks like a typo error since total Leaf Switch is only 8 at DC and DR. Kindly revalidate the port requirement from day-1 and scalability requirement of the Spine Switch.	Clause modified as under: Spine Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 100 G ports connectivity i.e. Each Spine must have minimum 32 nos. of line rate 40G/100G ports minimum scalable to 64 nos. with consideration of leaf to SPINE over subscription ratio of 3:1 or more
6.	91	Leaf Switch (Copper) Requirements	Must have 4 or more no. of 40G/100G QSFP based Fiber ports per switch for uplinks with spine switch	Since old servers with 1G network connectivity will be used in the leaf switch (copper), requesting to consider 6 x 40G uplinks to the Spine Switch for leaf switch (copper).	Clause stands as per RFP
7.	92	Leaf Switch (Copper) Requirements	Minimum 4GB Flash	4 GB Flash is too low to accommodate multiple OS and log files required for root cause analysis during failure. Request to increase to at least 16 GB.	It is clarified that minimum 4GB Flash is required however bidder can quote higher flash memory to meet the SLA & uptime.

8.	92	Leaf Switch (Copper) Requirements	Minimum System buffer 16 MB	Kindly accept "Minimum System buffer 12 MB" for participant of more OEMs.	Minimum System buffer 12 MB, however bidder can quote higher system buffer to meet the SLA & uptime
9.	99	Leaf Switch (Fiber) Requirements	Minimum 4GB Flash	4 GB Flash is too low to accommodate multiple OS and log files required for root cause analysis during failure. Request to increase to at least 16 GB.	It is clarified that minimum 4GB Flash is required however bidder can quote higher flash memory to meet the SLA & uptime.
10.	99	Leaf Switch (Fiber) Requirements	Minimum System buffer 16 MB	Kindly accept "Minimum System buffer 12 MB" for participant of more OEMs.	Minimum System buffer 12 MB, however bidder can quote higher system buffer to meet the SLA & uptime
11.	106	Layer 3 Switch Requirements	Electrical: Frequency: 50/60 Hz Maximum Heat Dissipation: 528 BTU/hr (557.04 KJ/hr) Voltage: 100-240 Vac, rated Maximum Power Rating: 155 W	Power rating and heat dissipation varies from OEM to OEM and should be removed to allow more OEM participation.	It is clarified that the supplied equipment should be compatible with tier 3 data centre environment.
12.	107	TECHNICAL REQUIREMENTS OF VPN MODULES	VPN modules Processors should have minimum 4GB of flash memory or more to support multiple software images for backup purposes, log report and future scalability	4 GB Flash is too low to accommodate all the feature support asked. May kindly revisit the minimum requirement.	It is clarified that minimum flash memory requirement is 4 GB, however bidder can quote higher Flash memory to meet the SLA & uptime.
13.	108	TECHNICAL REQUIREMENTS OF VPN MODULES	VPN concentrator must support 6 Gbps of Crypto throughput for IPSEC performance and 10000 IPSEC tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at	As per tender specification the VPN concentrator need to support at least 10,000 VPN tunnels and crypto throughput is only 6 Gbps. So per tunnel throughput is only around 600 Kbps, which would be limiting factor for smooth operation of the branch. So we request you to revisit the crypto	Clause modified as under: VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have

			least 6 x 1GE interfaces and 4 no. of 10 G interface (SFP) from Day1.	throughput requirement and we believe it should be at least 50 Gbps for large frame so that each tunnel can deliver 5 Mbps of throughput. Since the VPN concentrator would be connected to high speed backbone, please revisit the interface requirement (6 x 1 GigE and 4 x 10 GigE) to 8 x 10G and 2 x 40G.	redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any point of time (at start, re-start or throughout the day)
14.	108	TECHNICAL REQUIREMENTS OF VPN MODULES	VPN concentrator must support 6 Gbps of Crypto throughput for IPSEC performance and 10000 IPSEC tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 4 no. of 10 G interface (SFP) from Day1.	All the East-West and North-South traffic would travel through the Core Firewall. So the Core Firewall need to be connected to the backbone network using high speed interfaces. Kindly revisit the interface requirement (6 x 10 GigE and 6 x 1GigE) to 8 x 10 GigE and 2 x 40 GigE ports.	Clause modified as under: VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any point of time (at start, re-start or throughout the day)
15.	109	TECHNICAL REQUIREMENTS OF VPN MODULES	8000 IPSec VPN tunnels	Under clause 19, 10,000 VPN tunnel is asked for.	Clause modified as under: 10000 IPSec VPN tunnels

16.	109	TECHNICAL REQUIREMENTS OF VPN MODULES	VPN modules should have hardware encryption capabilities with a minimum throughput of 6 Gbp	As per tender specification the VPN concentrator need to support at least 10,000 VPN tunnels and crypto throughput is only 6 Gbps. So per tunnel throughput is only around 600 Kbps, which would be limiting factor for smooth operation of the branch. So we request you to revisit the crypto throughput requirement and we believe it should be at least 50 Gbps for large frame so that each tunnel can deliver 5 Mbps of throughput.	Clause modified as under: VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any point of time (at start, re-start or throughout the day)
17.	114	2 PAIR OF CORE FIREWALL TYPE 1 TECHNICAL REQUIREMENTS AT DC & DR	Firewall should have at least 6 no. of 10 GE ports SFP port and 6 no, 1 Gbps Ethernet port	All the East-West and North-South traffic would travel through the Core Firewall. So the Core Firewall need to be connected to the backbone network using high speed interfaces. Kindly revisit the interface requirement (6 x 10 GigE and 6 x 1GigE) to 8 x 10 GigE and 2 x 40 GigE ports.	Clause modified as under: Firewall should have at least 6 no. of 10 G ports SFP port and 4 nos. of 40G/100 G port and 2 nos. 1 Gbps Ethernet port.
18.	114	2 PAIR OF CORE FIREWALL TYPE 1 TECHNICAL REQUIREMENTS AT DC & DR	Firewall performance should be minimum real world throughput 100 Gbps after enabling all function like IPS, QoS, malware protection and Anti-virus	The Anti-virus protection is usually taken care at the Internet Gateway level and would not be required at the Core Firewall which would be deployed at server farm zone. So requesting to change "Firewall performance should be minimum real world throughput 100 Gbps after enabling all function like IPS, QoS, malware protection and Anti-	Clause modified as under: Firewall performance should be minimum real world throughput 60 Gbps after enabling the IPS, QoS, malware protection function. However bidder can quote higher specification to meet the SLA & uptime.

				virus" to "Firewall performance should be minimum real world throughput 100 Gbps after enabling all function like IPS, QoS, and malware protection".	
19.	114	2 PAIR OF CORE FIREWALL TYPE 1 TECHNICAL REQUIREMENTS AT DC & DR	Firewall should support minimum 1000,0000 concurrent connections Firewall should support minimum 200000 new connections per second (cps)	Minimum concurrent connections and connections per second asked are only 1, 000,0000 and 200,000 respectively. For such a critical firewall Minimum concurrent connections and connections per second should be 10,000,0000 and 1,000,000 respectively.	Clause modified as under: Firewall with IPS features should support minimum 2,00,00,000 concurrent connections Firewall with IPS features should support minimum 10,00,000 new connections per second (cps)
20.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL Type-2 TECHNICAL REQUIREMENTS AT DC & DR	Chassis based & modular architecture for scalability	The functional requirement of the Internet Firewall can be addressed using fixed configuration firewall. Requesting to allowing fixed configuration firewall along with Chassis based & modular architecture. Kindly revisit the interface requirement (6 x 10 GigE and 6 x 1GigE) to 8 x 1/10 GigE ports.	Clause modified as under: Chassis based or modular architecture for scalability & other than Checkpoint OEM.
21.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	deliver VPN throughput minimum 300 Mbps	Kindly revisit the VPN throughput requirement.	Clause stands as per RFP

22.	9	ELIGIBILITY CRITERIA	Additional Clause	To have best quality product for your esteemed organization, we request you to consider products that belongs to the Leaders quadrant of the latest Gartner Magic Quadrant for Data Center Networking.	Not admissible
23.	9	ELIGIBILITY CRITERIA	Bidder should have positive net worth for last three financial years (2016-17, 2017-18 & 2018-19).	Please accept credentials of Parent company as well or consider the Bidders Positive Profitability in any two financial years (2017-18, 2018-19) out of three.	Clause stands as per RFP
24.	114	2. PAIR OF CORE FIREWALL TYPE 1 TECHNICAL REQUIREMENTS AT DC & DR	Chassis based & modular architecture for scalability & other than Checkpoint OEM.	Modular or Fixed architecture for scalability & other than Checkpoint OEM.	Clause modified as under: Chassis based or modular architecture for scalability & other than Checkpoint OEM.
25.	114	2.. PAIR OF CORE FIREWALL TYPE 1 TECHNICAL REQUIREMENTS AT DC & DR	Firewall should have at least 6 no. of 10 GE ports SFP port and 6 no, 1 Gbps Ethernet port	Firewall should have at least 4 x 100/1000/10G Cu, 16 x 1G/10G SFP/ SFP+ populated with 6 x 10 G optical transceivers and 4 x 40G/100G QSFP28 ports from day one	Clause modified as under: Firewall should have at least 6 no. of 10 G ports SFP port and 4 nos. of 40G/100 G port and 2 nos. 1 Gbps Ethernet port.
26.	114	2.. PAIR OF CORE FIREWALL TYPE 1 TECHNICAL	Firewall performance should be minimum real world throughput 100 Gbps after enabling all function like IPS, QoS, malware protection and Anti-virus	Minimum Next Generation Threat prevention throughput in real world/production environment (by enabling and measured with Application-ID/AVC, User-ID/Agent-ID, NGIPS, Anti-Virus, Anti-Spyware, Anti-	Clause modified as under: Firewall performance should be minimum real world throughput 60 Gbps after enabling the IPS, QoS, malware protection function. However bidder can quote higher

		REQUIREMENTS AT DC & DR		Bot, Zero-day attacks and all other security threat prevention features enabled with 64 K HTTP transactions size and traffic mix such as HTTPS, SMTP and other protocols and logging enabled)– 33 Gbps. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.	specification to meet the SLA & uptime.
27.	114	2.. PAIR OF CORE FIREWALL TYPE 1 TECHNICAL REQUIREMENTS AT DC & DR	Firewall should support minimum 1000,0000 concurrent connections	Firewall should support minimum 8,000,000 concurrent connections with Layer 7 inspection enabled	Clause modified as under: Firewall with IPS features should support minimum 2,00,00,000 concurrent connections. However bidder can quote higher specification to meet the SLA & uptime.
28.	114	2.. PAIR OF CORE FIREWALL TYPE 1 TECHNICAL REQUIREMENTS AT DC & DR	Proposed solution should have automatic bypass for IPS in case of performance suffer beyond defined administrative threshold or IPS function/engine fails	Request to remove this clause	Clause stands as per RFP
29.	114	2.. PAIR OF CORE FIREWALL TYPE 1 TECHNICAL	IPS should have the functionality of Software Fail Open.	Request to remove this clause. Same has been asked in clause 138	Clause is self-explanatory

		REQUIREMENTS AT DC & DR			
30.	114	2.. PAIR OF CORE FIREWALL TYPE 1 TECHNICAL REQUIREMENTS AT DC & DR	IPS Software Fail Open functionality can be defined in terms Gateway Threshold of Memory or CPU and should have an option to trigger the mail if required.	Request to remove this clause. Same has been asked in clause 138 and 139	Clause is self-explanatory
31.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	Chassis based & modular architecture for scalability	Modular or Fixed architecture for scalability	Clause modified as under: Chassis based or modular architecture for scalability & other than Checkpoint OEM.
32.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	Firewall should have at least 6 no. of 1 GE ports and 6 no of 10 G fiber port	Firewall should have at least 12 x 100/1000 Cu, 8 x 1G/10G SFP/ SFP+ populated with 6 x 10 G optical transceivers and 4 x 40G QSFP+ ports from day one	Clause stands as per RFP

33.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	Firewall performance should be minimum real world throughput 20 Gbps after enabling all function like IPS, QoS, and malware protection.	Minimum Next Generation Threat prevention throughput in real world/production environment (by enabling and measured with Application-ID/AVC, User-ID/Agent-ID, NGIPS, Anti-Virus, Anti-Spyware, Anti-Bot, Zero-day attacks and all other security threat prevention features enabled with 64 K HTTP transactions size and traffic mix such as HTTPS, SMTP and other protocols and logging enabled)– 4.5 Gbps. The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.	Clause stands as per RFP
34.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	Firewall should support minimum 500,0000 concurrent connections	Firewall should support minimum 300,0000 concurrent connections with Layer 7 inspection enabled	Clause stands as per RFP
35.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL	The proposed device should have Intrusion prevention sensors delivering a minimum of 10 Gbps of context-aware , real-world traffic inspection (enabling all functions)	Request to remove this clause as TP throughput has been asked in clause no 8	Clause stands as per RFP

		REQUIREMENTS AT DC & DR			
36.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	Proposed IPS should support a minimum of average inspection throughput of 10 Gbps	Request to remove this clause as TP throughput has been asked in clause no 8. Also the same has been asked in clause no 125	Clause stands as per RFP
37.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	IPS must support a minimum of 5 million concurrent connections	Request to remove this clause as required concurrent connections for NGFW has been asked in clause no 10.	Clause stands as per RFP
38.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	Proposed solution should have automatic bypass for IPS in case of performance suffer beyond defined administrative threshold or IPS function/engine fails	Request to remove this clause	Clause stands as per RFP

39.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	IPS should have the functionality of Software Fail Open.	Request to remove this clause. Same has been asked in clause 140	Clause is self-explanatory
40.	125	3 PAIR OF INTERNET & EXTRANET FACING FIREWALL TECHNICAL REQUIREMENTS AT DC & DR	IPS Software Fail Open functionality can be defined in terms Gateway Threshold of Memory or CPU and should have an option to trigger the mail if required.	Request to remove this clause. Same has been asked in clause 140 and 141	Clause is self-explanatory
41.	83	Annexure – XVI, Spine Switch Requirements, under Architecture.	The Solution should support logical device separation for each individual server farm infrastructure at zone level (No Virtualization / No Virtual Chassis /Stacking), Zone details as per current setup (3 zones - Non-prod servers, Tandem and CBS). It should support minimum 16 zones	Request to please change this as "The Solution should support logical device separation for each individual server farm infrastructure at zone level (No Virtualization / No Virtual Chassis /Stacking), Zone details as per current setup (3 zones - Non-prod servers, Tandem and CBS). It should support minimum 8 zones". So that leader OEM can participate.	Clause modified as under: The Solution should support logical device separation for each individual server farm infrastructure at zone level (No Virtualization / No Virtual Chassis /Stacking), Zone details as per current setup (3 zones - Non-prod servers, Tandem and CBS). It should support minimum 8 zones
42.	83	Annexure – XVI, Spine Switch Requireme	Spine Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 100	Requesting the clarity, as the asked port count is very high respect to day-1 requirement. Also scalability is very much higher than the requirement. Request to change this as "Spine	Clause modified as under: Spine Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to

		nts, under Performance.	G ports connectivity i.e. Each Spine must have 200 nos. of line rate 40G/100G ports scalable to 128 nos with consideration of leaf to SPINE over subscription ration of 6:1	Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 100 G ports connectivity i.e. Each Spine must have 120. of line rate 40G/100G ports scalability consideration of leaf to SPINE over subscription ration of 3:1	Each Spine using minimum 1 x 100 G ports connectivity i.e. Each Spine must have minimum 32 nos. of line rate 40G/100G ports minimum scalable to 64 nos. with consideration of leaf to SPINE over subscription ratio of 3:1 or more
43.	83	Annexure – XVI, Spine Switch Requirements, under Performance.	Should support minimum 5 Tbps switching capacity/throughput or more	Compare to switch scalability the asking throughput is on lower side .Request to please change this as "Should support minimum 14 Tbsp. switching capacity/throughput or more". This will ensure better ROI and no further investment for fabric upgradation or replacement.	It is clarified that minimum switching capacity/throughput is 5 Tbps however bidder can quote higher switching capacity/ throughput to meet the SLA & uptime.
44.	83	Annexure – XVI, Spine Switch Requirements, under Performance.	Switch must support at least 48 or more wire-speed 40/100 GBE ports.	Request to please change this as "Switch must support at least 32 or more wire-speed 40/100 GBE ports from day-1".This is sufficient with 4x scalability than present requirement.	Switch must support at least 32 or more wire-speed 40/100 GBE ports. However bidder can quote higher specification to meet the SLA & uptime.
45.	84	Annexure – XVI, Spine Switch Requirements, under Port Requirements with	48 no. of 40G/100G QSFP based Fiber ports per switch	Request to please change this as"32 no. of 40G/100G QSFP based Fiber ports per switch"	Minimum 32 no. of 40G/100G QSFP based Fiber ports per switch, however bidder can quote higher nos. to meet the SLA & uptime

		redundancy			
46.	84	Annexure – XVI, Spine Switch Requirements, under Switch Hardware features and High availability	Switch should support Graceful Restart for OSPF, BGP etc.	Request to please change this as "Switch should support Graceful Restart for OSPF, BGP,IS-IS,MPLS from day-1.This will ensure no further investment and better ROI.	This is the minimum technical requirement however bidder may offer more functionalities to meet the SLA within the quoted cost.
47.	84	Annexure – XVI, Spine Switch Requirements, under Switch Hardware features and High availability	The Proposed switch should support FCOE (Desirable) and DCB center bridging feature.	Request to please change this as "The Proposed switch should support FCOE (Desirable) and DCB center bridging feature. From day-1".This will ensure no further investment and better ROI.	The Proposed switch should support FCOE and DCB center bridging feature from the date of implementation.
48.	84	Annexure – XVI, Spine Switch Requirements, under Switch Hardware features	Each SPINE switch must connect with each Super Spine Switch using 40/100G uplinks while maintaining the desired (6:1) over subscription ratio. Each Super Spine Should connect to each DMZ Switch with 40/100G	Request to please change this as"32 no. of 40G/100G QSFP based Fiber ports per switch "Each SPINE switch must connect with each Super Spine Switch using 40/100G uplinks while maintaining the desired (3:1) over subscription ratio. Each Super Spine Should connect to each DMZ Switch with 40/100G".	**Clause stands deleted**.

		and High availability			
49.	84	Annexure – XVI, Spine Switch Requirements, under Scalability	The proposed switch should support minimum 90K MAC address table entries.	Request to please change this as "The proposed switch should support minimum 120K MAC address table entries". To ensure better capacity as this Spine switch.	Clause stands as per RFP
50.	85	Annexure – XVI, Spine Switch Requirements, under Resilient Control Plane	Minimum Quad Core x86 CPU	Request to please remove/change as "Minimum Quad Core processor".x86 is relevant for server not switch. Requesting the clarity.	Clause modified as under : Minimum Quad Core x86 CPU or equivalent.
51.	85	Annexure – XVI, Spine Switch Requirements, under Resilient Control Plane	Minimum 8GB Flash	The architecture and technology differs from OEM to OEMs and RAM and FLASH size not related to performance of the switch. 8GB RAM and 1GB flash are sufficient to store the IOS, Configuration files and Log files in HPE switches without any degradation of performance because all the features, application and protocols supports from day one. No additional licenses are required for upgradation for features and protocols. Request you to modify the clause so that leading OEM can participate.	Clause stands as per RFP

52.	86	Annexure – XVI, Spine Switch Requirements, under Layer 3 Switch features	Must support 100K or more IPv6 Unicast entries	Request to please change this as "Must support minimum 60K or more IPv6 Unicast entries". So that leading OEM can participate. Request to relax.	Clause stands as per RFP
53.	86	Annexure – XVI, Spine Switch Requirements, ,under Layer 3 Switch features	Must support 10K IPv4 Multicast entries	Request to please change this as "Must support 8K IPv4 Multicast entries". So that leading OEM can participate. Request to relax.	Clause stands as per RFP
54.	86	Annexure – XVI, Spine Switch Requirements, under Layer 3 Switch features	Must support 64-way ECMP routing for load balancing and Redundancy	Request to please modify as "Must support 16-way ECMP routing for load balancing and Redundancy". So that leading OEM can participate.	Clause modified as under : Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher specification to meet the SLA & uptime.
55.	91	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Performance	The switch should support 200,000 IPv4 and IPv6 routes entries in the routing table including multicast routes	Request to please modify this as "The switch should support 120,000 IPv4 and IPv6 routes entries in the routing table including multicast routes	Clause modified as under: The switch should support minimum 1,00,000 IPv4 and IPv6 routes entries in the routing table including multicast routes. However bidder can quote higher specification to meet the SLA & uptime.

56.	91	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Performance	Minimum Multicast Routing table – 10000	Request to please change this as "Minimum Multicast Routing table – 8000"	Clause modified as under: Minimum Multicast Routing table – 8000. However bidder can quote higher specification to meet the SLA & uptime.
57.	92	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Switch Hardware features and High availability	Switch should support Graceful Restart for OSPF, BGP etc.	Request to please change this as "Switch should support Graceful Restart for OSPF, BGP,IS-IS,MPLS from day-1.This will ensure no further investment and better ROI.	This is the minimum technical requirement however bidder may offer more functionalities to meet the SLA within the quoted cost.
58.	92	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Switch Hardware features and High availability	The Proposed switch should support FCOE (Desirable) and DCB center bridging feature.	Request to please change this as "The Proposed switch should support FCOE (Desirable) and DCB center bridging feature. From day-1".This will ensure no further investment and better ROI.	The Proposed switch should support FCOE and DCB center bridging feature from the date of implementation.
59.	92	Annexure – XVI,LEAF SWITCH (COPPER) Requireme	The proposed switch should support minimum 90K MAC address table entries.	Request to please change this as "The proposed switch should support minimum 100K MAC address table entries". To ensure better capacity as this Spine switch.	Clause stands as per RFP

		nts, under Scalability			
60.	92	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Control Plane	Minimum Quad Core x86 CPU	Request to please remove/change as "Minimum Quad Core processor".x86 is relevant for server not switch. Requesting the clarity.	Clause modified as under: Minimum Quad Core x86 CPU or equivalent
61.	92	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Control Plane	Minimum 4GB Flash	The architecture and technology differs from OEM to OEMs and RAM and FLASH size not related to performance of the switch. 8GB RAM and 1GB flash are sufficient to store the IOS, Configuration files and Log files in HPE switches without any degradation of performance because all the features, application and protocols supports from day one. No additional licenses are required for upgradation for features and protocols. Request you to modify the clause so that leading OEM can participate.	It is clarified that minimum 4GB Flash is required however bidder can quote higher flash memory to meet the SLA & uptime.
62.	92	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Layer 2	Must support minimum 4096 VLAN	Request to please change this as "Must support minimum 4094 VLAN".	Clause modified as under: Must support minimum 4094 VLAN

		Switch features			
63.	93	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Multi-Cast	Bootstrap router (BSR) and Static RP	Request to remove this clause, not relevant for Bank environment.	Clause modified as under: Bootstrap router (BSR) and Static RP (optional)
64.	93	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, Layer 3 Switch features	Must support 64-way ECMP routing for load balancing and Redundancy	Request to please modify as "Must support 8-way ECMP routing for load balancing and redundancy". So that leading OEM can participate.	Clause modified as under : Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher specification to meet the SLA & uptime.
65.	97	Annexure – XVI,LEAF SWITCH (Fiber) Requirements, under Performance	The switch should support 200,000 IPv4 and IPv6 routes entries in the routing table including multicast routes	Request to please modify this as 'The switch should support 150,000 IPv4 and IPv6 routes entries in the routing table including multicast routes	Clause modified as under: The switch should support minimum 1,00,000 IPv4 and IPv6 routes entries in the routing table including multicast routes. However bidder can quote higher specification to meet the SLA & uptime.
66.	98	Annexure – XVI,LEAF SWITCH (Fiber) Requirements, under Switch Hardware	Switch should support Graceful Restart for OSPF, BGP etc.	Request to please change this as "Switch should support Graceful Restart for OSPF, BGP,IS-IS,MPLS from day-1.This will ensure no further investment and better ROI.	This is the minimum technical requirement however bidder may offer more functionalities to meet the SLA within the quoted cost.

		features and High availability			
67.	98	Annexure – XVI,LEAF SWITCH (Fiber) Requirements, under Switch Hardware features and High availability	The Proposed switch should support FCOE (Desirable) and DCB center bridging feature.	Request to please change this as "The Proposed switch should support FCOE (Desirable) and DCB center bridging feature. From day-1".This will ensure no further investment abd better ROI.	The Proposed switch should support FCOE and DCB center bridging feature from the date of implementation.
68.	98	Annexure – XVI,LEAF SWITCH (Fiber) Requirements, under Scalability	The proposed switch should support minimum 90K MAC address table entries.	Request to please change this as "The proposed switch should support minimum 100K MAC address table entries". To ensure better capacity as this Spine switch.	Clause stands as per RFP
69.	99	Annexure – XVI,LEAF SWITCH (Fiber) Requirements, under Control Plane	Minimum Quad Core x86 CPU	Request to please remove/change as "Minimum Quad Core processor".x86 is relevant for server not switch. Requesting the clarity.	Clause modified as under: Minimum Quad Core x86 CPU or equivalent
70.	99	Annexure – XVI,LEAF SWITCH (Fiber) Requireme	Minimum 4GB Flash	The architecture and technology differs from OEM to OEMs and RAM and FLASH size not related to performance of the switch. 8GB RAM and 1GB flash are sufficient to store	It is clarified that minimum 4GB Flash is required however bidder can quote higher flash memory to meet the SLA & uptime.

		nts, under Control Plane		the IOS, Configuration files and Log files in HPE switches without any degradation of performance because all the features, application and protocols supports from day one. No additional licenses are required for upgradation for features and protocols. Request you to modify the clause so that leading OEM can participate.	
71.	99	Annexure – XVI,LEAF SWITCH (Fiber) Requirements, under Layer 2 Switch features	Must support minimum 4096 VLAN	Request to please change this as "Must support minimum 4094 VLAN".	Clause modified as under: Must support minimum 4094 VLAN
72.	100	Annexure – XVI,LEAF SWITCH (Fiber) Requirements, under Multi-Cast	Bootstrap router (BSR) and Static RP	Request to remove this clause, not relevant for Bank environment.	Clause modified as under: Bootstrap router (BSR) and Static RP (optional)
73.	92	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Layer 2 Switch features	Minimum Number of MAC addresses entries 90K	Request to please change this as "Minimum Number of MAC addresses entries 100K".To ensure better capacity as this Spine switch.	Clause stands as per RFP

74.	100	Annexure – XVI,LEAF SWITCH (COPPER) Requirements, under Layer 3 Switch features	Must support 64-way ECMP routing for load balancing and Redundancy	Request to please modify as "Must support 8-way ECMP routing for load balancing and redundancy". So that leading OEM can participate.	Clause modified as under : Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher specification to meet the SLA & uptime.
75.	104	Annexure – XVI,TECHNICAL REQUIREMENTS OF L3 SWITCH,	Switch should have minimum 300 Gbps Switching capacity all the services enabled on switch	Request to please change this as "Switch should have minimum 176 Gbps Switching capacity all the services enabled on switch". As per non-blocking architecture calculation (48x2+80 Gbps).This is standard calculation.	Clause modified as under: Switch should have minimum 170 Gbps Switching capacity all the services enabled on switch
76.	105	Annexure – XVI,TECHNICAL REQUIREMENTS OF L3 SWITCH,	Must support Layer2 Ping and Layer 2 Trace route for connectivity and Fault Management Must support multicast Trace route.	This is restrictive; Request to please change this as "Must support Layer2 /Layer 3 Ping and Layer 2/Layer 3 Trace route for connectivity and Fault Management Must support multicast Tracer out .Layer 3 is latest and can cross WAN boundary which is more effective.	Clause modified as under: Must support Layer2 /Layer 3 Ping and Layer 2/Layer 3 Trace route for connectivity and Fault Management Must support multicast Trace route.
77.	105	Annexure – XVI,TECHNICAL REQUIREMENTS OF L3 SWITCH,	Must support minimum 128K IPv4 Unicast entries Must support minimum 64K or more IPv6 Unicast entries Must support minimum 8K IPv4 Multicast entries Must support minimum 8K ACL Must support basic layer-3 routing – static routes, BGP, OSPF, ISIS VRF: VRF-lite (IP VPN), VRF-aware unicast (BGP, OSPF, and RIP),	This is restrictive. Layer 3 switch is required for management only amd the specification has been asked with very much higher than the requirement. Request to modify as "Must support minimum 32K IPv4 Unicast entries Must support minimum 16K or more IPv6 Unicast entries Must support minimum 2K IPv4 Multicast entries	Clause stands as per RFP

			and VRF-aware multicast. Must support VRRP or equivalent Must support 64-way ECMP routing for load balancing and redundancy	Must support minimum 2K ACL Must support basic layer-3 routing – static routes, BGP, OSPF, ISIS VRF: VRF-lite (IP VPN), VRF-aware unicast (BGP, OSPF, and RIP),and VRF-aware multicast from day-1. Must support VRRP or equivalent. Must support 8-way ECMP routing for load balancing and redundancy. Which is sufficient for this scope.	
78.	105	Annexure – XVI,TECHNICAL REQUIREMENTS OF L3 SWITCH	Must support 64-way ECMP routing for load balancing and Redundancy	Request to please modify as "Must support 8-way ECMP routing for load balancing and redundancy". So that leading OEM can participate.	Clause modified as under : Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher specification to meet the SLA & uptime.
79.	31	Scope of Work Point 21	Preparation and processing of Change requests as per the requirement of the Bank.	How the change requests will be raised. Does the bank has an ITSM tool.	Shall be shared with successful bidder.
80.	31	Scope of Work Point 21	Supporting IS audit, VA & PT and closure of identified vulnerabilities.	As the RFP does not has any tool for VA, the task of onsite engineers should be for the closure of any vulnerabilities found in the Device/Software asked in the RFP. Need more clarity on it.	The successful bidder will be responsible for providing solution for closure of vulnerabilities.
81.	33	Scope of Work Point 41	DC Fabric should support both IPv4 and IPv6 from day one. At present, IPv6 is not implemented in Bank's Network. Bidder need to implement IPv6 without any additional cost whenever Bank decides to implement.	IPV6 implementation would require a complete redesigning of the Network infrastructure and a separate Scope and commercials would be required for the same. Hence we would request the bank to modify the clause.	Clause modified as under: DC Fabric should support both IPv4 and IPv6 from day one. At present, IPv6 is not implemented in Bank's Network. Bidder need to implement IPv6 on proposed devices in this RFP without any additional cost whenever Bank decides to implement.

82.	36	Scope of Work //Firewall Point T	The Firewall should have the ability to integrate seamlessly with Active Directory, proposed PIM tool to provide complete user identification and enable application-based policy definition per user or group.	The Firewall policies can be configured to provide application control over custom ports as well. The Firewall will be integrated with Active directory to provide granularity of who, what and when can access a certain application. Request the bank to please modify the clause as **"The Firewall should have the ability to integrate seamlessly with Active Directory to provide complete user identification and enable application-based policy definition per user or group."**	Clause modified as under: The Firewall should have the ability to integrate seamlessly with Active Directory to provide complete user identification and enable application-based policy definition per user or group.
83.	38	Delivery and Installation //Point A	The successful bidder should complete the entire project (delivery, Installation, configuration of proposed DC fabric, Firewall, VPN devices, Switches and integration with existing network architecture) within 8 weeks (for all locations) from the issuance of Purchase order.	The timeline of 8 weeks to complete the Delivery, Installation and Configuration of all Hardware on all locations is quiet less as the Delivery itself will take 8 Weeks by the OEM. In order to implement the project fully there will be dependencies on different teams and devices to be readily configured. the stages of Design Workshop, Design freezing, LLD creation would require the SI, Bank and OEM to give the final output and commence the configuration. Hence we request the bank to modify the timeline to 32 weeks (for all locations) from the issuance of Purchase order.	Clause modified as under: The successful bidder should complete the entire project (delivery, Installation, configuration of proposed DC fabric, Firewall, VPN devices, Switches and integration with existing network architecture) within 12 weeks (for all locations) from the issuance of Purchase order.

84.	34	Spine Switch//Point 1	Switch each with minimum 48 nos. Slot based switches along with fibre SFPs. Fibre ports should support 10G/40g/100G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M port capacity. Switch should work in High Availability (HA) Active-Active mode.	100/1000M SFP port is compatible over 10G/40G/100G module only with QSA module. Kindly specify if the same module is required and what would be the quantity.	Clause modified as under: Each Switch should have minimum 32 nos. of ports along with fiber SFPs module. Fiber ports should support 10G/40g/100G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M port capacity. Switch should work in High Availability (HA) Active-Active mode.
85.	33	Spine Switch//Point 44	Bank existing servers will be connected with leaf switch (copper) with 1G port & upcoming new server will be connected with leaf switch (fibre) with 10G fibre port. All said servers should have the dual connectivity with two separate leaf switches for redundancy.	The SFP ports on servers should be compatible with the one bidder will proposed on leaf switches hence UCO bank has to consider the same while procuring the SFP for the servers.	Clause stands as per RFP
86.	33	PART –IV Scope of work//Point 45	Latency proposed network architecture should be less than 1 ms	What is the parameters and reference point to calculate the latency	Clause modified as under: The latency in-between proposed leaf, spine and Type-1 core firewall should be less than 1 Microsecond at maximum load.
87.	35	Leaf Switch (Fiber Switch)//Point 1	Switch each with minimum 48 nos. Slot based switches along with fiber SFPs. Fiber ports should support 1G/10G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M/ 10000M port capacity. Switch should work	Which type of transceiver is required since it has been mentioned 1/10G. Need clarification.	All ports of proposed leaf & spine switches should have SFP-SR module.

			in High Availability (HA) Active-Active mode.		
88.	34	Spine Switch//Point 1	Switch each with minimum 48 nos. Slot based switches along with fiber SFPs. Fiber ports should support 10G/40g/100G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M port capacity. Switch should work in High Availability (HA) Active-Active mode.	Since as per the RFP, we are connecting 6 leafs per switch hence need clarity do we have to populate reaming ports with fiber transceiver module and if so than which transceiver is required (10G/40G/100G)	Clause modified as under: Each Switch should have minimum 32 nos. of ports along with fiber SFPs module. Fiber ports should support 10G/40g/100G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M port capacity. Switch should work in High Availability (HA) Active-Active mode.
89.	34	Spine Switch//Point 1	Switch should have 2 supervisor engines per switch to have redundancy at supervisor layer of switch.	Referring page no 34, point 37, it has been mentioned "Spine switch either Chassis based or fixed switch meeting the port requirement mentioned above with redundancy/high availability for control and data plane in each zone." But since as per the mentioned clause here, redundant supervisor has been asked. Hence both the statements are contradicted since no supervisor are available in modular switches. Kindly remove the clause at page no 34 point no 37.	Clause stands as per RFP.
90.	4	ELIGIBILITY CRITERIA// Point 4	The bidder must have supplied, implemented and maintaining/maintained proposed OEM's SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3	We have implemented VPN for multiple customer over the Cisco Router acting as a concentrator along with the other pieces as asked in the RFP. We would kindly ask the bank to	Clause modified as under: The bidder must have supplied, implemented and maintaining / maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN

			Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI in India	please consider the Purchase order for the same as the technology is VPN.	Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Further, the proposed OEM product SDN / SDN ready Data Centre Fabric of Spine switches & Leaf switches, VPN Concentrator, Firewall and L3 Switches should be running as on RFP date in minimum 1 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted.
91.	4	Page 4// ELIGIBILITY CRITERIA// Point 4		Kindly clarify if both the PO's submitted should contain all the technologies or DC fabric with other security components of the same OEM will suffice	It should be either in a single PO or in multiple POs from 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India.
92.	10	ELIGIBILITY CRITERIA	The bidder must have supplied, implemented and maintaining /maintained proposed OEM's SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI in India.	We request the honorable tendering committee to include PSU/Government under organizations. Also request Bank to consider proposed OEM only for switches and leave aside VPN concentrator and Firewalls. We are requesting the same as all solutions as asked in your RFP, from the same OEM in single PO is not possible. Also VPN concentrator is an old	Clause modified as under: The bidder must have supplied, implemented and maintaining / maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private

				technology and providing PO/completion for the same is not possible as it comes by default with NGFW for all the leading OEM's.	Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Further, the proposed OEM product SDN / SDN ready Data Centre Fabric of Spine switches & Leaf switches, VPN Concentrator, Firewall and L3 Switches should be running as on RFP date in minimum 1 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted.
93.	9	Section 3, Point 4		Since this is a new technology with limited adaptation, we request the Bank to consider 1 reference under implementation	Clause modified as under: The bidder must have supplied, implemented and maintaining / maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Further, the proposed OEM product SDN / SDN ready Data Centre Fabric of Spine switches & Leaf switches, VPN Concentrator, Firewall and L3 Switches should be running as on RFP date in minimum

					1 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted.
94.	10	3. Eligibility Criteria	The bidder must have supplied, implemented and maintaining/maintained proposed OEM's SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI in India.	Request Bank to modify as 'The **bidder/OEM** must have supplied, implemented and maintaining/maintained proposed OEM's SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in **minimum 1 organizations** out of PSBs / Private Sector Banks/ BSE / NPCI / RBI in India/**Govt. Owned Bank, Financial Institute"**	Clause modified as under: The bidder must have supplied, implemented and maintaining / maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Further, the proposed OEM product SDN / SDN ready Data Centre Fabric of Spine switches & Leaf switches, VPN Concentrator, Firewall and L3 Switches should be running as on RFP date in minimum 1 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted.

95.	10	3. ELIGIBILITY CRITERIA		**Request you to change the same as** "The bidder must have supplied, implemented or maintaining/maintained SDN ready Data Centre Fabric of minimum 8 Leaf/Spine Switches, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI /RRB/ State/Central Govt. Organization in India."	Clause modified as under: The bidder must have supplied, implemented and maintaining / maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Further, the proposed OEM product SDN / SDN ready Data Centre Fabric of Spine switches & Leaf switches, VPN Concentrator, Firewall and L3 Switches should be running as on RFP date in minimum 1 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted.
96.	10	Eligibility Criteria	The bidder must have supplied, implemented and maintaining/maintained proposed OEM's SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private	Please change clause as any type of SDN solution and for not just the proposed OEM's SDN.	Clause modified as under: The bidder must have supplied, implemented and maintaining / maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2

			Sector Banks/ BSE / NPCI / RBI in India		organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Further, the proposed OEM product SDN / SDN ready Data Centre Fabric of Spine switches & Leaf switches, VPN Concentrator, Firewall and L3 Switches should be running as on RFP date in minimum 1 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted.
97.	9	Point No 03, Sl No 04, Eligibility Criteria		The bidder must have minimum two experience of supplied, implemented and maintaining/maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in PSBs / Private Sector Banks/ BSE / NPCI / RBI/Government Organization in India.	Clause modified as under: The bidder must have supplied, implemented and maintaining / maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Further, the proposed OEM product SDN / SDN ready Data Centre Fabric of Spine switches & Leaf switches, VPN Concentrator, Firewall and L3 Switches should be

					running as on RFP date in minimum 1 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India. Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted.
98.		Annexure-XI. P No.-74	FM Services 24x7x365 DC (1(Seat), DR (1(Seat))	Please clarify what means by 1 Seat at DC & DR. How many engineers would be present in each DC & DR location to support 24X7X365?	At any point of time one source should be available at DC & DR
99.	90	Annexure – XVI,	Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period.	Does this mean non EoS document need to be provided for 7 years?	Clause modified as under: Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period i.e. End of support or End of life should be 7 years form the date of PO.
100.	53	SERVICE LEVEL AGREEMENT,	Uptime for all Branches	Please clarify the SoW related to the branches hence activates related to the DC & DR only.	Please refer corrigendum
101.	27	SCOPE OF THE WORK,	The successful bidder should provide support for all the supplied devices on 24X7X365 basis and should replace the equipment within 4 hours of time, in case of any failure. (SLA penalty applicable in case of default).	Is the penalty mentioned in this clause related to Uptime calculation only? Please clarify.	Clause is self-explanatory

102.	41	CONTRACT PERIOD,	SLA will cover performance and availability of the solution deployed for a period of Six years	Please clarify why it has been mentioned a Six (6) years where as entire contract is for Five (5) yrs.	Clause modified as under: SLA will cover performance and availability of the solution deployed for a period of five years.
103.		LIQUIDATED DAMAGE, P No. 55	If Bidder fails to commission the link as per feasibility report (this includes change of media) 10% of the link cost will be deducted from payment of other link or from Performance Bank Guarantee and bank will place the order to any other selected bidder.	N.A as per RFP, please exclude the clause or give more clarity.	Any delay in delivery/installation/ commissioning/shifting/upgradation of the device/equipment/ solution beyond the stipulated time period as per clause no. 47, Bank will charge penalty at 1 % of the order value for that device/equipment/implementation cost per week or part thereof, subject to a maximum of 10%. The bank may at its discretion also waive or reduce the penalty if the reasons for delay are considered to be justified. After elapsing of stipulated time period including 12 Weeks Liquidated damages period, if selected bidder fails to implement, the order will be deemed cancelled after imposing necessary penalty amount & Bank will deduct the same from Performance Bank Guarantee or from any outstanding payment.
104.	32	PART –IV, SCOPE OF THE WORK, Point No: 30,	30. The successful bidder should complete the entire project (delivery, configuration, migration of proposed DC fabric and integration with existing network architecture) within 8 weeks (for all locations) from the	Requesting Bank to change the delivery timeline as per below: 1) Delivery of the HW/SW/Lic will be 8 Weeks from the Date of Purchase Order. 2) Installation of the supplied	Clause modified as under: The successful bidder should complete the entire project (delivery, configuration, migration of proposed DC fabric and integration with existing

			issuance of Purchase order. (Damages applicable in case of default).	HW/SW/Lic will be within 8 weeks from the Date of Delivery.	network architecture) within 12 weeks (for all locations) from the issuance of Purchase order. (Damages applicable in case of default).
105.	32	PART –IV, SCOPE OF THE WORK, Point No: 31	31. If Bank decides to shift the data center location, in case of any exigencies, the bidder should shift the equipments without any additional cost to the Bank. However, Bank will bear the transportation cost, if any	Request Bank to keep this activity outside the one time implementation signoff. Also requesting Bank to owning the shipment of the materials	Clause stands as per RFP
106.	34	PART –IV, SCOPE OF THE WORK	34. OEM onsite support should be provided during the process of network devices Installation and Configuration of DC fabric and for resolution of complaints related to core components during the contract period.	Requesting Bank to clarify the same in details.	Clause modified as under: If required, bidder should arrange for OEM support during the process of network devices Installation and Configuration of DC fabric and for resolution of complaints related to core components during the contract period.
107.		DELIVERY & INSTALLATION,	b) The bidder is responsible for transit insurance, storage, insurance upto installation at the Bank side.	Requesting bank to keep the responsibility of the materials till delivery at the Bank side.	Clause modified as under: b) The bidder is responsible for transit insurance, storage, insurance upto delivery at the Bank side.
108.	28	PART –IV, SCOPE OF THE WORK, Point No: 2,	2. The bidder has to provide all necessary hardware, software and Network cabling (copper & fiber) required to make the solution work strictly as per technical specifications. The specifications given are minimum. Bidders can quote equivalent or	Requesting bank to share the followings: 1) Technical specification of Passive cabling components. 2) BoM for passive cabling to be incorporate. 3) Distance between the racks where respective new active hardware to be	Please refer corrigendum

			higher technical specifications to meet the Bank's requirements. However, no weightage would be given for higher configurations.	placed. 4) Requesting Bank to clarify whether bidder has to consider the passive cabling required between existing/new servers to new supplied hardware connectivity.	
109.	34	Spine Switch	Switch each with minimum 48 nos. Slot based switches along with fiber SFPs. Fiber ports should support 10G/40g/100G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M port capacity. Switch should work in High Availability (HA) Active-Active mode.	**Switch each with minimum 32 nos. Slot based switches along with fiber SFPs. Fiber ports should support 40g/100G port capacity. Switch should work in High Availability (HA) Active-Active mode.** We understand that the total number of leaf at DC is 8 as of now which can scale upto 32. 48 number of ports are specific to one OEM. Spine supposed to be used for the leaf connectivity which should be high speed fabric and things are connected on high speed ports. I do not see any scenario where 1/10 G will be connected to spine directly. Every other thing apart from leaf should be connected to leaf only for industry best practices for spine leaf architecture.	Clause modified as under: Each Switch should have minimum 32 nos. of ports along with fiber SFPs module. Fiber ports should support 10G/40g/100G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M port capacity. Switch should work in High Availability (HA) Active-Active mode.
110.	83	Architectu re, 1.1	The Solution should support logical device separation for each individual server farm infrastructure at zone level (No Virtualization / No Virtual Chassis /Stacking), Zone details as per current setup (3 zones - Non-prod servers, Tandem and CBS). It should support minimum 16 zones.	We request you to please clarify the architecture for better understanding of the solution. There are industry best practices using tenanting on the common infrastructure and also make sure there is isolation of resources for each environment.	Clause modified as under: The Solution should support logical device separation for each individual server farm infrastructure at zone level (No Virtualization / No Virtual Chassis /Stacking), Zone details as per current setup (3 zones - Non-

					prod servers, Tandem and CBS). It should support minimum 8 zones
111.	83	Performance, 2.1	Spine Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 100 G ports connectivity i.e. Each Spine must have 200 nos. of line rate 40G/100G ports scalable to 128 nos with consideration of leaf to SPINE over subscription ration of 6:1	**Spine Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 100 G ports connectivity i.e. Each Spine must have 128 nos. of line rate 40G/100G ports scalable to 288 nos with consideration of leaf to SPINE over subscription ration of 6:1**.We understand that every OEM has 8 slot modular chassis supporting 40/100 G line cards with 36 ports in each line card. The modular switch should support minimum 288 or more wire speed 40/ 100 G ports.	Clause modified as under: Spine Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 100 G ports connectivity i.e. Each Spine must have minimum 32 nos. of line rate 40G/100G ports minimum scalable to 64 nos. with consideration of leaf to SPINE over subscription ratio of 3:1 or more
112.	83	Performance, 2.2	Should support minimum 5 Tbps switching capacity/throughput or more.	The given throughput of 5 Tbps is for 48 ports fixed switch. In case of modular switch. **Switch should support total aggregate system throughput minimum 50 Tbps minimum of switching capacity (Full Duplex:- Bi-Directional).** This will make sure the bank will get the enterprise grade data center switch for the DC infrastructure.	It is clarified that minimum switching capacity/throughput is 5 Tbps however bidder can quote higher switching capacity/ throughput to meet the SLA & uptime.
113.	83	Port requirements with redundancy 2.3	Switch must support at least 48 or more wire-speed 40/100 GBE ports.	What's the number of port requirement for a modular switch ? We understand that every OEM has 8 slot modular chassis supporting 40/100 G line cards with 36 ports in each line card. **The modular switch should**	Switch must support at least 32 or more wire-speed 40/100 GBE ports. However bidder can quote higher specification to meet the SLA & uptime.

				support minimum 288 or more wire speed 40/ 100 G ports.	
114.	83	Port requirements with redundancy 2.3	Should support minimum of 64 VRFs or more	Since the IP MPLS Core Network components like the Core Routers, Internet Gateway etc would also terminate on the Core Switch based on the Network Design point, the switch would need **"Switch should support more than 1000 VRF instances from day 1"** This is important to maintain virtualization end to end.	Clause stands as per RFP
115.	83	Switch Hardware features and High availability, 4.3	Should support both front to back and back to front reversible air flow	**Should support front to back air flow or back to front air flow.** Most of the OEM provides front to back air flow which provides optimal front-to-back airflow and helps the switch operate with less power.	Clause modified as under: Should support both front to back or back to front reversible air flow
116.	84	Switch Hardware features and High availability, 4.7	The proposed switch should not be more than 11 Rack Units in size	The 11 RU form factor is proprietary to Arista DCS-7508. Which will give advantage to one particular OEM. Rest of the OEM required 13RU to support 8 slot modular Switch. Hence requesting you to change it to **"The proposed switch should not be more than 13 Rack Units in size.**	Clause modified as under: The proposed switch should not be more than 15 Rack Units in size
117.	85	L2 Switch Features, 8.8	The proposed switch should support VXLAN (Bridging and Routing) and NVGRE overlay encapsulation protocol (desirable) in hardware to support multiple hypervisor deployment in the Data Centre. Minimum 4096 VXLAN should be supported	The proposed switch should support VXLAN (Bridging and Routing) and NVGRE overlay encapsulation protocol (desirable) in hardware to support multiple hypervisor deployment in the Data Centre.	Clause modified as under: The proposed switch should support VXLAN (Bridging and Routing) and NVGRE overlay encapsulation protocol (desirable) in hardware to support multiple

					hypervisor deployment in the Data Centre.
118.	86	L3 Switch Features, 9.14	Must support 64-way ECMP routing for load balancing and redundancy	In spine leaf DC fabric topology with redundant spines, 64 way ECMP for Multicast traffic as a requirement would NOT come up. The number of uplink ports on leaf switches are at a maximum of 6 (from all vendors). Hence request you to change the spec as **"Must support Minimum 6-way ECMP routing for load balancing and redundancy"**	Clause modified as under : Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher specification to meet the SLA & uptime.
119.	87	QoS Features	The proposed switch must support minimum 32 MB packet buffer to avoid packet drops due to buffer queue entries are exhausted which results in poor and unpredictable performance	The given buffer is for the fixed 48 port switch. **For Modular switch each line card should support minimum 160 MB packet buffer to avoid packet drops due to buffer queue entries are exhausted which results in poor and unpredictable performance.**	Clause stands as per RFP
120.	88	Virtualization Features. 13.1	Virtualization switch should communicate with vSphere 4.0 and above, and vCenter to support adaptive network virtualization	**Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization.** We understand that Vsphere 4.0 should not be running in any of the production environment because of end of support announced long back.	Clause modified as under: Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization
121.	98	Port requirement with redundancy , 3.1	Switch should have 48 ports or more, capable of 1/10 Gbps copper ports	**Switch should have 48 ports or more, capable of 100M/1G/10G Copper ports with 2 Tbps of throughput.** It gives flexible port configuration to get the leaf connected to the old infrastructure supporting 100 Mbps.	Clause modified as under: Switch should have 48 ports or more, capable of 100M/1G/10G Copper ports.

122.	92	Control Plane 6.4	Minimum System buffer 16 MB	**Minimum System buffer 32 MB.** As per the QOS specification, packet buffer has been asked as 16 MB for better performance in an enterprise grade DC. Here system buffer is mentioned as 16 Mb, which is not possible. Hence to provide the 16 MB packet buffer the requirement of system buffer should be minimum 32Mb.	Minimum System buffer 12 MB, however bidder can quote higher system buffer to meet the SLA & uptime
123.	93	L2 Switch Features, 8.4	Must support minimum 4096 VLAN	Even though most vendors support 4096 VLANs, 128 vlan-ids are reserved for internal use, leaving with 3967 usable vlan-ids. Hence request you to relax the clause to **"Switch should support VLAN Trunking (802.1q) and should support minimum 3967 VLAN"**	Clause modified as under: Must support minimum 4094 VLAN
124.	93	L2 Switch Features, 8.17	Minimum Number of Ether Channels should be 64	**Minimum Number of Ether Channels should be 32.**, The number of ports asked in the switch is 48, hence we request you to downsize it to 32 which is optimum for a 48 ports switch.	Clause modified as under: Minimum Number of Ether Channels should be 32. However bidder can quote higher specification to meet the SLA & uptime.
125.	93	L3 Switch Features, 9.3	Must support minimum 8K IPv4 Multicast entries	**Must support minimum 32K IPv4 Multicast entries**. 8K multicast entries are very minimal for the enterprise grade DC fabric. Suggest you to increase it to 32K so that a proper enterprise grade DC switch is quoted.	Must support minimum 8K IPv4 Multicast entries. However bidder can quote higher specification to meet the SLA & uptime.
126.	93	L3 Switch Features, 9.8	Must support 64-way ECMP routing for load balancing and redundancy	In spine leaf DC fabric topology with redundant spines, 64 way ECMP for Multicast traffic as a requirement would NOT come up. The number of uplink ports on leaf switches are at a maximum of 6 (from all vendors).	Clause modified as under : Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher

				Hence request you to change the spec as **"Must support Minimum 6-way ECMP routing for load balancing and redundancy"**	specification to meet the SLA & uptime.
127.	94	Multi-Cast. 10.1	Multicast: PIM-SMv2, and PIM-SSM	**Multicast: PIM-SM, and PIM-SSM.** Request you to change it to PIM-SM which is generic and widely used and accepted in the DC environment. SMv2 is supported by some specific OEMs.	Clause modified as under: Multicast: PIM-SM, and PIM-SSM
128.	94	DC Advance Feature, 13.1	Should support 4096 VxLAN. Should support both VRF and VxLAN, bridging and routing from day 1,	**Should support both VRF and VxLAN, bridging and routing from day 1. As per the spine switch there is no need to mention the number of VXLAN required.**	Clause modified as under: Should support both VRF and VxLAN, bridging and routing from day 1.
129.	98	Virtualization Features. 14.1	Virtualization switch should communicate with vSphere 4.0 and above, and vCenter to support adaptive network virtualization	**Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization.** We understand that Vsphere 4.0 should not be running in any of the production environment because of end of support announced long back.	Clause modified as under: Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization
130.	99	Port requirement with redundancy , 3.1	Switch should have 48 ports or more, capable of 1/10 Gbps ports	**Switch should have 48 ports or more, capable of 1/10/25Gbps SFP for factor ports. Switch should support native 25G ports and provide 3.5 tbps of throughput.** The industry is moving from 10G to 25G SFPs for the servers and the same switch can provide the 25G form factor to provide more flexibility and future ready infrastructure with the investment protection.	Clause modified as under: Switch should have 48 ports or more, copper ports
131.	99	Control Plane 6.4	Minimum System buffer 16 MB	**Minimum System buffer 32 MB.** As per the QOS specification, packet buffer	Minimum System buffer 12 MB, however bidder can quote higher

				has been asked as 16 MB for better performance in an enterprise grade DC. Here system buffer is mentioned as 16 Mb, which is not possible. Hence to provide the 16 MB packet buffer the requirement of system buffer should be minimum 32Mb.	system buffer to meet the SLA & uptime.
132.	99	L2 Switch Features, 8.4	Must support minimum 4096 VLAN	Even though most vendors support 4096 VLANs ,128 vlan-ids are reserved for internal use, leaving with 3967 usable vlan-ids. Hence request you to relax the clause to **"Switch should support VLAN Trunking (802.1q) and should support minimum 3967 VLAN"**	Clause modified as under Must support minimum 4094 VLAN
133.	100	L2 Switch Features, 8.17	Minimum Number of Ether Channels should be 64	**Minimum Number of Ether Channels should be 32.**, The number of ports asked in the switch is 48, hence we request you to downsize it to 32 which is optimum for a 48 ports switch.	Clause modified as under: Minimum Number of Ether Channels should be 32. however bidder can quote higher system buffer to meet the SLA & uptime
134.	100	/L3 Switch Features, 9.3	Must support minimum 8K IPv4 Multicast entries	**Must support minimum 32K IPv4 Multicast entries**. 8K multicast entries are very minimal for the enterprise grade DC fabric. Suggest you to increase it to 32K so that a proper enterprise grade DC switch is quoted.	Clause stands as per RFP
135.	100	L3 Switch Features, 9.8	Must support 64-way ECMP routing for load balancing and redundancy	In spine leaf DC fabric topology with redundant spines, 64 way ECMP for Multicast traffic as a requirement would NOT come up. The number of uplink ports on leaf switches are at a maximum of 6 (from all vendors). Hence request you to change the spec as **"Must support Minimum 6-way**	Clause modified as under : Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher specification to meet the SLA & uptime.

				ECMP routing for load balancing and redundancy"	
136.	101	Multi-Cast. 10.1	Multicast: PIM-SMv2, and PIM-SSM	**Multicast: PIM-SM, and PIM-SSM.** Request you to change it to PIM-SM which is generic and widely used and accepted in the DC environment. SMv2 is supported by some specific OEMs.	Clause modified as under: Multicast: PIM-SM, and PIM-SSM
137.	101	DC Advance Feature, 13.1	Should support 4096 VxLAN. Should support both VRF and VxLAN, bridging and routing from day 1,	**Should support both VRF and VxLAN, bridging and routing from day 1. As per the spine switch there is no need to mention the number of VXLAN required.**	Clause modified as under: Should support both VRF and VxLAN, bridging and routing from day 1.
138.		Virtualization Features. 14.1	Virtualization switch should communicate with vSphere 4.0 and above, and vCenter to support adaptive network virtualization	**Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization.** We understand that Vsphere 4.0 should not be running in any of the production environment because of end of support announced long back.	Clause modified as under: Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization
139.			Request to add, Scope of work	Request to add :"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 and also act as a State-less distributed firewall with the logging capability." **Justification: The DC Fabric must have the ability to enforce security policies**	**New clause added**: Fabric must support 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 and also act as a State-less distributed firewall with the logging capability."

				to defend itself against security vulnerabilities	
140.			Request to add, Scope of work	Request to add:"Fabric must support VM attribute based zoning and policy. It must also support Micro Segmentation for the Virtualized environment" **Justification: The DC fabric must support granular control of traffic and reduce the attack surface by minimizing the possibilities for lateral movement in the event of a security breach.**	No change
141.			Request to add, Scope of work	Request to add: "The DC Fabric must provide redundant (N+1/N+2) Centralized Management Appliance based Single pane of Glass for managing, monitoring and provisioning the entire Fabric including L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager. " **Justification: A Centralized DC Fabric Management solution is necessary to simplify and automate the provisioning of the DC fabric network based on application requirements.**	No change
142.			Request to add, Scope of work	Request to add : Switch and optics from the same OEM **Justification: To ensure that OEM certified HW and optics in order to avoid any compatibility and support issues in future.**	No change

143.			Request to add, Scope of work	Request to add : All relevant licenses for all the above features and scale should be quoted along with switch **Justification: To ensure that there is no additional cost escalation in future.**	No change
144.			Spine Switch, Suggestions	Switch should support MPLS segment routing and VRF route leaking functionality from day 1 **Justification:** There are certain benefits of segment routing in the DC fabric. With Segment Routing, your network is more resilient. Whenever and wherever a node or a link fails in the network, connectivity is restored in under 50 milliseconds. Low-latency network service ensures that time-sensitive applications are always directed over the optimal low-latency path.	No change
145.			Spine Switch, Suggestions	Switch should support layer 2 extension over VXLAN (RFC7348) across all Datacenter to enable VM mobility & availability **Justification:** This gives flexibility to move VMs across DCs which will make the DC environment for agile in terms of VM placement.	No change
146.	33	Point 44	Proposed core firewall should connect with leaf switch/spine switch with minimum 100G port.	Request to reword "Proposed core firewall should connect with leaf switch/spine switch with minimum 10G port." The interface ask on the type 1 firewall is 10 G only. Please clarify and advise on this.	Clause stands as per RFP

147.	114	Point No.1	Chassis based & modular architecture for scalability & other than Checkpoint OEM.	Request to reword as "Proposed solution should be purpose built NGFW chassis based hardware & the OEM should be present in Gartner's Leader Quadrant in latest published report named "Magic Quadrant for Enterprise Network Firewalls" published in 2019." Every OEM had different hardware for different scales of throughput and so the ask should be for the purpose built appliance instead of modular architecture fulfilling the throughput ask.	Clause modified as under: Chassis based or modular architecture for scalability & other than Checkpoint OEM.
148.	114	Point no.8	Firewall performance should be minimum real world throughput 100 Gbps after enabling all function like IPS, QoS, malware protection and Anti-virus	Request to reword "Firewall performance should be minimum real world throughput 35 Gbps after enabling all function like IPS, QoS, malware protection and Anti-virus" The throughput ask of 100 Gbps is not syncing with the concurrent connections and new connections per second & the interface ask.	Clause modified as under: Firewall performance should be minimum real world throughput 60 Gbps after enabling the IPS, QoS, malware protection function. However bidder can quote higher specification to meet the SLA & uptime.
149.	114	Point No.10	Firewall should support minimum 1000,0000 concurrent connections	Request to reword "Firewall should support minimum 20,000,000 concurrent connections with application visibility turned on" The ask concurrent connection limit is very less and not inline with the throughput ask.	Clause modified as under: Firewall should support minimum 2000,0000 concurrent connections. However bidder can quote higher specification to meet the SLA & uptime.
150.	114	point No.11	Firewall should support minimum 200000 new connections per second (cps)	Request to reword "Firewall should support minimum 250,000 new connections per second (cps) with application visibility turned on" The ask new connection / pre sec limit	Clause modified as under: Firewall should support minimum 10,00,000 new connections per second (cps). However bidder

				is very less and not inline with the throughput ask.	can quote higher specification to meet the SLA & uptime.
151.	115	Point No.13	Firewall should support memory at least 8 GB Memory for better and faster processing.	Request to reword "Firewall should support memory at least 192 GB Memory for better and faster processing." Ask of 8 GB memory throughput is very less for handling 35 Gbps of traffic. 192 GB will ensure enough resources are available on system for processing the traffic.	Clause modified as under: Firewall should support memory at least 60 GB Memory for better and faster processing.
152.	116	point No.44	The solution should support the following File/Media Types for Malware identification: PDF, ZIP, 7Z, RAR, CAB, PKZIP, EXE, DLL, SYS, SCR, CPL, OCX, Java, Flash, MS office files.	Request to reword "The solution should support the following File/Media Types for Malware identification: "BAT ,.BZ2 ,.ZIP,.CHM,.DLL,.DOC, .DOCX ,.EML ,.EXE,.GZ - gzip ,.HTA ,.HWP, .HWT, .HWPX ,.ISO,PDF, ZIP,EXE, DLL,OCX, Java, Flash,JAR,JS,JSE,JTD,JTT, JTDC,JTTC,.LNK etc." The list of sample file types that are supported by every OEM sandboxing solution will be different. So requesting to consider the extended coverage for better security posture or relax this clause.	Clause modified as under: The solution should support the following File/Media Types for Malware identification: "BAT ,.BZ2 ,.ZIP,.CHM,.DLL,.DOC, .DOCX ,.EML ,.EXE,.GZ - gzip ,.HTA ,.HWP, .HWT, .HWPX ,.ISO,PDF, ZIP,EXE, DLL,OCX, Java, Flash,JAR,JS,JSE,JTD ,JTT,JTDC,JTTC,.LNK etc
153.	117	Point No.54	The solution should provide the ability to upload gold image and analyze threats under conditions of actual host environment.	Request to make this optional as this will not provide a true identification. Certain types of malware require user activity in order to launch, such as selecting a checkbox on the UI, or opening a file attachment to an email message. To emulate a user automatically during sample analysis	Clause stands as per RFP

				for which the sandboxing images are customized any modification will in turn will degrade the detection capabilities.	
154.	118	Point No.63	The proposed system shall support One-arm IDS (sniffer mode)	Request to Relax this clause. Ask if for a NGFW and not an IPS solution.	Clause stands as per RFP
155.	119	Point No.76	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero -day threats, etc.)which require license for cloud sandboxing feature with hash only	Request to reword "The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero -day threats, etc.)which require on Premises sandboxing" Cloud based sandboxing may not adhere with the BANK privacy guidelines so we would request to consider on premises sandboxing appliance. Please clarify and advise on this.	Clause stands as per RFP
156.	119	point No.82	The solution should be capable of providing network -based detection of malware by checking the disposition of known files in the cloud using the SHA -256 file -hash as they transit the network (SHA -256 and target IP address should be given to aid remediation efforts) with enabling just advance malware license if require in near future	Request to reword "The solution should be capable of providing network -based detection of malware by checking the disposition of known files in the cloud using the SHA -256 file -hash as they transit the network (SHA -256 and target IP address should be given to aid remediation efforts) all the license required for said functionality should be considered from day 1" All the feature ask in the RFP points towards protection against the	Clause modified as under: The solution should be capable of providing network -based detection of malware by checking the disposition of known files in the cloud using the SHA -256 file -hash as they transit the network (SHA -256 and target IP address should be given to aid remediation efforts) all the license required for said functionality should be considered from day 1

				malware attacks so the license for the same should be considered from day 1.	
157.	123	Point No.134	Proposed IPS should support a minimum of average inspection throughput of 10 Gbps	Request to reword "Proposed IPS should support a minimum of average inspection throughput of 35 Gbps" The throughput ask contradicts with the NGFW throughput ask in point 8 on page number 114. Additionally the point number 124-161 in type 1 NGFW starting from page 122-124 are pointing towards a dedicated IPS appliance solution and not as a part of NGFW. Please advice and clarify on this.	Clause stands as per RFP.
158.	123	Point No.136	IPS must support a minimum of 5 million concurrent connections.	Request to reword "IPS must support a minimum of 10 million concurrent connections. With application visibility turned on" The ask concurrent connection limit is very less and not in line with the throughput ask. Additionally the point number 125-163 in type 2 NGFW starting from page 133-135 are pointing towards a dedicated IPS appliance solution and not as a part of NGFW. Please advise and clarify on this.	Clause stands as per RFP.
159.	123	Point No.137	Support more than 1, 00,000 new sessions per second processing	Request to reword "Support more than 180,000 new sessions per second processing with application visibility turned on" The ask new connection /	Clause stands as per RFP.

				pre sec limit is very less and not in line with the throughput ask. Additionally the point number 125-163 in type 2 NGFW starting from page 133-135 are pointing towards a dedicated IPS appliance solution and not as a part of NGFW. Please advise and clarify on this.	
160.	125	point No.1	Chassis based & modular architecture for scalability	Request to reword as "Proposed solution should be purpose built NGFW chassis based hardware & the OEM should be present in Gartner's Leader Quadrant in latest published report named "Magic Quadrant for Enterprise Network Firewalls" published in 2019." Every OEM had different hardware for different scales of throughput and so the ask should be for the purpose built appliance instead of modular architecture fulfilling the throughput ask.	Clause modified as under: Chassis based or modular architecture for scalability & other than Checkpoint OEM.
161.	125	Point No.10	Firewall should support minimum 500,0000 concurrent connections	Request to reword "Firewall should support minimum 10,000,000 concurrent connections with application visibility turned on" The ask concurrent connection limit is very less and not inline with the throughput ask.	Clause stands as per RFP
162.	125	Point No.11	Firewall should support minimum 100000 new connections per second (cps)	Request to reword "Firewall should support minimum 180,000 new connections per second (cps) with application visibility turned on" The ask new connection / pre sec limit	Clause stands as per RFP

				is very less and not inline with the throughput ask.	
163.	125	point No.12	deliver VPN throughput minimum 300 Mbps	Request to reword "deliver VPN throughput minimum 8 Gbps" The VPN throughput ask is very less and not inline with the enterprise firewall ask.	Clause stands as per RFP
164.	126	Point No.14	Firewall should support memory at least 8 GB Memory for better and faster processing.	Request to reword "Firewall should support memory at least 192 GB Memory for better and faster processing." Ask of 8 GB memory throughput is very less for handling 35 Gbps of traffic. 192 GB will ensure enough resources are available on system for processing the traffic.	Clause modified as under: Firewall should support memory at least 60 GB Memory for better and faster processing.
165.	127	Point No.45	The solution should support the following File/Media Types for Malware identification: PDF, ZIP, 7Z, RAR, CAB, PKZIP, EXE, DLL, SYS, SCR, CPL, OCX, Java, Flash, MS office files.	Request to reword "The solution should support the following File/Media Types for Malware identification: "BAT ,.BZ2 ,.ZIP,.CHM,.DLL,.DOC, .DOCX ,.EML ,.EXE,.GZ - gzip ,.HTA ,.HWP, .HWT, .HWPX ,.ISO,PDF, ZIP,EXE, DLL,OCX, Java, Flash,JAR,JS,JSE,JTD,JTT, JTDC,JTTC,.LNK etc." The list of sample file types that are supported by every OEM sandboxing solution will be different. So requesting to consider the extended coverage for better security posture or relax this clause.	Clause modified as under: The solution should support the following File/Media Types for Malware identification: "BAT ,.BZ2 ,.ZIP,.CHM,.DLL,.DOC, .DOCX ,.EML ,.EXE,.GZ - gzip ,.HTA ,.HWP, .HWT, .HWPX ,.ISO,PDF, ZIP,EXE, DLL,OCX, Java, Flash,JAR,JS,JSE,JTD ,JTT,JTDC, JTTC,.LNK etc
166.	128	point No. 55	The solution should provide the ability to upload gold image and analyses threats under conditions of actual host environment.	Request to make this optional as this will not provide a true identification. Certain types of malware require user activity in order to launch, such as	Clause stands as per RFP

				selecting a checkbox on the UI, or opening a file attachment to an email message. To emulate a user automatically during sample analysis for which the sandboxing images are customized any modification will in turn will degrade the detection capabilities.	
167.	129	Point No.64	The proposed system shall support One-arm IDS (sniffer mode)	Request to Relax this clause. Ask if for a NGFW and not an IPS solution.	Clause stands as per RFP
168.	130	Point No.77	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero -day threats, etc.)which require license for cloud	Request to reword "The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero - day threats, etc.) which require on Premises sandboxing" Cloud based sandboxing may not adhere with the BANK privacy guidelines so we would request to consider on premises sandboxing appliance. Please clarify and advise on this.	Clause stands as per RFP
169.	133	Page No.83	The solution should be capable of providing network -based detection of malware by checking the disposition of known files in the cloud using the SHA - 256 file -hash as they transit the network (SHA -256 and target IP address should be given to aid remediation efforts) with enabling	Request to reword "The solution should be capable of providing network - based detection of malware by checking the disposition of known files in the cloud using the SHA -256 file - hash as they transit the network (SHA - 256 and target IP address should be given to aid remediation efforts) all the license required for said	Clause modified as under: The solution should be capable of providing network -based detection of malware by checking the disposition of known files in the cloud using the SHA -256 file -hash as they transit the network (SHA - 256 and target IP address should

			just advance malware license if require in near future	functionality should be considered from day 1" All the feature ask in the RFP points towards protection against the malware attacks so the license for the same should be considered from day 1.	be given to aid remediation efforts) all the license required for said functionality should be considered from day 1
170.	134	Point No.125	The proposed device should have Intrusion prevention sensors delivering a minimum of 10 Gbps of context-aware , real-world traffic inspection (enabling all functions)	Request to reword "The proposed device should have Intrusion prevention sensors delivering a minimum of 20 Gbps of context-aware , real-world traffic inspection (enabling all functions)" The throughput ask contradicts with the NGFW throughput ask in point 8 on page number 125. Additionally the point number 125-163 in type 2 NGFW starting from page 133-135 are pointing towards a dedicated IPS appliance solution and not as a part of NGFW. Please advise and clarify on this.	Clause stands as per RFP
171.	134	point No.136	Proposed IPS should support a minimum of average inspection throughput of 10 Gbps	Request to reword "Proposed IPS should support a minimum of average inspection throughput of 20 Gbps" The throughput ask contradicts with the NGFW throughput ask in point 8 on page number 125. Additionally the point number 125-163 in type 2 NGFW starting from page 133-135 are pointing towards a dedicated IPS appliance solution and	Clause stands as per RFP

				not as a part of NGFW. Please advise and clarify on this.	
172.			Additional Recommendation	Request to please consider" 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." Recommendation based on general ask by other banks referring the RFP PSB/HOIT/RFP/138/2019-20. Most ASIC-based firewall companies have developed their own custom Operating System (OS), it becomes problematic to port new applications to a custom OS. Both ASIC hardware and software designs can contain security flaws. Vulnerabilities in an ASIC design may be problematic to rapidly change and address. The customers will need to replace their ASIC hardware components (not a trivial process) or replace the entire appliance. This can be an expensive and time consuming process to correct a serious security issue. Software-based engines can use software-based updates to correct the security flaw with minimal down time and cost.	Not admissible

				Software-based firewalls can more easily be integrated with other network devices. Performance comparisons have shown that software-based products had both performance and reliability advantages over ASIC-based firewalls.	
173.			Additional Recommendation	Request to please consider "Should support more than 15,000 (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." Since IPS leverages signature to match against pattern, hence it is critical that solution should have high number of signature or extreme database.	Not admissible
174.	35	Point III	VPN concentrator must support 6 Gbps of Crypto throughput for IPSEC performance and 10000 IPSEC tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 4 no. of 10 G interface (SFP) from Day1.	Request to reword "III. VPN concentrator must support 6 Gbps of Crypto throughput for IPSEC performance and 8000 IPSEC tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 4 x 1GE interfaces and 4 no. of 10 G interface (SFP) from Day1." RFP page no. 106 under "TECHNICAL REQUIREMENTS OF VPN MODULES" point no. 57 it is mentioned 8000 IPSec tunnels whereas page no. 35 it is mentioned 10000 IPSec tunnels which is creating confusion - kindly change it	Clause modified as under: VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any

				to 8000 IPSec Tunnels and 4 x 1G & 4 x 10G Interface from Day1	point of time (at start, re-start or throughout the day)
175.	106	Point No.2	The VPN modules should be modular in architecture with a services-based hardware, Should be a single chassis solution	Request to reword "The VPN modules should be modular/fixed in architecture with a services-based hardware, Should be a single chassis/integrated solution" kindly amend the clause because when the requirement is a single chassis then that should be a fixed and integrated solution	Clause Modified as under: The VPN modules should be modular/fixed in architecture with a services-based hardware, Should be a single chassis/integrated solution
176.	106	Point No.3	VPN modules should have support for redundant Router processors /Routing engines	Request to reword "VPN modules should have support for redundant/Integrated Router processors /Routing engines" Architecture differs from OEM to OEM kindly consider Integrated Router processor	Clause stands as per RFP
177.	106	Point No.4	VPN modules should support a dedicated Service Processor card	Request to reword "VPN modules should support a dedicated Service Processor card/ESP" Architecture differs from OEM to OEM kindly consider ESP	Clause Modified as under: VPN modules should support a dedicated Service Processor card/ESP
178.	106	Point No.7	VPN modules should support system throughput of minimum 80 Gbps from day 1	Request to reword "VPN modules should support system throughput of minimum 60 Gbps from day 1" kindly amend the clause to 60 Gbps as per the requirements and other parameters 60 Gbps is more than sufficient	Clause stands as per RFP
179.	106	Point No.8	VPN modules should support minimum Traffics handling capacity of 55 Mpps	Request to reword "VPN modules should support minimum Traffics handling capacity of 40 Mpps"	Clause stands as per RFP

				kindly amend the clause to 40 Mpps as per the requirements and other parameters 40 Mpps is more than sufficient	
180.	114	Point No.12	All modules, fan trays & Power supplies should be hot swappable	Request to reword "Power supplies should be hot swappable" when high availability already asked in the solution for DC and DR then hot swappable modules and fan trays not required	Clause stands as per RFP
181.	114	Point No.17	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.	Request to reword "Hot Swap ability: The router must support on line hot insertion and removal of cards/power supply. Any insertion line card/power supply should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way." Architecture differs from OEM to OEM kindly reword the clause	Clause stands as per RFP
182.	114	Point No.19	VPN concentrator must support 6 Gbps of Crypto throughput for IPSEC performance and 10000 IPSEC tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 4 no. of 10 G interface (SFP) from Day1.	Request to reword "VPN concentrator must support 6 Gbps of Crypto throughput for IPSEC performance and 8000 IPSEC tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 4 x 1GE interfaces and 4 no. of 10 G interface (SFP) from Day1." RFP page no. 106 under "TECHNICAL REQUIREMENTS OF VPN MODULES" point no. 57 it is mentioned 8000 IPSec tunnels whereas page no. 35 it is mentioned 10000 IPSec tunnels which is creating confusion - kindly change it	Clause modified as under: VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any

				to 8000 IPSec Tunnels and 4 x 1G & 4 x 10G Interface from Day1	point of time (at start, re-start or throughout the day)
183.	114	Point No.22	Track the status of various system components like the software, services processor, line cards, fan trays, PSU etc & provide an out of band access method to the router in case of a software crash	Request to reword "Track the status of various system components like the software, services processor/line cards/fan trays/PSU etc & provide an out of band access method to the router in case of a software crash" Request to change the clause as mentioned	Clause Modified as under: Track the status of various system components like the software, services processor/line cards/fan trays/PSU etc & provide an out of band access method to the router in case of a software crash
184.	114	Point No.23	8000 VPLS instances. 4000 GRE tunnels, 14 million flows 512000 MAC addresses Should support at least 3 Million 1Pv4 and IPv6 routes.	Request to reword "8000 VPLS instances/PW per system. 4000 GRE tunnels, 2 million flows 64000 MAC addresses Should support at least 1 Million 1Pv4 and IPv6 routes." Request to make the minimum value	Clause stands as per RFP
185.	114	Point No.26	Should support RIPv1 & RIPv2, OSPF, IS-1S and BGP4, LDP, BFP routing protocols & IP multicast routing protocols: PIM , IGMP	Request to reword "Should support RIPv1 & RIPv2, OSPF, IS-1S and BGP4, LDP, BFD routing protocols & IP multicast routing protocols: PIM , IGMP" Kindly amend this clause there may be typo	Clause modified as under: Should support RIPv1 & RIPv2, OSPF, IS-1S and BGP4, LDP, BFD routing protocols & IP multicast routing protocols: PIM , IGMP
186.	114	Point No.40	Should support protection from nested applications with threat prevention	Kindly remove this clause This is the function of advanced threat prevention and not VPN Concentrator	**Clause stands deleted**
187.	114	Point No.55	Routing Table Size: The router must support minimum 2,000,000 IPv4 or 2,000,000 IPv6 routes entries in the routing table and should be scalable.	Request to reword "Routing Table Size: The router must support minimum 1,000,000 IPv4 or 1,000,000 IPv6 routes entries in the routing table and should be scalable."	Clause modified as under: Routing Table Size: The router must support minimum 10,00,000 IPv4 or 10,00,000 IPv6 routes entries in the routing table and should be scalable. However bidder can

				Request to make the minimum value to 1 Million	quote higher specification to meet the SLA & uptime.
188.	114	Point No.56	The VPN modules should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.	Request to reword "The VPN modules should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card/Integrated controller failure." Architecture differs from OEM to OEM kindly reword the clause	Clause Modified as under: The VPN modules should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high- availability during primary controller card/Integrated controller failure.
189.	114	Point No.57	VPN modules must support 6 Gbps of Crypto throughput for IPSEC performance and 8000 IPSEC tunnels from day 1 (internal/external). In case of an external box, The vpn concentrator must have redundant power supply & at least 6 x 1GE interfaces from Day 1.	Request to reword "VPN modules must support 6 Gbps of Crypto throughput for IPSEC performance and 8000 IPSEC tunnels from day 1 (internal/external). In case of an external box, The vpn concentrator must have redundant power supply & at least 4 x 1GE interfaces from Day 1." Kindly change the 1G interface to 4 x 1G and 4 x 10G Interface from Day 1	Clause modified as under: VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any point of time (at start, re-start or throughout the day)
190.	114	Point No.62-74	Point no. 62-74 of VPN MODULES	Kindly remove this clauses from point no. 62 to 74 because These points generally asking for a NGFW. URL Filtering/Proxy solution and not a VPN Concentrator	**Clause stands deleted**

191.		VPN MODULES / VPN concentrator / VPN Router suggestion	The Router OS should be at least EAL2 (Common Criteria Certificate) or above or NIAP Certified.	This point is suggested to include for Security Evaluated certified products because this is a banking environment	Clause stands as per RFP
192.		VPN MODULES / VPN concentrator / VPN Router suggestion	The Router should IPv6 Ready Logo Phase-2 certified	This point needs to be included to have IPv6 Logo certified products	Clause stands as per RFP
193.		VPN MODULES / VPN concentrator / VPN Router suggestion	OEM should be Leader/Challenger in Gartner Magic Quadrant for Wired and Wireless LAN in last consecutive 3 years (2017, 2018, 2019)	This point also needs to be included for standard products which is the requirement of the bank	This is optional requirement
194.	104-106	Point No.4	Switch should have minimum 300 Gbps Switching capacity all the services enabled on switch	Request to reword "Switch should have minimum 300 Gbps Switching capacity with Stacking & all the services enabled on switch" As per switch port numbers and switing capacity is not matching hence requesting the amend the clause	Switch should have minimum 170 Gbps Switching capacity all the services enabled on switch
195.	104-106	point No13	Must support minimum 128K IPv4 Unicast entries	Request to reword "Must support minimum 32K IPv4 Unicast entries" for a 48 port L3 switch 128K IPv4 entries is very high	Must support minimum 32K IPv4 Unicast entries. However bidder can quote higher specification to meet the SLA & uptime.

196.	104-106	point No.13	Must support minimum 64K or more IPv6 Unicast entries	Request to reword "Must support minimum 16K or more IPv6 Unicast entries" for a 48 port L3 switch 64K IPv6 entries is very high	Must support minimum 16K or more IPv6 Unicast entries. However bidder can quote higher specification to meet the SLA & uptime.
197.	104-106	Point No. 13	Must support minimum 8K ACL	Request to reword "Must support minimum 5K ACL" for a 48 port L3 switch 8K ACL is very high	Must support minimum 5K ACL. However bidder can quote higher specification to meet the SLA & uptime.
198.	104-106	Point No. 13	Must support 64-way ECMP routing for load balancing and redundancy	Request to reword "Must support ECMP routing for load balancing and redundancy"	Clause modified as under : Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher specification to meet the SLA & uptime.
199.	104-106	Point No. 20	Electrical: Frequency: 50/60 Hz Maximum Heat Dissipation: 528 BTU/hr (557.04 KJ/hr) Voltage: 100-240 Vac, rated Maximum Power Rating: 155 W	Request to reword "Electrical: Frequency: 50/60 Hz Maximum Heat Dissipation: 1194 BTU/hr Total Output BTU Voltage: 100-240 Vac, rated Maximum Power Rating: 350W Power Supply Rated Maximum" The Heat Dissipation and Power Rating mentioned should be minimum and not maximum because present days switches required higher Heat Dissipation and Power Rating	It is clarified that the supplied equipment should be compatible with tier 3 data centre environment.
200.		L3 switch suggestion	Switch OS should be at least EAL2 (Common Criteria Certificate) or above or NIAP Certified.	This point is suggested to include for Security Evaluated certified products because this is a banking environment	Clause stands as per RFP

201.		L3 switch suggestion	The Switch should IPv6 Ready Logo Phase-2 certified	This point needs to be included to have IPv6 Logo certified products	Clause stands as per RFP
202.		L3 switch suggestion	OEM should be Leader/Challenger in Gartner Magic Quadrant for Wired and Wireless LAN in last consecutive 3 years (2017, 2018, 2019)	This point also needs to be included for standard products which is the requirement of the bank	This is optional requirement
203.	11	Point 7	The proposed OEMs should have warehouse on its own/through partner in Kolkata and Bangalore.	The OEM should have Min.20 and above spares depot in India including one each in Delhi-NCR, BANGALORE and Kolkata. Bidder shall submit OEM certification which should be legally signed by the OEM legal entity	Clause stands as per RFP
204.			Additional Recommendation - for better Integration, Management & operational efficiency and cost	Spine-Leaf Switch, VPN Concentrator & L3 Switch should be from single OEM	No change
205.			Additional Recommendation	OEM must have ISO9001, ISO 14001 and ISO 27000	No change
206.			Additional Recommendation	Bidder have valid ISO 9000 / 9001, ISO 20000 and ISO 27001 certification	No change
207.			Additional Recommendation	Proposed OEM of each Category must have their own 24x7 Customer support center in operation since last five years. 24x7 Customer support center must be manned by at-least 100+ Engineers.	No change
208.	10	Eligibility		The bidder submitting the offer should have minimum average turnover of Rupees 500 Crores for the last three financial years i.e. 2016-17, 2017-18 &	Clause stands as per RFP

				2018-19. This must be the individual company turnover and not of any group of companies.	
209.		Not in the RFP	Eligibility	Bidder should have at least 20 certified professionals on their payroll with minimum two CISA/CISM/CISSP certifications, declaration from CEO/COO/CS has to be submitted.	Clause stands as per RFP
210.			Not there in the RFP	To make the contract feasible for business we request Liability should be limited up to the extent mentioned below: Neither party shall, in any event, regardless of the form of claim, be liable for any indirect, special, punitive, exemplary, speculative or consequential loss or damages. Subject to the above and to the extent allowed by local laws, the maximum aggregate liability of each party under this proposal/Contract/PO for any claim or series of claims regardless of the form of claim, damage and legal theory shall not exceed the annual value of the Contract.	Not admissible
211.	46	Clause no. 13	Selected bidder shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly	We request that the clarity be provided in the RFP that - Indemnity shall only be restricted to third party claim for (i) IPR Infringement indemnity, and (ii) bodily injury and death and tangible property damage due to gross negligence and willful misconduct. The process of	Clause stands as per RFP

			from i. an act or omission of the Vendor, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract, ii. breach of any of the terms of this RFP or breach of any representation or warranty by the Vendor, iii. use of the deliverables and or services provided by the Vendor, iv. Infringement of any patent, trademarks, copyrights etc. Or such other statutory infringements in respect of all components provided to fulfil the scope of this project. Vendor shall further indemnify the Bank against any loss or damage to the Bank premises or property, loss of life, etc., due to the acts of the Vendor's employees or representatives. The Vendor shall further indemnify the Bank against any loss or damage arising out of claims of infringement of third-party copyright, patents, or other intellectual property, and third-party claims on the Bank for malfunctioning of the equipment or software or deliverables at all points of time, provided however, i. the Bank notify the vendor in writing immediately on becoming aware of such claim, ii. the Vendor has sole control of defence and all	indemnification shall provide the requirement of notice, right to defend and settle, and the concept of apportionment (liable only to the extent of its claim), mitigation and carve-outs.	

			related settlement negotiations, iii. the Bank provides the Vendor with the assistance, information and authority reasonably necessary to perform the above, and iv. The Bank does not make any statement or comments or representations about the claim without prior written consent of the Vendor, except under due process of law or order of the court. It is clarified that the vendor shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the Bank (and/or its customers, users and service providers) rights, interest and reputation. Vendor shall be responsible for any loss of life, etc, due to acts of Vendor's representatives, and not just arising out of gross negligence or misconduct, etc, as such liabilities pose significant risk. Vendor should take full responsibility for its and its employee's actions.		
212.	45	11. Price	The Selected bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid, over the validity period of the bid.	Import Duty, Taxes etc. are levied by Honorable Government of India. Hence in case of any revision in these levies, taxes, etc., the bidder requests the bank to revise price bid after incorporating these additional costs whether upward or downward.	Clause stands as per RFP

213.		Penalties		Kindly request the bank to levy total penalties (SLA and Liquidated Damages) upto maximum of 10% of Total Contract Value of 5 years.	Clause stands as per RFP
214.		22	The complete Data Centre Fabric including but not limited to Spine & Leaf switches, SFP/QSFP, Data Centre Network Management Software, other components / software etc. should be from same OEM and should have comprehensive onsite support for the entire contract period from the date of sign-off by the Bank on completion of this project	The complete Data Centre Fabric including but not limited to Spine & Leaf switches, SFP/QSFP, Data Centre Network Management Software, other components / software etc. should be from same OEM (Excluding Type-2 firewall as mentioned as mentioned page no. 38) and should have comprehensive onsite support for the entire contract period from the date of sign-off by the Bank on completion of this project	The complete Data Centre Fabric including but not limited to Spine & Leaf switches, SFP/QSFP, Data Centre Network Management Software, other components / software etc. should be from same OEM (Excluding Type-2 firewall as mentioned page no. 38 of RFP) and should have comprehensive onsite support for the entire contract period from the date of sign-off by the Bank on completion of this project
215.		1	Chassis based & modular architecture for scalability	Chassis based & modular architecture for scalability. The operating system of the proposed firewall solution should not have any reported vulnerability in last 3 years as per Miter Vulnerability database in www.cvedetails.com.	Clause modified as under: Chassis based or modular architecture for scalability & other than Checkpoint OEM.
216.	125	8	Firewall performance should be minimum real world throughput 20 Gbps after enabling all function like IPS, QoS, and malware protection.	Firewall performance should be minimum real world throughput 20 Gbps after enabling all function like IPS, URL Filtering, QoS, Zero-day protection, and malware protection.	Clause stands as per RFP
217.	126	14	Firewall should support memory at least 8 GB Memory for better and faster processing.	Firewall should support memory at least 8 GB Memory for better and faster processing and should be scalable upto 128 GB to achieve the highest performance parameter of the proposed appliance.	Clause modified as under: Firewall should support memory at least 60 GB Memory for better and faster processing.

218.		40	Site-to-site VPN tunnels: full-mesh/ star topology shall be supported.	Site-to-site VPN tunnels: full-mesh/ star topology shall be supported with minimum 25 Gbs of overall VPN throughput.	Clause stands as per RFP
219.		55	The solution should provide the ability to upload gold image and analyses threats under conditions of actual host environment.	Kindly delete this clause.	This is optional requirement
220.		59	Solution should provide high Threat protection rate minimum of 99%.	Solution should provide high Threat protection rate. The proposed OEM must have received at-least 99% live exploit block rate in the latest NSS Labs Breach Prevention Report. .	Clause stands as per RFP
221.		84	The 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.	Please remove this clause. This clause intends to specific vendors who provides integrated network and security solution including port/os based vulnerability scanners. This feature can be easily catered by point no. 107 mentioned later in page no. 132	This is optional requirement
222.		88	The 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.	Please remove this clause. This clause intends to specific vendors who provides integrated network and security solution including port/os based vulnerability scanners. This feature can be easily catered by point no. 107 mentioned later in page no. 132	This is optional requirement
223.		99	The proposed solution should provide an option to include URL filtering for enforcing Internet content filtering so as to reduce	The proposed solution should provide an option to include URL filtering and Anti-SPAM/Mail filtering modules for enforcing Internet content filtering so	Clause stands as per RFP

			web born threats and improve productivity	as to reduce web and mail born threats and improve productivity	
224.			New Clause	The Proposed solution must be from leading security OEMs considered as leaders in the Enterprise Firewall Magic Quadrant of Gartner consistently for last 3 years.	Not admissible
225.			New Clause	The Proposed OEM must have received at least 97% recommendations in NSS Labs SVM for NGFW in last 2 years.	Not admissible
226.	43	PAYMENT TERMS	>40% of the value of new network equipment/devices/solutions/ upgradation of along with Taxes, will be paid after delivery on submission of proof of delivery. > 50% of the value network equipment/devices/solutions/ upgradation of completion of successful installation & operational, the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. The balance 10% of order value will be paid after 3 months successful running.	We request to modify the clause to: >70% of the value of new network equipment/devices/solutions/ upgradation of along with Taxes, will be paid after delivery on submission of proof of delivery. >20% of the value network equipment/devices/solutions/ upgradation of completion of successful installation & operational, the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. > The balance 10% of order value will be paid after 3 months successful running against equivalent amount of PBG.	Clause stands as per RFP

227.	13	Part-II/Clause 4/Earnest Money Deposit	The EMD will not bear any interest and EMD made by the bidder will be impounded if: d) The bidder violates any of the provisions of the terms and conditions of this tender specification.	The EMD will not bear any interest and EMD made by the bidder will be impounded if: d) The bidder violates any of the provisions of the material terms and conditions of this tender specification.	Clause stands as per RFP
228.	20	Part-II/Clause 26/	26. Acceptance of Terms A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated in the RFP.	A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated in the RFP along with the assumptions as set forth in our Bid Proposal	Clause stands as per RFP
229.	41	Part-V/Clause 4/Point d	d. Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.	d. Both the parties accept that the Monitors have the right to access all the documents relating to the project / procurement, including minutes of meetings **excluding Bidder's procurement cost.**	Clause stands as per RFP
230.	52	Part-V/Clause 24	The products & services offered to the Bank must be incompliance with all laws, regulations & Govt. guidelines of India. It also not violet any of the provisions of the IT act in anyway or any other legal provisions relating to such products or services in India.	The products & services offered to the Bank must be incompliance with all laws, regulations & Govt. guidelines of India. It also not violet any of the provisions of the IT act in anyway or any other legal provisions relating to such products or services in India. applicable to BIDDER'S SCOPE OF WORK	Clause stands as per RFP
231.	41	Part-V/Clause 5	The performance of the vendor shall be reviewed monthly, if not found satisfactory, Bank may terminate the contract at its sole discretion by giving three months' notice without assigning any reasons. Any offer falling short of	Bidder requests to delete the word Satisfactory and amend the clause as it is subjective and open ended The performance of the vendor shall be reviewed quarterly monthly, if not found satisfactory, Bank may terminate the contract for convenience after giving 90 days' notice period along	Clause stands as per RFP

			the contract period is liable for rejection.	with following: 1) Payment of for the hardware and the services rendered till the date of termination. 2) Payment of exit fee along with wind down / shut down expenses.	
232.	46	Part-V/Clause 13	13. Indemnity Selected bidder shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from i. an act or omission of the Vendor, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract, ii. breach of any of the terms of this RFP or breach of any representation or warranty by the Vendor	13. Indemnity Selected bidder shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from i. an act or omission of the Vendor, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract, ii. breach of any of the **material** terms of this RFP ~~or breach of any representation or warranty by the Vendor~~	Clause stands as per RFP
233.	49	Part-V/Clause 20	The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions: Ø Delay in offering equipments for pre-delivery Inspection; Ø Delay in delivery beyond the specified period; Ø Delay in completing installation	The wordings serious discrepancy is very open ended wordings and request bank to delete for S.No. (a) of Clause 20. 20. Exit Option and Contract Re-Negotiation: The Bank reserves the right to cancel the contract **after failing to remedy the cause beyond 30 days** in the event of happening one or more of	Clause stands as per RFP

			/ implementation of Network devices / checks beyond the specified periods;	the following Conditions: Ø Delay in offering equipments for pre-delivery Inspection & beyond any period extended by the bank; Ø Delay in delivery beyond the specified period & any period extended by the bank; Ø Delay in completing installation / implementation of Network devices /checks beyond the specified periods & any period extended by the bank;	
234.	49	Part-V/Clause 20/Point c.	c) The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favorable terms for Bank in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.	c) The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favorable terms for Bank in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality ***before contract sign off***.	Clause stands as per RFP
235.	49	Part-V/Clause 20/Point e.	e) As aforesaid the Bank would procure the equipment from the third party only in the event that the equipment was available at more favorable terms in the industry, and secondly,	e) As aforesaid the Bank would procure the equipment from the third party **before contract sign off** only in the event that the equipment was available at more favorable terms in the industry, and secondly,	Clause stands as per RFP
	51	Part-V/Clause 22	22 Termination: The Bank shall be entitled to terminate the agreement with the selected bidder at any time by giving Thirty (30) days prior written notice to the selected bidder. The Bank shall be entitled to terminate the agreement at any	22 Termination: The Bank shall be entitled to terminate the agreement with the selected bidder at any time by giving Thirty (30) days prior written notice to the selected bidder. The Bank shall be entitled to terminate the agreement at any time by giving	Clause stands as per RFP

			time by giving notice if: Ø The Selected bidder breaches its obligations under the scope document or the subsequent agreement and if the breach is not cured within 30 days from the date of notice.	notice if: Ø The Selected bidder breaches its **material** obligations under the scope document or the subsequent agreement and if the breach is not cured within 30 days from the date of notice.	
236.	44	Part-V/Clause 9/Note	In case of States having Road Permit /entry tax, the successful Bidder will have to liaison with local tax authorities at each of the locations to obtain the necessary permissions from the respective authorities. Obtaining the necessary permission will be the responsibility of the Bidder. The Bank will not arrange for any Road Permit / Sales Tax clearance for delivery of Network devices & other equipments to different locations. UCO Bank will not provide any C Form or Way Bill etc. Clearance of the equipment from Tax Authorities would be the responsibility of the bidder. Delay in delivery due to these will be considered under liquidity damage.	In case of States having Road Permit /entry tax, the successful Bidder will have to liaison with local tax authorities at each of the locations to obtain the necessary permissions from the respective authorities. Obtaining the necessary permission will be the responsibility of the Bidder. The Bank will not arrange for any Road Permit / Sales Tax clearance for delivery of Network devices & other equipments to different locations. UCO Bank will not provide any C Form or Way Bill etc. Clearance of the equipment from Tax Authorities would be the responsibility of the bidder. Delay in delivery due to these will be considered **for contract extension of time.** ~~under liquidity damage.~~	Clause stands as per RFP
237.	**47**	**New Clause**		Limitation of Liability Bidder's aggregate liability under the contract shall be limited to a maximum of the annual contract value. This limit shall not apply to third party claims for a. IP Infringement indemnity.	Clause stands as per RFP

				Neither Party shall be liable to the other Party (including under any indemnity) for any amounts in respect of: loss of revenue, loss of profit, loss of goodwill, business interruption, diminished business value, loss of anticipated savings; or for any special, incidental, indirect, exemplary, punitive or consequential damages of any party, including third parties	
238.	57	Annexure – I Tender offer forwarding letter	Until a formal contract is executed, this tender offer, together with the Bank's written acceptance thereof and Bank's notification of award, shall constitute a binding contract between us.	Until a formal contract is executed, this tender offer along with Bidder's response & assumptions set forth in it, together with the Bank's written acceptance thereof and Bank's notification of award, shall constitute a binding contract between us.	Clause stands as per RFP
239.	65	Annexure – VI Format of Bank Guarantee (EMD)	2. If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into the contract in accordance with the Terms and Conditions of the RFP or the terms and conditions mutually agreed subsequently	2. If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into a mutually agreed contract in accordance with the Terms and Conditions of the RFP or the terms and conditions mutually agreed subsequently	Clause stands as per RFP
240.	60	Annexure –III	We ……. [indicate the name of Bank ISSUING THE GUARANTEE] further agree with UCO BANK that UCO BANK shall have the fullest liberty without our consent and	Contract terms once signed cannot be varied	Clause stands as per RFP

			without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Agreement or to extend time of performance by the said VENDOR from time or to postpone for any time, or from time to time any of the powers exercisable by UCO BANK against the said VENDOR and to forebear or enforce any of the terms and conditions relating to the said agreement and we shall not be relieved from our liability by reason of any variation,		
241.	72	Annexure –IX	We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP	We hereby agree to comply with all the mutually agreed terms and conditions / stipulations as contained in the RFP	Clause stands as per RFP
242.	138	Annexure-XIX	c) Further, we hereby undertake and agree to abide by all terms and conditions and guidelines stipulated by the Bank.	c) Further, we hereby undertake and agree to abide by all mutually agreed terms and conditions and guidelines stipulated by the Bank.	Clause stands as per RFP
243.	73	Annexure - VIII	We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP	We hereby agree to comply with all the mutually agreed terms and conditions / stipulations as contained in the RFP	Clause stands as per RFP
244.	72	Annexure – IX	We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP and the related addendums and other documents including the changes made to the original tender documents if any, issued by the Bank. The Bank is not	We hereby agree to comply with all the **mutually agreed** terms and conditions / stipulations as contained in the RFP and the related addendums and other documents including the changes made to the original tender documents if any, issued by the Bank. The Bank is not	Clause stands as per RFP

			bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.	bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us **other than assumptions as set forth in our Bid response.**	
245.	149	Annexure – XXII	(d) Indemnification: The Receiving Party shall indemnify the Bank and hold the Bank harmless against any loss caused to it as a result of the non-performance or improper performance of this Agreement by the Receiving Party, or its servants or agents to perform any aspect of its obligations forming part of the subject matter of this Agreement.	Bidder had given indemnity undertaking at various places of contract and hence a specific undertaking shall not be issued separately by the Bidder	Clause stands as per RFP
246.	64	Annexure-V	We are responsible for the due performance as per the scope of work and terms & conditions as per mentioned in RFP.	We are responsible for the due performance as per the scope of work and mutually agreed terms & conditions as per mentioned in RFP.	Clause stands as per RFP
247.	13	Part-II/Clause 4	The EMD of unsuccessful bidders will be returned to them on completion of the tender process	The EMD of unsuccessful bidders will be returned to them **after 180 days of opening of the bid o**r completion of the tender process, **whichever is earlier.**	Clause stands as per RFP

248.	45	Part-V/Clause 12	Provided either party shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes. The Selected bidder or the Bank shall not be liable for delay in performing his/her obligations resulting from any Force Majeure cause as referred to and / or defined above.	Bidder requests to amend the clause to include the following at the end of the main clause: Provided either party shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes. The Selected bidder or the Bank shall not be liable for delay in performing his/her obligations resulting from any Force Majeure cause as referred to and / or defined above. **Bidder shall be excused from the performance or punctual performance of its obligations under the contract for so long as the delay is due to the act/omission of the Bank.**	Clause stands as per RFP
249.	41	5	The performance of the vendor shall be reviewed monthly, if not found satisfactory, Bank may terminate the contract at its sole discretion by giving three months' notice without assigning any reasons.	Contract shall be terminated only for serious and material breaches. We further request that the bidder should be allowed a cure period of a minimum of 30 days prior to issuance of notice of default for termination of the contract.	Clause stands as per RFP
250.	42	6	The vendor, within 15 days from the date of issue of LOI & will have to furnish a Performance Bank Guarantee, format as per Annexure-III of the RFP, issued by any scheduled commercial bank equivalent to 10% of the total cost of the Project (TCO)/Order value	1. Performance guarantee (PBG) to be provided at 10% of annual contract value and shall be renewed yearly at 10% of relevant subsequent year's contract value. 2. Customer shall invoke the PBG only on occurrence of material breach and after providing 30 days cure period to the service provider to rectify the material breach for which the PBG is sought to be invoked.	Clause stands as per RFP

251.	43	8	Payment Terms	Request for following changes into payment terms 1) Payment for Hardware shall be made 100% on delivery. 2) AMC shall be paid yearly in advance. 3) Facility Management & support cost shall be paid basis monthly in arrears.	Clause stands as per RFP
252.	49	20	The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions	Contract shall be terminated only for serious and material breaches. We further request that the bidder should be allowed a cure period of a minimum of 30 days prior to issuance of notice of default for termination of the contract.	Clause stands as per RFP. Please refer page 51 clause 22.
253.	49	20-C 20-D 20-E 20-F	The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favorable terms for Bank in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality. The Bank shall have the option of purchasing the equipment from third-party suppliers, in case such equipment is available at a lower price and the Selected Bidder's offer does not match such lower price. Notwithstanding the foregoing, the Selected Bidder shall continue to have the	Request for deletion of these clauses, as this contract will be awarded after a competitive bid process.	Clause stands as per RFP

			same obligations as contained in this scope document in relation to such equipment procured from third-party suppliers. As aforesaid the Bank would procure the equipment from the third party only in the event that the equipment was available at more favorable terms in the industry, and secondly The Equipment procured here from third parties is functionally similar, so that the Selected Bidder can maintain such equipment.		
254.	53	28	SLA Penalty	The total SLA penalty shall be capped at 5% of the monthly billing.	Clause stands as per RFP
255.	150	10	This Agreement may be terminated by either Party giving sixty (60) days' prior written notice to the other Party	Bank may terminate the contract for convenience after giving 90 days' notice period along with following: 1) Payment of for the hardware and the services rendered till the date of termination. 2) Payment of exit fee along with wind down / shut down expenses.	Clause stands as per RFP
256.	NA	NA	Additional Clause	Bidder seeks right to terminate or suspend services in the event of delay in payment of undisputed invoice.	Not admissible
257.	NA	NA	Additional Clause	All payments shall be made within 30 days from the date of invoice.	Not admissible

258.	7	Control Sheet Table	Last Date and Time for receipts of tender bids is 26/12/2019	We would request Bank to please allow minimum 3 weeks from the date of Pre-bid query response & Corrigendum published by Bank Authority. Kindly note that all the OEMs including Bidder like us are closed during December end. This is comprehensive bid. We request you to please keep the submission in the week begining 13th of January 2020.	Clause stands as per RFP
259.	10	Eligibility Criteria	The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one public sector Bank in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.	Request Bank to modify as "The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one public sector Bank/**Govt of India owned Bank**, **Financial Institute in India**. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services."	Clause modified as under: The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.
260.	11	6. Eligibility Criteria	The Bidder should be an authorized partner with the highest level of partnership with proposed OEMs at-least for the last 3 years.	Request Bank to modify as "The Bidder should be an authorized partner ~~with the highest level of partnership~~ with proposed OEMs at-least for the last 3 years."	Clause modified as under: The Bidder should be an authorized partner with proposed OEMs at least for the last 3 years
261.			Additional Recommendation	Proposed OEM of each Category must have their own 24x7 Customer support center in operation since last five years. 24x7 Customer support	Clause stands as per RFP

				center must be manned by at-least 100+ Engineers.	
262.			Additional Recommendation	All the Networking products proposed should be supported by a "Malicious code free" Declaration Letter legally vetted by the OEM	New Clause added: (under scope of work) All the Networking products proposed should be supported by a "Malicious code free" Declaration Letter legally vetted by the OEM
263.	31	Part IV - Scope of Work	23. The software & hardware quoted by bidder should not be declared as End of Sale (EOS) by the OEM at least for two years from the date of installation. In the event of the supplied equipment being declared End of Sale within the mentioned period, the bidder has to replace the equipment with equipment having equivalent or higher configurations without any additional cost to the Bank.	Request you to modify this as " The software & hardware quoted by bidder should not be declared as End of Sale (EOS) by the OEM on the date of supply. In the event of the supplied equipment being declared End of Sale within the mentioned period, the bidder has to replace the equipment with equipment having equivalent or higher configurations without any additional cost to the Bank.	Clause modified as under: The software & hardware quoted by bidder should not be declared as End of Sale (EOS) by the OEM from the date of Installation. In the event of the supplied equipment being declared End of Sale within the mentioned period, the bidder has to replace the equipment with equipment having equivalent or higher configurations without any additional cost to the Bank. The proposed device should not reach End of support/End of life during the contract period. In the event of the supplied equipment being declared End of support within the mentioned period, the bidder has to replace the equipment with equipment having equivalent or higher configurations without any additional cost to the Bank

264.	74	BILL OF MATERIAL AND PRICE SCHEDULE	FM Services 24x7x365 , DC(1 seat0 and DR(1 Seat)	Please confirm whether the resource required is L1/L2/L3 per shift and also confirm other than DC & DR do we need to deploy any additional resource at Bank's Project Office at Salk Lake	**DR** One L2 resource- **Shift 1**: 07:00 hrs to 15:00 hrs One L2 resource - **Shift 2**: 15:00 hrs to 23:00 hrs One L1 resource - **Shift 3**: 23:00 hrs to 07:00 hrs **DC** One L2 resource- **Shift 1**: 07:00 hrs to 15:00 hrs One L1 resource - **Shift 2**: 15:00 hrs to 23:00 hrs **Shift 3:** 23:00 hrs to 07:00 hrs (no resource required)
265.	31	Part IV - Scope of Work	27. The successful bidder should provide support for all the supplied devices on 24X7X365 basis and should replace the equipment within 4 hours of time, in case of any failure. (SLA penalty applicable in case of default).	Request you to remove the clause as all the devices are in cluster and individual device failure will not have any impact.	Clause stands as per RFP
266.	54	PART-V 28. SERVICE LEVEL AGREEMENT	Uptime: on monthly basis as mentioned below: DC -DR and Branch Network - Uptime SLA 99.9%	The branch Network is not in the scope of this RFP and request you to remove the same along with the associated penalties	Please refer corrigendum
267.	54	PART-V 28. SERVICE LEVEL AGREEMENT	PAYMENT AGAINST DELIVERY OF SLAS:	The % of Payment , penalty is very high and request you to kindly review the same	Clause stands as per RFP

268.	10	3. ELIGIBILITY CRITERIA	The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one public sector Bank in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.	**Request you to change the same as** "The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one public sector Bank/ RRB/State/Central Govt Organization in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.	Clause modified as under: The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.
269.		General	Limitation of Liability	**Request you to include:** Bidder's aggregate liability under the contract shall be limited to a maximum of the contract value. This limit shall not apply to third party claims for a. IP Infringement indemnity. b. Bodily injury (including Death) and damage to real property and tangible property caused by Bidder/s' gross negligence. For the purpose of this section, contract value at any given point of time, means the aggregate value of the purchase orders placed by Bank on the Bidder that gave rise to claim, under this RFP. c. Bidder shall not be liable for any indirect, consequential, incidental or	Clause stands as per RFP

				special damages under the agreement/ purchase order.	
270.	149	D. Indemnification	The Receiving Party shall indemnify the Bank and hold the Bank harmless against any loss caused to it as a result of the non-performance or improper performance of this Agreement by the Receiving Party, or its servants or agents to perform any aspect of its obligations forming part of the subject matter of this Agreement.	Request you to change the same as : "The selected bidder agrees to indemnify and keep indemnified the Bank against actual, direct and proven losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any claim for infringement of intellectual property rights. The selected Bidder agrees to indemnify and keep indemnified Bank at times against all actual, direct and proven claims, demands, actions, costs, expenses which may arise or be brought against the Bank, by third parties on account of gross negligence or deliberate failure to fulfil obligations by the selected bidder or its employees/personnel. All indemnities shall survive notwithstanding expiry or termination of Service Level Agreement and the Vendor shall continue to be liable under the indemnities. "	Clause stands as per RFP
271.	51	22. TERMINATION	Termination Rights	Request you to include" "Bidder/Service Provider may terminate this Agreement and / or any SOW upon written notice to the Bank if the Bank commits a default or material breach and does not remedy the default or material breach within 30	No change

				days of notice from the Bidder/Service Provider"	
272.	9	Point No 03, Sl No 05, Eligibility Criteria	The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one public sector Bank in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.	The Bidder must be in Core Business of IT Network services & solution for **minimum 2 years** and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one public sector Bank/**ANY Government Organization in India**. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services	Clause modified as under: The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.
273.	9	Point No 03, Sl No 06, Eligibility Criteria	The Bidder should be an authorized partner with the highest level of partnership with proposed OEMs at least for the last 3 years	The Bidder should be an authorized partner with proposed OEM	Clause modified as under: The Bidder should be an authorized partner with proposed OEMs at least for the last 3 years
274.	9	Point No 08,, Payment Terms	Bank will make the payment subject to signing of the contract as follows: Ø 40% of the value of new network equipment/devices/solutions/ upgradation of along with Taxes, will be paid after delivery on submission of proof of delivery. Ø 50% of the value network	Bank will make the payment subject to signing of the contract as follows: Ø 60% of the value of new network equipment/devices/solutions/ upgradation of along with Taxes, will be paid after delivery on submission of proof of delivery. Ø 40% of the value network equipment/devices/solutions/ upgradation of completion of successful installation & operational,	Clause stands as per RFP

			equipment/devices/solutions/ upgradation of completion of successful installation & operational, the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. The balance 10% of order value will be paid after 3 months successful running. Ø 100 % of implementation cost will be paid after successful installation & operational, the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. Ø Payment towards Facility Management & AMC will be made quarterly in arrears after issuing of necessary invoice and submission of monthly reports including SLA and after deduction of penalties if any. In case of termination	the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. . Ø 100 % of implementation cost will be paid after successful installation & operational, the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. Ø Payment towards Facility Management will be made quarterly in arrears and AMC in yearly advance after issuing of necessary invoice and submission of monthly reports including SLA and after deduction of penalties if any. In case of termination of services, the payment will be made on pro rata basis for the duration for which the services were provided.	

			of services, the payment will be made on pro rata basis for the duration for which the services were provided.		
275.	30	SCOPE OF THE WORK	18. The spine and leaf network switches in the proposed data centre fabric should be interoperable with the Bank's existing network & security devices of OEM HPE, Checkpoint and Cisco.	Request you to please share the interface details of the existing devices like HPE, Checkpoint and Cisco, so that compatible interfaces can be proposed.	Details will be shared with the successful bidder
276.	31	SCOPE OF THE WORK	25. The bidder should provide adequate training on the proposed DC fabric setup to Bank officials preferably at DC & DR.	Please clarify, how many days of training would be required and for how many users training would be required, along with the training location. Training required would be L1 / L2 / L3. Please clarify.	The same will be shared with the successful bidder
277.	32	SCOPE OF THE WORK	35. Bank has deployed various OEMs router, switches, Firewall and security devices in Bank's Intranet and the proposed DC Fabric Network, Firewalls, VPN concentrators, L3 switches should be Interoperable with these equipment.	As bidder understand scope is only for the DC & DR network and interoperability of the existing DC & DR devices. There is no scope outside DC & DR for network or anything else. Please confirm.	The device should be functional and compatible with branch/office devices.
278.	28	SCOPE OF THE WORK	1. The bidder should supply, deliver, install, configure and maintain the Data center fabric (SDN ready from day one) along with the software, hardware in Spine-Leaf architecture, Core Firewall, VPN Concentrator and other network devices (L3 Switches) as mentioned	Migration expected would be As-Is migration or it would it would be new implementation? IP addresses of the end servers and devices would change or not? Please clarify.	Clause stands as per RFP

			Annexure-XI and said seamless migration and integration with existing Network Architecture of Bank.		
279.	28	SCOPE OF THE WORK	1. The bidder should supply, deliver, install, configure and maintain the Data center fabric (SDN ready from day one) along with the software, hardware in Spine-Leaf architecture, Core Firewall, VPN Concentrator and other network devices (L3 Switches) as mentioned Annexure-XI and said seamless migration and integration with existing Network Architecture of Bank.	For migration, IP addressing would be new or existing IP addressing would be used with the servers and network devices. Please clarify.	The same shall be shared with the successful bidder
280.	41	Contract Period	SLA will cover performance and availability of the solution deployed for a period of Six years from the date of each installation and acceptance by the bank.	How would performance of the devices and network would be measured? What would be the KPI for the performance?	Based on the SLA.
281.	41	Contract Period	SLA will cover performance and availability of the solution deployed for a period of Six years from the date of each installation and acceptance by the bank.	Bank is using any tool for SLA measurement? If yes, please provide the details of the tools?	The same shall be shared with the successful bidder
282.		General Query		As per the understanding, Any integration with the branches would be out of scope. Please clarify.	The device should be configured to be used at the branches/ offices
283.		General Query		Request you to please let us know the purpose of L3 switches. Will the L3 switches part of spine and leaf architecture? Where L3 switches	L3 Switch will may be Integrated with leaf spine switches

				would be used. What sort of connectivity would terminate on L3 switches?	
284.		General Query		Request you to please share the existing network design for DC & DR along with devices details. This will help us with the efforts calculation for migration, implementation and configuration of network.	The same shall be shared with the successful bidder

3 .ELIGIBILITY CRITERIA (Part-I)

Existing Clause		
SL. No.	**Eligibility Criteria**	**(Proof of Documents required /must be submitted)**
4	The bidder must have supplied, implemented and maintaining/maintained proposed OEM's SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organisations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI in India.	Purchase order in name of bidder And execution/installation certificate from existing customer(s).
5	The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and Configuration of Data Centre Network Fabric Infrastructure in at-least one public sector Bank in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.	Purchase order in name of bidder And execution/installation certificate from existing customer(s).
6	The Bidder should be an authorized partner with the highest level of partnership with proposed OEMs at least for the last 3 years.	The bidder should submit Manufacturer Authorization Form as per format given in the RFP.
Modified Clause		
SL. No.	**Eligibility Criteria**	**(Proof of Documents required /must be submitted)**
4	The bidder must have supplied, implemented and maintaining / maintained SDN / SDN ready Data Centre Fabric of minimum 2 Spine switches & 8 Leaf switches, VPN Concentrator, Firewall and L3 Switches in minimum 2 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India.	Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted.
5	The Bidder must be in Core Business of IT Network services & solution for minimum 5 years and should have expertise in Design, Supply, Implementation and	Purchase order in name of bidder And execution/installation certificate from existing customer(s).

	Configuration of Data Centre Network Fabric Infrastructure in at-least one PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs in India. The Bidder must also have experience across diverse networking technologies i.e. Switching, Routing, Security Solutions and Network management services.	
6	The Bidder should be an authorized partner with proposed OEMs at least for the last 3 years	The bidder should submit Manufacturer Authorization Form as per format given in the RFP
11 (New Clause added)	The proposed OEM product SDN / SDN ready Data Centre Fabric of Spine switches & Leaf switches, VPN Concentrator, Firewall and L3 Switches should be running as on RFP date in minimum 1 organizations out of PSBs / Private Sector Banks/ BSE / NPCI / RBI/ PSUs/State data centers in India.	Purchase order in name of bidder And execution/installation certificate from existing customer(s) to be submitted

Scope of the Work (Part-IV)

Clause No	Existing Clause	Modified Clause
Clause no. 23	The software & hardware quoted by bidder should not be declared as End of Sale (EOS) by the OEM at least for two years from the date of installation. In the event of the supplied equipment being declared End of Sale within the mentioned period, the bidder has to replace the equipment with equipment having equivalent or higher configurations without any additional cost to the Bank.	The software & hardware quoted by bidder should not be declared as End of Sale (EOS) by the OEM from the date of Installation. In the event of the supplied equipment being declared End of Sale within the mentioned period, the bidder has to replace the equipment with equipment having equivalent or higher configurations without any additional cost to the Bank. The proposed device should not reach End of support/End of life during the contract period. In the event of the supplied equipment being declared End of support within the mentioned period, the bidder has to replace the equipment with equipment having equivalent or higher configurations without any additional cost to the Bank
Clause no. 30	The successful bidder should complete the entire project (delivery, configuration, migration of proposed DC fabric and integration with existing network architecture) within 8 weeks (for all locations) from the issuance of Purchase order. (Damages applicable in case of default).	The successful bidder should complete the entire project (delivery, configuration, migration of proposed DC fabric and integration with existing network architecture) within 12 weeks (for all locations) from the issuance of Purchase order. (Damages applicable in case of default).
Clause no. 34	OEM onsite support should be provided during the process of network devices Installation and Configuration of DC fabric and for resolution of complaints related to	If required, bidder should arrange for OEM support during the process of network devices Installation and Configuration of DC fabric and for resolution of complaints

	core components during the contract period.	related to core components during the contract period.
Clause no. 41	DC Fabric should support both IPv4 and IPv6 from day one. At present, IPv6 is not implemented in Bank's Network. Bidder need to implement IPv6 without any additional cost whenever Bank decides to implement.	DC Fabric should support both IPv4 and IPv6 from day one. At present, IPv6 is not implemented in Bank's Network. Bidder need to implement IPv6 on proposed devices in this RFP without any additional cost whenever Bank decides to implement.
Clause no. 45	Latency proposed network architecture should be less than 1 ms	The latency in-between proposed leaf, spine and Type-1 core firewall should be less than 1 Microsecond at maximum load.
Page No. 34 Spine Switch requirement Point No. (I)	Switch each with minimum 48 nos. Slot based switches along with fibre SFPs. Fibre ports should support 10G/40g/100G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M port capacity. Switch should work in High Availability (HA) Active-Active mode.	Each Switch should have minimum 32 nos. of ports along with fiber SFPs module. Fiber ports should support 10G/40g/100G port capacity. Same slots of switches should also be compatible for copper based SFPs which should support 100M/1000M port capacity. Switch should work in High Availability (HA) Active-Active mode
Page No- 35 VPN concentrator Point -III	VPN concentrator must support 6 Gbps of Crypto throughput for IPSEC performance and 10000 IPSEC tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 4 no. of 10 G interface (SFP) from Day1.	VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any point of time (at start, re-start or throughout the day)
Page No. 38 Firewall Point (t)	The Firewall should have the ability to integrate seamlessly with Active Directory, proposed PIM tool to provide complete user identification and enable application-based policy definition per user or group.	The Firewall should have the ability to integrate seamlessly with Active Directory to provide complete user identification and enable application-based policy definition per user or group.
Clause no. 47 Delivery & Installation	a) The successful bidder should complete the entire project (delivery, Installation, configuration of proposed DC fabric, Firewall, VPN devices, Switches and integration with existing network architecture) within 8 weeks (for all locations) from the issuance of Purchase order b) The bidder is responsible for transit insurance, storage, insurance upto installation at the Bank side	a) The successful bidder should complete the entire project (delivery, Installation, configuration of proposed DC fabric, Firewall, VPN devices, Switches and integration with existing network architecture) within 12 weeks (for all locations) from the issuance of Purchase order. b) The bidder is responsible for transit insurance, storage, insurance upto delivery at the Bank side.
Clause no. 48 (New clause added)		All the Networking products proposed should be supported by a "Malicious code free" Declaration Letter legally vetted by the OEM

Clause no. 49 (New Clause added)		Fabric must support 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 and also act as a State-less distributed firewall with the logging capability."
Clause no. 50 (New Clause added		Any upgrade/update of patches of the proposed network devices should be malicious free during the contract period.
Clause no. 51 (New Clause added)		**51.1)** Bidder should supply and installed required 100Gig (12 Fiber) uplink between Leaf to Spine and 10Gig for between Server to Leaf switch
		51.2) Bidder will propose the BoM for network cabling as per their active solution design
		51.3) All New servers will be placed within 12 adjacent Racks. And all existing servers will be placed within 4 nos of adjacent Racks. Maximum distance between switches will be 60Mtr
		51.4) Maximum distance between one left switch to server will be 4 adjacent rack distance. Bidder needs to factor 10G fiber cable accordingly. Maximum no of server to leaf switch connectivity will be 200 nos.

28. SERVICE LEVEL AGREEMENT (Part-V)

<table>
<tr><th>Clause No</th><th>Existing Clause</th><th>Modified Clause</th></tr>
<tr><td>III</td><td>Uptime: on monthly basis as mentioned below:
<table><tr><th>SL No</th><th>Link Category</th><th>Uptime (24X7 basis)</th></tr><tr><td>1</td><td>DC-DR and Branch</td><td>99.9 %</td></tr></table></td><td>Uptime: on monthly basis as mentioned below:
<table><tr><th>SL No</th><th>Locations</th><th>Uptime (24X7 basis)</th></tr><tr><td>1</td><td>DC & DR</td><td>99.9 %</td></tr></table></td></tr>
</table>

29. LIQUIDATED DAMAGE (Part-V)

Existing Clause
Any delay in delivery/installation/commissioning/shifting/upgradation of the link/device/equipment/ solution beyond the stipulated time period as per clause no. 5.3, Bank will charge penalty at 1 % of the order value for that device/equipment/implementation cost per week or part thereof, subject to a maximum of 10%. The bank may at its discretion also waive or reduce the penalty if the reasons for delay are considered to be justified. After elapsing of stipulated time period including 8 Weeks Liquidated damages period, if selected bidder fails to implement, the order will be deemed cancelled after imposing necessary penalty amount and bank will place the order to any other selected bidder. If Bidder fails to commission the link as per feasibility report (this includes change of media) 10% of the link cost will be deducted from payment of other link or from Performance Bank Guarantee and bank will place the order to any other selected bidder.
Modified Clause
Any delay in delivery/installation/ commissioning/shifting/upgradation of the device/equipment/ solution beyond the stipulated time period as per clause no. 47, Bank will charge penalty at 1 % of the order value for that device/equipment/implementation cost per week or part thereof, subject to a maximum of 10%. The bank may at its discretion also waive or reduce the penalty if the reasons for delay are considered to be justified. After elapsing of stipulated time period including 12 Weeks Liquidated damages period, if selected bidder fails to implement, the order will be deemed cancelled after imposing necessary penalty amount & Bank will deduct the same from Performance Bank Guarantee or from any outstanding payment.

BILL OF MATERIAL AND PRICE SCHEDULE
(TO BE SUBMITTED WITH TECHNICAL BID)

Component of Network devices:

Sl. No.	Description	Unit		Make	Model and Part no. (Device and AMC)
		DC	DR		
1	Minimum 32 Port Spine Switches with Fiber module	2	2		
2	48 Port Leaf Switches-(Copper) with copper port module if any	2	2		
3	24 Port Leaf Switches-(Copper) with copper port module if any	6	6		
4	48 Port Leaf Switches-(Fiber) with Fiber module	6	6		
5	Firewall (HA) –Type 1	1 pair	1 pair		
6	Firewall (HA)- Type 2	1 pair	2 pair		
7	VPN Concentrator (HA)	1 pair	1 pair		
8	L3 Switches	2	6		
9	Network Cabling	As required	As required		
10	FM Services 24x7x365	1(Seat)	1(Seat)		
11	AMC of minimum 32 Port Spine Switches with Fiber module	2	2		
12	AMC of 48 Port Leaf Switches-(Copper) with copper port module if any	2	2		
13	AMC of 24 Port Leaf Switches-(Copper) with copper port module if any	6	6		
14	AMC of 48 Port Leaf Switches-(Fiber) with Fiber module	6	6		
15	AMC of Firewall (HA) –Type 1	1 pair	1 pair		
16	AMC of Firewall (HA)- Type 2	1 pair	2 pair		
17	AMC of VPN Concentrator (HA)	1 pair	1 pair		
18	AMC of L3 Switches	2	6		
19	AMC of Network Cabling	As required	As required		

COMMERCIAL TEMPLATE

Table A Devices Cost with 3 Years Warranty & Implementation Cost								
Sl. No.	**Description**	**Qty. (A)**		**Make**	**Model and device part no**	**Unit Price without tax (B)**	**Tax (C)**	**Total Price with Tax D= (AxB)+C**
		DC	**DR**					
1	Minimum 32 Port Spine Switches with Fiber module	2	2					
2	48 Port Leaf Switches-(Copper) with copper port module if any	2	2					
3	24 Port Leaf Switches-(Copper) with copper port module if any	6	6					
4	48 Port Leaf Switches-(Fiber) with Fiber module	6	6					
5	Firewall (HA)- type 1	1 pair	1 pair					
6	Firewall (HA)- type 2	1 pair	2 pair					
7	VPN Concentrator (HA)	1 pair	1 pair					
8	L3 Switches	2	6					
9	Network Cabling	As required	As required					
10	Additional devices/Items required for the compliance of the scope of work as per the Annexure –XVI, if any.							
11	Implementation Cost	All supplied devices with network cabling	All supplied devices with network cabling					
Sub Total of Table A								

Table B 4th & 5th Year Comprehensive AMC										
Sl. No.	Description	Unit (A)		Make	Model and AMC part no	4th year AMC Unit Price (B)	Tax (c)	5h year AMC Unit Price (D)	Tax (E)	Total Price with tax F=A(B+D)+C+E
		DC	DR							
1	Minimum 32 Port Spine Switches with Fiber module	2	2							
2	48 Port Leaf Switches-(Copper) with copper port module if any	2	2							
3	24 Port Leaf Switches-(Copper) with copper port module if any	6	6							
4	48 Port Leaf Switches-(Fiber) with Fiber module	6	6							
5	Firewall (HA)- type 1	1 pair	1 pair							
6	Firewall (HA)- type 2	1 pair	2 pair							
7	VPN Concentrator (HA)	1 pair	1 pair							
8	L3 Switches	2	6							
9	Network Cabling	As required	As required							
10	Additional devices/Items required for the compliance of the scope of work as per the Annexure –XVI, if any.									
Sub Total of Table B										

Table C FM Services 24x7x365 (1 seat) for 5 years			
SL No	**Years**	**Tax**	**Total price With Tax**
1	1st year		
2	2nd Years		
3	3rd Years		
4	4th Year		
5	5th Year		
Sub Total of Table C			

Table D Total Project Cost (TCO)	
Sub Total of Table A (Devices Cost with 3 Years Warranty & Implementation Cost)	
Sub Total of Table B (4th & 5th Year Comprehensive AMC)	
Sub Total of Table C (FM Server 24x7x365 (1 seat) for 5 years)	
Total Project Cost (TCO) = (Sub Total of Table A+ Sub Total of Table B +Sub Total of Table C)	

Note:

1. The calculation for arriving at TCO is properly mentioned in the appropriate columns and we confirm that the above mentioned rates are accurate. In case of any anomalies in the calculation for arriving at TCO, the Bank will have the right to rectify the same and it will be binding upon our company.

2. If the cost for any line item is indicated as zero or blank then Bank may assume that the said item is provided to the Bank without any cost.
3. Bank has discretion to keep any of the line item mentioned above as optional as per Bank's requirement.
4. We have ensured that the price information is filled in the Commercial Offer at appropriate column without any typographical or arithmetic errors. All fields have been filled in correctly.
5. We have not added or modified any clauses/ statements/ recordings/ declarations in the commercial offer, which is conditional and/or qualified or subjected to suggestions.
6. We have not added or modified any clauses/ statements/ recordings/ declarations in the commercial offer, which contain any deviation in terms & conditions or any specification.
7. We have understood that in case of non-adherence to any of the above, our offer will be summarily rejected.
8. In case of any discrepancy between figures and words, the amount in words shall prevail.
9. Please note that any Commercial offer which is conditional and/ or qualified or subjected to suggestions will also be summarily rejected. This offer shall not contain any deviation in terms & condition or any specifications, if so such offer will be summarily rejected.
10. All prices should be quoted in (INR) only.
11. The TCO (Total cost of ownership) will be inclusive of GST and other applicable taxes. However the GST and other applicable taxes will be paid as per actuals at time of billing.
12. **While TCO shall be used by the Bank to discover L1 bidder, Order may be placed for all or selected line items mentioned above on the L1 bidder price.**

Place:
Date:

AUTHORISED SIGNATORY
Name:
Designation:

TECHNICAL REQUIREMENTS

SPINE SWITCH REQUIREMENTS

SL. No.	Feature Description	Compliance Yes/No
1	**Architecture**	
1.1	The Solution should support logical device separation for each individual server farm infrastructure at zone level (No Virtualization / No Virtual Chassis /Stacking), Zone details as per current setup (3 zones - Non-prod servers, Tandem and CBS). It should support minimum 8 zones	
1.2	The proposed switching system/solution should be of modular chassis with redundancy / high availability for control and Data plane.	
2	**Performance**	
2.1	Spine Switches must have adequate number of line rate 40G/100G ports to support desired Leaf Scale. Each Leaf connects to Each Spine using minimum 1 x 100 G ports connectivity i.e. Each Spine must have minimum 32 nos. of line rate 40G/100G ports minimum scalable to 64 nos. with consideration of leaf to SPINE over subscription ratio of 3:1 or more	
2.2	Should support minimum 5 Tbps switching capacity/throughput or more	
2.3	Switch must support at least 32 or more wire-speed 40/100 GBE ports.	
2.4	Switch must at least 2 BPPS or more wire-speed L2 & L3	
2.5	Switch must support Non-blocking architecture	
2.6	Switch must support QSFP of 40/100 GBE capacity	
2.7	Should support 40G/100 GBE long range and short range QSFPs.	
2.8	Switch must support for different logical interface types like loopback, VLAN, SVI/RBI, Port Channel/LAG, multi chassis port channel etc.	
2.9	Switch must support VLAN tagging (IEEE 802.1q)	
2.10	Switch should support IEEE Link Aggregation or Ethernet Bonding	
2.11	The switch should support hardware based load-balancing at wire speed using LACP and multi chassis ether-channel/LAG	
2.12	Switch should have wire rate switching capacity including the services:	
2.13.1	Switching	
2.13.2	IP Routing (Static/Dynamic)	
2.13.3	IP Forwarding	
2.13.4	Policy Based Routing	
2.13.5	QoS	
2.13.6	ACL and Global Control Plane Policing	
2.13.7	IP V6 host and IP V6 routing	
2.14	Should support minimum of 64 VRFs or more	
3	**Port Requirements with redundancy**	
3.1	Minimum 32 no. of 40G/100G QSFP based Fiber ports per switch	
3.2	Should support at least 32 or more wire-speed 40/100 GBE ports.	

3.3	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	
4	**Switch Hardware features and High availability**	
4.1	Switch should be rack mountable and support side rails, if required	
4.2	Switch should have redundant power supply and fans for High availability.	
4.3	Should support both front to back and back to front reversible air flow	
4.4	Switch should support in-line hot insertion and removal of different parts like modules/ power supplies/ fan tray etc. and should not require switch reboot & should not disrupt the functionality of the system	
4.5	Switch should support for BFD For Fast Failure Detection as per RFC (5880)	
4.6	Switch should support Graceful Restart for OSPF, BGP etc.	
4.7	The proposed switch should not be more than 11 Rack Units in size	
4.8	The proposed switch must have Redundant Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies.	
4.9	Switch should have redundant fan modules with hot swappable support.	
4.10	The proposed switch must have Line-rate traffic throughput on all ports at Layer 2 with non-blocking architecture.	
4.11	The proposed switch must have Line-rate traffic throughput on all ports at Layer 3 with non-blocking architecture	
4.12	The Proposed switch should support FCOE(Desirable) and DCB center bridging feature.	
5	**Scalability**	
5.1	The proposed switch should support minimum 90K MAC address table entries.	
5.2	The proposed switch must allow to build very large L2 domain using logical chassis or virtual logical chassis to support Multi-Path Ethernet technologies across multiple switches.	
5.3	The proposed switch must support port channelling across multiple switches	
6	**Resilient Control Plane**	
6.1	Minimum Quad Core x86 CPU or equivalent	
6.2	Minimum 8 GB DRAM	
6.3	Minimum 8GB Flash	
6.4	Minimum System buffer of 32 MB	
7	**Operating System**	
7.1	Should support modern modular operating system designed for data center scalability and reliability	
7.2	Should support auto process recovery from failures	
7.3	Should support Health monitoring and self-healing	
7.4	Should support Single Operating System binary image for all switch models	
7.5	Should support Industry standard CLI	
8	**Layer 2 Switch features**	
8.1	Must support IEEE 802.1d - Spanning-Tree Protocol, IEEE 802.1w - Rapid Spanning Tree, IEEE 802.1s - Multiple Spanning Tree Protocol and IEEE 802.1q - VLAN encapsulation with 4096 VLANs	
8.2	Should support up to 32 ports per Link Aggregation Group (LAG)	

8.3	Should support 64 Link Aggregation Groups (LAG)	
8.4	Should support Port Mirroring	
8.5	Should support Jumbo Frames 9216 Bytes	
8.6	Should support 64 ports active/active layer2/Layer3 multi-path Redundancy	
8.7	Should support active/active layer-2 topology without STP where host are dual homed to switch	
8.8	The proposed switch should support VXLAN (Bridging and Routing) and NVGRE overlay encapsulation protocol (desirable) in hardware to support multiple hypervisor deployment in the Data Centre. Minimum 4096 VXLAN should be supported.	
8.9	The proposed switch should support GRE (Generic routing encapsulation) Tunnel (desirable)	
8.10	The proposed switch should support BFD (Bidirectional Forwarding detection)	
8.11	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP) with up to 16 port channel, IEEE 802.1ab - Link Layer Discovery Protocol (LLDP) and IEEE 802.3x Flow Control	
9	**Layer 3 Switch features**	
9.1	The proposed switch must support Static IP routing, OSPF (RFC2328),IS-IS, BGPv4 (RFC 1771) and Policy Base Routing.	
9.2	The proposed switch must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP) , and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)	
9.3	The proposed switch must support Interior Gateway Management Protocol (IGMP) v2/v3 snooping groups	
9.4	The proposed switch should support Virtual Route forwarding (VRF) functionality with minimum 64 VRF support	
9.5	The proposed switch Must support minimum 128k IPV4 routes and 100k IPV6 routes	
9.6	Switch should support First Hop Routing protocols like VRRP or Equivalent	
9.7	The proposed switch must have minimum 100 Ether Channel support	
9.8	Switch must be able to load balance across a logical bundle using the following algorithms:	
9.9.1	Source IP	
9.9.2	Destination IP	
9.9.3	Source and Destination IP	
9.9.4	Source MAC	
9.9.5	Destination MAC	
9.9.6	Source and Destination MAC	
9.9.7	TCP Port (destination and/or source)	
9.9.8	UDP Port (destination and/or source)	
9.10	Must support 128K IPv4 Unicast entries	
9.11	Must support 100K or more IPv6 Unicast entries	
9.12	Must support 10K IPv4 Multicast entries	

9.13	Must support minimum 5K ACL	
9.14	Must support 64-way ECMP routing for load balancing and Redundancy	
9.15	Must support OSPF v2 with MD5 auth, BGP v4 with MD5 auth, ISIS using MD5 Authentication and MP BGP	
9.16	Must support PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP) multicast routing, IGMP V.1, V.2 and V.3	
9.17	Must support Route Maps	
9.18	Must support Anycast RP	
10	**Security features**	
10.1	Switch must support Remote Authentication Dial-In User Service (RADIUS), Privilege Identity Management(PIM) and Terminal Access Controller Access Control System Plus (TACACS+)	
10.2	Must support ACLs (Standard & Extended) on Ethernet and virtual Ethernet ports using Layer 2, Layer 3 and Layer 4 fields.	
10.3	Must support Standard and extended Layer 2 ACLs: MAC addresses, protocol type, etc.	
10.4	Must support Standard and extended Layer 3 to 4 ACLs: IPv4 and v6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP), etc.	
10.5	Must support VLAN based ACLs (VACLs) and Port-Based ACLs (PACLs)	
10.6	Should Support MAC Security	
11	**QoS features**	
11.1	Switch must have Egress strict-priority queuing	
11.2	Up to 8 queues per port	
11.3	802.1p based classification	
11.4	Switch must have ACL-based QoS classification (Layers 2, 3, and 4)	
11.5	DSCP based qualification and remarking	
11.6	Rate limiting	
11.7	Switch must support for different type of QoS features for real time traffic differential treatment using	
11.7.1	a. Weighted Random Early Detection	
11.7.2	b. Strict Priority Queuing	
11.8	The proposed switch must support minimum 32 MB packet buffer to avoid packet drops due to buffer queue entries are exhausted which results in poor and unpredictable performance	
11.9	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
12	**Data Centre Advanced Feature and Network Virtualization**	
12.1	Should support VRF,VxLAN, routing and bridging from day 1.	
12.2	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN	
12.3	Switch should support VXLAN and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center	
12.4	Switch should support Data Center Bridging	

12.5	Switch must have support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically, using orchestration layer from Day 1	
13	**Virtualization and Next Gen DC features**	
13.1	Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization	
13.2	VLAN auto provision - Auto create/configure VM VLAN when new VM is created in vCenter	
13.3	VM Auto Discovery – Find exactly which ESX Hosts and VMs are on a given port in the network. Displays the full Physical Port to Virtual Switch to VM Binding.VM Auto Discovery – Find exactly which ESX Hosts and VMs are on a given port in the network. Displays the full Physical Port to Virtual Switch to VM Binding on the supplied management software GUI.	
13.4	Should Dynamically create VLAN policy based on VM movement.	
13.5	Should be able to extract vNIC information from the VM Host and must be able to display the VM to vNIC to Switch mapping in the proposed management software GUI.	
14	**Management features**	
14.1	Switch must provide management using 10/100/1000-Mbps management or console ports	
14.2	Switch must have In-band switch management as well	
14.3	Switch must Support RS-232 serial console port	
14.4	Switch must Support USB port	
14.5	Switch must support Management over IPv4, IPv6	
14.6	Switch must have Configuration rollback feature	
14.7	Switch must support DHCP Snooping	
14.8	Switch must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3	
14.9	Switch should support Open Stack to support orchestration in future	
14.10	Switch must support DHCP Syslog	
14.11	Switch must support AAA	
14.12	Switch must support sFlow / NetFlow - industry standard technology for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defense against security threats	
14.13	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
14.13.1	a. SNMP V1 and V.2	
14.13.2	b. SNMP V3 with encryption	
14.13.3	c. Filtration of SNMP using Access list	
15	**Troubleshooting capabilities**	
15.1	Switch must support for basic administrative like Ping and Traceroute	
15.2	Switch must support built in TCP Dump or Wireshark trouble shooting tool or equivalent	

15.3	Switch should be integrated with Security Information and Event Management (SIEM)server. Also should support multiple centralized syslog server, for monitoring and audit trail.	
15.4	Switch should support central time server synchronization using Network Time Protocol NTP V.4	
15.5	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	
15.6	Switch should provide different privilege for login in to the system for monitoring and management	
15.7	Protection from unnecessary or DoS traffic by using storm control functions for unicast/multicast/broadcast.	
15.8	Switch should support spanning tree root guard	
15.9	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
16	**Standards Compliance**	
16.1	Must Support IEEE 802.1D Bridging and Spanning Tree	
16.2	Must Support IEEE 802.1p QOS/COS	
16.3	Must Support IEEE 802.1Q VLAN Tagging	
16.4	Must Support IEEE 802.1w Rapid Spanning Tree	
16.5	Must Support IEEE 802.1s Multiple Spanning Tree Protocol	
16.6	Must Support IEEE 802.1AB Link Layer Discovery Protocol	
16.7	Must Support IEEE 802.3ad Link Aggregation with LACP	
16.8	Must Support IEEE 802.3x Flow Control	
16.9	Must Support IEEE 802.3ba 40/100Gigabit Ethernet	
17	**Monitoring and Provisioning**	
17.1	Must support Advance Event Management or equivalent for pro- active network monitoring	
17.2	Must support Restoration of Operating System & Configuration from USB	
17.3	Must support CLI scheduler, Shell script, for timed automation, and event manager for triggered automation.	
17.4	Must support sFlow or Netflow or equivalent	
17.5	Must support centralized script/system to configure a switch without user intervention	
18	**Miscellaneous**	
18.1	Switch should support the complete STACK of IP V4 and IP V6 services	
18.2	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied.	
18.3	Switch should support Configuration roll-back and check point	
18.4	Switch should support for BFD For Fast Failure Detection as per RFC (5880)	
18.5	The transceivers should be from same OEM of the proposed switch	
19	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
20	Solution should integrate seamlessly with Bank's existing network Infrastructure.	

21	Proposed Solution should have 3 years warranty & 2 years of comprehensive AMC service. Product must not be End of Life and Support during 5 years of contract period. If offered product declared End of Life and Support within 5 years contact period, then bidder should provide latest product with same specification or higher without any cost to the Bank. Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period.	

LEAF SWITCH (COPPER) REQUIREMENTS

SL. No.	Feature Description	Compliance Yes/No
1	**Architecture**	
1.1	The Solution should support in co-ordination with spine switch. Zones and segments should be decided by spine switch and same should be reflected on Leaf switches.	
1.2	1RU fixed form factor	
2	**Performance**	
2.1	Switch should support Min 1.5 Tbps switching capacity/throughput or more	
2.2	Switch should support at least 1 Billion packets per second	
2.3	Should support Non-blocking architecture and wire-speed Layer-2 and Layer-3 forwarding	
2.4	Should support fixed 1G/10G copper ports	
2.5	The switch should support minimum 1,00,000 IPv4 and IPv6 routes entries in the routing table including multicast routes. However bidder can quote higher specification to meet the SLA & uptime	
2.6	Minimum Multicast Routing table – 8000	
2.7	Switch should have management interface for Out of Band Management	
2.8	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP	
2.9	Switch should support IEEE Link Aggregation or Ethernet Bonding functionality to group multiple ports for redundancy	
2.10	Switch should support Configuration roll-back and check point	
2.11	Switch should support for different logical interface types like loopback, VLAN, SVI/RBI, Port Channel/LAG, multi chassis port channel etc.	
2.12	Line-rate traffic throughput (both Layer 2 and 3) on all ports	
3	**Port Requirements with redundancy**	
3.1	Switch should have Type 1- 48 ports or more, capable of 1/10 Gbps ports Type2- 24 48 ports or more, capable of 1/10 Gbps ports	
3.2	Must support at least 24/48 or more wire-speed 10G ports	
3.3	Must have 4 or more no. of 40G/100G QSFP based Fibre ports per switch for uplinks with spine switch	

3.4	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	
4	**Switch Hardware features and High availability**	
4.1	Switch should be rack mountable and support side rails, if required	
4.2	The proposed switch must have Redundant Power Supply Units (PSUs),Hot-swappable, field-replaceable power supplies.	
4.3	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant	
4.4	Should support both front to back and back to front reversible air flow	
4.5	Switch should support in-line hot insertion and removal of different parts like modules/ power supplies/ fan tray etc. and should not require switch reboot & should not disrupt the functionality of the system	
4.6	Switch should support for BFD For Fast Failure Detection as per RFC (5880)	
4.7	Switch should support Graceful Restart for OSPF, BGP etc.	
4.8	The proposed switch should be of 1 Rack Units in size	
4.9	The proposed switch should support FCOE (Fiber channel over Ethernet) and DCB (Data Center bridging) features (Desirable)	
4.10	The proposed switch must have Line-rate traffic throughput on all ports at Layer 2 with non-blocking architecture.	
4.11	The proposed switch must have Line-rate traffic throughput on all ports at Layer 3 with non-blocking architecture	
5	**Scalability**	
5.1	The proposed switch should support minimum 90K MAC address table entries.	
5.2	The proposed switch must allow to build very large L2 domain using logical chassis or virtual logical chassis to support Multi-Path Ethernet technologies across multiple switches.	
5.3	The proposed switch must support port channeling across multiple switches	
6	**Control Plane**	
6.1	Minimum Dual Core x86 CPU or equivalent	
6.2	Minimum 8GB DRAM	
6.3	Minimum 4GB Flash	
6.4	Minimum System buffer 16 MB	
7	**Operating System**	
7.1	Must support modern modular operating system designed for data center scalability and reliability.	
7.2	Must support auto process recovery from failures.	
7.3	Must support Health monitoring and self-healing.	
7.4	Must support Live patching or hitless upgrade without disruption of other processes/system modules while upgrading operating system.	
7.5	Must support Industry standard CLI.	
8	**Layer 2 Switch features**	
8.1	Minimum Number of MAC addresses entries 90K	
8.2	Spanning Tree Protocol (IEEE 802.1.D, 802.1W, 802.1S)	

8.3	must support IEEE 802.1Q VLAN encapsulation	
8.4	Must support minimum 4096 VLAN	
8.5	Internet Group Management Protocol (IGMP) Versions1, 2 and 3	
8.6	Should support Rapid Per VLAN Spanning Tree (RPVST+)	
8.7	Must support Link aggregation LACP: IEEE 802.3ad with up to 16 ports/channels	
8.8	Must support up to 32 ports per Link Aggregation Group (LAG)	
8.9	Must support 100 Link Aggregation Groups (LAG)	
8.10	Must support 64 ports active/active layer2/Layer3 multi-pathing Redundancy	
8.11	Must support 64 ports active/active layer2/Layer3 multi-pathing Redundancy	
8.12	Must support 802.1AB Link Layer Discovery Protocol (LLDP)	
8.13	Must support Port Mirroring	
8.14	Must support 802.3x Flow Control	
8.15	Configurable maximum transmission units (MTUs) of up to 9216 bytes (jumbo frames)	
8.16	Must support active/active layer-2 topology without STP where host are dual homed to switch using vPC or MLAG	
8.17	Minimum Number of EtherChannels should be 64	
8.18	Advanced Ether Channel hashing based on Layer 2, 3, and 4 information	
9	**Layer 3 Switch features**	
9.1	Must support minimum 128K IPv4 Unicast entries	
9.2	Must support minimum 16K or more IPv6 Unicast entries	
9.3	Must support minimum 8K IPv4 Multicast entries	
9.4	Must support minimum 5K ACL	
9.5	Must support basic layer-3 routing – static routes, BGP, OSPF, ISIS	
9.6	VRF: VRF-lite (IP VPN), VRF-aware unicast (BGP, OSPF, and RIP), and VRF-aware multicast	
9.7	Must support VRRP or equivalent	
9.8	Must support 6-way ECMP routing for load balancing and redundancy	
9.9	Must support Route Maps	
9.10	Must support Anycast RP	
10	**Multi-Cast**	
10.1	Multicast: PIM-SMv2, and PIM-SSM	
10.2	Bootstrap router (BSR) and Static RP	
10.3	Multicast Source Discovery Protocol (MSDP) and Anycast RP	
11	**Security features**	
11.1	Must Support ACLs using Layer 2, Layer 3, Layer 4 fields	
11.2	Must Support MAC Security	
11.3	Should Support Privilege Identity Management(PIM), TACACS+&RADIUS	
11.4	Should Support SNMP v2, v3 with encryption	
11.5	Switch should support DHCP Snooping (Desirable)	
11.6	Must Support SIEM and Syslog	
11.7	Must Support AAA	

11.8	Must Support Port Mirroring	
11.9	Must Support sFlow / netFlow industry standard technology for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defense against security threats	
11.10	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail	
11.11	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces	
11.12	Storm control (unicast, multicast, and broadcast)	
11.13	CoPP (Control plane protection)	
11.14	Switch should provide different privilege for login in to the system for monitoring and management	
12	**QoS features**	
12.1	Switch must have Egress strict-priority queuing	
12.2	8 hardware queues per port and should support per port QOS Configuration	
12.3	802.1p based classification (COS)	
12.4	Switch must have ACL-based QoS classification (Layers 2, 3, and 4)	
12.5	DSCP based qualification and remarking	
12.6	Rate limiting	
12.7	Switch must support for different type of QoS features for real time traffic differential treatment using	
12.8	a. Weighted Random Early Detection	
12.9	b. Strict Priority Queuing	
12.10	The proposed switch must support minimum 16 MB packet buffer to avoid packet drops due to buffer queue entries are exhausted which results in poor and unpredictable performance	
12.11	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
13	**Data Centre Advanced Feature and Network Virtualization**	
13.1	Should support 4096 VxLAN. Should support both VRF and VxLAN, bridging and routing from day 1,	
13.2	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN	
13.3	Switch should support VXLAN and EVPN or equivalent for supporting Spine-Leaf architecture to optimize the east - west traffic flow inside the data center	
13.4	Switch should support Data Center Bridging	
13.5	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically, may orchestation layer from day 1	
14	**Virtualization features**	
14.1	Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization	
14.2	VLAN auto provision - Auto create/configure VM VLAN when new VM is created in vCenter	

14.3	VM Auto Discovery – Find exactly which ESX Hosts and VMs are on a given port in the network. Displays the full Physical Port to Virtual Switch to VM Binding on the supplied management software GUI.	
14.4	Should Dynamically create VLAN policy based on VM movement.	
14.5	Should be able to extract vNIC information from the VM Host and must be able to display the VM to vNIC.	
14.6	VmWare Multi-Tenancy – Connecting up to 4 separate vCenter administrative domain.	
15	**Management features**	
15.1	Zero Touch provisioning of firmware and configuration of the switch to reduce provisioning time.	
15.2	Switch should have console port	
15.3	Must have 100/1000 management port	
15.4	Must Support USB port	
15.5	Must Support Management over IPv4, IPv6	
15.6	Switch should provide remote login for administration using:	
15.6.1	a. Telnet	
15.6.2	b. SSHV2	
15.7	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
15.7.1	a. SNMP V1 and V.2	
15.7.2	b. SNMP V.3 with encryption	
15.7.3	c. Filtration of SNMP using Access list	
15.8	Switch should support for basic administrative tools like:	
15.8.1	a. Ping	
15.8.2	b. Traceroute	
15.9	Should support built in TCP Dump or Wireshark trouble shooting tool or equivalent	
15.10	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
15.11	Switch should support central time server synchronization using Network Time Protocol NTP	
16	**Troubleshooting capabilities**	
16.1	Switch must support for basic administrative like Ping and Traceroute	
16.2	Switch must support built in TCP Dump or Wireshark trouble shooting tool or equivalent	
16.3	Switch must support for sending logs to multiple centralised syslog server for monitoring and audit trail	
16.4	Switch should support central time server synchronization using Network Time Protocol NTP V.4	
16.5	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	
16.6	Switch should provide different privilege for login in to the system for monitoring and management	
16.7	Protection from unnecessary or DoS traffic by using storm control functions for unicast/multicast/broadcast.	

16.8	Switch should support spanning tree root guard	
16.9	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
16.10	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
16.11	Configuration rollback and NTP Support	
16.12	Must have XML Support	
17	**Standards Compliance**	
17.1	Should Support IEEE 802.1D Bridging and Spanning Tree	
17.2	Should Support IEEE 802.1p QOS/COS	
17.3	Should Support IEEE 802.1Q VLAN Tagging	
17.4	Should Support IEEE 802.1w Rapid Spanning Tree	
17.5	Should Support IEEE 802.1s Multiple Spanning Tree Protocol	
17.6	Should Support IEEE 802.1AB Link Layer Discovery Protocol	
17.7	Should Support IEEE 802.3ad Link Aggregation with LACP	
17.8	Should Support IEEE 802.3x Flow Control	
17.9	Should Support IEEE 802.3ab 1000BASE-T	
17.10	Should Support IEEE 802.3z Gigabit Ethernet	
17.11	Should Support IEEE 802.3ae 10 Gigabit Ethernet	
17.12	Should Support IEEE 802.3by 25 Gigabit Ethernet (desirable)	
18	**Monitoring and Provisioning**	
18.1	Should support Advance Event Management for pro-active network monitoring or equivalent	
18.2	Should support Restoration of Operating System & Configuration from USB	
18.3	The platform should the capability to collect telemetry information at line rate across all the ports without adding any latency to the packets or negatively affecting switch performance. This information must consists Flow information and Interpacket variations.	
18.4	Should support sFlow or Netflow or equivalent	
18.5	Should support centralized script/system to configure a switch without user intervention	
19	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
20	Solution should integrate seamlessly with Bank's existing network Infrastructure.	
21	Proposed Solution should have 3 years warranty & 2 years of comprehensive AMC service. Product must not be End of Life and Support during 5 years of contract period. If offered product declared End of Life and Support within 5 years contact period, then bidder should provide latest product with same specification or higher without any cost to the Bank. Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period.	

LEAF SWITCH (FIBRE) REQUIREMENTS

SL. No.	Feature Description	Compliance Yes/No
1	**Architecture**	
1.1	The Solution should support in co-ordination with spine switch. Zones and segments should be decided by spine switch and same should be reflected on Leaf switches.	
1.2	1RU fixed form factor	
2	**Performance**	
2.1	Switch should support Min 1.5 Tbps switching capacity/ throughput or more	
2.2	Switch should support at least 1 Billion packets per second	
2.3	Should support Non-blocking architecture and wire-speed Layer-2 and Layer-3 forwarding	
2.4	Should support 1G/10 GbE SFP/SFP+ based ports	
2.5	The switch should support minimum 1,00,000 IPv4 and IPv6 routes entries in the routing table including multicast routes. However bidder can quote higher specification to meet the SLA & uptime	
2.6	Minimum Multicast Routing table - 10000	
2.7	Switch should have management interface for Out of Band Management	
2.8	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP	
2.9	Switch should support IEEE Link Aggregation or Ethernet Bonding functionality to group multiple ports for redundancy	
2.10	Switch should support Configuration roll-back and check point	
2.11	Switch should support for different logical interface types like loopback, VLAN, SVI/RBI, Port Channel/LAG, multi chassis port channel etc.	
2.12	Line-rate traffic throughput (both Layer 2 and 3) on all ports	
3	**Port Requirements with redundancy**	
3.1	Switch should have 48 ports or more, copper ports	
3.2	Must support at least 48 or more wire-speed 10G ports.	
3.3	Must have 4 or more no. of 40G/100G QSFP based Fibre ports per switch for uplinks with spine switch	
4	**Switch Hardware features and High availability**	
4.1	Switch should be rack mountable and support side rails, if required	
4.2	The proposed switch must have Redundant Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies.	
4.3	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant	

4.4	Should support both front to back and back to front reversible air flow	
4.5	Switch should support in-line hot insertion and removal of different parts like modules/ power supplies/ fan tray etc. and should not require switch reboot & should not disrupt the functionality of the system	
4.6	Switch should support for BFD For Fast Failure Detection as per RFC (5880)	
4.7	Switch should support Graceful Restart for OSPF, BGP etc.	
4.8	The proposed switch should be of 1 Rack Units in size	
4.9	The proposed switch should support FCOE (Fiber channel over Ethernet) and DCB (Data Center bridging) features (Desirable)	
4.10	The proposed switch must have Line-rate traffic throughput on all ports at Layer 2 with non-blocking architecture.	
4.11	The proposed switch must have Line-rate traffic throughput on all ports at Layer 3 with non-blocking architecture	
5	**Scalability**	
5.1	The proposed switch should support minimum 90K MAC address table entries.	
5.2	The proposed switch must allow to build very large L2 domain using logical chassis or virtual logical chassis to support Multi-Path Ethernet technologies across multiple switches.	
5.3	The proposed switch must support port channelling across multiple switches	
6	**Control Plane**	
6.1	Minimum Dual Core x86 CPU or equivalent	
6.2	Minimum 8GB DRAM	
6.3	Minimum 4GB Flash	
6.4	Minimum System buffer 16 MB	
7	**Operating System**	
7.1	Must support modern modular operating system designed for data center scalability and reliability.	
7.2	Must support auto process recovery from failures.	
7.3	Must support Health monitoring and self-healing.	
7.4	Must support Live patching or hitless upgrade without disruption of other processes/system modules while upgrading operating system.	
7.5	Must support Industry standard CLI.	
8	**Layer 2 Switch features**	
8.1	Minimum Number of MAC addresses entries 90K	
8.2	Spanning Tree Protocol (IEEE 802.1.D, 802.1W, 802.1S)	
8.3	must support IEEE 802.1Q VLAN encapsulation	
8.4	Must support minimum 4096 VLAN	
8.5	Internet Group Management Protocol (IGMP) Versions1, 2 and 3	
8.6	Should support Rapid Per VLAN Spanning Tree (RPVST+)	
8.7	Must support Link aggregation LACP: IEEE 802.3ad with up to 16 ports/channels	
8.8	Must support up to 32 ports per Link Aggregation Group (LAG)	
8.9	Must support 100 Link Aggregation Groups (LAG)	

8.10	Must support 64 ports active/active layer2/Layer3 multi-pathing Redundancy	
8.11	Must support 64 ports active/active layer2/Layer3 multi-pathing Redundancy	
8.12	Must support 802.1AB Link Layer Discovery Protocol (LLDP)	
8.13	Must support Port Mirroring	
8.14	Must support 802.3x Flow Control	
8.15	Configurable maximum transmission units (MTUs) of up to 9216 bytes (jumbo frames)	
8.16	Must support active/active layer-2 topology without STP where host are dual homed to switch using vPC or MLAG	
8.17	Minimum Number of Ether Channels should be 64	
8.18	Advanced Ether Channel hashing based on Layer 2, 3, and 4 information	
9	**Layer 3 Switch features**	
9.1	Must support minimum 128K IPv4 Unicast entries	
9.2	Must support minimum 64K or more IPv6 Unicast entries	
9.3	Must support minimum 8K IPv4 Multicast entries	
9.4	Must support minimum 5K ACL	
9.5	Must support basic layer-3 routing – static routes, BGP, OSPF, ISIS	
9.6	VRF: VRF-lite (IP VPN), VRF-aware unicast (BGP, OSPF, and RIP), and VRF-aware multicast	
9.7	Must support VRRP or equivalent	
9.8	Must support 6-way ECMP routing for load balancing and redundancy	
9.9	Must support Route Maps	
9.10	Must support Anycast RP	
10	**Multi-Cast**	
10.1	Multicast: PIM-SMv2, and PIM-SSM	
10.2	Bootstrap router (BSR) and Static RP	
10.3	Multicast Source Discovery Protocol (MSDP) and Anycast RP	
11	**Security features**	
11.1	Must Support ACLs using Layer 2, Layer 3, Layer 4 fields	
11.2	Must Support MAC Security	
11.3	Should Support Privilege Identity Management(PIM), TACACS+ & RADIUS	
11.4	Should Support SNMP v2, v3 with encryption	
11.5	Switch should support DHCP Snooping (Desirable)	
11.6	Must Support SIEM and Syslog	
11.7	Must Support AAA	
11.8	Must Support Port Mirroring	
11.9	Must Support sFlow / netFlow industry standard technology for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defense against security threats	
11.10	Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail	

11.11	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces	
11.12	Storm control (unicast, multicast, and broadcast)	
11.13	CoPP (Control plane protection)	
11.14	Switch should provide different privilege for login in to the system for monitoring and management	
12	**QoS features**	
12.1	Switch must have Egress strict-priority queuing	
12.2	8 hardware queues per port and should support per port QOS Configuration	
12.3	802.1p based classification (COS)	
12.4	Switch must have ACL-based QoS classification (Layers 2, 3, and 4)	
12.5	DSCP based qualification and remarking	
12.6	Rate limiting	
12.7	Switch must support for different type of QoS features for real time traffic differential treatment using	
12.7.1	a. Weighted Random Early Detection	
12.7.2	b. Strict Priority Queuing	
12.8	The proposed switch must support minimum 16 MB packet buffer to avoid packet drops due to buffer queue entries are exhausted which results in poor and unpredictable performance	
12.9	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
13	**Data Centre Advanced Feature and Network Virtualization**	
13.1	Should support 4096 VxLAN. Should support both VRF and VxLAN, bridging and routing from day 1,	
13.2	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN	
13.3	Switch should support VXLAN and EVPN or equivalent for supporting Spine-Leaf architecture to optimize the east - west traffic flow inside the data center	
13.4	Switch should support Data Center Bridging	
13.5	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically, may orchestration layer from day 1	
14	**Virtualization features**	
14.1	Virtualization switch should communicate with vSphere 5.5 and above, and vCenter to support adaptive network virtualization	
14.2	VLAN auto provision - Auto create/configure VM VLAN when new VM is created in vCenter	
14.3	VM Auto Discovery – Find exactly which ESX Hosts and VMs are on a given port in the network. Displays the full Physical Port to Virtual Switch to VM Binding on the supplied management software GUI.	
14.4	Should Dynamically create VLAN policy based on VM movement.	

14.5	Should be able to extract vNIC information from the VM Host and must be able to display the VM to vNIC.	
14.6	VmWare Multi-Tenancy – Connecting up to 4 separate vCenter Administrative domain.	
15	**Management features**	
15.1	Zero Touch provisioning of firmware and configuration of the switch to reduce provisioning time.	
15.2	Switch should have console port	
15.3	Must have 100/1000 management port	
15.4	Must Support USB port	
15.5	Must Support Management over IPv4, IPv6	
15.6	Switch should provide remote login for administration using:	
15.6.1	a.Telnet	
15.6.2	b.SSHV2	
15.7	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
15.7.1	a.SNMP V1 and V.2	
15.7.2	b.SNMP V.3 with encryption	
15.7.3	c.Filtration of SNMP using Access list	
15.8	Switch should support for basic administrative tools like:	
15.8.1	a.Ping	
15.8.2	b.Traceroute	
15.9	Should support built in TCP Dump or Wireshark trouble shooting tool or equivalent	
15.10	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	
15.11	Switch should support central time server synchronization using Network Time Protocol NTP	
16	**Troubleshooting capabilities**	
16.1	Switch must support for basic administrative like Ping and Traceroute	
16.2	Switch must support built in TCP Dump or Wireshark trouble shooting tool or equivalent	
16.3	Switch must support for sending logs to multiple centralised syslog server for monitoring and audit trail	
16.4	Switch should support central time server synchronization using Network Time Protocol NTP V.4	
16.5	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	
16.6	Switch should provide different privilege for login in to the system for monitoring and management	
16.7	Protection from unnecessary or DoS traffic by using storm control functions for unicast/multicast/broadcast.	
16.8	Switch should support spanning tree root guard	

16.9	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
16.10	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
16.11	Configuration rollback and NTP Support	
16.12	Must have XML Support	
17	**Standards Compliance**	
17.1	Should Support IEEE 802.1D Bridging and Spanning Tree	
17.2	Should Support IEEE 802.1p QOS/COS	
17.3	Should Support IEEE 802.1Q VLAN Tagging	
17.4	Should Support IEEE 802.1w Rapid Spanning Tree	
17.5	Should Support IEEE 802.1s Multiple Spanning Tree Protocol	
17.6	Should Support IEEE 802.1AB Link Layer Discovery Protocol	
17.7	Should Support IEEE 802.3ad Link Aggregation with LACP	
17.8	Should Support IEEE 802.3x Flow Control	
17.9	Should Support IEEE 802.3ab 1000BASE-T	
17.10	Should Support IEEE 802.3z Gigabit Ethernet	
17.11	Should Support IEEE 802.3ae 10 Gigabit Ethernet	
17.12	Should Support IEEE 802.3by 25 Gigabit Ethernet (desirable)	
18	**Monitoring and Provisioning**	
18.1	Should support Advance Event Management for pro-active network monitoring or equivalent	
18.2	Should support Restoration of Operating System & Configuration from USB	
18.3	The platform should the capability to collect telemetry information at line rate across all the ports without adding any latency to the packets or negatively affecting switch performance. This information must consists flow information and Interpacket variations.	
18.4	Should support sFlow or Netflow or equivalent	
18.5	Should support centralized script/system to configure a switch without user intervention	
19	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
20	Solution should integrate seamlessly with Bank's existing network Infrastructure.	
21	Proposed Solution should have 3 years warranty & 2 years of comprehensive AMC service. Product must not be End of Life and Support during 5 years of contract period. If offered product declared End of Life and Support within 5 years contact period, then bidder should provide latest product with same specification or higher without any cost to the Bank. Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period.	

TECHNICAL REQUIREMENTS OF L3 SWITCH

Sl. No.	Technical requirement for full-fledged Layer 3 Switch	Compliance (Y/N)
1	Full-fledged L3 Switch capability including L3 VLAN capability and routing capability.	
2	Switch must be eligible as aggregation point for access layer switches.	
3	Should be a single box configuration for ease of management.	
4	Switch should have minimum 170 Gbps Switching capacity all the services enabled on switch	
5	Switch should support VCS or VSS or equivalent architecture by which two separate switches can be combined in a single switch fabric and managed as single switch.	
6	Switch should support IPv4 and IPv6 switching and routing in hardware from day 1.	
7	Switch should have minimum 48 10/100/1000 Mbps Ethernet port, 4 no. 1G/10 G SFP Port.	
8	IEEE 802.1Q VLAN encapsulation. Upto 64 VLANs should be supported. Support for 4000 VLAN IDs. Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically. Should support 802.1d, 802.1s, 802.1w, 802.3ad, Port Aggregation, Link Aggregation Protocol (LACP). Support for Detection of Unidirectional Links and to disable them to avoid, Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.	
9	Support for minimum 1000 MAC addresses	
10	Should support Private VLAN , VLAN Aggregation , Translation and 802.1v	
11	Must support Layer2 Ping and Layer 2 Traceroute for connectivity and Fault Management Must support multicast Traceroute.	
12	Should support SNMP and syslog Notification for MAC addition, deletion and movement across ports	
13	Must support minimum 32K IPv4 Unicast entries Must support minimum 64K or more IPv6 Unicast entries Must support minimum 8K IPv4 Multicast entries Must support minimum 5K ACL Must support basic layer-3 routing – static routes, BGP, OSPF, ISIS VRF: VRF-lite (IP VPN), VRF-aware unicast (BGP, OSPF, and RIP), and VRF-aware multicast Must support VRRP or equivalent Must support minimum 6-way ECMP routing for load balancing and Redundancy. However bidder can quote higher specification to meet the SLA & uptime. Must support Route Maps Must support Anycast RP Should Support Privilege Identity Management(PIM), TACACS+ & RADIUS	

	Should Support SNMP v2, v3 with encryption Switch should support DHCP Snooping (Desirable) Must Support SIEM and Syslog Must Support AAA Must Support Port Mirroring Must Support sFlow / netFlow industry standard technology for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defense against security threats Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces Storm control (unicast, multicast, and broadcast) CoPP (Control plane protection) Switch should provide different privilege for login in to the system for monitoring and management	
14	Should support DHCP	
15	Should have out of band management through console and an external modem for remote management	
16	Switch must be capable of inter VLAN routing.	
17	Management should support : Telnet, Simple Network Management Protocol (SNMP), CLI/Web based HTTP management, RADIUS	
18	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
19	Solution should integrate seamlessly with Bank's existing network Infrastructure.	
20	Equipment should be compatible with tier 3 data centre environment.	
21	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
22	Solution should integrate seamlessly with Bank's existing network Infrastructure.	
23	Proposed Solution should have 3 years warranty & 2 years of comprehensive AMC service. Product must not be End of Life and Support during 5 years of contract period. If offered product declared End of Life and Support within 5 years contact period, then bidder should provide latest product with same specification or higher without any cost to the Bank. Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period.	

TECHNICAL REQUIREMENTS OF VPN MODULES

Sl no.	Item	Feature description	Compliance (y/n)
1.	Form Factor	Rack Mountable (Rack mounting kit for securing the router in standard rack are to be provided)	
2.	**Architecture**	The VPN modules should be modular/fixed in architecture with a services-based hardware, Should be a single chassis/integrated solution	
3.		VPN modules should have support for redundant Router processors /Routing engines	
4.		VPN modules should support a dedicated Service Processor card/ESP	
5.		VPN modules Processors should have minimum 4GB of flash memory or more to support multiple software images for backup purposes, log report and future scalability	
6.		VPN modules Processor should have 4GB of RAM/DRAM to support large routing tables & other memory intensive processes	
7.		VPN modules should support system throughput of minimum 80 Gbps from day 1	
8.		VPN modules should support minimum Traffics handling capacity of 55 Mpps	
9.		VPN modules should be able to maintain 2000 targeted LDP sessions	
10.		VPN modules should support Redundant Power supply from day one	
11.		Should support front-to-back/side-to-side airflow	
12.		All modules, fan trays & Power supplies should be hot swappable	
13.		VPN modules shall have 1:1 operating system redundancy or dual control Module from Day 1 and 1:1/1:N PSU redundancy from day one	
14.		The processing engine architecture must be multi processor based for enhanced performance.	
15.		VPN modules processor should support hardware accelerated, parallelized and programmable IP forwarding and switching.	
16.		Redundancy Feature: The router must support Operating System (OS) redundancy or dual control	

		module in 1:1 mode to ensure high-availability of the system. The router in the event of failure of any one OS or control module should switchover to the redundant OS or redundant control module without dropping any traffic flow. There should not be any impact on the performance in the event of active processing engine failure.	
17.		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.	
18.		Clock: The VPN modules must derive clock from the hired links. The hired links will provide Stratum II/III Clock. The router must sync to the Network Time Protocol (NTP) server.	
19.	**Interfaces**	VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any point of time (at start, re-start or throughout the day)	
20.		All the above ports should be in compliance with 802.3 standards	
21.		The Gigabit Ethernet port should support multimode and single mode fiber connectivity	
22.	Route Processor/ engine function	• Route Processor /engines should perform the following control processor functions: • build L2 & L3 forwarding information tables. • allow for centralized configuration of router including services like routing protocols • control plane functionality. • The router shall support Control Plane Policing protect the router CPU from attacks. • Track the status of various system components like the software, services processor/line cards/fan trays/PSU etc & provide an out of band access method to the router in case of a software crash	
23.		Dedicated Processor should perform the following functions in hardware : • QoS classification, policing and shaping.	

		• NAPT44, NAPT64, NAT-PT, NAPT66,NAT44, 6to4,Twice-NAT44, 6in4, PAT-PP, Dynamic-NAT. • 8000 VPLS instances. • Multicast replication, Security access control lists (ACLs). • 10000 IPSec VPN tunnels. • Support flow mechanism The Services Processor should additionally support the following functions in hardware & should be enabled using appropriate software licenses only if required, without the need for additional hardware: • Firewalls & detection of denial-of-service (DoS) attacks . • Nested Application Recognition • Network Address Translation (NAT) as per 1631. The Service Processor should meet the following performance specifications: • More than 3500 ACLs/filters • 4000 GRE tunnels, 14 million flows • 512000 MAC addresses. • 7000 VRFs. • Should support at least 3 Million 1Pv4 and IPv6 routes.	
24.	VPN throughput	VPN modules should have hardware encryption capabilities with a minimum throughput of 6 Gbps	
25.	Firewall Features	Firewall Feature required from day 1.	
26.	Protocol Support	Should support RIPv1 & RIPv2, OSPF, IS-1S and BGP4, LDP, BFD routing protocols & IP multicast routing protocols: PIM , IGMP	
27.		Should support Multicast VPN (mVPN)	
28.		Should support Enterprise Services feature set with support for protocols like Multiprotocol Label Switching (MPLS), PWE3, FRR, Layer2 circuits, VPLS	
29.		Should support Layer 3 Routing Protocols	
30.		The VPN modules should support multiple level of privileges and authentication for user access	
31.		Should support AAA features through RADIUS and TACACS+	
32.		The software should support Network Address Translation (NAT) and Port Address Translation (PAT) to hide internal IP addresses while connecting to external networks.	
33.		Should support source and destinations based ACLs, time based ACLs	
34.		Should support MD5 authentication for routing protocols	

35.		The VPN modules should support IPv6 for IPSec encryption for data confidentiality	
36.		The VPN modules 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	
37.		The VPN modules shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunnelling, IPv6 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, 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)	
38.		The VPN modules should support 3DES and AES encryption standards	
39.		System shall support to identify encrypted applications (for e.g. SSL/TLS based)	
40.		IPSec implementation should be IETF compliant	
41.		Should be capable of supporting 802.1q VLANs and VLAN trunking	
42.		Should support port aggregation for higher bandwidth and redundancy	
43.		The VPN modules must perform Hardware assisted GREtunnelling as per RFC 1701 and RFC 1702.	
44.		The router must support router redundancy protocol like VRRP.	
45.		The VPN modulesmust support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).	
46.		The multicast implementation must support Rendezvous Points on both leaf and non-leaf nodes.	
47.		The multicast implementation must support source specific multicast.	
48.		The VPN modules must support multiprotocol BGP extensions for multicast.	
49.		The router must support multicast load balancing traffic across multiple interfaces.	
50.		The VPN modules must support RFC 3618 Multicast SourceDiscovery Protocol (MSDP).	
51.		The router shall support unicast RPF (uRPF) feature to block any communications and attacks that are being sourced from Randomly generated IP addresses.	
52.		The router must support Any cast Rendezvous Point (RP) mechanism using PIM and Multicast Source Discovery Protocol (MSDP) as defined in RFC 3446.	

53.		Should support RSVP	
54.	Router Performance Parameter	Routing Table Size: The router must support minimum 10,00,000 IPv4 or 10,00,000 IPv6 routes entries in the routing table and should be scalable	
55.		The VPN modules should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high- availability during primary controller card/Integrated controller failure.	
56.		VPN concentrator must support 10 Gbps of Crypto throughput for IPSEC tunnel and 5000 IPSEC full loaded (2 Mbps) tunnels from day 1. In case of an external box, The VPN concentrator must have redundant power supply & at least 6 x 1GE interfaces and 6 no. of 10 G interface (SFP) from Day1. VPN concentrator should have capabilities to handle 5000 IPSEC fully loaded (2 Mbps) tunnel at any point of time (at start, re-start or throughout the day)	
57.		The VPN modules solution must be a Equipment supporting the following: • In-band and out-band management. • Software rollback feature • Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.	
58.		The proposed router should support modular OS and simply the changes through In-Service OS upgrade mechanism	
59.		The VPN modules should be able to select a WAN/LAN path based on interface parameters such as reachability, load, throughput, and link cost of using a path	
60.		The VPN modules or system must have support for Application level Visibility using Deep Packet Inspection Technology to identify the non-critical traffic and set the lowest priority or drop the traffic and prioritise the legitimate critical applications traffic using QOS from day one.	
61.		System shall support to granularly identify applications in the enterprise (For e.g. Oracle, SAP, WebEx etc.) from day one .	
62.	Solution should integrate seamlessly with Bank's existing network Infrastructure.		
63.	Proposed Solution should have 3 years warranty & 2 years of comprehensive AMC service. Product must not be End of Life and Support during 5 years of contract period. If offered product declared End of Life and Support within 5 years contact period, then bidder should provide latest product with same specification or higher without		

	any cost to the Bank. Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period.	

2 PAIR OF CORE FIREWALL (TYPE 1) TECHNICAL REQUIREMENTS AT DC & DR

Sl. No.	Feature Description	Compliance Yes/No
1	Chassis based or modular architecture for scalability & other than Checkpoint OEM.	
2	Firewall should have at least 6 no. of 10 G ports SFP port and 4 nos. of 40G/100 G port and 2 nos. 1 Gbps Ethernet port.	
3	The appliance should be capable of providing Firewall and Next Generation Firewall feature.	
4	The platform should support VLAN tagging (IEEE 802.1q)	
5	The platform shall have dedicated interface for out-of bound management	
6	The Firewall should support CA functionality	
7	Support for minimum 1000 MAC addresses	
8	Firewall performance should be minimum real world throughput 60 Gbps after enabling the IPS, QoS, malware protection function.	
9	Firewall should be capable configuring Policies using Command Line (CLI) as a last resort in case of Emergency.	
10	Firewall with IPS features should support minimum 2,00,00,000 concurrent connections	
11	Firewall with IPS features should support minimum 10,00,000 new connections per second (cps)	
12	Should support grouping of physical interfaces whiting and across Fixed and Expansion ports into one single physical or logical interface	
13	Firewall should support memory at least 60 GB Memory for better and faster processing	
14	Should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.	
15	The firewall shall be deployed in high availability mode (hot stand-by redundancy), have fault tolerance and shall provide stateful failover	
16	The firewall shall have a powerful OS that is hardened and is based upon minimal feature sets.	
17	There shall be support for traffic based and user based access control.	

18	The broad default policy for the firewall for handling inbound traffic shall be to block all packets and connections unless the traffic type and connections have been specifically permitted	
19	It shall support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.	
20	Firewall should support Single Sign On (SSO)	
21	Should support translating between IPv4 and IPv6 for the following inspections: DNS, FTP,ICMP,HTTP	
22	Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.	
23	Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT shall be supported.	
24	Port address translation/Masquerading shall be provided for	
25	Dynamic Host Configuration Protocol (DHCP) over Virtual Private Network (VPN) shall be supported for dynamic allocation of IP addresses.	
26	The firewall shall support a number of routing options and configurations. Routing protocol support shall include static routes, Open Shortest Path First (OSPF), RIPv1/v2 etc.	
27	Virtual LAN (VLAN) support, high port density, WAN support and expandability of interfaces over time are some important network integration features shall be supported.	
28	The firewall IP stack shall be IPv6 ready.	
29	The firewall shall mask the internal network from the external world.	
30	The firewall shall provide robust access control capability and be fast in making access control decisions. Access Control shall be done based on criteria such as source, destination IPs, port number, protocol, traffic type, application, date information (day of week, time of day), etc.	
31	Multi-layer, stateful, application based filtering shall be done	
32	It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access	
33	There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.	
34	Firewall itself shall be resistant to attack and shall have protection against firewall evasion techniques.	
35	Some basic attack protection features listed below but not limited to : Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite It shall enable rapid detection of network attacks TCP reassembly for fragmented packet protection Brute force attack mitigation. SYN cookie protection , SYN Flood, Half Open Connections and NUL Packets Protection against IP spoofing Malformed packet protection Java blocking, and real-time alerts	

36	Full H.323v1-5 (Firewall Traversal), SIP (Session Initiation Protocol), gatekeeper support, outbound bandwidth management, full interoperability with common and popular VoIP/VC gateway and communications devices shall be supported, apart from supporting all protocols.	
37	The firewall shall support Internet Protocol Security (IPSec) & SSL	
38	Key exchange with latest Internet Key Exchange (IKE), IKEv2, Public Key Infrastructure PKI (X.509) shall be catered to.	
39	Site-to-site VPN tunnels: full-mesh / star topology shall be supported.	
40	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES(Data Encryption Standard) etc.	
41	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.,	
42	IPSec NAT traversal shall be supported.	
43	VPN supporting atleast 300 IPSec / SSL VPN peers	
44	The solution should support the following File/Media Types for Malware identification: "BAT ,.BZ2 ,.ZIP,.CHM,.DLL,.DOC, .DOCX ,.EML ,.EXE,.GZ - gzip ,.HTA ,.HWP, .HWT, .HWPX ,.ISO,PDF, ZIP,EXE, DLL,OCX, Java, Flash,JAR,JS,JSE,JTD ,JTT,JTDC,JTTC,.LNK etc	
45	The solution should support down selection and only analyzes files deemed suspicious.	
46	The solution should have the ability to heuristically detect and decode the presence of shell code	
47	The solution should have the ability to detect and scan pdf files for embedded code	
48	The solution should have capability to fully reveal malware's current and potential payloads.	
49	The solution should provide detection, analysis and repair capability against malware-based attacks	
50	The solution should provide a detailed list of every DLL and API referenced, all header information about the binary, and complete assembly-language listing of the binary code.	
51	The solution should provide reports to shows all the activities the malware code performs related to file systems, Windows registry, network operations, Processes and any other miscellaneous operations	
52	The solution should provide summary for instance, whether the malware wrote into a certain file, modified a registry setting, opened a port or communicated to a specific url, or changed the name of a running process to hide itself.	
53	The solution should identify any logic bombs (time based execution delays) hidden in the malware waiting for a trigger to cause damage at a later time	
54	The solution should provide the ability to upload gold image and analyze threats under conditions of actual host environment.	
55	Solution should provide Detailed Technical Report, Behavior Summary Report and a Logic Execution Path Map.	

56	The solution should recognize new variants of existing malware families and identify new families.	
57	The Solution should support the following multiple advanced malware analysis methods:	
58	Solution should provide high Threat protection rate minimum of 99%.	
59	The solution shall give CVE number for the Intrustion events detected and shall capture packet for each intrusion event	
60	The solution should automatically map event to the IP, Geography information, to the user, system affected	
61	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	
62	The IPS detection methodologies shall consist of Signature based detection using real time updated database & Anomaly based detection that is based on thresholds	
63	The proposed system shall support One-arm IDS (sniffer mode)	
64	The device shall allow administrators to create Custom IPS signatures	
65	Consists of vendor's original threat intelligence and is not overly dependent on information available in the public domain.	
66	Is continuously updated with new threat intelligence, including detailed help text, in an automated fashion and without physical access to the unit.	
67	Security information is meaningful, comprehensive and freely available to customers and non-customers via a publicly accessible database.	
68	Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).	
69	Allows users to control the number of times a sensor notifies the console when a flood type attack occurs. For example, the sensor must be configurable to send a single alert every five minutes vs. sending an alert for every single packet associated with the attack. This will avoid overwhelming the console and the internal network with alerts.	
70	Must be capable of performing packet-level forensics and capturing raw packet data in response to individual events	
71	The detection engine must support multiple options for directly responding to events, such as monitor only, block offending traffic, replace packet payload, and capture packets	
72	The solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.	
73	Accurately detects intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids, and zero-day attacks.	
74	Detection rules must be based on an extensible, open language (API) that enables users to create their own rules, as well as to customize any vendor-provided rules.	

75	Detection rules provided by the vendor must be documented, with full descriptions of the identity, nature, and severity of the associated vulnerabilities and threats being protected against.	
77	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit -based signatures, vulnerability -based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Identify and explain each type of detection mechanism supported.	
78	The detection engine must inspect not only Network Layer details and information resident in packet headers, but a broad range of protocols across all layers of the computing stack and packet payloads as well.	
79	The detection engine must be resistant to various URL obfuscation techniques common to HTML -based attacks	
80	The solution must be capable of detecting and blocking IPv6 attack	
81	The solution must provide IP reputation feed that comprised of several regularly updated collections of IP addresses determined by the proposed security vendor to have a poor reputation.	
82	The solution should be capable of providing network -based detection of malware by checking the disposition of known files in the cloud using the SHA -256 file -hash as they transit the network (SHA -256 and target IP address should be given to aid remediation efforts) with enabling just advance malware license if require in near future	
83	The 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.	
84	The solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.	
85	The solution must be capable of storing user -defined host attributes, such as host criticality or administrator contact information, to assist with compliance monitoring.	
86	The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.	
87	The 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.	
88	The solution must provide a detailed, interactive graphical summary that includes data on applications, application statistics, connections, intrusions events, hosts, servers, users, file -types, malwares and relevant URLs. These data should be presented by detailed lists (Administrator should easily create and apply custom filters to fine -tune the analysis).	
89	Appliance have capacity to block source based on geo -location	
90	The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and	

	behaviour of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.	
91	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	
92	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
93	Should have identification support for at least 3000 applications and the identification should be regardless of ports. The application needs to be predefined on the box.	
94	The proposed system shall have the ability to identify, block the following common P2P applications: Gnutella (Napshare, iMesh, Mldonkey, morph, Xolox, BearShare, FOXY), Bittorrent, Kaaza, WinY, edonkey).	
95	The solution must integrate application control to reduce risks associated with applications usage and client -side attacks. It should provide a means of enforcing acceptable use policies of up to 3000 application detectors.	
96	The solution must support creation of user -defined application protocol detectors.	
97	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.	
98	The proposed solution should provide an option to include URL filtering for enforcing Internet content filtering so as to reduce web born threats and improve productivity.	
99	Each URL in the data set must has an associated category and reputation. URL category is a general classification for the URL while URL reputation represents how likely the URL is to be used for purposes that might be against the organization's security policy.	
100	The solution must be capable of easily identifying all hosts that exhibit a specific attribute or non - compliance condition.	
101	The management platform must be capable of centralized, life cycle management for all NGFW services/devices.	
102	The management platform must be delivered in virtual appliance form factor (management system and UI must provide the same features and functions as in the physical appliance).	
103	The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events.	
104	The management platform must be accessible via a web-based interface/ client software.	
105	The management platform must provide a highly customizable dashboard.	
106	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.	

107	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.	
108	The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application.	
109	The management platform must include one or more default (i.e., pre-defined) detection policy configurations to help simplify initial deployment.	
110	The management platform must provide the capability to easily view, enable, disable, and modify individual rules, as well as groups or categories of rules.	
111	The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to sensors.	
112	The management platform must be capable of backup and rollback for sensor configurations and the management platform itself.	
113	The management platform must provide the ability to view the corresponding detection rule for each detected event, along with the specific packet(s) that caused it to be triggered.	
114	The management platform must support both internal and external databases/systems for storage of event data, logs, and other system generated information..	
115	The management platform must be capable of synchronizing time between all components of the system via NTP.	
116	The management platform must be capable of logging all administrator activities, both locally and to a remote log server.	
117	The solution must support LDAP for single sign-on to sensors and the management console.	
118	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.	
119	The reporting tool needs to be bundled or quoted along with the solution. The logging and analysis should either be an appliance or on a dedicated PC/ Server platform. The bidder should take the responsibility of supplying the hardware and the OS with suitable warranty.	
120	The management platform must allow quick report customization by importing from dashboards, workflows and statistics summaries.	
121	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
122	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
123	Firewall should able to handle all ATM, NPCI, Payment gateway traffic at existing Bank's Network.	

124	IPS device should perform stateful pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.	
125	The proposed IPS must perform protocol decoding and validation for network traffic including: IP, TCP, UDP, and ICMP.	
126	IPS should provide anomaly identification for attacks that may cover multiple sessions and connections, using techniques based on identifying changes in normal network traffic patterns	
127	Should support creation of baseline of normal network traffic and then uses baseline to detect worm-infected hosts	
128	Should support creation of baseline of normal network traffic and then uses baseline to detect worm-infected hosts	
129	Must be able to identify Layer 2 Address Resolution Protocol (ARP) attacks and man-in-the-middle attacks	
130	The sensors should be able to detect attacks running inside of these tunnelling protocols such as GRE, IP-in-IP, MPLS, and IPv4/IPv6.	
131	The IPS should be able to inspect SSL/https traffic	
132	Can exceptions be setup to filter out, fine-tune or adjust the actions for specific attacker or destination IP on a per signature basis	
133	The proposed product should be resistant to IPS evasion and protection from anti-NIPS (Network Intrusion Prevention System) techniques.	
135	The average latency of the proposed IPS should be less than 150 microseconds	
136	IPS must support a minimum of 5 million concurrent connections.	
137	Support more than 1, 00,000 new sessions per second processing	
138	Proposed solution should have automatic bypass for IPS in case of performance suffer beyond defined administrative threshold or IPS function/engine fails	
139	IPS should have the functionality of Software Fail Open.	
140	IPS Software Fail Open functionality can be defined in terms Gateway Threshold of Memory or CPU and should have an option to trigger the mail if required.	
141	The IPS should support Active/Active and Active/ Standby High Availability feature.	
142	Proposed IPS solution must be capable to detect device failure, link and path failure	
143	IPS appliance failover should be complete stateful in nature without any manual intervention	
144	Proposed IPS solution should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behaviour-based detection and reputation based filtering	
145	IPS profile can be defined to Deactivate protections with Severity, Confidence level, Performance impact, Protocol Anomalies	
146	IPS Profile should have an option to select or re-select specific signatures that can be deactivated	
147	Intrusion Prevention should have the option to add exceptions for network and services.	

148	IPS should provide rate shaping to prioritize known, normal traffic flows and unknown traffic flows	
149	IPS Policy to Block the traffic by country should have an option to configure in incoming direction, Outgoing direction or both.	
150	IPS events/protection exclusion rules should be created and the packet data should be viewed directly from log entries.	
151	Application Intelligence should have controls for Instant Messenger, Peer-to-Peer, Malware Traffic etc.	
152	Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance	
153	The proposed IPS should have an option to create your own signatures with an open signature language	
154	IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc.	
155	Proposed IPS must have an embedded GUI Based Management interface.	
156	Proposed IPS should have the options of policy configuration, event management, health management and reporting.	
157	IPS device should have features to prioritize and send alerts to users after an alert action is taken place	
158	Proposed IPS should be constantly updated with new defences against emerging threats.	
159	IPS updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time	
160	Should have flexibility to define newly downloaded protections will be set in Detect or Prevent mode.	
161	Activation of new protections based on parameters like Performance impact, Confidence index, Threat severity etc	
162	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
163	Solution should integrate seamlessly with Bank's existing network Infrastructure.	
164	Proposed Solution should have 3 years warranty & 2 years of comprehensive AMC service. Product must not be End of Life and Support during 5 years of contract period. If offered product declared End of Life and Support within 5 years contact period, then bidder should provide latest product with same specification or higher without any cost to the Bank. Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period.	

3 PAIR OF INTERNET & EXTRANET FACING FIREWALL (TYPE-2) TECHNICAL REQUIREMENTS AT DC & DR

Sl. No.	Feature Description	Compliance Yes/No
1	Chassis based or modular architecture for scalability	
2	Firewall should have at least 6 no. of 1 GE ports and 6 no of 10 G fibre port	
3	The appliance should be capable of providing Firewall, VPN Services and Next Generation Firewall feature. 300 remote VPN license required with 1 pare of Firewall.	
4	The platform should support VLAN tagging (IEEE 802.1q)	
5	The platform shall have dedicated interface for out-of bound management	
6	The Firewall should support CA functionality	
7	Support for minimum 1000 MAC addresses	
8	Firewall performance should be minimum real world throughput 20 Gbps after enabling all function like IPS, QoS, and malware protection.	
9	Firewall should be capable configuring Policies using Command Line (CLI) as a last resort in case of Emergency.	
10	Firewall should support minimum 500,0000 concurrent connections	
11	Firewall should support minimum 100000 new conections per second (cps)	
12	deliver VPN throughput minimum 300 Mbps	
13	Should support grouping of physical interfaces withing and across Fixed and Expansion ports into one single physical or logical interface	
14	Firewall should support memory atleast 8 GB Memory for better and faster processing.	
15	Should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	
16	The firewall shall be deployed in high availability mode (hot stand-by redundancy), have fault tolerance and shall provide stateful failover	
17	The firewall shall have a powerful OS that is hardened and is based upon minimal feature sets.	
18	There shall be support for traffic based and user based access control.	
19	The broad default policy for the firewall for handling inbound traffic shall be to block all packets and connections unless the traffic type and connections have been specifically permitted	
20	It shall support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.	
21	Firewall should support Single Sign On (SSO)	
22	Should support translating between IPv4 and IPv6 for the following inspections: DNS, FTP,ICMP,HTTP	
23	Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.	

24	Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT shall be supported.	
25	Port address translation/Masquerading shall be provided for	
26	Dynamic Host Configuration Protocol (DHCP) over Virtual Private Network (VPN) shall be supported for dynamic allocation of IP addresses.	
27	The firewall shall support a number of routing options and configurations. Routing protocol support shall include static routes, Open Shortest Path First (OSPF), RIPv1/v2 etc.	
28	Virtual LAN (VLAN) support, high port density, WAN support and expandability of interfaces over time are some important network integration features shall be supported.	
29	The firewall IP stack shall be IPv6 ready.	
30	The firewall shall mask the internal network from the external world.	
31	The firewall shall provide robust access control capability and be fast in making access control decisions. Access Control shall be done based on criteria such as source, destination IPs, port number, protocol, traffic type, application, date information (day of week, time of day), etc.	
32	Multi-layer, stateful, application based filtering shall be done	
33	It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access	
34	There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.	
35	Firewall itself shall be resistant to attack and shall have protection against firewall evasion techniques.	
36	Some basic attack protection features listed below but not limited to : Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite It shall enable rapid detection of network attacks TCP reassembly for fragmented packet protection Brute force attack mitigation. SYN cookie protection , SYN Flood, Half Open Connections and NUL Packets Protection against IP spoofing Malformed packet protection Java blocking, and real-time alerts	
37	Full H.323v1-5 (Firewall Traversal), SIP (Session Initiation Protocol), gatekeeper support, outbound bandwidth management, full interoperability with common and popular VoIP/VC gateway and communications devices shall be supported, apart from supporting all protocols.	
38	The firewall shall support Internet Protocol Security (IPSec) & SSL	
39	Key exchange with latest Internet Key Exchange (IKE), IKEv2, Public Key Infrastructure PKI (X.509) shall be catered to.	
40	Site-to-site VPN tunnels: full-mesh / star topology shall be supported.	

41	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES(Data Encryption Standard) etc.	
42	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.,	
43	IPSec NAT traversal shall be supported.	
44	VPN supporting atleast 300 IPSec / SSL VPN peers	
45	The solution should support the following File/Media Types for Malware identification: "BAT ,.BZ2 ,.ZIP,.CHM,.DLL,.DOC, .DOCX ,.EML ,.EXE,.GZ - gzip ,.HTA ,.HWP, .HWT, .HWPX ,.ISO,PDF, ZIP,EXE, DLL,OCX, Java, Flash,JAR,JS,JSE,JTD ,JTT,JTDC,JTTC,.LNK etc	
46	The solution should support down selection and only analyzes files deemed suspicious.	
47	The solution should have the ability to heuristically detect and decode the presence of shell code	
48	The solution should have the ability to detect and scan pdf files for embedded code	
49	The solution should have capability to fully reveal malware's current and potential payloads.	
50	The solution should provide detection, analysis and repair capability against malware-based attacks	
51	The solution should provide a detailed list of every DLL and API referenced, all header information about the binary, and complete assembly-language listing of the binary code.	
52	The solution should provide reports to shows all the activities the malware code performs related to file systems, Windows registry, network operations, Processes and any other miscellaneous operations	
53	The solution should provide summary for instance, whether the malware wrote into a certain file, modified a registry setting, opened a port or communicated to a specific url, or changed the name of a running process to hide itself.	
54	The solution should identify any logic bombs (time based execution delays) hidden in the malware waiting for a trigger to cause damage at a later time	
55	The solution should provide the ability to upload gold image and analyse threats under conditions of actual host environment.	
56	Solution should provide Detailed Technical Report, Behaviour Summary Report and a Logic Execution Path Map.	
57	The solution should recognize new variants of existing malware families and identify new families.	
58	The Solution should support the following multiple advanced malware analysis methods:	
59	Solution should provide high Threat protection rate minimum of 99%.	
60	The solution shall give CVE number for the Instruction events detected and shall capture packet for each intrusion event	
61	The solution should automatically map event to the IP, Geography information, to the user, system affected	

62	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	
63	The IPS detection methodologies shall consist of Signature based detection using real time updated database & Anomaly based detection that is based on thresholds	
64	The proposed system shall support One-arm IDS (sniffer mode)	
65	The device shall allow administrators to create Custom IPS signatures	
66	Consists of vendor's original threat intelligence and is not overly dependent on information available in the public domain.	
67	Is continuously updated with new threat intelligence, including detailed help text, in an automated fashion and without physical access to the unit.	
68	Security information is meaningful, comprehensive and freely available to customers and non-customers via a publicly accessible database.	
69	Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).	
70	Allows users to control the number of times a sensor notifies the console when a flood type attack occurs. For example, the sensor must be configurable to send a single alert every five minutes vs. sending an alert for every single packet associated with the attack. This will avoid overwhelming the console and the internal network with alerts.	
71	Must be capable of performing packet-level forensics and capturing raw packet data in response to individual events	
72	The detection engine must support multiple options for directly responding to events, such as monitor only, block offending traffic, replace packet payload, and capture packets	
73	The solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.	
74	Accurately detects intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids, and zero-day attacks.	
75	Detection rules must be based on an extensible, open language (API) that enables users to create their own rules, as well as to customize any vendor-provided rules.	
76	Detection rules provided by the vendor must be documented, with full descriptions of the identity, nature, and severity of the associated vulnerabilities and threats being protected against.	
77	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero -day threats, etc.)which require license for cloud sandboxing feature with hash only	
78	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit -based signatures,	

	vulnerability -based rules, protocol anomaly detection, and behavioural anomaly detection techniques. Identify and explain each type of detection mechanism supported.	
79	The detection engine must inspect not only Network Layer details and information resident in packet headers, but a broad range of protocols across all layers of the computing stack and packet payloads as well.	
80	The detection engine must be resistant to various URL obfuscation techniques common to HTML -based attacks	
81	The solution must be capable of detecting and blocking IPv6 attack	
82	The solution must provide IP reputation feed that comprised of several regularly updated collections of IP addresses determined by the proposed security vendor to have a poor reputation.	
83	The solution should be capable of providing network -based detection of malware by checking the disposition of known files in the cloud using the SHA -256 file -hash as they transit the network (SHA -256 and target IP address should be given to aid remediation efforts) all the license required for said functionality should be considered from day 1	
84	The 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.	
85	The solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.	
86	The solution must be capable of storing user -defined host attributes, such as host criticality or administrator contact information, to assist with compliance monitoring.	
87	The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.	
88	The 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.	
89	The solution must provide a detailed, interactive graphical summary that includes data on applications, application statistics, connections, intrusions events, hosts, servers, users, file -types, malwares and relevant URLs. These data should be presented by detailed lists (Administrator should easily create and apply custom filters to fine -tune the analysis).	
90	Appliance have capacity to block source based on geo -location	
91	The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behaviour of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.	
92	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts,	

	ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	
93	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
94	Should have identification support for atleast 3000 applications and the identification should be regardless of ports. The application needs to be predefined on the box.	
95	The proposed system shall have the ability to identify, block the following common P2P applications: Gnutella (Napshare, iMesh, Mldonkey, morph, Xolox, BearShare, FOXY), Bittorrent, Kaaza, WinY, edonkey).	
96	The solution must integrate application control to reduce risks associated with applications usage and client -side attacks. It should provide a means of enforcing acceptable use policies of up to 3000 application detectors.	
97	The solution must support creation of user -defined application protocol detectors.	
98	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.	
99	The proposed solution should provide an option to include URL filtering for enforcing Internet content filtering so as to reduce web born threats and improve productivity.	
100	Each URL in the data set must has an associated category and reputation. URL category is a general classification for the URL while URL reputation represents how likely the URL is to be used for purposes that might be against the organization's security policy.	
101	The solution must be capable of easily identifying all hosts that exhibit a specific attribute or non - compliance condition.	
102	The management platform must be capable of centralized, life cycle management for all NGFW services/devices.	
103	The management platform must be delivered in virtual appliance form factor (management system and UI must provide the same features and functions as in the physical appliance).	
104	The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events.	
105	The management platform must be accessible via a web-based interface/ client software.	
106	The management platform must provide a highly customizable dashboard.	
107	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.	
108	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.	
109	The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application.	
110	The management platform must include one or more default (i.e., pre-defined) detection policy configurations to help simplify initial deployment.	
111	The management platform must provide the capability to easily view, enable, disable, and modify individual rules, as well as groups or categories of rules.	
112	The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to sensors.	
113	The management platform must be capable of backup and rollback for sensor configurations and the management platform itself.	
114	The management platform must provide the ability to view the corresponding detection rule for each detected event, along with the specific packet(s) that caused it to be triggered.	
115	The management platform must support both internal and external databases/systems for storage of event data, logs, and other system generated information..	
116	The management platform must be capable of synchronizing time between all components of the system via NTP.	
117	The management platform must be capable of logging all administrator activities, both locally and to a remote log server.	
118	The solution must support LDAP for single sign-on to sensors and the management console.	
119	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.	
120	The reporting tool needs to be bundled or quoted along with the solution. The logging and analysis should either be an appliance or on a dedicated PC/ Server platform. The bidder should take the responsibility of supplying the hardware and the OS with suitable warranty.	
121	The management platform must allow quick report customization by importing from dashboards, workflows and statistics summaries.	
122	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
123	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
124	Firewall should able to handle all ATM, NPCI, Payment gateway traffic at existing Bank's Network.	
125	The proposed device should have Intrusion prevention sensors delivering a minimum of 10 Gbps of context-aware , real-world traffic inspection (enabling all functions)	

126	IPS device should perform stateful pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.	
127	The proposed IPS must perform protocol decoding and validation for network traffic including: IP, TCP, UDP, and ICMP.	
128	IPS should provide anomaly identification for attacks that may cover multiple sessions and connections, using techniques based on identifying changes in normal network traffic patterns	
129	Should support creation of baseline of normal network traffic and then uses baseline to detect worm-infected hosts	
130	Should support creation of baseline of normal network traffic and then uses baseline to detect worm-infected hosts	
131	Must be able to identify Layer 2 Address Resolution Protocol (ARP) attacks and man-in-the-middle attacks	
132	The sensors should be able to detect attacks running inside of these tunnelling protocols such as GRE, IP-in-IP, MPLS, and IPv4/IPv6.	
133	The IPS should be able to inspect SSL/https traffic	
134	Can exceptions be setup to filter out, fine-tune or adjust the actions for specific attacker or destination IP on a per signature basis	
135	The proposed product should be resistant to IPS evasion and protection from anti-NIPS (Network Intrusion Prevention System) techniques.	
136	Proposed IPS should support a minimum of average inspection throughput of 10 Gbps	
137	The average latency of the proposed IPS should be less than 150 microseconds	
138	IPS must support a minimum of 5 million concurrent connections.	
139	Support more than 1, 00,000 new sessions per second processing	
140	Proposed solution should have automatic bypass for IPS in case of performance suffer beyond defined administrative threshold or IPS function/engine fails	
141	IPS should have the functionality of Software Fail Open.	
142	IPS Software Fail Open functionality can be defined in terms Gateway Threshold of Memory or CPU and should have an option to trigger the mail if required.	
143	The IPS should support Active/Active and Active/ Standby High Availability feature.	
144	Proposed IPS solution must be capable to detect device failure, link and path failure	
145	IPS appliance failover should be complete stateful in nature without any manual intervention	
146	Proposed IPS solution should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behaviour-based detection and reputation based filtering	
147	IPS profile can be defined to Deactivate protections with Severity, Confidence level, Performance impact, Protocol Anomalies	
148	IPS Profile should have an option to select or re-select specific signatures that can be deactivated	

149	Intrusion Prevention should have the option to add exceptions for network and services.	
150	IPS should provide rate shaping to prioritize known, normal traffic flows and unknown traffic flows	
151	IPS Policy to Block the traffic by country should have an option to configure in incoming direction, Outgoing direction or both.	
152	IPS events/protection exclusion rules should be created and the packet data should be viewed directly from log entries.	
153	Application Intelligence should have controls for Instant Messenger, Peer-to-Peer, Malware Traffic etc.	
154	Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance	
155	The proposed IPS should have an option to create your own signatures with an open signature language	
156	IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc.	
157	Proposed IPS must have an embedded GUI Based Management interface.	
158	Proposed IPS should have the options of policy configuration, event management, health management and reporting.	
159	IPS device should have features to prioritize and send alerts to users after an alert action is taken place	
160	Proposed IPS should be constantly updated with new defences against emerging threats.	
161	IPS updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time	
162	Should have flexibility to define newly downloaded protections will be set in Detect or Prevent mode.	
163	Activation of new protections based on parameters like Performance impact, Confidence index, Threat severity etc	
164	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
165	Solution should integrate seamlessly with Bank's existing network Infrastructure.	
166	Proposed Solution should have 3 years warranty & 2 years of comprehensive AMC service. Product must not be End of Life and Support during 5 years of contract period. If offered product declared End of Life and Support within 5 years contact period, then bidder should provide latest product with same specification or higher without any cost to the Bank. Offer product must not be End of Life and Support for next 2 years after expiry of 5 years of contract period.	