Proof of Concept Checklist

Annexure 19

Sr. No.	POC Description	Test Cases Description	Expected Result	Mandatory(M)/ Optional (O)	Compliance (Yes / No)	Remarks
1	**Branch Device**					
		Health Check of Router	Should Pass all basic hardware Test (Power on Self Test)	M		
		DHCP Server /DHCP Relay /DHCP Client	Should Work as DHCP server to assigne IP to Branch Desktop	M		
		Interoperate with Other Devices	Should operate with Other OEM devices	M		
		Fast Boot	Should Boot in minimum time i.e. < 5 Min	M		
		Port Security/DOT1X/Mac Binding/	Should be Configurerable	M		
		High Mean Time between Failure	Minimum 7 Years	O		
2	**Data Center Device**					
		Health Check of Router	Should Pass all basic hardware Test (Power on Self Test)	M		
		Interoperate with Other Devices	Should operate with Other OEM devices	M		
		Fast Boot	Should Boot in minimum time i.e. < 10 Min	M		
		HA/Autofailover	Traffic flow without session disconnect	M		
		High Mean Time between Failure	Minimum 7 Years	O		
3	**Link Parameter at Branch**					
		Packet Drop Test	Traffic flow without session disconnect	M		If any of Link Shows Packet drop
		Latency Test	Traffic flow without session disconnect	M		If any of Link Shows latency
		Jitter test	Traffic flow without session disconnect	M		If any of Link Shows Flapping
		HA Test/ Link Auto Failover Test	Traffic flow without session disconnect	M		If any of Link Shows goes down
		Maximum Throughput	Appliance should support the cumulative Bandwidth of all the WAN links available at the site	M		when Both Link utilised at a time
		Load Balancing	Traffic flow without session disconnect	M		when one Link is over utilised
		Real Time Packet Correction	Traffic flow without session disconnect	M		When packet Lost during Tranfer
		Real-time Packet Duplication	Traffic flow without session disconnect	M		Real-time traffic duplication across multiple links to mitigate against latency and packet drops
		Seamless application accessibility	Traffic flow without session disconnect	M		
		Congestion Mitigation	Traffic flow without session disconnect	M		Auto Bandwidth change as per QoS already in place
		Use of Multiple links simultaneously for a single application session/Dynamic adjustment Bandwith Usage	Traffic flow without session disconnect	M		Auto Bandwidth change as per QoS already in place
		Persistency	send packets on a same path (persistency)	M		When there is no issue in the links
		Partial Mesh and Full Mesh Topology	On-Demand Tunnel between branch to branch on the same MPLS ISP	M		Communication between Branches
4	**Security**					
		Separation of Data plane and control plane	Should have cleary visible Control Plane and Data Plane	M		
		Auto FormationIP SEC Tunnel	Should form IP Sec Tunnel without manual intervention	M		
		Time based Encryption of Traffic	Auto generation of certficate for encryption without manual intervention and affecting any traffic	M		
		Network wide Policy Enforcement	Can Deploy from central location for single device or multiple or all devices	M		
		IPS	Should Demonstrate IPS features	M		When MPLS and Internet Link Both Provided at Branch level
		Firewall - Statefull	Should demonstrate Firewall features	M		When MPLS and Internet Link Both Provided at Branch level
		Neutralize any vulnerability issues (ARP spoofing, MAC, DNS, DHCP, Ping, Routing, TCP attacks, VLAN hopping)	Should demonstrate neutralizing the vulnerability	M		When MPLS and Internet Link Both Provided at Branch level

		Breakout at Branch level for Cloud SaaS	Should demonstrate zone wise firewall and IPS feature to allow the Saas Traffic or any other allowed Internet traffic	M		When MPLS and Internet Link Both Provided at Branch level
		URL/URI/IP whitelisting/Anti Malware protection	Should allow URL/URI/IP whitelisting from central location as per branch specific Policy	M		When MPLS and Internet Link Both Provided at Branch level
5	**Quality of Service (QoS)**					
		Application detection and Visibility (DPI)		M		
		Application Aware Routing (AAR) with SLA		M		
		Congestion Mitigation -Quality determinations	Traffic flow without session disconnect	M		
		Traffic Priority a. Application b. Destination IP and TCP/UDP port c. Source IP address	Traffic flow without session disconnect	M		
		Minimum Guaranteed Bandwidth with maximum Cap a. Application b. Destination IP and TCP/UDP port c. Source IP address	Traffic flow without session disconnect	M		
		Burst above the maximum bandwidth usage cap	utilize the available bandwidth if No congestion/or other application not using the bandwidth	M		
		select path based on link Quality, Policy & link Capacity based on network analysis	Traffic flow without session disconnect	M		
		Network Performance, Traffic Management & Path Steering	Traffic flow without session disconnect	M		
6	**Management and Control**					
		Maximum Details to be added while onboarding any Branch Device to Track asset as well as Link with historical data per Branch		M		
		Role-based access control	Should Support Role Based Access	M		
		Centralized configuration/Management	Should Support Centralized configuration/Management	M		
		Upgrade of iOS/ Patch Management with RollBack	Should Support Centralized configuration/Management	M		
		Global/Specific Template Provisioning	Should Support Centralized configuration/Management	M		
		Subnet advertisement	Should Support Centralized configuration/Management	M		
		Zero Touch provissioning/Ease of Provisioning & Deployment	Minimum configuration to be done device to make in active network and after comming in network necessary policy should be pushed from central device	M		
		Troubleshooting Tools a. Packet Capture b. Simulate Traffice Flow c. Speed Test	Should Support Centralized configuration/Management	M		
		Authentication of Device	Unauthticated Device Should not be connected in Bank Network	M		
		Disabling of Device From Network when the device remain isolated for more than defined time	Isolated Device should be isolated from network and require manual intervention	M		
		AD, NTP Server, TACACS, PIM, Monitoring tool, incident management tool	Should Support Centralized configuration/Management	M		
		Asset Tracking		M		When the devices where moved from one location ot other location

		SMS and Mail Notification	Should support SMS and Mail Notification	M		
7	**Visibility, Analytics, Monitoring & Reporting**					
		Real Time Alerting Notifications with Drill Down with historical data	All report should be generated from Central Location only	M		
		Real-Time Performance statistics with Drill Down with historical data	All report should be generated from Central Location only	M		
		Single customizable Console Dashboard for Health of Link and Devices with Drill Down with historical data	All report should be generated from Central Location only	M		
		Integration with Existing Tool for Network Statistics/SEIM/Ticketing/Incident Tools	All report should be generated from Central Location only	M		
		Reports for daily, weekly, monthly, yearly with Drill Down such as SLA/Down/ etc should be by default	All report should be generated from Central Location only	M		
		Logs Collection at Central Device and and Branch Device	All Logs should be preserved as per Bank requirement	M		
		Reports must be exportable to Excel /CSV format / PDF format	All report should be generated from Central Location only	M		
		Customization of report	Easy Customization of Report at User Level by Default	M		
		Total				

Note :

a. Any Specification declared compliant , however, it is found non-compliant during POC will lead to disqualification

b. Each desirable should be available by default.

c. This above tests are minimum in nature as per Scope of Work. Any Details missed out in this but mentioned in Scope of Work is also form part of POC by default.

d. Current Network Link Parameter for "Packet Loss < 1 % , Latency (round trip delays) < 120 msec (Branch) and < 70 msec (MPLS Backhaul), Jitter < 25 msec."

Technical Specifications
A. Branch Router Type A

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
A. General Feature			
1	Proposed Device should be able to run as both traditional router and sdwan router mode without changing the operating system. When running in SDWAN mode all control plane traffic should be manged by Central Controller only.		
2	Proposed Device should be automatically able to retrieve the network LAN information without running any separate routing protocols like BGP, OSPF between the edge devices		
3	Proposed Device should support multiple VPN solutions like IPSEC site-to-site, DMVPN and GET VPN along with SD-WAN in near future.		
4	Proposed Device should support End to End link Quality detection based on loss, latency and jitter and traffic routing based on link quality		
5	Proposed Device should providing end to end segmentation for different traffic and creating multiple virtual topology based on traffic segment		
6	Proposed Device should support SD WAN functionality & also provide on prem support for Stateful App Aware Firewall, IPS/IDS, URL filtering and Anti Malware protection from Day 1		
7	Proposed Device should be capable of Building various IPSec Tunnel/VRF like Hub and Spoke , full mesh , partial mesh, as per policy pushed from the Central controller and changing overlay tunnel/VRF by pushing policy from Central controller.		
8	Proposed Device should automatically build IPSec overlay tunnel/VRF once device is connected on WAN		
9	Proposed Device should support embedded hardware based IP SEC encryption and acceleration and support auto rotating encryption keys.		
10	Proposed Device should perform two factor device authentication with proposed Central Device before it starts communicating on WAN		
11	Proposed Device should support Centralized Path Computation and Policy Provisioning based on templates		
12	Proposed Device should support packet forwarding rate of minimum 290 KBPS for 64 byte packets per second on a single chassis.		
13	Proposed Device should have a default DRAM of minimum 8 GB and should be minimum scalable to 16 GB		
14	Proposed Device should have minimum flash RAM should be at least 8 GB for proper operation and scalable upto 16 GB to ensure storage of multiple router software images and logs.		
15	In Porposed Device, it must be possible to fast boot the router to ensure that for software upgrades can be done with minimum network downtime.		
16	Proposed Device should have High Mean Time Between Failure values to ensure long life of hardware.		
17	Proposed Device should be capable of booting from a remote node, where the image is present.		
18	Proposed Device should be hardened appliance from OEM and should have capability to boot from OEM provided image only and not from non-standard/unauthorized software		
19	Proposed Device should be a Single Box configuration and modular, so that to have the flexibility to use the appropriate choice of interfaces as and when required.		
20	Proposed Device should have Rack mounting kit for securing the device in standard Rack and are to be provided with Indian Standard Plug as per rating of the device		
21	Proposed Devices must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active/working software or configuration.		
22	Proposed Devices should be capable to send Email alerts and SMS alerts on meeting/exceeding the user defined thresholds.		
23	Proposed Device should not communicate with cloud controller which is placed by the OEM in cloud		
24	Proposed Device should not connect to central controller without authentication, if link /Power failure happens for the specified time period.		

25	Proposed Device should be able to access only through web based from the Bank network for configuring and controlling. SSH, USB port and telnet should be disabled by default and console should be password protected.		
26	Proposed Device shall function as Edge device in branch sites and in coordination with Controller, Centralized Management Device and any additional device supplied (if required) will achieve the functional requirements of the SD WAN solution.		
27	Proposed Device should have authentication and authorization only with the preconfigured Controller/Management server/Management Console which is placed in DC/DR.		
28	Proposed Device must support an authentication capability to authenticate a remote peer WAN device before forming overlay network.		
29	Proposed Device should be scalable to support up to 100 Mbps of throughput with all services enabled like IPSec, Firewall, IPS, URL filtering etc.		
30	Proposed Device should be provided with 10 Mbps SD-WAN license (in each direction) with encryption		
31	Proposed Device all the functionality and feature license should be pre-installed and it should be usable from day one of operation.		
32	Proposed Device all the license part should be applied to all SD-WAN devices through central controller and not from cloud		
33	Proposed Device should support IP SLA to track the reachability and measure the health of the links		
34	Proposed Device should support Scripts to take the action on the events happened on the device.		
35	Proposed Device should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		
36	Proposed Device should be able to secure large Layer 2 or MPLS networks to provide full-mesh connectivity by providing tunnel-less VPN without any impact on SDWAN router performance		
37	Proposed Model should support at least 10000 IP routes		
38	Proposed Model Should support minimum 10 segments/VRF/virtual domain for End to End Segmentation of traffic like - ATM , Corporate Users , Vendors		
39	Proposed Model Shall have traffic load balancing capability on all available WAN Links, based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
40	Proposed Model should support deep packet inspection to identify applications and should able to apply QoS based on application		
41	Proposed Model should support minimum 50 concurrent IPSec tunnels		
42	Proposed devices should have capability to bind with any static hardware (i.e. switch, ATM etc.) MAC IDs available in the LAN at respective location. The Control/Management of MAC-ID binding and MAC-ID repository should be at central controller. The central controller/device should probe the binded MAC-IDs for that Branch device on periodical basis/reboot/restart/power-on time. The Branch device should be automatically disabled if binded MAC IDs are Unrecognized/Unreachable by the central controller/device . OR Proposed devices should have capability to white-list devices (i.e. PC, NW Switch, ATM, Kiosk etc.) MAC IDs available in the LAN at respective location and SDWAN device should not allow access to any unrecognized/unknown MAC ID(s). The control/management of MAC-ID white-listing and MAC-ID repository should be at central controller.		
B. Physical Interfaces			
1	Proposed Device should have a) Minimum 4x1 GE base WAN Port b)Minumum 2 Serial/Smart Serial Interface (incase if Serial interface is not avaialable then converter should be provided with minimum 2 Serial interface in the converter with two ethernet output)(Synchronous Serial Interfaces should support for speeds up to 2 Mbps.)(Async/Sync serial interfaces (V.35) for speeds up to 115 Kbps.)		

2	Proposed Device should also have one free slot for future scalability to support Gigabit Ethernet/3G/4G/LTE/Wireless.		
3	Proposed Device should have OOB Port for management of Device or Console Ports		
4	Proposed Device Should have USB Ports		
5	Proposed Device must sync to the Network Time Protocol (NTP) server.		
C. Software Features: **Routing Protocols and General Features :**			
1	Proposed device should support Routing Information Protocol (RIPv1 and RIPv2), Layer 2 Tunneling Protocol (L2TP), Port Address Translation (PAT)		
2	Proposed device should support Dynamic Host Control Protocol (DHCP) server/relay/client		
3	Proposed device should support Access control lists (ACLs), Generic routing encapsulation (GRE)		
4	Proposed device should support Dynamic DNS Support		
5	Proposed Device should be capable of IP routing protocols like OSPF, BGP, policy routing, NAT or equivalent		
6	Proposed Device should Support for 802.1q VLANs, Demilitarized Zone (DMZ)		
7	Proposed Device Should Support for Multicast Routing Protocol - PIM Sparse Mode, PIM Sparse-Dense Mode / Source Specific Mode, Auto route processing (Auto-RP), ASM, SSM, IGMPv2 and v3 , BSR or equivalent		
8	Proposed Device Should support following routing protocols, IPv4, IPv6, static routes, RIP, OSPFv2, OSPFv3 , BGPv4, BGPv6, MPBGP, VRRP, BFD, DHCP server, DHCP relay, AAA RADIUS, TACACS+ , policy routing, NAT and 802.1q		
9	Proposed Device should be capable of WAN protocols like PPP, Multilink PPP,PAP & CHAP support. etc. or equivalent		
Support for IPv6 Features:			
1	Proposed Device Should support IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
2	Proposed Device Should support IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
3	Proposed Device Should support ICMPv6, IPv6 DHCP		
4	Proposed Device Should support should be on the IPv6 Ready Logo Program Approved List and should have passed the IPv6 Ready Logo Program Phase II		
5	Proposed Device Should support for the following IPv6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, IPv6 Policy based Routing, and IPv6 QoS.		
6	Proposed Device Should support following IP v6 Tunneling mechanisms : Automatic 6 to 4 tunnels, Automatic IP v4 compatible tunnels, IP v6 over IP v4 GRE Tunnels, ISATAP Tunneling Support. Or equivalent		
Security Features			
1	Proposed Device should have Secure SSH, HTTP (HTTPS), FTP,SFTP, and Telnet authentication		
2	Proposed Device should not have Service Password Recovery		
3	Proposed Device should support Hardware-accelerated IPSec 3DES/AES (256 Bit) termination/initiation, IPSec passthrough, Hardware-accelerated AES for IPSec		
4	Proposed Device Should support L2TP passthrough, 802.1X		
5	Proposed Device should support for System Logging through SNMP trap		
6	Proposed Device Should support Standard Access Lists, Extended Access Lists and Time based Access lists		
7	Proposed Device should Control SNMP access through the use of SNMP with MD5 authentication.		
8	Proposed Device can implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
9	Proposed Device Should support for Remote Authentication Dial-In User Service (RADIUS) and AAA.		
10	Proposed Device should support both IPsec and GRE encapsulation		

Management Features :			
1	Porposed Device Management should support: Telnet, Simple Network Management Protocol (SNMP), CLI, and Web based HTTP management / management software, RADIUS		
2	Proposed Device should have SNMP over IPV6 & AES & 3DES encryption and also support for SNMP Version 3		
3	Proposed Device should have Secure access through SSH and HTTPS		
4	Proposed Device should support SSL for access to the management webGUI.		
5	Proposed Device should have Multiple Privilege Levels based on Role and Responsibilties		
6	Proposed Model should have the feature of Zero-Touch Provisioning.		
Firewall and IPS Features			
1	Proposed devices should have Stateful Inspection Firewall, Transparent Bridging firewall or equivalent feature		
2	Proposed Device should have NAT transparency, Firewall support for skinny clients or equivalent feature		
3	Proposed Device Should have E-mail Inspection Engine & HTTP Inspection Engine		
4	Proposed Device Should have Advanced Application Inspection and Control		
5	Proposed Device should support for Intrusion Detection System / Intrusion Prevention System (IDS / IPS) functionality		
6	Proposed Device should support in-line IPS functionality with ability to schedule & automatically update signatures without requiring human intervention.		
7	Proposed Devices should have IPS functionality and should support tuning of the signatures i.e. changing the alert severity rating of signatures.		
8	Proposed Device should have IPS functionality and should support multiple event actions to block attacks i.e deny-attacker-inline, deny-connection-inline, deny-packet-inline, produce-alert & reset tcp connection.		
9	Proposed Device should support user based firewall functionality to create policies based on different classes of users/zones/Services.		
QOS Feature / High Performance			
1	Proposed Device should have Weighted Fair Queuing (WFQ), Class-Based WFQ (CBWFQ) or equivalent feature		
2	Proposed Device should have Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB or equivalent features		
3	Proposed Device should have Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED) or equivalent feature		
4	Proposed Device should have Support for LFI		
5	Proposed Device should have Support for RSVP, cRTP or equivalent feature, DiffServ, QoS Preclassify & Pre-fragmentation or equivalent feature, Class-Based Marking (CBM) or equivalent feature		
6	Proposed Device should able to support various traffic QoS methods i.e. priority queue, LLQ, Class based waited fair queue.		
7	Proposed Device should support Qos at Physical and subinterface level		
8	Proposed Device should support dual ended QoS where network parameters like latencies are measured and actions taken for the to-and-fro path.		
9	Proposed Device must be able to perform priority queuing in order to prioritize packet/traffic flows for each traffic class		
10	Proposed Device must support the use of diverse network links as WAN links. This must include the ability to use MPLS, DSL, Cable, Ethernet, 4G ,Satellite ,LTE etc.		
11	Proposed Device should direct traffic to use multiple queues simultaneously If DSCP tags are used to assign traffic to an MPLS queue and if the demand exceed the amount of traffic available on a given queue		
12	Proposed Device link failover should completed within milliseconds.		
13	Proposed Device must have ability to reorder any packets that are retransmitted during a failover.		

14	Proposed Device must include the ability to shift application traffic off of the degraded link on to a better performing link without any perceptable interruption in application continuity or lost packets.		
15	The proposed Device should adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth		
16	Proposed Device should be able to leverage multiple links simultaneously for a single application session, to ensure high application performance for bandwidth intensive applications such as multi-media streaming, backups, and large file transfers,		
17	Proposed Device should be able to load balance across links simultaneously, or leverage the secondary link for spill-over if the bandwidth required for one session exceeds the available bandwidth on the best link. This lets high bandwidth applications have as much bandwidth as they need to perform optimally.		
18	Proposed Device should bound together must include the ability to bind multiple MPLS links and an MPLS link with a public Internet link.		
19	In Proposed Device If the bandwidth of a single session exceeds that available on any single link, the application session must be able to use multiple links simultaneously.		
20	Proposed Device should be able to duplicate a session’s traffic for a given application to ensure high application performance for real-time applications, such as voice, and duplication should occur across two diverse links in order to minimize the chance of loss impacting the same data.		
21	Proposed Device should Packet duplicate for selected applications only.		
22	Proposed Device should support Virtual Router Redundancy Protocol (VRRP) (RFC 2338)		

Technical Specifications

Annexure 20B

B. Branch Router Type B

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
A. General Feature			
1	Proposed Device should be able to run as both traditional router and sdwan router mode without changing the operating system. When running in SDWAN mode all control plane traffic should be manged by Central Controller only.		
2	Proposed Device should be automatically able to retrieve the network LAN information without running any separate routing protocols like BGP, OSPF between the edge devices		
3	Proposed Device should support multiple VPN solutions like IPSEC site-to-site, DMVPN and GET VPN along with SD-WAN in near future.		
4	Proposed Device should support End to End link Quality detection based on loss, latency and jitter and traffic routing based on link quality		
5	Proposed Device should providing end to end segmentation for different traffic and creating multiple virtual topology based on traffic segment		
6	Proposed Device should support SD WAN functionality & also provide on prem support for Stateful App Aware Firewall, IPS/IDS, URL filtering and Anti Malware protection from Day 1		
7	Proposed Device should be capable of Building various IPSec Tunnel/VRF like Hub and Spoke , full mesh , partial mesh, as per policy pushed from the Central controller and changing overlay tunnel/VRF by pushing policy from Central controller.		
8	Proposed Device should automatically build IPSec overlay tunnel/VRF once device is connected on WAN		
9	Proposed Device should support embedded hardware based IP SEC encryption and acceleration and support auto rotating encryption keys.		
10	Proposed Device should perform two factor device authentication with proposed Central Device before it starts communicating on WAN		
11	Proposed Device should support Centralized Path Computation and Policy Provisioning based on templates		
12	Proposed Device should support packet forwarding rate of minimum 290 KBPS for 64 byte packets per second on a single chassis.		
13	Proposed Device should have a default DRAM of minimum 8 GB and should be minimum scalable to 16 GB		
14	Proposed Device should have minimum flash RAM should be at least 8 GB for proper operation and scalable upto 16 GB to ensure storage of multiple router software images and logs.		
15	In Porposed Device, it must be possible to fast boot the router to ensure that for software upgrades can be done with minimum network downtime.		
16	Proposed Device should have High Mean Time Between Failure values to ensure long life of hardware.		
17	Proposed Device should be capable of booting from a remote node, where the image is present.		
18	Proposed Device should be hardened appliance from OEM and should have capability to boot from OEM provided image only and not from non-standard/unauthorized software		
19	Proposed Device should be a Single Box configuration and modular, so that to have the flexibility to use the appropriate choice of interfaces as and when required.		
20	Proposed Device should have Rack mounting kit for securing the device in standard Rack and are to be provided with Indian Standard Plug as per rating of the device		
21	Proposed Devices must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active/working software or configuration.		
22	Proposed Devices should be capable to send Email alerts and SMS alerts on meeting/exceeding the user defined thresholds.		
23	Proposed Device should not communicate with cloud controller which is placed by the OEM in cloud		
24	Proposed Device should not connect to central controller without authentication, if link /Power failure happens for the specified time period.		

25	Proposed Device should be able to access only through web based from the Bank network for configuring and controlling. SSH, USB port and telnet should be disabled by default and console should be password protected.		
26	Proposed Device shall function as Edge device in branch sites and in coordination with Controller, Centralized Management Device and any additional device supplied (if required) will achieve the functional requirements of the SD WAN solution.		
27	Proposed Device should have authentication and authorization only with the preconfigured Controller/Management server/Management Console which is placed in DC/DR.		
28	Proposed Device must support an authentication capability to authenticate a remote peer WAN device before forming overlay network.		
29	Proposed Device should be scalable to support up to 100 Mbps of throughput with all services enabled like IPSec, Firewall, IPS, URL filtering etc.		
30	Proposed Device should be supplied with 20 Mbps SD-WAN license (in each direction) with encryption		
31	Proposed Device all the functionality and feature license should be pre-installed and it should be usable from day one of operation.		
32	Proposed Device all the license part should be applied to all SD-WAN devices through central controller and not from cloud		
33	Proposed Device should support IP SLA to track the reachability and measure the health of the links		
34	Proposed Device should support Scripts to take the action on the events happened on the device.		
35	Proposed Device should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		
36	Proposed Device should be able to secure large Layer 2 or MPLS networks to provide full-mesh connectivity by providing tunnel-less VPN without any impact on SDWAN router performance		
37	Proposed Model should support at least 10000 IP routes		
38	Proposed Model Should support minimum 10 segments/VRF/virtual domain for End to End Segmentation of traffic like - ATM , Corporate Users , Vendors		
39	Proposed Model Shall have traffic load balancing capability on all available WAN Links, based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
40	Proposed Model should support deep packet inspection to identify applications and should able to apply QoS based on application		
41	Proposed Model should support minimum 50 concurrent IPSec tunnels		
42	Proposed devices should have capability to bind with any static hardware (i.e. switch, ATM etc.) MAC IDs available in the LAN at respective location. The Control/Management of MAC-ID binding and MAC-ID repository should be at central controller. The central controller/device should probe the binded MAC-IDs for that Branch device on periodical basis/reboot/restart/power-on time. The Branch device should be automatically disabled if binded MAC IDs are Unrecognized/Unreachable by the central controller/device . OR Proposed devices should have capability to white-list devices (i.e. PC, NW Switch, ATM, Kiosk etc.) MAC IDs available in the LAN at respective location and SDWAN device should not allow access to any unrecognized/unknown MAC ID(s). The control/management of MAC-ID white-listing and MAC-ID repository should be at central controller.		
B. Physical Interfaces			
1	Proposed Device should have a) Minimum 4x1 GE base WAN Port b)Minumum 2 Serial/Smart Serial Interface (incase if Serial interface is not avaialable then converter should be provided with minimum 2 Serial interface in the converter with two ethernet output)(Synchronous Serial Interfaces should support for speeds up to 2 Mbps.)(Async/Sync serial interfaces (V.35) for speeds up to 115 Kbps.)		

2	Proposed Device should also have one free slot for future scalability to support Gigabit Ethernet/3G/4G/LTE/Wireless.		
3	Proposed Device should have OOB Port for management of Device or Console Ports		
4	Proposed Device Should have USB Ports		
5	Proposed Device must sync to the Network Time Protocol (NTP) server.		
C. Software Features:			
Routing Protocols and General Features :			
1	Proposed device should support Routing Information Protocol (RIPv1 and RIPv2), Layer 2 Tunneling Protocol (L2TP), Port Address Translation (PAT)		
2	Proposed device should support Dynamic Host Control Protocol (DHCP) server/relay/client		
3	Proposed device should support Access control lists (ACLs), Generic routing encapsulation (GRE)		
4	Proposed device should support Dynamic DNS Support		
5	Proposed Device should be capable of IP routing protocols like OSPF, BGP, policy routing, NAT or equivalent		
6	Proposed Device should Support for 802.1q VLANs, Demilitarized Zone (DMZ)		
7	Proposed Device Should Support for Multicast Routing Protocol - PIM Sparse Mode, PIM Sparse-Dense Mode / Source Specific Mode, Auto route processing (Auto-RP), ASM, SSM, IGMPv2 and v3 , BSR or equivalent		
8	Proposed Device Should support following routing protocols, IPv4, IPv6, static routes, RIP, OSPFv2, OSPFv3 , BGPv4, BGPv6, MPBGP, VRRP, BFD, DHCP server, DHCP relay, AAA RADIUS, TACACS+ , policy routing, NAT and 802.1q		
9	Proposed Device should be capable of WAN protocols like PPP, Multilink PPP,PAP & CHAP support. etc. or equivalent		
Support for IPv6 Features:			
1	Proposed Device Should support IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
2	Proposed Device Should support IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
3	Proposed Device Should support ICMPv6, IPv6 DHCP		
4	Proposed Device Should support should be on the IPv6 Ready Logo Program Approved List and should have passed the IPv6 Ready Logo Program Phase II		
5	Proposed Device Should support for the following IPv6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, IPv6 Policy based Routing, and IPv6 QoS.		
6	Proposed Device Should support following IP v6 Tunneling mechanisms : Automatic 6 to 4 tunnels, Automatic IP v4 compatible tunnels, IP v6 over IP v4 GRE Tunnels, ISATAP Tunneling Support. Or equivalent		
Security Features			
1	Proposed Device should have Secure SSH, HTTP (HTTPS), FTP,SFTP, and Telnet authentication		
2	Proposed Device should not have Service Password Recovery		
3	Proposed Device should support Hardware-accelerated IPSec 3DES/AES (256 Bit) termination/initiation, IPSec passthrough, Hardware-accelerated AES for IPSec		
4	Proposed Device Should support L2TP passthrough, 802.1X		
5	Proposed Device should support for System Logging through SNMP trap		
6	Proposed Device Should support Standard Access Lists, Extended Access Lists and Time based Access lists		
7	Proposed Device should Control SNMP access through the use of SNMP with MD5 authentication.		
8	Proposed Device can implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
9	Proposed Device Should support for Remote Authentication Dial-In User Service (RADIUS) and AAA.		
10	Proposed Device should support both IPsec and GRE encapsulation		

Management Features :			
1	Porposed Device Management should support: Telnet, Simple Network		
2	Proposed Device should have SNMP over IPV6 & AES & 3DES encryption and also support for SNMP Version 3		
3	Proposed Device should have Secure access through SSH and HTTPS		
4	Proposed Device should support SSL for access to the management webGUI.		
5	Proposed Device should have Multiple Privilege Levels based on Role and Responsibilties		
6	Proposed Model should have the feature of Zero-Touch Provisioning.		
Firewall and IPS Features			
1	Proposed devices should have Stateful Inspection Firewall, Transparent Bridging		
2	Proposed Device should have NAT transparency, Firewall support for skinny clients or equivalent feature		
3	Proposed Device Should have E-mail Inspection Engine & HTTP Inspection Engine		
4	Proposed Device Should have Advanced Application Inspection and Control		
5	Proposed Device should support for Intrusion Detection System / Intrusion Prevention System (IDS / IPS) functionality		
6	Proposed Device should support in-line IPS functionality with ability to schedule & automatically update signatures without requiring human intervention.		
7	Proposed Devices should have IPS functionality and should support tuning of the signatures i.e. changing the alert severity rating of signatures.		
8	Proposed Device should have IPS functionality and should support multiple event actions to block attacks i.e deny-attacker-inline, deny-connection-inline, deny-packet-inline, produce-alert & reset tcp connection.		
9	Proposed Device should support user based firewall functionality to create policies based on different classes of users/zones/Services.		
QOS Feature / High Performance			
1	Proposed Device should have Weighted Fair Queuing (WFQ), Class-Based WFQ		
2	Proposed Device should have Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB or equivalent features		
3	Proposed Device should have Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED) or equivalent feature		
4	Proposed Device should have Support for LFI		
5	Proposed Device should have Support for RSVP, cRTP or equivalent feature, DiffServ, QoS Preclassify & Pre-fragmentation or equivalent feature, Class-Based Marking (CBM) or equivalent feature		
6	Proposed Device should able to support various traffic QoS methods i.e. priority queue, LLQ, Class based waited fair queue.		
7	Proposed Device should support Qos at Physical and subinterface level		
8	Proposed Device should support dual ended QoS where network parameters like latencies are measured and actions taken for the to-and-fro path.		
9	Proposed Device must be able to perform priority queuing in order to prioritize packet/traffic flows for each traffic class		
10	Proposed Device must support the use of diverse network links as WAN links. This must include the ability to use MPLS, DSL, Cable, Ethernet, 4G ,Satellite ,LTE etc.		
11	Proposed Device should direct traffic to use multiple queues simultaneously If DSCP tags are used to assign traffic to an MPLS queue and if the demand exceed the amount of traffic available on a given queue		
12	Proposed Device link failover should completed within milliseconds.		
13	Proposed Device must have ability to reorder any packets that are retransmitted during a failover.		
14	Proposed Device must include the ability to shift application traffic off of the degraded link on to a better performing link without any perceptable interruption in application continuity or lost packets.		

15	The proposed Device should adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth		
16	Proposed Device should be able to leverage multiple links simultaneously for a single application session, to ensure high application performance for bandwidth intensive applications such as multi-media streaming, backups, and large file transfers,		
17	Proposed Device should be able to load balance across links simultaneously, or leverage the secondary link for spill-over if the bandwidth required for one session exceeds the available bandwidth on the best link. This lets high bandwidth applications have as much bandwidth as they need to perform optimally.		
18	Proposed Device should bound together must include the ability to bind multiple MPLS links and an MPLS link with a public Internet link.		
19	In Proposed Device If the bandwidth of a single session exceeds that available on any single link, the application session must be able to use multiple links simultaneously.		
20	Proposed Device should be able to duplicate a session’s traffic for a given application to ensure high application performance for real-time applications, such as voice, and duplication should occur across two diverse links in order to minimize the chance of loss impacting the same data.		
21	Proposed Device should Packet duplicate for selected applications only.		
22	Proposed Device should support Virtual Router Redundancy Protocol (VRRP) (RFC 2338)		

Technical Specifications
C. Branch Router Type C

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
A. General	Feature		
1	Proposed Device should be able to run as both traditional router and sdwan router mode without changing the operating system. When running in SDWAN mode all control plane traffic should be manged by Central Controller only.		
2	Proposed Device should be automatically able to retrieve the network LAN information without running any separate routing protocols like BGP, OSPF between the edge devices		
3	Proposed Device should support multiple VPN solutions like IPSEC site-to-site, DMVPN and GET VPN along with SD-WAN in near future.		
4	Proposed Device should support End to End link Quality detection based on loss, latency and jitter and traffic routing based on link quality		
5	Proposed Device should providing end to end segmentation for different traffic and creating multiple virtual topology based on traffic segment		
6	Proposed Device should support SD WAN functionality & also provide on prem support for Stateful App Aware Firewall, IPS/IDS, URL filtering and Anti Malware protection from Day 1		
7	Proposed Device should be capable of Building various IPSec Tunnel/VRF like Hub and Spoke , full mesh , partial mesh, as per policy pushed from the Central controller and changing overlay tunnel/VRF by pushing policy from Central controller.		
8	Proposed Device should automatically build IPSec overlay tunnel/VRF once device is connected on WAN		
9	Proposed Device should support embedded hardware based IP SEC encryption and acceleration and support auto rotating encryption keys.		
10	Proposed Device should perform two factor device authentication with proposed Central Device before it starts communicating on WAN		
11	Proposed Device should support Centralized Path Computation and Policy Provisioning based on templates		
12	Proposed Device should support packet forwarding rate of minimum 290 KBPS for 64 byte packets per second on a single chassis.		
13	Proposed Device should have a default DRAM of minimum 8 GB and should be minimum scalable to 16 GB		
14	Proposed Device should have minimum flash RAM should be at least 8 GB for proper operation and scalable upto 16 GB to ensure storage of multiple router software images and logs.		
15	In Porposed Device, it must be possible to fast boot the router to ensure that for software upgrades can be done with minimum network downtime.		
16	Proposed Device should have High Mean Time Between Failure values to ensure long life of hardware.		
17	Proposed Device should be capable of booting from a remote node, where the image is present.		
18	Proposed Device should be hardened appliance from OEM and should have capability to boot from OEM provided image only and not from non-standard/unauthorized software		
19	Proposed Device should be a Single Box configuration and modular, so that to have the flexibility to use the appropriate choice of interfaces as and when required.		
20	Proposed Device should have Rack mounting kit for securing the device in standard Rack and are to be provided with Indian Standard Plug as per rating of the device		
21	Proposed Devices must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active/working software or configuration.		
22	Proposed Devices should be capable to send Email alerts and SMS alerts on meeting/exceeding the user defined thresholds.		
23	Proposed Device should not communicate with cloud controller which is placed by the OEM in cloud		
24	Proposed Device should not connect to central controller without authentication, if link /Power failure happens for the specified time period.		

25	Proposed Device should be able to access only through web based from the Bank network for configuring and controlling. SSH, USB port and telnet should be disabled by default and console should be password protected.		
26	Proposed Device shall function as Edge device in branch sites and in coordination with Controller, Centralized Management Device and any additional device supplied (if required) will achieve the functional requirements of the SD WAN solution.		
27	Proposed Device should have authentication and authorization only with the preconfigured Controller/Management server/Management Console which is placed in DC/DR.		
28	Proposed Device must support an authentication capability to authenticate a remote peer WAN device before forming overlay network.		
29	Proposed Device should be scalable to support up to 100 Mbps of throughput with all services enabled like IPSec, Firewall, IPS, URL filtering etc.		
30	Proposed Device should be supplied with 50 Mbps SD-WAN license (in each direction) with encryption		
31	Proposed Device all the functionality and feature license should be pre-installed and it should be usable from day one of operation.		
32	Proposed Device all the license part should be applied to all SD-WAN devices through central controller and not from cloud		
33	Proposed Device should support IP SLA to track the reachability and measure the health of the links		
34	Proposed Device should support Scripts to take the action on the events happened on the device.		
35	Proposed Device should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		
36	Proposed Device should be able to secure large Layer 2 or MPLS networks to provide full-mesh connectivity by providing tunnel-less VPN without any impact on SDWAN router performance		
37	Proposed Model should support at least 10000 IP routes		
38	Proposed Model Should support minimum 10 segments/VRF/virtual domain for End to End Segmentation of traffic like - ATM , Corporate Users , Vendors		
39	Proposed Model Shall have traffic load balancing capability on all available WAN Links, based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
40	Proposed Model should support deep packet inspection to identify applications and should able to apply QoS based on application		
41	Proposed Model should support minimum 50 concurrent IPSec tunnels		
42	Proposed devices should have capability to bind with any static hardware (i.e. switch, ATM etc.) MAC IDs available in the LAN at respective location. The Control/Management of MAC-ID binding and MAC-ID repository should be at central controller. The central controller/device should probe the binded MAC-IDs for that Branch device on periodical basis/reboot/restart/power-on time. The Branch device should be automatically disabled if binded MAC IDs are Unrecognized/Unreachable by the central controller/device . OR Proposed devices should have capability to white-list devices (i.e. PC, NW Switch, ATM, Kiosk etc.) MAC IDs available in the LAN at respective location and SDWAN device should not allow access to any unrecognized/unknown MAC ID(s). The control/management of MAC-ID white-listing and MAC-ID repository should be at central controller.		
B. Physical Interfaces			
1	Proposed Device should have a) Minimum 4x1 GE base WAN Port b)Minumum 2 Serial/Smart Serial Interface (incase if Serial interface is not avaialable then converter should be provided with minimum 2 Serial interface in the converter with two ethernet output)(Synchronous Serial Interfaces should support for speeds up to 2 Mbps.)(Async/Sync serial interfaces (V.35) for speeds up to 115 Kbps.)		

2	Proposed Device should also have one free slot for future scalability to support Gigabit Ethernet/3G/4G/LTE/Wireless.		
3	Proposed Device should have OOB Port for management of Device or Console Ports		
4	Proposed Device Should have USB Ports		
5	Proposed Device must sync to the Network Time Protocol (NTP) server.		
C. Software Features:			
Routing Protocols and General Features :			
1	Proposed device should support Routing Information Protocol (RIPv1 and RIPv2), Layer 2 Tunneling Protocol (L2TP), Port Address Translation (PAT)		
2	Proposed device should support Dynamic Host Control Protocol (DHCP) server/relay/client		
3	Proposed device should support Access control lists (ACLs), Generic routing encapsulation (GRE)		
4	Proposed device should support Dynamic DNS Support		
5	Proposed Device should be capable of IP routing protocols like OSPF, BGP, policy routing, NAT or equivalent		
6	Proposed Device should Support for 802.1q VLANs, Demilitarized Zone (DMZ)		
7	Proposed Device Should Support for Multicast Routing Protocol - PIM Sparse Mode, PIM Sparse-Dense Mode / Source Specific Mode, Auto route processing (Auto-RP), ASM, SSM, IGMPv2 and v3 , BSR or equivalent		
8	Proposed Device Should support following routing protocols, IPv4, IPv6, static routes, RIP, OSPFv2, OSPFv3 , BGPv4, BGPv6, MPBGP, VRRP, BFD, DHCP server, DHCP relay, AAA RADIUS, TACACS+ , policy routing, NAT and 802.1q		
9	Proposed Device should be capable of WAN protocols like PPP, Multilink PPP,PAP & CHAP support. etc. or equivalent		
Support for IPv6 Features:			
1	Proposed Device Should support IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
2	Proposed Device Should support IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
3	Proposed Device Should support ICMPv6, IPv6 DHCP		
4	Proposed Device Should support should be on the IPv6 Ready Logo Program Approved List and should have passed the IPv6 Ready Logo Program Phase II		
5	Proposed Device Should support for the following IPv6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, IPv6 Policy based Routing, and IPv6 QoS.		
6	Proposed Device Should support following IP v6 Tunneling mechanisms : Automatic 6 to 4 tunnels, Automatic IP v4 compatible tunnels, IP v6 over IP v4 GRE Tunnels, ISATAP Tunneling Support. Or equivalent		
Security Features			
1	Proposed Device should have Secure SSH, HTTP (HTTPS), FTP,SFTP, and Telnet authentication		
2	Proposed Device should not have Service Password Recovery		
3	Proposed Device should support Hardware-accelerated IPSec 3DES/AES (256 Bit) termination/initiation, IPSec passthrough, Hardware-accelerated AES for IPSec		
4	Proposed Device Should support L2TP passthrough, 802.1X		
5	Proposed Device should support for System Logging through SNMP trap		
6	Proposed Device Should support Standard Access Lists, Extended Access Lists and Time based Access lists		
7	Proposed Device should Control SNMP access through the use of SNMP with MD5 authentication.		
8	Proposed Device can implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
9	Proposed Device Should support for Remote Authentication Dial-In User Service (RADIUS) and AAA.		
10	Proposed Device should support both IPsec and GRE encapsulation		

Technical Specifications
C. Branch Router Type C

Management Features :			
1	Porposed Device Management should support: Telnet, Simple Network		
2	Proposed Device should have SNMP over IPV6 & AES & 3DES encryption and also support for SNMP Version 3		
3	Proposed Device should have Secure access through SSH and HTTPS		
4	Proposed Device should support SSL for access to the management webGUI.		
5	Proposed Device should have Multiple Privilege Levels based on Role and Responsibilties		
6	Proposed Model should have the feature of Zero-Touch Provisioning.		
Firewall and IPS Features			
1	Proposed devices should have Stateful Inspection Firewall, Transparent Bridging		
2	Proposed Device should have NAT transparency, Firewall support for skinny clients or equivalent feature		
3	Proposed Device Should have E-mail Inspection Engine & HTTP Inspection Engine		
4	Proposed Device Should have Advanced Application Inspection and Control		
5	Proposed Device should support for Intrusion Detection System / Intrusion Prevention System (IDS / IPS) functionality		
6	Proposed Device should support in-line IPS functionality with ability to schedule & automatically update signatures without requiring human intervention.		
7	Proposed Devices should have IPS functionality and should support tuning of the signatures i.e. changing the alert severity rating of signatures.		
8	Proposed Device should have IPS functionality and should support multiple event actions to block attacks i.e deny-attacker-inline, deny-connection-inline, deny-packet-inline, produce-alert & reset tcp connection.		
9	Proposed Device should support user based firewall functionality to create policies based on different classes of users/zones/Services.		
QOS Feature / High Performance			
1	Proposed Device should have Weighted Fair Queuing (WFQ), Class-Based WFQ		
2	Proposed Device should have Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB or equivalent features		
3	Proposed Device should have Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED) or equivalent feature		
4	Proposed Device should have Support for LFI		
5	Proposed Device should have Support for RSVP, cRTP or equivalent feature, DiffServ, QoS Preclassify & Pre-fragmentation or equivalent feature, Class-Based Marking (CBM) or equivalent feature		
6	Proposed Device should able to support various traffic QoS methods i.e. priority queue, LLQ, Class based waited fair queue.		
7	Proposed Device should support Qos at Physical and subinterface level		
8	Proposed Device should support dual ended QoS where network parameters like latencies are measured and actions taken for the to-and-fro path.		
9	Proposed Device must be able to perform priority queuing in order to prioritize packet/traffic flows for each traffic class		
10	Proposed Device must support the use of diverse network links as WAN links. This must include the ability to use MPLS, DSL, Cable, Ethernet, 4G ,Satellite ,LTE etc.		
11	Proposed Device should direct traffic to use multiple queues simultaneously If DSCP tags are used to assign traffic to an MPLS queue and if the demand exceed the amount of traffic available on a given queue		
12	Proposed Device link failover should completed within milliseconds.		
13	Proposed Device must have ability to reorder any packets that are retransmitted during a failover.		
14	Proposed Device must include the ability to shift application traffic off of the degraded link on to a better performing link without any perceptable interruption in application continuity or lost packets.		

15	The proposed Device should adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth		
16	Proposed Device should be able to leverage multiple links simultaneously for a single application session, to ensure high application performance for bandwidth intensive applications such as multi-media streaming, backups, and large file transfers,		
17	Proposed Device should be able to load balance across links simultaneously, or leverage the secondary link for spill-over if the bandwidth required for one session exceeds the available bandwidth on the best link. This lets high bandwidth applications have as much bandwidth as they need to perform optimally.		
18	Proposed Device should bound together must include the ability to bind multiple MPLS links and an MPLS link with a public Internet link.		
19	In Proposed Device If the bandwidth of a single session exceeds that available on any single link, the application session must be able to use multiple links simultaneously.		
20	Proposed Device should be able to duplicate a session’s traffic for a given application to ensure high application performance for real-time applications, such as voice, and duplication should occur across two diverse links in order to minimize the chance of loss impacting the same data.		
21	Proposed Device should Packet duplicate for selected applications only.		
22	Proposed Device should support Virtual Router Redundancy Protocol (VRRP) (RFC 2338)		

Technical Specifications
D. Branch Router Type D

Sr. No. A. General Feature	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	Proposed Device should be able to run as both traditional router and sdwan router mode without changing the operating system. When running in SDWAN mode all control plane traffic should be manged by Central Controller only.		
2	Proposed Device should be automatically able to retrieve the network LAN information without running any separate routing protocols like BGP, OSPF between the edge devices		
3	Proposed Device should support multiple VPN solutions like IPSEC site-to-site, DMVPN and GET VPN along with SD-WAN in near future.		
4	Proposed Device should support End to End link Quality detection based on loss, latency and jitter and traffic routing based on link quality		
5	Proposed Device should providing end to end segmentation for different traffic and creating multiple virtual topology based on traffic segment		
6	Proposed Device should support SD WAN functionality & also provide on prem support for Stateful App Aware Firewall, IPS/IDS, URL filtering and Anti Malware protection from Day 1		
7	Proposed Device should be capable of Building various IPSec Tunnel/VRF like Hub and Spoke , full mesh , partial mesh, as per policy pushed from the Central controller and changing overlay tunnel/VRF by pushing policy from Central controller.		
8	Proposed Device should automatically build IPSec overlay tunnel/VRF once device is connected on WAN		
9	Proposed Device should support embedded hardware based IP SEC encryption and acceleration and support auto rotating encryption keys.		
10	Proposed Device should perform two factor device authentication with proposed Central Device before it starts communicating on WAN		
11	Proposed Device should support Centralized Path Computation and Policy Provisioning based on templates		
12	Proposed Device should support packet forwarding rate of minimum 290 KBPS for 64 byte packets per second on a single chassis.		
13	Proposed Device should have a default DRAM of minimum 16 GB and should be minimum scalable to 32 GB		
14	Proposed Device should have minimum flash RAM should be at least 16 GB for proper operation and scalable upto 32 GB to ensure storage of multiple router software images and logs.		
15	In Porposed Device, it must be possible to fast boot the router to ensure that for software upgrades can be done with minimum network downtime.		
16	Proposed Device should have High Mean Time Between Failure values to ensure long life of hardware.		
17	Proposed Device should be capable of booting from a remote node, where the image is present.		
18	Proposed Device should be hardened appliance from OEM and should have capability to boot from OEM provided image only and not from non-standard/unauthorized software		
19	Proposed Device should be a Single Box configuration and modular, so that to have the flexibility to use the appropriate choice of interfaces as and when required.		
20	Proposed Device should have Rack mounting kit for securing the device in standard Rack and are to be provided with Indian Standard Plug as per rating of the device		
21	Proposed Devices must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active/working software or configuration.		
22	Proposed Devices should be capable to send Email alerts and SMS alerts on meeting/exceeding the user defined thresholds.		
23	Proposed Device should not communicate with cloud controller which is placed by the OEM in cloud		
24	Proposed Device should not connect to central controller without authentication, if link /Power failure happens for the specified time period.		

25	Proposed Device should be able to access only through web based from the Bank network for configuring and controlling. SSH, USB port and telnet should be disabled by default and console should be password protected.		
26	Proposed Device shall function as Edge device in branch sites and in coordination with Controller, Centralized Management Device and any additional device supplied (if required) will achieve the functional requirements of the SD WAN solution.		
27	Proposed Device should have authentication and authorization only with the preconfigured Controller/Management server/Management Console which is placed in DC/DR.		
28	Proposed Device must support an authentication capability to authenticate a remote peer WAN device before forming overlay network.		
29	Proposed Device should be scalable to support up to 200 Mbps of throughput with all services enabled like IPSec, Firewall, IPS, URL filtering etc.		
30	Proposed Device should be supplied with 100 Mbps SD-WAN license (in each direction) with encryption		
31	Proposed Device all the functionality and feature license should be pre-installed and it should be usable from day one of operation.		
32	Proposed Device all the license part should be applied to all SD-WAN devices through central controller and not from cloud		
33	Proposed Device should support IP SLA to track the reachability and measure the health of the links		
34	Proposed Device should support Scripts to take the action on the events happened on the device.		
35	Proposed Device should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		
36	Proposed Device should be able to secure large Layer 2 or MPLS networks to provide full-mesh connectivity by providing tunnel-less VPN without any impact on SDWAN router performance		
37	Proposed Model should support at least 10000 IP routes		
38	Proposed Model Should support minimum 10 segments/VRF/virtual domain for End to End Segmentation of traffic like - ATM , Corporate Users , Vendors		
39	Proposed Model Shall have traffic load balancing capability on all available WAN Links, based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
40	Proposed Model should support deep packet inspection to identify applications and should able to apply QoS based on application		
41	Proposed Model should support minimum 50 concurrent IPSec tunnels		
42	Proposed devices should have capability to bind with any static hardware (i.e. switch, ATM etc.) MAC IDs available in the LAN at respective location. The Control/Management of MAC-ID binding and MAC-ID repository should be at central controller. The central controller/device should probe the binded MAC-IDs for that Branch device on periodical basis/reboot/restart/power-on time. The Branch device should be automatically disabled if binded MAC IDs are Unrecognized/Unreachable by the central controller/device . OR Proposed devices should have capability to white-list devices (i.e. PC, NW Switch, ATM, Kiosk etc.) MAC IDs available in the LAN at respective location and SDWAN device should not allow access to any unrecognized/unknown MAC ID(s). The control/management of MAC-ID white-listing and MAC-ID repository should be at central controller.		
B. Physical Interfaces			
1	Proposed Device should have a) Minimum 4x1 GE base WAN Port b)Minumum 2 Serial/Smart Serial Interface (incase if Serial interface is not avaialable then converter should be provided with minimum 2 Serial interface in the converter with two ethernet output)(Synchronous Serial Interfaces should support for speeds up to 2 Mbps.)(Async/Sync serial interfaces (V.35) for speeds up to 115 Kbps.)		

2	Proposed Device should also have one free slot for future scalability to support Gigabit Ethernet/3G/4G/LTE/Wireless.		
3	Proposed Device should have OOB Port for management of Device or Console Ports		
4	Proposed Device Should have USB Ports		
5	Proposed Device must sync to the Network Time Protocol (NTP) server.		
C. Software Features:			
Routing Protocols and General Features :			
1	Proposed device should support Routing Information Protocol (RIPv1 and RIPv2), Layer 2 Tunneling Protocol (L2TP), Port Address Translation (PAT)		
2	Proposed device should support Dynamic Host Control Protocol (DHCP) server/relay/client		
3	Proposed device should support Access control lists (ACLs), Generic routing encapsulation (GRE)		
4	Proposed device should support Dynamic DNS Support		
5	Proposed Device should be capable of IP routing protocols like OSPF, BGP, policy routing, NAT or equivalent		
6	Proposed Device should Support for 802.1q VLANs, Demilitarized Zone (DMZ)		
7	Proposed Device Should Support for Multicast Routing Protocol - PIM Sparse Mode, PIM Sparse-Dense Mode / Source Specific Mode, Auto route processing (Auto-RP), ASM, SSM, IGMPv2 and v3 , BSR or equivalent		
8	Proposed Device Should support following routing protocols, IPv4, IPv6, static routes, RIP, OSPFv2, OSPFv3 , BGPv4, BGPv6, MPBGP, VRRP, BFD, DHCP server, DHCP relay, AAA RADIUS, TACACS+ , policy routing, NAT and 802.1q		
9	Proposed Device should be capable of WAN protocols like PPP, Multilink PPP,PAP & CHAP support. etc. or equivalent		
Support for IPv6 Features:			
1	Proposed Device Should support IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
2	Proposed Device Should support IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
3	Proposed Device Should support ICMPv6, IPv6 DHCP		
4	Proposed Device Should support should be on the IPv6 Ready Logo Program Approved List and should have passed the IPv6 Ready Logo Program Phase II		
5	Proposed Device Should support for the following IPv6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, IPv6 Policy based Routing, and IPv6 QoS.		
6	Proposed Device Should support following IP v6 Tunneling mechanisms : Automatic 6 to 4 tunnels, Automatic IP v4 compatible tunnels, IP v6 over IP v4 GRE Tunnels, ISATAP Tunneling Support. Or equivalent		
Security Features			
1	Proposed Device should have Secure SSH, HTTP (HTTPS), FTP,SFTP, and Telnet authentication		
2	Proposed Device should not have Service Password Recovery		
3	Proposed Device should support Hardware-accelerated IPSec 3DES/AES (256 Bit) termination/initiation, IPSec passthrough, Hardware-accelerated AES for IPSec		
4	Proposed Device Should support L2TP passthrough, 802.1X		
5	Proposed Device should support for System Logging through SNMP trap		
6	Proposed Device Should support Standard Access Lists, Extended Access Lists and Time based Access lists		
7	Proposed Device should Control SNMP access through the use of SNMP with MD5 authentication.		
8	Proposed Device can implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
9	Proposed Device Should support for Remote Authentication Dial-In User Service (RADIUS) and AAA.		
10	Proposed Device should support both IPsec and GRE encapsulation		

Technical Specifications
D. Branch Router Type D

Management Features :			
1	Porposed Device Management should support: Telnet, Simple Network		
2	Proposed Device should have SNMP over IPV6 & AES & 3DES encryption and also support for SNMP Version 3		
3	Proposed Device should have Secure access through SSH and HTTPS		
4	Proposed Device should support SSL for access to the management webGUI.		
5	Proposed Device should have Multiple Privilege Levels based on Role and Responsibilties		
6	Proposed Model should have the feature of Zero-Touch Provisioning.		
Firewall and IPS Features			
1	Proposed devices should have Stateful Inspection Firewall, Transparent Bridging		
2	Proposed Device should have NAT transparency, Firewall support for skinny clients or equivalent feature		
3	Proposed Device Should have E-mail Inspection Engine & HTTP Inspection Engine		
4	Proposed Device Should have Advanced Application Inspection and Control		
5	Proposed Device should support for Intrusion Detection System / Intrusion Prevention System (IDS / IPS) functionality		
6	Proposed Device should support in-line IPS functionality with ability to schedule & automatically update signatures without requiring human intervention.		
7	Proposed Devices should have IPS functionality and should support tuning of the signatures i.e. changing the alert severity rating of signatures.		
8	Proposed Device should have IPS functionality and should support multiple event actions to block attacks i.e deny-attacker-inline, deny-connection-inline, deny-packet-inline, produce-alert & reset tcp connection.		
9	Proposed Device should support user based firewall functionality to create policies based on different classes of users/zones/Services.		
QOS Feature / High Performance			
1	Proposed Device should have Weighted Fair Queuing (WFQ), Class-Based WFQ		
2	Proposed Device should have Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB or equivalent features		
3	Proposed Device should have Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED) or equivalent feature		
4	Proposed Device should have Support for LFI		
5	Proposed Device should have Support for RSVP, cRTP or equivalent feature, DiffServ, QoS Preclassify & Pre-fragmentation or equivalent feature, Class-Based Marking (CBM) or equivalent feature		
6	Proposed Device should able to support various traffic QoS methods i.e. priority queue, LLQ, Class based waited fair queue.		
7	Proposed Device should support Qos at Physical and subinterface level		
8	Proposed Device should support dual ended QoS where network parameters like latencies are measured and actions taken for the to-and-fro path.		
9	Proposed Device must be able to perform priority queuing in order to prioritize packet/traffic flows for each traffic class		
10	Proposed Device must support the use of diverse network links as WAN links. This must include the ability to use MPLS, DSL, Cable, Ethernet, 4G ,Satellite ,LTE etc.		
11	Proposed Device should direct traffic to use multiple queues simultaneously If DSCP tags are used to assign traffic to an MPLS queue and if the demand exceed the amount of traffic available on a given queue		
12	Proposed Device link failover should completed within milliseconds.		
13	Proposed Device must have ability to reorder any packets that are retransmitted during a failover.		
14	Proposed Device must include the ability to shift application traffic off of the degraded link on to a better performing link without any perceptable interruption in application continuity or lost packets.		

15	The proposed Device should adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth		
16	Proposed Device should be able to leverage multiple links simultaneously for a single application session, to ensure high application performance for bandwidth intensive applications such as multi-media streaming, backups, and large file transfers,		
17	Proposed Device should be able to load balance across links simultaneously, or leverage the secondary link for spill-over if the bandwidth required for one session exceeds the available bandwidth on the best link. This lets high bandwidth applications have as much bandwidth as they need to perform optimally.		
18	Proposed Device should bound together must include the ability to bind multiple MPLS links and an MPLS link with a public Internet link.		
19	In Proposed Device If the bandwidth of a single session exceeds that available on any single link, the application session must be able to use multiple links simultaneously.		
20	Proposed Device should be able to duplicate a session’s traffic for a given application to ensure high application performance for real-time applications, such as voice, and duplication should occur across two diverse links in order to minimize the chance of loss impacting the same data.		
21	Proposed Device should Packet duplicate for selected applications only.		
22	Proposed Device should support Virtual Router Redundancy Protocol (VRRP) (RFC 2338)		

Annexure 20E

Technical Specifications
E. Branch Router Type E

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
A. General Feature			
1	Proposed Device should be able to run as both traditional router and sdwan router mode without changing the operating system. When running in SDWAN mode all control plane traffic should be manged by Central Controller only.		
2	Proposed Device should be automatically able to retrieve the network LAN information without running any separate routing protocols like BGP, OSPF between the edge devices		
3	Proposed Device should support multiple VPN solutions like IPSEC site-to-site, DMVPN and GET VPN along with SD-WAN in near future.		
4	Proposed Device should support End to End link Quality detection based on loss, latency and jitter and traffic routing based on link quality		
5	Proposed Device should providing end to end segmentation for different traffic and creating multiple virtual topology based on traffic segment		
6	Proposed Device should support SD WAN functionality & also provide on prem support for Stateful App Aware Firewall, IPS/IDS, URL filtering and Anti Malware protection from Day 1		
7	Proposed Device should be capable of Building various IPSec Tunnel/VRF like Hub and Spoke , full mesh , partial mesh, as per policy pushed from the Central controller and changing overlay tunnel/VRF by pushing policy from Central controller.		
8	Proposed Device should automatically build IPSec overlay tunnel/VRF once device is connected on WAN		
9	Proposed Device should support embedded hardware based IP SEC encryption and acceleration and support auto rotating encryption keys.		
10	Proposed Device should perform two factor device authentication with proposed Central Device before it starts communicating on WAN		
11	Proposed Device should support Centralized Path Computation and Policy Provisioning based on templates		
12	Proposed Device should support packet forwarding rate of minimum 290 KBPS for 64 byte packets per second on a single chassis.		
13	Proposed Device should have a default DRAM of minimum 16 GB and should be minimum scalable to 32 GB		
14	Proposed Device should have minimum flash RAM should be at least 16 GB for proper operation and scalable upto 32 GB to ensure storage of multiple router software images and logs.		
15	In Porposed Device, it must be possible to fast boot the router to ensure that for software upgrades can be done with minimum network downtime.		
16	Proposed Device should have High Mean Time Between Failure values to ensure long life of hardware.		
17	Proposed Device should be capable of booting from a remote node, where the image is present.		
18	Proposed Device should be hardened appliance from OEM and should have capability to boot from OEM provided image only and not from non-standard/unauthorized software		
19	Proposed Device should be a Single Box configuration and modular, so that to have the flexibility to use the appropriate choice of interfaces as and when required.		
20	Proposed Device should have Rack mounting kit for securing the device in standard Rack and are to be provided with Indian Standard Plug as per rating of the device		
21	Proposed Devices must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active/working software or configuration.		
22	Proposed Devices should be capable to send Email alerts and SMS alerts on meeting/exceeding the user defined thresholds.		
23	Proposed Device should not communicate with cloud controller which is placed by the OEM in cloud		
24	Proposed Device should not connect to central controller without authentication, if link /Power failure happens for the specified time period.		

25	Proposed Device should be able to access only through web based from the Bank network for configuring and controlling. SSH, USB port and telnet should be disabled by default and console should be password protected.		
26	Proposed Device shall function as Edge device in branch sites and in coordination with Controller, Centralized Management Device and any additional device supplied (if required) will achieve the functional requirements of the SD WAN solution.		
27	Proposed Device should have authentication and authorization only with the preconfigured Controller/Management server/Management Console which is placed in DC/DR.		
28	Proposed Device must support an authentication capability to authenticate a remote peer WAN device before forming overlay network.		
29	Proposed Device should be scalable to support up to 500 Mbps of throughput with all services enabled like IPSec, Firewall, IPS, URL filtering etc.		
30	Proposed Device should suppilied with 200 Mbps SD-WAN license (in each direction) with encryption		
31	Proposed Device all the functionality and feature license should be pre-installed and it should be usable from day one of operation.		
32	Proposed Device all the license part should be applied to all SD-WAN devices through central controller and not from cloud		
33	Proposed Device should support IP SLA to track the reachability and measure the health of the links		
34	Proposed Device should support Scripts to take the action on the events happened on the device.		
35	Proposed Device should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		
36	Proposed Device should be able to secure large Layer 2 or MPLS networks to provide full-mesh connectivity by providing tunnel-less VPN without any impact on SDWAN router performance		
37	Proposed Model should support at least 10000 IP routes		
38	Proposed Model Should support minimum 10 segments/VRF/virtual domain for End to End Segmentation of traffic like - ATM , Corporate Users , Vendors		
39	Proposed Model Shall have traffic load balancing capability on all available WAN Links, based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
40	Proposed Model should support deep packet inspection to identify applications and should able to apply QoS based on application		
41	Proposed Model should support minimum 50 concurrent IPSec tunnels		
42	Proposed devices should have capability to bind with any static hardware (i.e. switch, ATM etc.) MAC IDs available in the LAN at respective location. The Control/Management of MAC-ID binding and MAC-ID repository should be at central controller. The central controller/device should probe the binded MAC-IDs for that Branch device on periodical basis/reboot/restart/power-on time. The Branch device should be automatically disabled if binded MAC IDs are Unrecognized/Unreachable by the central controller/device . OR Proposed devices should have capability to white-list devices (i.e. PC, NW Switch, ATM, Kiosk etc.) MAC IDs available in the LAN at respective location and SDWAN device should not allow access to any unrecognized/unknown MAC ID(s). The control/management of MAC-ID white-listing and MAC-ID repository should be at central controller.		
B. Physical Interfaces			
1	Proposed Device should have a) Minimum 4x1 GE base WAN Port b)Minumum 2 Serial/Smart Serial Interface (incase if Serial interface is not avaialable then converter should be provided with minimum 2 Serial interface in the converter with two ethernet output)(Synchronous Serial Interfaces should support for speeds up to 2 Mbps.)(Async/Sync serial interfaces (V.35) for speeds up to 115 Kbps.)		

2	Proposed Device should also have one free slot for future scalability to support Gigabit Ethernet/3G/4G/LTE/Wireless.		
3	Proposed Device should have OOB Port for management of Device or Console Ports		
4	Proposed Device Should have USB Ports		
5	Proposed Device must sync to the Network Time Protocol (NTP) server.		
C. Software Features:			
Routing Protocols and General Features :			
1	Proposed device should support Routing Information Protocol (RIPv1 and RIPv2), Layer 2 Tunneling Protocol (L2TP), Port Address Translation (PAT)		
2	Proposed device should support Dynamic Host Control Protocol (DHCP) server/relay/client		
3	Proposed device should support Access control lists (ACLs), Generic routing encapsulation (GRE)		
4	Proposed device should support Dynamic DNS Support		
5	Proposed Device should be capable of IP routing protocols like OSPF, BGP, policy routing, NAT or equivalent		
6	Proposed Device should Support for 802.1q VLANs, Demilitarized Zone (DMZ)		
7	Proposed Device Should Support for Multicast Routing Protocol - PIM Sparse Mode, PIM Sparse-Dense Mode / Source Specific Mode, Auto route processing (Auto-RP), ASM, SSM, IGMPv2 and v3 , BSR or equivalent		
8	Proposed Device Should support following routing protocols, IPv4, IPv6, static routes, RIP, OSPFv2, OSPFv3 , BGPv4, BGPv6, MPBGP, VRRP, BFD, DHCP server, DHCP relay, AAA RADIUS, TACACS+ , policy routing, NAT and 802.1q		
9	Proposed Device should be capable of WAN protocols like PPP, Multilink PPP,PAP & CHAP support. etc. or equivalent		
Support for IPv6 Features:			
1	Proposed Device Should support IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
2	Proposed Device Should support IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
3	Proposed Device Should support ICMPv6, IPv6 DHCP		
4	Proposed Device Should support should be on the IPv6 Ready Logo Program Approved List and should have passed the IPv6 Ready Logo Program Phase II		
5	Proposed Device Should support for the following IPv6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, IPv6 Policy based Routing, and IPv6 QoS.		
6	Proposed Device Should support following IP v6 Tunneling mechanisms : Automatic 6 to 4 tunnels, Automatic IP v4 compatible tunnels, IP v6 over IP v4 GRE Tunnels, ISATAP Tunneling Support. Or equivalent		
Security Features			
1	Proposed Device should have Secure SSH, HTTP (HTTPS), FTP,SFTP, and Telnet authentication		
2	Proposed Device should not have Service Password Recovery		
3	Proposed Device should support Hardware-accelerated IPSec 3DES/AES (256 Bit) termination/initiation, IPSec passthrough, Hardware-accelerated AES for IPSec		
4	Proposed Device Should support L2TP passthrough, 802.1X		
5	Proposed Device should support for System Logging through SNMP trap		
6	Proposed Device Should support Standard Access Lists, Extended Access Lists and Time based Access lists		
7	Proposed Device should Control SNMP access through the use of SNMP with MD5 authentication.		
8	Proposed Device can implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
9	Proposed Device Should support for Remote Authentication Dial-In User Service (RADIUS) and AAA.		
10	Proposed Device should support both IPsec and GRE encapsulation		

Management Features :			
1	Porposed Device Management should support: Telnet, Simple Network		
2	Proposed Device should have SNMP over IPV6 & AES & 3DES encryption and also support for SNMP Version 3		
3	Proposed Device should have Secure access through SSH and HTTPS		
4	Proposed Device should support SSL for access to the management webGUI.		
5	Proposed Device should have Multiple Privilege Levels based on Role and Responsibilties		
6	Proposed Model should have the feature of Zero-Touch Provisioning.		
Firewall and IPS Features			
1	Proposed devices should have Stateful Inspection Firewall, Transparent Bridging		
2	Proposed Device should have NAT transparency, Firewall support for skinny clients or equivalent feature		
3	Proposed Device Should have E-mail Inspection Engine & HTTP Inspection Engine		
4	Proposed Device Should have Advanced Application Inspection and Control		
5	Proposed Device should support for Intrusion Detection System / Intrusion Prevention System (IDS / IPS) functionality		
6	Proposed Device should support in-line IPS functionality with ability to schedule & automatically update signatures without requiring human intervention.		
7	Proposed Devices should have IPS functionality and should support tuning of the signatures i.e. changing the alert severity rating of signatures.		
8	Proposed Device should have IPS functionality and should support multiple event actions to block attacks i.e deny-attacker-inline, deny-connection-inline, deny-packet-inline, produce-alert & reset tcp connection.		
9	Proposed Device should support user based firewall functionality to create policies based on different classes of users/zones/Services.		
QOS Feature / High Performance			
1	Proposed Device should have Weighted Fair Queuing (WFQ), Class-Based WFQ		
2	Proposed Device should have Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB or equivalent features		
3	Proposed Device should have Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED) or equivalent feature		
4	Proposed Device should have Support for LFI		
5	Proposed Device should have Support for RSVP, cRTP or equivalent feature, DiffServ, QoS Preclassify & Pre-fragmentation or equivalent feature, Class-Based Marking (CBM) or equivalent feature		
6	Proposed Device should able to support various traffic QoS methods i.e. priority queue, LLQ, Class based waited fair queue.		
7	Proposed Device should support Qos at Physical and subinterface level		
8	Proposed Device should support dual ended QoS where network parameters like latencies are measured and actions taken for the to-and-fro path.		
9	Proposed Device must be able to perform priority queuing in order to prioritize packet/traffic flows for each traffic class		
10	Proposed Device must support the use of diverse network links as WAN links. This must include the ability to use MPLS, DSL, Cable, Ethernet, 4G ,Satellite ,LTE etc.		
11	Proposed Device should direct traffic to use multiple queues simultaneously If DSCP tags are used to assign traffic to an MPLS queue and if the demand exceed the amount of traffic available on a given queue		
12	Proposed Device link failover should completed within milliseconds.		
13	Proposed Device must have ability to reorder any packets that are retransmitted during a failover.		
14	Proposed Device must include the ability to shift application traffic off of the degraded link on to a better performing link without any perceptable interruption in application continuity or lost packets.		

15	The proposed Device should adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth		
16	Proposed Device should be able to leverage multiple links simultaneously for a single application session, to ensure high application performance for bandwidth intensive applications such as multi-media streaming, backups, and large file transfers,		
17	Proposed Device should be able to load balance across links simultaneously, or leverage the secondary link for spill-over if the bandwidth required for one session exceeds the available bandwidth on the best link. This lets high bandwidth applications have as much bandwidth as they need to perform optimally.		
18	Proposed Device should bound together must include the ability to bind multiple MPLS links and an MPLS link with a public Internet link.		
19	In Proposed Device If the bandwidth of a single session exceeds that available on any single link, the application session must be able to use multiple links simultaneously.		
20	Proposed Device should be able to duplicate a session’s traffic for a given application to ensure high application performance for real-time applications, such as voice, and duplication should occur across two diverse links in order to minimize the chance of loss impacting the same data.		
21	Proposed Device should Packet duplicate for selected applications only.		
22	Proposed Device should support Virtual Router Redundancy Protocol (VRRP) (RFC 2338)		

Technical Specifications
F. DC-DR Central Device

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
A.	General Feature		
1	The Proposed Central Device for DC -DR should support 10000 Branches with throughput of 40 GBPS with encryption from Day 1 and sclable upto 100 GBPS in future		
2	The Proposed Central Device have redundency on the critical component i.e. 1:1 Supervisor/dual control Module from Day 1 and 1:1 Power supply unit edundancy from day one		
3	The Proposed Central Device must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multi processor based for enhanced performance.		
4	The Proposed Central Device must support intelligent traffic management and QoS features to allocate network resources on application needs and QoS priorities.		
5	The Proposed Central Device must have onboard support for intelligent traffic measurement and analysis.		
6	The Proposed Central Device must support flow/packet based traffic analysis feature.		
7	The Proposed Central Device must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631		
8	Rack mounting kit for securing the Proposed Central Device in standard rack are to be provided with Indian Standard Plug as well as C14/C19 cables		
9	Proposed Central Device must support configuration rollback feature to detect and recover from software and configuration errors by reverting back to previously active/working software or configuration.		
10	Proposed Central Device should be capable to send Email alerts and SMS alerts on meeting/exceeding the user defined thresholds.		
11	Proposed Central Device shall function as Central device in DC/DR and in coordination with Controller, Centralized Management Device and any additional device supplied (if required) will achieve the functional requirements of the SD WAN solution.		
12	Proposed Central Device should have authentication and authorization only with the preconfigured Controller/Management server/Management Console which is placed in DC/DR.		
13	Proposed Central Device should not communicate with cloud controller which is placed by the OEM in cloud		
14	Proposed Central Device should not connect to central controller without manual intervention, for authentication, if link /Power failure happens for the specified time period.		
15	Proposed Central Device should be able to access only through web based from the Bank network for configuring and controlling. SSH, USB port and telnet should be disabled by default and console should be password protected.		
16	From the central controller we must be able to fix the location of the Branch device geographically based on the Latitude and Longitude position using GPS. If Latitude and Longitude of the mapped device changes (precision 10m) at controller, then the device should be disabled automatically from the central controller. Precision can be set for device wise/location wise, and should not be only global parameter.		
17	All the functionality and feature license should be pre-installed and it should be usable from day one of operation.		
18	All the license part should be applied to all proposed central devices through central controller and not from cloud		
19	Proposed Central Device should have the feature of Zero-Touch Provisioning.		
20	Proposed Central Device should be able to run as both traditional router and sdwan router mode without changing the operating system. When running in SDWAN mode all control plane traffic should be manged by Central Controller only.		

21	Proposed Central Device should be automatically able to retrieve the network LAN information without running any separate routing protocols like BGP, OSPF between the edge devices		
22	Proposed Central Device should support multiple VPN solutions like IPSEC site-to-site, DMVPN and GET VPN along with SD-WAN in near future.		
23	Proposed Central Device should support End to End link Quality detection based on loss, latency and jitter and traffic routing based on link quality		
24	Proposed Central Device should provide end to end segmentation for different traffic and creating multiple virtual topology based on traffic segment to Cater the need of 10000 Barnches		
25	Porposed Central Device should support stateful firewall from Day-1		
26	Porposed Central Device should support SD WAN functionality & also provide on prem support for Stateful App Aware Firewall, IPS/IDS, URL filtering and Anti Malware protection		
27	Porposed Central Device should be capable of Building various IPSec Tunnel/VRF like Hub and Spoke , full mesh , partial mesh, as per policy pushed from the Central controller and changing overlay tunnel/VRF by pushing policy on controller only and should cater the need of 10000 Branches		
28	Proposed Central Device should automatically build IPSec overlay tunnel/VRF once device is connected on WAN and should cater the need of 10000 Branches		
29	Proposed Central Device should be able to rotate encryption keys periodically , without impacting IPSec network and should cater need of 10000 Branches		
30	Proposed Central Device should perform two factor device authenticaltion before it starts communicating on WAN		
31	Proposed Central Device should provide Application visiblity per Branch		
32	Proposed Central Device should Perfrom Centralized Path Computation and Policy Provisioning based on templates for 10000 Branches		
B	**Proposed Central Device Architecture**		
1	Architecture: The architecture of the Proposed Central Device must be modular and redundant. Proposed Central Device should have a dedicated data plane Processor, independent of the control plane Processor. The performance should be at least 40 Gbps on Day 1 and should be scalable upto 100 Gbps in future.		
2	Power Supply: The Proposed Central Device must have redundant power supply module. The Proposed Central Device must support 220V AC power supply module. There should not be any impact on the Proposed Central Device performance in case of one power supply fails.		
3	Proposed Central Device Processor Architecture: The Proposed Central Device processor architecture must be multi-processor based and should support hardware accelerated, parallelised and programmable IP forwarding and switching.		
4	Redundancy Feature: The Proposed Central Device must support Operating System (OS) redundancy or dual control module in 1:1 mode to ensure high-availability of the system. The Proposed Central Device 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.		
5	Hot Swapability: The Proposed Central Device must support online hot insertion and removal of cards. Any insertion line card should not call for Proposed Central Device rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way.		
6	Clock: The Proposed Central Device must sync to the Network Time Protocol (NTP) server.		
7	The Proposed Central Device must have support for flash memory/HDD/SDD for configuration and OS backup.		

8	The Proposed Central Device hardware should be scalable to support up to 100Gbps of encryption throughput and cater the need of 10000 Branches		
C	**Proposed Central Device Performance Parameter:**		
1	Routing Table Size: The Proposed Central Device must support minimum 2,000,000 IPv4 or 2,000,000 IPv6 routes entries in the routing table and should be scalable.		
2	The Proposed Central Device should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.		
3	Proposed Central Device must support 40 Gbps of Crypto throughput (IMIX) for IPSEC performance and 20000 IPSEC tunnels from day 1 (internal/external) to cater the need of 10000 Branches. In case of an external box, The proposed Central Device must have redundant power supply & 2X100Gig, 2X40Gig and 4x10Gig for Data fiber/optical interface and 2 x1/10 Gig ethernet interface from Day 1.		
4	Proposed Central Device solution must be a carrier-grade Equipment supporting the following: a. In-band and out-band management b. Software rollback feature c. Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.		
5	Proposed Central Device should support modular OS and simply the changes through In-Service OS upgrade mechanism		
6	The Proposed Central Device 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		
7	The Proposed Central Device 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		
8	Proposed Central Device Should support of granularly identify applications in the enterprise (For e.g. Oracle, SAP, WebEx etc.) from day one		
9	Proposed Central Device Should support of identifying L3, L4 and L7 applications from day one		
10	Proposed Central Device Should support of identifying encrypted applications (for e.g. SSL/TLS based)		
11	Proposed Central Device Should support of identifying native IPv6 applications granularly		
12	Proposed Central Device Should support of identifying IPv6 applications tunnelled in IPV4 granularly(Advance)		
13	Proposed Central Device Should support of classifying applications based on the category they belong to (For e.g. file sharing, voice, video-conferencing, business-tools etc.) from day one		
14	Proposed Central Device Should support of identifying home grown or custom applications used in the enterprise from day one		
15	Proposed Central Device Should support customized categories for applications from day one		
16	Proposed Central Device Should support of a custom application be defined based on multiple criteria: Port numbers,payload analysis or URL/URI from day one		
17	Proposed Central Device Should support of providing application aware reporting capabilities (For e.g. to know which URL's are used the most)		
18	Proposed Central Device Should support of help identifying distinctly the voice and video streams in the network from day one		
19	Proposed Central Device Should have support for newer application identification periodically without downtimes from day one		
20	Proposed Central Device Should support of exporting the learnt application information to third party management systems from day one		
21	Proposed Central Device Should support to provide the ability to filter and gather application information in a flexible manner from day one		

D.	**Physical Parameters:**		
1	The Proposed Central Device must have the following interface a. Fiber Port of 2X100Gig, 2X40Gig and 4x10Gig for Data and 2 x1/10 Gig ethernet interface b. OOB Port for management of Device or Console Ports c. USB Ports		
2	The Proposed Central Device 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.		
3	The Proposed Central Device must support OSPF, BGPv4 and IS-IS routing protocol.		
4	The Proposed Central Device should support minimum 40000 VRF instances from day one to cater the need of 10000 Branches		
5	The Proposed Central Device should support MPLS OAM - LSP Ping/Trace route for MPLS core		
6	The Proposed Central Device should support Multicast VPN (mVPN)		
7	The Proposed Central Device should have at-least 128 GB of DRAM from day one and scaleble upto 256 GB DRAM.		
E	**IPv6 Support**		
1	The Proposed Central Device Should support IP version 6 in hardware.		
2	The Proposed Central Device should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.		
3	The Proposed Central Device 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)		
4	The Proposed Central Device should support for IPv6 security – Access Control lists (standard & extended), SSH over IPv6.		
5	The Proposed Central Device should support for IPv6 Multicast.		
6	The Proposed Central Device should support IPv6 stateless auto-configuration, IPv6 neighbour discovery and, Neighbour Discovery Duplicate Address Detection.		
7	The Proposed Central Device should support IPv6 Quality of Service		
8	The Proposed Central Device should support IPv6 dual stack		
9	The Proposed Central Device should perform IPv6 transport over IPv4 network (6to4 tunnelling).		
10	The Proposed Central Device should support SNMP over IPv6 for management.		
11	The Proposed Central Device must perform Hardware assisted GRE tunnelling as per RFC 1701 and RFC 1702.		
12	The Proposed Central Device must support Proposed Central Device redundancy protocol like VRRP.		
13	The proposed Proposed Central Device should be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum		
F.	**Multicast**		
1	The Proposed Central Device must support Protocol Independent Multicast Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).		
2	The multicast implementation must support Rendezvous Points on both leaf and non-leaf nodes.		
3	The multicast implementation must support source specific multicast.		
4	The Proposed Central Device must support multiprotocol BGP extensions for multicast.		
5	The Proposed Central Device must support multicast load balancing traffic across multiple interfaces.		