Pre Bid Queries Reply

Tender Name	Request for Proposal for Procurement, Installation,Commissioning and Management of SDWAN for MSEDCL Remote Offices up to Circle level					
Tender No	MSEDCL/IT/SDWAN/2022-23					
Sr No	Page No.	Section (Name & No.)	Statement as per RFP	Query by Bidder	Justification for query (if any)	MSEDCL Reply
1				Unified Secure Access Service Edge, or SASE (pronounced “sassy”), is an enterprise security architectural model for networking that’s designed to support the fast application access needs of today’s workforce. SASE architectures converge networking and cloud-delivered security into a high-performance, single-pass architecture with unified management.	New Addition	Please Refer Corrigendum
2				True SDN based SD-WAN solution, made up of four segregated planes – Orchestration plane, Management Plane, Control Plane, and Data Plane. Each plane has its own functions and responsibilities and is abstracted away from the other planes. * The Orchestration Plane of the SD-WAN system job is to orchestrate the process of onboarding new unconfigured devices to the SD-WAN System. It’s responsible for the authentication and whitelisting of Edge devices and control/management information distribution. *The Management Plane takes care of the wider network configuration, monitoring and management processes across all layers of the network stack. *The Control Plane refers to the network architecture component that defines the traffic routing and network topology. * The Data Plane is the network architecture layer that physically handles the traffic based on the configurations supplied from the Control Plane.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
3				Secure Zero Touch Provisioning (SZTP) as per RFC 8572.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
4				Full Mesh Topology, SD-WAN should supports a full dynamic mesh topology, in addition to the hub-spoke topology. The mesh can consist of branches with or without hubs. Use full mesh when the branches need to communicate with each other directly.	New Addition	Please Refer Corrigendum
5				Passive Scanning Sensor and Vulnerability sensor, automatically detect and profile all network-connected systems, eliminating blind spots across your IT environment.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
6				Fail-to-Wire (FTW) Functionality Ethernet bypass for inline mode that allows traffic to bypass SD-WAN and flow directly across a pair of bridged interfaces in the event of appliance restart or failure.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.

7				Layer 2 & 3 Interoperability: With directly connected switch and/or router.	New Addition	Please Refer Corrigendum
8				Edge devices capable of Headless forwarding (if it lose connectivity to route reflector, still be able to continue forwarding traffic.)	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
9				Spoke redundancy by interconnecting two edge devices to create a single logical edge.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
10				LTE WAN backup link, in case of all WAN link failure.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
11				Request for increase valuation of the tender	New Addition	As per RFP
12				Unified Secure Access Service Edge, or SASE (pronounced “sassy”), is an enterprise security architectural model for networking that’s designed to support the fast application access needs of today’s workforce. SASE architectures converge networking and cloud-delivered security into a high-performance, single-pass architecture with unified management.	New Addition	Please Refer Corrigendum
13				True SDN based SD-WAN solution, made up of four segregated planes – Orchestration plane, Management Plane, Control Plane, and Data Plane. Each plane has its own functions and responsibilities and is abstracted away from the other planes. * The Orchestration Plane of the SD-WAN system job is to orchestrate the process of onboarding new unconfigured devices to the SD-WAN System. It’s responsible for the authentication and whitelisting of Edge devices and control/management information distribution. *The Management Plane takes care of the wider network configuration, monitoring and management processes across all layers of the network stack. *The Control Plane refers to the network architecture component that defines the traffic routing and network topology. * The Data Plane is the network architecture layer that physically handles the traffic based on the configurations supplied from the Control Plane.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
14				Secure Zero Touch Provisioning (SZTP) as per RFC 8572.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
15				Full Mesh Topology, SD-WAN should supports a full dynamic mesh topology, in addition to the hub-spoke topology. The mesh can consist of branches with or without hubs. Use full mesh when the branches need to communicate with each other directly.	New Addition	Please Refer Corrigendum
16				Passive Scanning Sensor and Vulnerability sensor, automatically detect and profile all network-connected systems, eliminating blind spots across your IT environment.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
17				Fail-to-Wire (FTW) Functionality Ethernet bypass for inline mode that allows traffic to bypass SD-WAN and flow directly across a pair of bridged interfaces in the event of appliance restart or failure.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
18				Layer 2 & 3 Interoperability: With directly connected switch and/or router.	New Addition	Please Refer Corrigendum
19				Edge devices capable of Headless forwarding (if it lose connectivity to route reflector, still be able to continue forwarding traffic.)	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
20				Spoke redundancy by interconnecting two edge devices to create a single logical edge.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
21				LTE WAN backup link, in case of all WAN link failure.	New Addition	Requirement Present in RFP. Refer Corrigendum for modifications in the clause.
22	43	4. Payment Terms	Delivery of all SD-WAN Solution hardware - 30 % of SDWAN Solution Charges	We request you to change payment terms as "70% against delivery of SDWAN Solution Hardware".		As per RFP
23	43	4. Payment Terms	Installation & Commissioning of all SD-WAN solution hardware - 40% of A1 of Price SDWAN Solution Charges	We request you to change payment terms as "20% against installation & Commissioning of SDWAN Solution Hardware".		As per RFP

24	43	4. Payment Terms	Stabilization of all SD-WAN Solution hardware - 30 % of SDWAN Solution Charges	We request you to change payment term as "10% of SDWAN Solution Hardware against stabilization of SDWAN solution".		As per RFP
25	49	6. Contract Performance Security	The Bidder should provide the contract performance guarantee for the sum of 10% (ten percent) of the Contract Price for due performance of contract. This Contract Performance Security shall be valid till the expiry of 180 days after the end of Contract period	As per Government recent guidelines, request you to change the Performance Guarantee from 10% to 5% of the Contract Value.		As per RFP
26	18	Section – D Scope of Work 1. Scope of Work	iv. Bidder has to provide WI-FI connectivity via wi-fi enabled SD-WAN device having 5G capability and supplied WI-FI access points to the respective offices .	We assume proposed SD WAN devices should support 5G capability in future as and when 5G technology is available in India. Also request MSEDCL to confirm can we propose external modem for 5G support whenever 5G technology is available in India & without any additional cost implication to MSEDCL	Currently in India 5G option is not available, once it is available in India, so we assume 5G is support is required for future and it can be provided within the appliance or using external modem without any additional cost implication to MSEDCL whenever 5G technology is available in India.	As per RFP
27	23	4.2 Technology	I. Solution should support MPLS, FTTH, 4G, 5G (SIM/Dongle) wired /broadband links with link speed minimum 8 Mbps to 1 Gbps.	We request MSEDCL to amend this clause ad " Solution should support MPLS, FTTH, 4G, 5G (SIM/Dongle/**external modem**) wired /broadband links with link speed minimum 8 Mbps to 1 Gbps."	Currently in India 5G option is not available, once it is available in India, so we assume 5G is support is required for future and it can be provided within the appliance or using external modem without any additional cost implication to MSEDCL whenever 5G technology is available in India.	As per RFP
28	23	4.2 Technology	V.The remote SD_WAN appliance should be Wi-Fi enabled with integrated or external access point and securely configured SSID along with standard Wi-Fi security features	We assume Wi-Fi solution can be provided using external access point and Wi-Fi management tool deployed in cloud. Pls confirm if our understanding is correct.	As most of the reputed SD WAN OEM doesn't support inbuilt Wi-Fi capability in their SD WAN device, so we assume bidder can quote external access point and management tool for managing the wireless solution.	As per RFP
29	23	4.3 Network Integration	V. Solution should support WAN optimization functionality	We assume MSEDCL is looking for WAN optimization as utilizing multiple links, load sharing of the traffic on multiple links, dynamic steering of traffic from one WAN link to another. Pls confirm if our understanding is correct.	We request MSEDCL to elaborate on WAN optimization.	As per RFP Section Section – E Mandatory Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud Sr No.4,5,6,7 15,26,27,28,29,30
30	24	4.5 Performance	a. Deduplication/Forward Error Correction	For FEC, "We have specific algorithms to ensure better QoE for Voice and Video applications by using link quality/Capacity per tunnel, throughput metrics, packet by packet load balancing, flow spraying, duplication etc. Hence request MSEDCL to modify the clause as " Deduplication/Forward Error Correction/**equivalent**."	Every OEM have their own algorithms or ways to achieve the desired functionality, so request MSEDCL to consider equivalent technology as well.	As per RFP,Name of equivalent technology not provided for verification
31	24	4.6 Security	IX. Solution should have RADIUS/TACACS based authentication for device management	We request MSEDCL to amend this clause as "Solution should have RADIUS/TACACS/**TACACS+** based authentication for device management	As TACACS+ is the latest way for authenticating the device management, so we request MSEDCL to consider TACACS+ as well	As per RFP
32	26	Section – E Mandatory Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	4. SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	We request MSEDCL to amend this clause a " SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication or **equivalent** with capability to send duplicate packets over a single tunnel."	Every OEM have their own algorithms or ways to achieve the desired functionality, so request MSEDCL to consider equivalent technology as well.	As per RFP,Name of equivalent technology not provided for verification
33	27	Section – E Mandatory Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	10. SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall,IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL.	We assume SD-WAN controller should be available to support 2Gbps throughput after enabling all the features (Like Firewall,IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) from day 1.Pls confirm if our understanding is correct.	Request MSEDCL to confirm on this.	OK,As per RFP
34	30	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	1. Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Pls confirm bidder can proposed external access point and Wi-Fi management tool deployed in cloud for managing the wireless solution.	As most of the reputed SD WAN OEM doesn't support inbuilt Wi-Fi capability in their SD WAN device, so we assume bidder can quote external access point and management tool for managing the wireless solution.	As per RFP
35	30	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	3.SD-WAN device must support multiple WAN connectivity mediums such as MPLS, ILL, Broadband, P2P leased Line, 4G and upgradable to 5G in future on USB port or SIM slot with automatic fail-over capability.	We request MSEDCL to amend this clause as "SD-WAN device must support multiple WAN connectivity mediums such as MPLS, ILL, Broadband, P2P leased Line, 4G and upgradable to 5G in future on USB port or SIM slot or external modem with automatic fail-over capability."	We request MSEDCL to consider 5G support using USB port or SIM slot or external modem in future without any additional cost implication to MSEDCL whenever 5G technology is available in India.	As per RFP
36	30	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	4.SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	We request MSEDCL to amend this clause as "SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication **or equivalent** with capability to send duplicate packets over a single tunnel."	Every OEM have their own algorithms or ways to achieve the desired functionality, so request MSEDCL to consider equivalent technology as well.	As per RFP

37	30	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	9. SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.)	We assume SD-WAN edge device should be available to support 200Mbps throughput after enabling all the features ((Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.) from day 1. Pls confirm if our understanding is correct.	Request MSEDCL to confirm on this.	OK,As per RFP
38	31	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	14. SD-WAN appliance should support minimum 250 SDWAN Nodes	We request MSEDCL to remove this clause from technical specification of "Remote Location SD-WAN Appliance" as branch devices doesn't support SD WAN nodes	SD WAN nodes are supported by SD WAN controller and not by branch device, so we request MSEDCL to remove this clause from remote location SD-WAN appliance specification.	As per RFP,Requirement is of FULL MESH topology between SD-WAN nodes
39	31	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	19. The solution MUST provide administrator authentication via TACAS,RADIUS,LDAP	We request MSEDCL to amend the clause as "The solution MUST provide administrator authentication via TACACS/TACACS+/RADIUS/LDAP	Request MSEDCL to consider TACACS+	As per RFP
40	32	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	33. The proposed SD-WAN solution should provide Active- Active resource utilization at WAN edge and WAN link layers. The solution should support Active-Active dual router topology without using external upstream switches.	Request MSEDCL to confirm whether bidder need to provide 2 WAN edge device in each locations from day 1?	Request MSEDCL to confirm on this.	As per the RFP One number of SDWAN device (WAN Edge Device) per location is required to be installed .
41	32	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	36. The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1	Request MSEDCL to confirm on the use case for 15 segments from day 1 on edge devices	It is very rare to have 15 segments in branch setup, request MSEDCL to provide where they want to use 15 segments at branch end.	The segments are required for the different types of networking traffic via the SD-WAN appliance
42	34	Section – E Mandatory Technical Specifications 4. NMS ,Orchestration, Administration, Management and Logging Tool	2. Separate reporting solution must be offered with sufficient storage to store 12 Months log and Solution should be able to handle minimum 100 devices. Minimum 15 users can be created out of which 5 should be administrators. The solution should support Role based access control.	If we provide virtual instance with the required sizing detail to MSEDCL for their cloud , then MSEDCL will maintain the 12 months logs in their cloud. Request MSEDCL to confirm on this.	As per RFP, bidder are free to quote controller and management tool in either their cloud or in MSEDCL hosted cloud. If bidder choose to quote MSEDCL hosted cloud option, then we assume MSEDCL will be responsible to provide storage space to store the 12 months logs.	As per RFP, Bidder need to provide requirement in Annexure 18
43	18	Section – D Scope of Work 1. Scope of Work	iv. Bidder has to provide WI-FI connectivity via wi-fi enabled SD-WAN device having 5G capability and supplied WI-FI access points to the respective offices .	We assume proposed SD WAN devices should support 5G capability in future as and when 5G technology is available in India. Also request MSEDCL to confirm can we propose external modem for 5G support whenever 5G technology is available in India & without any additional cost implication to MSEDCL	Currently in India 5G option is not available, once it is available in India, so we assume 5G is support is required for future and it can be provided within the appliance or using external modem without any additional cost implication to MSEDCL whenever 5G technology is available in India.	As per RFP
44	23	4.2 Technology	I. Solution should support MPLS, FTTH, 4G, 5G (SIM/Dongle) wired /broadband links with link speed minimum 8 Mbps to 1 Gbps.	We request MSEDCL to amend this clause ad " Solution should support MPLS, FTTH, 4G, 5G (SIM/Dongle/**external modem**) wired /broadband links with link speed minimum 8 Mbps to 1 Gbps."	Currently in India 5G option is not available, once it is available in India, so we assume 5G is support is required for future and it can be provided within the appliance or using external modem without any additional cost implication to MSEDCL whenever 5G technology is available in India.	As per RFP
45	23	4.2 Technology	V.The remote SD_WAN appliance should be Wi-Fi enabled with integrated or external access point and securely configured SSID along with standard Wi-Fi security features	We assume Wi-Fi solution can be provided using external access point and Wi-Fi management tool deployed in cloud. Pls confirm if our understanding is correct.	As most of the reputed SD WAN OEM doesn't support inbuilt Wi-Fi capability in their SD WAN device, so we assume bidder can quote external access point and management tool for managing the wireless solution.	As per RFP
46	23	4.3 Network Integration	V. Solution should support WAN optimization functionality	We assume MSEDCL is looking for WAN optimization as utilizing multiple links, load sharing of the traffic on multiple links, dynamic steering of traffic from one WAN link to another. Pls confirm if our understanding is correct.	We request MSEDCL to elaborate on WAN optimization.	As per RFP
47	24	4.5 Performance	a. Deduplication/Forward Error Correction	For FEC, "We have specific algorithms to ensure better QoE for Voice and Video applications by using link quality/Capacity per tunnel, throughput metrics, packet by packet load balancing, flow spraying, duplication etc. Hence request MSEDCL to modify the clause as " Deduplication/Forward Error Correction/**equivalent**."	Every OEM have their own algorithms or ways to achieve the desired functionality, so request MSEDCL to consider equivalent technology as well.	As per RFP
48	24	4.6 Security	IX. Solution should have RADIUS/TACACS based authentication for device management	We request MSEDCL to amend this clause as "Solution should have RADIUS/TACACS/**TACACS+** based authentication for device management	As TACACS+ is the latest way for authenticating the device management, so we request MSEDCL to consider TACACS+ as well	As per RFP
49	26	Section – E Mandatory Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	4. SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	We request MSEDCL to amend this clause a " SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication or **equivalent** with capability to send duplicate packets over a single tunnel."	Every OEM have their own algorithms or ways to achieve the desired functionality, so request MSEDCL to consider equivalent technology as well.	As per RFP

50	27	Section – E Mandatory Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	10. SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall,IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL.	We assume SD-WAN controller should be available to support 2Gbps throughput after enabling all the features (Like Firewall,IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) from day 1.Pls confirm if our understanding is correct.	Request MSEDCL to confirm on this.	Device performance should not be degraded after enabling all the functionality mentioned in RF
51	30	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	1. Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Pls confirm bidder can proposed external access point and Wi-Fi management tool deployed in cloud for managing the wireless solution.	As most of the reputed SD WAN OEM doesn't support inbuilt Wi-Fi capability in their SD WAN device, so we assume bidder can quote external access point and management tool for managing the wireless solution.	As per RFP
52	30	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	3.SD-WAN device must support multiple WAN connectivity mediums such as MPLS, ILL, Broadband, P2P leased Line, 4G and upgradable to 5G in future on USB port or SIM slot with automatic fail-over capability.	We request MSEDCL to amend this clause as "SD-WAN device must support multiple WAN connectivity mediums such as MPLS, ILL, Broadband, P2P leased Line, 4G and upgradable to 5G in future on USB port or SIM slot or external modem with automatic fail-over capability."	We request MSEDCL to consider 5G support using USB port or SIM slot or external modem in future without any additional cost implication to MSEDCL whenever 5G technology is available in India.	As per RFP
53	30	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	4.SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	We request MSEDCL to amend this clause as "SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication **or equivalent** with capability to send duplicate packets over a single tunnel."	Every OEM have their own algorithms or ways to achieve the desired functionality, so request MSEDCL to consider equivalent technology as well.	As per RFP
54	30	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	9. SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.)	We assume SD-WAN edge device should be available to support 200Mbps throughput after enabling all the features ((Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.) from day 1. Pls confirm if our understanding is correct.	Request MSEDCL to confirm on this.	SDWAN through put should not be less than 200 mbps.Device performance should not be degraded after enabling all the functionality mentioned in RF
55	31	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	14. SD-WAN appliance should support minimum 250 SDWAN Nodes	We request MSEDCL to remove this clause from technical specification of "Remote Location SD-WAN Appliance" as branch devices doesn't support SD WAN nodes	SD WAN nodes are supported by SD WAN controller and not by branch device, so we request MSEDCL to remove this clause from remote location SD-WAN appliance specification.	As per RFP
56	31	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	19. The solution MUST provide administrator authentication via TACAS,RADIUS,LDAP	We request MSEDCL to amend the clause as "The solution MUST provide administrator authentication via TACACS/TACACS+/RADIUS/LDAP	Request MSEDCL to consider TACACS+	As per RFP
57	32	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	33. The proposed SD-WAN solution should provide Active- Active resource utilization at WAN edge and WAN link layers. The solution should support Active-Active dual router topology without using external upstream switches.	Request MSEDCL to confirm whether bidder need to provide 2 WAN edge device in each locations from day 1?	Request MSEDCL to confirm on this.	As per RFP
58	32	Section – E Mandatory Technical Specifications 2. Remote Location SD-WAN Appliance	36. The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1	Request MSEDCL to confirm on the use case for 15 segments from day 1 on edge devices	It is very rare to have 15 segments in branch setup, request MSEDCL to provide where they want to use 15 segments at branch end.	Isolation of the different traffic type and to maintain the security
59	34	Section – E Mandatory Technical Specifications 4. NMS ,Orchestration, Administration, Management and Logging Tool	2. Separate reporting solution must be offered with sufficient storage to store 12 Months log and Solution should be able to handle minimum 100 devices. Minimum 15 users can be created out of which 5 should be administrators. The solution should support Role based access control.	If we provide virtual instance with the required sizing detail to MSEDCL for their cloud , then MSEDCL will maintain the 12 months logs in their cloud. Request MSEDCL to confirm on this.	As per RFP, bidder are free to quote controller and management tool in either their cloud or in MSEDCL hosted cloud. If bidder choose to quote MSEDCL hosted cloud option, then we assume MSEDCL will be responsible to provide storage space to store the 12 months logs.	Bidder need to provide requirement in Annexure 18
60	35	Pre-Qualification Criteria	The Bidder should have a positive net worth during each of the last three audited financial years (FY 18-19 ,19-20,20-21or FY 19-20, 20-21,21-22).	We would request you to consider Bidder/Bidder parent company to submit the audited financial sheet for positive net worth	BASL is a fully owned subsidary for BAL.	As per RFP

61	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS and Vulnerability management capabilties	Please modify the clause as follows for wider participation of OEMs: "SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS/Vulnerability management capabilties"	Please clarify if the specification ask for DDOS protection of SDWAN Controller and remote edge SDWAN devices? Also, as an OEM have a Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to our products and networks. Please confirm if this is what department is looking for or else please modify the clause as vulnerability management should not part of the SDWAN solution and this fucntionality should be met by third part dedicated solution.	
62	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	Please modify the clause as follows for wider participation of OEMs: "SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single/multiple tunnel"	Packet Duplication is an SD-WAN feature designed to overcome packet loss in network designs where a WAN edge router has multiple overlay tunnels to the next-hop router. The feature instructs a SDWAN edge router to transmit one copy of each packet over multiple IPsec tunnels. If a packet is lost over the transient path, the receiving SDWAN router can use another copy of the same packet received over another tunnel. If no packets are lost, all unnecessary duplicates are silently discarded.	Refer Corrigendum
63	27	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall, IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL	Please modify the clause as follows for wider participation of OEMs: "SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL"	The virtual HUB SD-WAN edge appliance will be deployed in the AWS cloud where all the applications are hosted. The SD-WAN head end device will decrypt the traffic forward it to internal security infrastructure for traffic filtering. Hence request you to modify the clause for wider participation of OEMs.	As per RFP
64	27	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller should support dynamic routing protocols - OSPF, BGP. SD-WAN controller should be able to create FULL MESH topology with optimal routing	SD-WAN controller/head end device should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology or on-demand tunneling between branches for optimal routing	Our solution supports dynamic on-demand tunnels between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage.	As per RFP
65	28	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify the clause as follows for wider participation of OEMs: The proposed solution must have ability to reorder/re-transmit failed packets during the failover.	Different OEMs have different mechanisms to deal with Packet loss. Request you to modify the clause for wider participation of OEMs.	Refer Corrigendum
66	28	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links simultaneously for a single application.	Please modify the clause as follows for wider participation of OEMs: To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links for a single application.	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, we use application aware routing and use specific virtual path for traffic destined towards specifis application/ IP address. With this method, solution can use multiple links to load balance all the traffic and critical traffic gets high performance as those applications are running on specific virtual path which are having high SLA. In case of failover/ detorattion on the high sla path, traffic will switch over to another virtual path/tunnel.	As per RFP
67	30	2. Remote Location SD-WAN Appliance	Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Please modify the clause as follows for wider participation of OEMs: Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and the SDWAN solution should have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Wireless is not part of the SDWAN solution. The SDWAN Controller supports zero touch deplohyment of SDWAN devices only. Hence request you to modify the clause for wider participation of OEMs.	As per RFP

68	30	2. Remote Location SD-WAN Appliance	SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	Please modify the clause as follows for wider participation of OEMs: SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single/dual tunnel.	Packet duplication sends copies of packets on alternate available paths to reach SD-WAN devices. The feature instructs a WAN edge router to transmit one copy of each packet over multiple IPsec tunnels. If a packet is lost over the transient path, the receiving router can use another copy of the same packet received over another tunnel. If no packets are lost, all unnecessary duplicates are silently discarded. This feature requires atleast two tunnels to be configured between the sending the receiving SDWAN router.	Refer Corrigendum
69	30	2. Remote Location SD-WAN Appliance	SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.)	Please modify the clause as follows: SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.). The security features can be delivered on-premise or through cloud.	Secure access service edge (SASE) combines networking and security functions in the cloud to deliver seamless, secure access to applications, anywhere users work. Since MSEDCL is already using AWS for hosting their applications and SAAS applications : -More workloads are running in the cloud than in the enterprise data center. -SaaS applications are used more frequently than locally installed ones. -More traffic is destined to public cloud services than to the enterprise data center. -More traffic from branch offices is heading to public clouds and will now require Direct Internet Access SASE is the right approach for MSEDCL as it will provide the following benefits: Reduced Complexity, Increased and Optimized performance, Consistent Security and Threat prevention with reduced risk, Centralized orchestration.	As per RFP. For inclusion of SASE architecture refer Corrigendum
70	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology with optimal routing	Please modify the clause as follows: SD-WAN branch end device should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology or on-demand tunneling between branches for optimal routing	Our solution supports dynamic on-demand tunnels between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage.	As per RFP

71	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance should support minimum 250 SDWAN Nodes	Please modify the clause as follows for wider participation of OEMs: "SD-WAN appliance should support minimum 200 SDWAN Nodes"	We intent to deploy ON demand tunneling between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage. As the number of locations are just 66 is nos. even with 100% scalibility and with ON demand tunneling turned ON, support for 200 tunnels should be more than enough.	As per RFP
72	32	2. Remote Location SD-WAN Appliance	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify the clause as follows for wider participation of OEMs: The proposed solution must have ability to reorder/re-transmit failed packets during the failover.	Different OEMs have different mechanisms to deal with Packet loss. Request you to modify the clause for wider participation of OEMs.	Refer Corrigendum
73	32	2. Remote Location SD-WAN Appliance	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links simultaneously for a single application.	Please modify the clause as follows for wider participation of OEMs: To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links for a single application.	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, we use application aware routing and use specific virtual path for traffic destined towards specifis application/ IP address. With this method, solution can use multiple links to load balance all the traffic and critical traffic gets high performance as those applications are running on specific virtual path which are having high SLA. In case of failover/ detorattion on the high sla path, traffic will switch over to another virtual path/tunnel.	As per RFP
74	32	2. Remote Location SD-WAN Appliance	The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1	Please modify the clause as follows: The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1. SD-WAN branch device should support logical segmentation of WAN, LAN and Management interfaces.	This will ensure improved security and end to end segmentation. Hence request you to make the required change.	As per RFP
75	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN branch hardware should be a hardened appliance of OEM running SD-WAN firmware on top of it and all function, scale tests should be done along with hardware and software together	Please add this clause to ensure that the appliance provided can perform in MSEDCL's environment and has undergone performance and scale tests with hardware and software together.	As per RFP
76	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should provide local internet breakout from branches to access SAAS/IAAS applications directly. SD-WAN solution should have built in intelligence to find out the best optimized path from multiple paths to access SAAS applications like O365, webex, Salesforce, box etc.	MSEDCL will deploy direct internet access at its branch locations. Also, MSEDCL is/will be using SAAS applications like O365, MS Teams/Webex, Salesforce, box etc. Hence it is requested to add this clause which will benefit MSEDCL through improved performance of SAAS based applications.	As per RFP
77	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should have automation and guided worflows to configure Virtual edge devices hosted in multiple Cloud providers like AWS/AZURE/GCP to access customer applications within host VPC/VNET	This will ensure automated deployment of HUB devices in AWS cloud without any manual intervention.	As per RFP
78	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should support real-time network performance measurement and visibility for applications along with policy validations	This is an important feature which will ensure that the policies applied by MSEDCL are working properly and will also provide real time visibility into network performance.	As per RFP ,Refer point no 4. NMS ,Orchestration, Administration, Management and Logging Tool 1

79	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should support Geolocation-based firewall rules to configure firewall rules for allowing or denying network traffic based on the specified source and destination locations	This is a very important security feature especially when MSEDCL is going to deploy Direct internet Access at branch locations: Use-Case Scenario A client (192.168.11.10) in a local area network (LAN) initiates traffic over Dedicated Internet Access (DIA) to a destination IP addresses belonging to France (FRA) and China (CHN). As per the security firewall policy, traffic to France should be inspected and that to China should be dropped. Benefits of Geolocation-Based Firewall Rules: 1) You can restrict access to particular countries without needing to know the associated IP addresses for those countries. 2) A geolocation can be a country, a continent, or a list containing both continents and countries. 3) You can add multiple geolocation lists or geolocations using a single policy.	As per RFP
80	19	1. Scope of Work	Perform load balancing for improving the performance with reachability, jitter, latency , packet loss and bandwidth utilization.	Please modify the clause as follows for wider participation of OEMs: Perform load balancing for improving the performance with reachability, jitter, latency , packet loss and/or bandwidth utilization.	Bandwidth utilization is not the correct method to perform load balancing, it leads to challenges in packet forwarding method and unnecessary re-transmissions.	As per RFP
81	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS and Vulnerability management capabilties	Please modify the clause as follows for wider participation of OEMs: "SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS/Vulnerability management capabilties"	Please clarify if the specification ask for DDOS protection of SDWAN Controller and remote edge SDWAN devices? Also, as an OEM have a Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to our products and networks. Please confirm if this is what department is looking for or else please modify the clause as vulnerability management should not part of the SDWAN solution and this fucntionality should be met by third part dedicated solution.	As per RFP
82	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS and Vulnerability management capabilties	Please modify the clause as follows for wider participation of OEMs: "SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS/Vulnerability management capabilties"	Please clarify if the specification ask for DDOS protection of SDWAN Controller and remote edge SDWAN devices? Also, as an OEM have a Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to our products and networks. Please confirm if this is what department is looking for or else please modify the clause as vulnerability management should not part of the SDWAN solution and this fucntionality should be met by third part dedicated solution.	As per RFP
83	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	Please modify the clause as follows for wider participation of OEMs: "SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single/multiple tunnel"	Packet Duplication is an SD-WAN feature designed to overcome packet loss in network designs where a WAN edge router has multiple overlay tunnels to the next-hop router. The feature instructs a SDWAN edge router to transmit one copy of each packet over multiple IPsec tunnels. If a packet is lost over the transient path, the receiving SDWAN router can use another copy of the same packet received over another tunnel. If no packets are lost, all unnecessary duplicates are silently discarded.	Refer Corrigendum
84	27	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall, IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL	Please modify the clause as follows for wider participation of OEMs: "SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL"	The virtual HUB SD-WAN edge appliance will be deployed in the AWS cloud where all the applications are hosted. The SD-WAN head end device will decrypt the traffic forward it to internal security infrastructure for traffic filtering. Hence request you to modify the clause for wider participation of OEMs.	As per RFP

85	27	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller should support dynamic routing protocols - OSPF, BGP. SD-WAN controller should be able to create FULL MESH topology with optimal routing	SD-WAN controller/head end device should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology or on-demand tunneling between branches for optimal routing	Our solution supports dynamic on-demand tunnels between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage.	As per RFP
86	28	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify the clause as follows for wider participation of OEMs: The proposed solution must have ability to reorder/re-transmit failed packets during the failover.	Different OEMs have different mechanisms to deal with Packet loss. Request you to modify the clause for wider participation of OEMs.	Refer Corrigendum
87	28	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links simultaneously for a single application.	Please modify the clause as follows for wider participation of OEMs: To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links for a single application.	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, we use application aware routing and use specific virtual path for traffic destined towards specifis application/ IP address. With this method, solution can use multiple links to load balance all the traffic and critical traffic gets high performance as those applications are running on specific virtual path which are having high SLA. In case of failover/ detorattion on the high sla path, traffic will switch over to another virtual path/tunnel.	As per RFP
88	30	2. Remote Location SD-WAN Appliance	Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Please modify the clause as follows for wider participation of OEMs: Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and the SDWAN solution should have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Wireless is not part of the SDWAN solution. The SDWAN Controller supports zero touch deplohyment of SDWAN devices only. Hence request you to modify the clause for wider participation of OEMs.	As per RFP
89	30	2. Remote Location SD-WAN Appliance	SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	Please modify the clause as follows for wider participation of OEMs: SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single/dual tunnel.	Packet duplication sends copies of packets on alternate available paths to reach SD-WAN devices. The feature instructs a WAN edge router to transmit one copy of each packet over multiple IPsec tunnels. If a packet is lost over the transient path, the receiving router can use another copy of the same packet received over another tunnel. If no packets are lost, all unnecessary duplicates are silently discarded. This feature requires atleast two tunnels to be configured between the sending the receiving SDWAN router.	Refer Corrigendum
90	30	2. Remote Location SD-WAN Appliance	SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.)	Please modify the clause as follows: SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.). The security features can be delivered on-premise or through cloud.	Secure access service edge (SASE) combines networking and security functions in the cloud to deliver seamless, secure access to applications, anywhere users work. Since MSEDCL is already using AWS for hosting their applications and SAAS applications : -More workloads are running in the cloud than in the enterprise data center. -SaaS applications are used more frequently than locally installed ones. -More traffic is destined to public cloud services than to the enterprise data center. -More traffic from branch offices is heading to public clouds and will now require Direct Internet Access SASE is the right approach for MSEDCL as it will provide the following benefits: Reduced Complexity, Increased and Optimized performance, Consistent Security and Threat prevention with reduced risk, Centralized orchestration.	As per RFP. For inclusion of SASE architecture refer Corrigendum

91	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology with optimal routing	Please modify the clause as follows: SD-WAN branch end device should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology or on-demand tunneling between branches for optimal routing	Our solution supports dynamic on-demand tunnels between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage.	As per RFP
92	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance should support minimum 250 SDWAN Nodes	Please modify the clause as follows for wider participation of OEMs: "SD-WAN appliance should support minimum 200 SDWAN Nodes"	We intent to deploy ON demand tunneling between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage. As the number of locations are just 66 is nos. even with 100% scalibility and with ON demand tunneling turned ON, support for 200 tunnels should be more than enough.	As per RFP
93	32	2. Remote Location SD-WAN Appliance	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify the clause as follows for wider participation of OEMs: The proposed solution must have ability to reorder/re-transmit failed packets during the failover.	Different OEMs have different mechanisms to deal with Packet loss. Request you to modify the clause for wider participation of OEMs.	Refer Corrigendum
94	32	2. Remote Location SD-WAN Appliance	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links simultaneously for a single application.	Please modify the clause as follows for wider participation of OEMs: To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links for a single application.	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, we use application aware routing and use specific virtual path for traffic destined towards specifis application/ IP address. With this method, solution can use multiple links to load balance all the traffic and critical traffic gets high performance as those applications are running on specific virtual path which are having high SLA. In case of failover/ detorattion on the high sla path, traffic will switch over to another virtual path/tunnel.	As per RFP
95	32	2. Remote Location SD-WAN Appliance	The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1	Please modify the clause as follows: The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1. SD-WAN branch device should support logical segmentation of WAN, LAN and Management interfaces.	This will ensure improved security and end to end segmentation. Hence request you to make the required change.	As per RFP
96	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN branch hardware should be a hardened appliance of OEM running SD-WAN firmware on top of it and all function, scale tests should be done along with hardware and software together	Please add this clause to ensure that the appliance provided can perform in MSEDCL's environment and has undergone performance and scale tests with hardware and software together.	As per RFP

97	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should provide local internet breakout from branches to access SAAS/IAAS applications directly. SD-WAN solution should have built in intelligence to find out the best optimized path from multiple paths to access SAAS applications like O365, webex, Salesforce, box etc.	MSEDCL will deploy direct internet access at its branch locations. Also, MSEDCL is/will be using SAAS applications like O365, MS Teams/Webex, Salesforce, box etc. Hence it is requested to add this clause which will benefit MSEDCL through improved performance of SAAS based applications.	As per RFP
98	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should have automation and guided worflows to configure Virtual edge devices hosted in multiple Cloud providers like AWS/AZURE/GCP to access customer applications within host VPC/VNET	This will ensure automated deployment of HUB devices in AWS cloud without any manual intervention.	As per RFP
99	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should support real-time network performance measurement and visibility for applications along with policy validations	This is an important feature which will ensure that the policies applied by MSEDCL are working properly and will also provide real time visibility into network performance.	As per RFP ,Refer point no 4. NMS ,Orchestration, Administration, Management and Logging Tool 1
100	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should support Geolocation-based firewall rules to configure firewall rules for allowing or denying network traffic based on the specified source and destination locations	This is a very important security feature especially when MSEDCL is going to deploy Direct internet Access at branch locations: Use-Case Scenario A client (192.168.11.10) in a local area network (LAN) initiates traffic over Dedicated Internet Access (DIA) to a destination IP addresses belonging to France (FRA) and China (CHN). As per the security firewall policy, traffic to France should be inspected and that to China should be dropped. Benefits of Geolocation-Based Firewall Rules: 1) You can restrict access to particular countries without needing to know the associated IP addresses for those countries. 2) A geolocation can be a country, a continent, or a list containing both continents and countries. 3) You can add multiple geolocation lists or geolocations using a single policy.	As per RFP
101	19	1. Scope of Work	Perform load balancing for improving the performance with reachability, jitter, latency , packet loss and bandwidth utilization.	Please modify the clause as follows for wider participation of OEMs: Perform load balancing for improving the performance with reachability, jitter, latency , packet loss and/or bandwidth utilization.	Bandwidth utilization is not the correct method to perform load balancing, it leads to challenges in packet forwarding method and unnecessary re-transmissions.	As per RFP
102	34	NMS ,Orchestration, Administration, Management and Logging Tool. Point 4	Solution must have zero touch deployment features	Not a Part of NMS tool. This point need to be removed		As per RFP,Requirement pertains to entire SD-WAN solution.
103	34	NMS ,Orchestration, Administration, Management and Logging Tool. Point 6	Logging and reporting solution must have ready-made report template such as Top Users/ Top IP Addresses, Top Application, Top Destinations, Interface utilization per device per link, CPU and Memory usage of each device, malware / threat analysis report etc.	Malware And Threat Analysis Reports is not a part of NMS tool. This point need to be removed		As per RFP,The Requirement must be provided as per the tender clause
104	34	NMS ,Orchestration, Administration, Management and Logging Tool. Point 10	Traffic reports : availability, Link Downtime , bandwidth usage per access circuit, bandwidth usage per application, latency, packet loss, QoS per access circuit and security reports as per features asked etc	QoS per Access Circuit and Security reports are out of Scope from NMS. This point need to be removed		As per RFP,The Requirement must be provided as per the tender clause
105	34	NMS ,Orchestration, Administration, Management and Logging Tool. Point 13	Solution should have support for configuration rollback	This feature is a part of SDWAN solution. Need to be removed from NMS requirement		As per RFP,Requirement pertains to entire SD-WAN solution and must be provided as per tender clause
106	34	NMS ,Orchestration, Administration, Management and Logging Tool. Point 15	SD-WAN solution should support integration with external workflow management solution to offer workflow functionality for authorization before any change management execution	Is there any requirement of Ticketing tool/ITSM tool for Change Management Process		As per tender the requirement of different activities which will be part of change management execution is mentioned under specifications of the NMS ,Orchestration, Administration, Management and Logging Tool
107	34	NMS ,Orchestration, Administration, Management and Logging Tool. Point 18	System should have the capability to applications priority based on their performance taking into account parameters like Bandwidth utilization, latency, jitter, loss etc.	This feature is a part of SDWAN solution. Need to be removed from NMS requirement		As per RFP,Requirement pertains to entire SD-WAN solution and must be provided as per tender clause

108	34	NMS ,Orchestration, Administration, Management and Logging Tool. Point 20	The proposed solution should also provide intelligent recommendations for application quality of service categorization and policy changes for predictable application performance	This feature is a part of SDWAN solution. Need to be removed from NMS requirement		As per RFP,Requirement pertains to entire SD-WAN solution and must be provided as per tender clause
109	34	NMS ,Orchestration, Administration, Management and Logging Tool. Point 22	Solution should able to support centralized single plane of management system to allow device configuration, Policy provisioning, Software updates and assurance capabilities	This feature is a part of SDWAN solution. Need to be removed from NMS requirement		As per RFP,Requirement pertains to entire SD-WAN solution and must be provided as per tender clause
110				1) how to provision charges for egress and ingress applicable inside the vlan, mpls, p2p , direct connect port and internet per GB as per network load		Refer Corrigendum.Bidder will be responsible for all the charges required to (like RACK Space ,Port Charges,Gateway Charges at GPX data centre etc) integrate proposed SD-WAN solution with MSEDCL cloud where all MSEDCL applications hosted .Bidder shall coordinate with MSEDCL MSP for integration to MSEDCL Cloud.
111				provision for quoting one time and Annual charges for commissioning and maintaining routing , interfaces, gateways devices required for end to end connectivity		Refer Corrigendum
112				2) the data sheet of all the products quoted should be readily available in the public domain from last 1-2 months. New data sheet uploaded recently should not be considered		No Change ,As per RFP MSEDCL may ask Clarifications about Product Datasheet from OEM, if required
113	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS and Vulnerability management capabilties	Please modify the clause as follows for wider participation of OEMs: "SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS/Vulnerability management capabilties"	Please clarify if the specification ask for DDOS protection of SDWAN Controller and remote edge SDWAN devices? Also, as an OEM have a Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to our products and networks. Please confirm if this is what department is looking for or else please modify the clause as vulnerability management should not part of the SDWAN solution and this fucntionality should be met by third part dedicated solution.	As per RFP
114	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	Please modify the clause as follows for wider participation of OEMs: "SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single/multiple tunnel"	Packet Duplication is an SD-WAN feature designed to overcome packet loss in network designs where a WAN edge router has multiple overlay tunnels to the next-hop router. The feature instructs a SDWAN edge router to transmit one copy of each packet over multiple IPsec tunnels. If a packet is lost over the transient path, the receiving SDWAN router can use another copy of the same packet received over another tunnel. If no packets are lost, all unnecessary duplicates are silently discarded.	Refer Corrigendum
115	27	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall, IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL	Please modify the clause as follows for wider participation of OEMs: "SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL"	The virtual HUB SD-WAN edge appliance will be deployed in the AWS cloud where all the applications are hosted. The SD-WAN head end device will decrypt the traffic forward it to internal security infrastructure for traffic filtering. Hence request you to modify the clause for wider participation of OEMs.	As per RFP

116	27	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller should support dynamic routing protocols - OSPF, BGP. SD-WAN controller should be able to create FULL MESH topology with optimal routing	SD-WAN controller/head end device should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology or on-demand tunneling between branches for optimal routing	Our solution supports dynamic on-demand tunnels between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage.	As per RFP
117	28	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify the clause as follows for wider participation of OEMs: The proposed solution must have ability to reorder/re-transmit failed packets during the failover.	Different OEMs have different mechanisms to deal with Packet loss. Request you to modify the clause for wider participation of OEMs.	Refer Corrigendum
118	28	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links simultaneously for a single application.	Please modify the clause as follows for wider participation of OEMs: To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links for a single application.	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, we use application aware routing and use specific virtual path for traffic destined towards specifis application/ IP address. With this method, solution can use multiple links to load balance all the traffic and critical traffic gets high performance as those applications are running on specific virtual path which are having high SLA. In case of failover/ detorattion on the high sla path, traffic will switch over to another virtual path/tunnel.	As per RFP
119	30	2. Remote Location SD-WAN Appliance	Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Please modify the clause as follows for wider participation of OEMs: Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and the SDWAN solution should have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Wireless is not part of the SDWAN solution. The SDWAN Controller supports zero touch deplohyment of SDWAN devices only. Hence request you to modify the clause for wider participation of OEMs.	As per RFP
120	30	2. Remote Location SD-WAN Appliance	SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	Please modify the clause as follows for wider participation of OEMs: SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single/dual tunnel.	Packet duplication sends copies of packets on alternate available paths to reach SD-WAN devices. The feature instructs a WAN edge router to transmit one copy of each packet over multiple IPsec tunnels. If a packet is lost over the transient path, the receiving router can use another copy of the same packet received over another tunnel. If no packets are lost, all unnecessary duplicates are silently discarded. This feature requires atleast two tunnels to be configured between the sending the receiving SDWAN router.	Refer Corrigendum
121	30	2. Remote Location SD-WAN Appliance	SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.)	Please modify the clause as follows: SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.). The security features can be delivered on-premise or through cloud.	Secure access service edge (SASE) combines networking and security functions in the cloud to deliver seamless, secure access to applications, anywhere users work. Since MSEDCL is already using AWS for hosting their applications and SAAS applications : -More workloads are running in the cloud than in the enterprise data center. -SaaS applications are used more frequently than locally installed ones. -More traffic is destined to public cloud services than to the enterprise data center. -More traffic from branch offices is heading to public clouds and will now require Direct Internet Access SASE is the right approach for MSEDCL as it will provide the following benefits: Reduced Complexity, Increased and Optimized performance, Consistent Security and Threat prevention with reduced risk, Centralized orchestration.	As per RFP. For inclusion of SASE architecture refer Corrigendum

122	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology with optimal routing	Please modify the clause as follows: SD-WAN branch end device should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology or on-demand tunneling between branches for optimal routing	Our solution supports dynamic on-demand tunnels between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage.	As per RFP
123	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance should support minimum 250 SDWAN Nodes	Please modify the clause as follows for wider participation of OEMs: "SD-WAN appliance should support minimum 200 SDWAN Nodes"	We intent to deploy ON demand tunneling between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage. As the number of locations are just 66 is nos. even with 100% scalibility and with ON demand tunneling turned ON, support for 200 tunnels should be more than enough.	As per RFP
124	32	2. Remote Location SD-WAN Appliance	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify the clause as follows for wider participation of OEMs: The proposed solution must have ability to reorder/re-transmit failed packets during the failover.	Different OEMs have different mechanisms to deal with Packet loss. Request you to modify the clause for wider participation of OEMs.	Refer Corrigendum
125	32	2. Remote Location SD-WAN Appliance	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links simultaneously for a single application.	Please modify the clause as follows for wider participation of OEMs: To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links for a single application.	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, we use application aware routing and use specific virtual path for traffic destined towards specifis application/ IP address. With this method, solution can use multiple links to load balance all the traffic and critical traffic gets high performance as those applications are running on specific virtual path which are having high SLA. In case of failover/ detorattion on the high sla path, traffic will switch over to another virtual path/tunnel.	As per RFP
126	32	2. Remote Location SD-WAN Appliance	The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1	Please modify the clause as follows: The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1. SD-WAN branch device should support logical segmentation of WAN, LAN and Management interfaces.	This will ensure improved security and end to end segmentation. Hence request you to make the required change.	As per RFP
127	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN branch hardware should be a hardened appliance of OEM running SD-WAN firmware on top of it and all function, scale tests should be done along with hardware and software together	Please add this clause to ensure that the appliance provided can perform in MSEDCL's environment and has undergone performance and scale tests with hardware and software together.	As per RFP

128	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should provide local internet breakout from branches to access SAAS/IAAS applications directly. SD-WAN solution should have built in intelligence to find out the best optimized path from multiple paths to access SAAS applications like O365, webex, Salesforce, box etc.	MSEDCL will deploy direct internet access at its branch locations. Also, MSEDCL is/will be using SAAS applications like O365, MS Teams/Webex, Salesforce, box etc. Hence it is requested to add this clause which will benefit MSEDCL through improved performance of SAAS based applications.	As per RFP
129	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should have automation and guided worflows to configure Virtual edge devices hosted in multiple Cloud providers like AWS/AZURE/GCP to access customer applications within host VPC/VNET	This will ensure automated deployment of HUB devices in AWS cloud without any manual intervention.	As per RFP
130	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should support real-time network performance measurement and visibility for applications along with policy validations	This is an important feature which will ensure that the policies applied by MSEDCL are working properly and will also provide real time visibility into network performance.	As per RFP ,Refer point no 4. NMS ,Orchestration, Administration, Management and Logging Tool 1
131	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should support Geolocation-based firewall rules to configure firewall rules for allowing or denying network traffic based on the specified source and destination locations	This is a very important security feature especially when MSEDCL is going to deploy Direct internet Access at branch locations: Use-Case Scenario A client (192.168.11.10) in a local area network (LAN) initiates traffic over Dedicated Internet Access (DIA) to a destination IP addresses belonging to France (FRA) and China (CHN). As per the security firewall policy, traffic to France should be inspected and that to China should be dropped. Benefits of Geolocation-Based Firewall Rules: 1) You can restrict access to particular countries without needing to know the associated IP addresses for those countries. 2) A geolocation can be a country, a continent, or a list containing both continents and countries. 3) You can add multiple geolocation lists or geolocations using a single policy.	As per RFP
132	19	1. Scope of Work	Perform load balancing for improving the performance with reachability, jitter, latency , packet loss and bandwidth utilization.	Please modify the clause as follows for wider participation of OEMs: Perform load balancing for improving the performance with reachability, jitter, latency , packet loss and/or bandwidth utilization.	Bandwidth utilization is not the correct method to perform load balancing, it leads to challenges in packet forwarding method and unnecessary re-transmissions.	As per RFP
133	16	2. Bidders Pre-Qualification Criteria-IV	**Qualification criteria for Bidder** Bidder should have experience for supply, installation and maintenance of IT networking and security infrastructure, during last 5 years from date of publishing of this tender. The Bidder should have executed similar works as follows : 1. One work order/Contract costing not less than Rs. 5.24 Crores OR 2. Two work orders/Contracts costing not less than Rs. 3.28 Crores each OR 3. Three work orders/Contracts costing not less than Rs. 2.62 Crores each. Note : All the projects submitted for above experience criteria should be completed projects only. **Document Required** Copies of Work order or LOA during the last 5 financial years AND Client certificate for each project mentioning scope of works and value of contract	**Qualification criteria for Bidder** Bidder should have experience for supply, installation and maintenance of IT networking/security infrastructure, during last 7 years from date of publishing of this tender. The Bidder should have executed works as follows : 1. One work order/Contract costing not less than Rs. 5.24 Crores OR 2. Two work orders/Contracts costing not less than Rs. 3.28 Crores each OR 3. Three work orders/Contracts costing not less than Rs. 2.62 Crores each. Note : All the projects submitted for above experience criteria should be completed projects only. **Document Required** Copies of Work order or LOA during the last 7 financial years OR Client certificate for each project mentioning scope of works and value of contract	Last two and half years were gone in COVID Lockdown, hence we requesting you to amend with Seven years of Work experience.	Refer Corrigendum
134	43	4. Payment Terms	Delivery of all SD-WAN Solution hardware :30 % of SDWAN Solution Charges	Delivery of all SD-WAN Solution hardware :80 % of SDWAN Solution Charges	We request you to amend the payment terms as we need the payment early in order to give lowest compititive rates which will be beneficial to MSEDCL.	As per RFP
135			Installation & Commissioning of all SD-WAN solution hardware :40% of A1 of Price SDWAN Solution Charges	Installation & Commissioning of all SD-WAN solution hardware :10% of A1 of Price SDWAN Solution Charges	We request you to amend the payment terms as we need the payment early in order to give lowest compititive rates which will be beneficial to MSEDCL.	As per RFP

136			Stabilization of all SD-WAN Solution hardware:30 % of SDWAN Solution Charges	Stabilization of all SD-WAN Solution hardware:10 % of SDWAN Solution Charges	We request you to amend the payment terms as we need the payment early in order to give lowest compititive rates which will be beneficial to MSEDCL.	As per RFP
137	23	4.2 Technology > V	The remote SD_WAN appliance should be Wi-Fi enabled with integrated or external access point and securely configured SSID	Please modify this Clause to "The remote site should have dedicated SD_WAN appliance and external access point and securely configured SSID"	Wi-Fi AP in SD-WAN appliance is security threat. Wi-fi attacks are different from wired attack and SDWAN is having Wired IPS not the Wireless IPS functionality. So if any hacker hack the Wi-Fi session then he can also hack the SW-WAN fabric as well.	As per RFP
138	23	4.3 Network Integration	VII. The solution should support non-disruptive integration into the existing networks with full interoperability during migration with existing routing hardware and routing	Could you please clarify on exact requirement of integration. Do you want existing SDWAN devices to be managed, monitored by our centralized management platform		for Clarification kindly refer tender sub section 4.3 Network Integration
139	24	4.6 Security -	VI. System should able to support centralized authentication system to authenticate network elements of NMS management tool	MSEDCL is looking for dedicated Ticketing tool (NMS) and NMS ,Orchestration Tool does not support Ticketing feature		Bidder has to provide solution as per requirement given in Tender specification
140	24	4.6 Security -	IX - Solution should have RADIUS/TACACS based authentication for device management	MSDECL looking for separate TACACS based authentication solution or device should support RADIUS/TACACS Protocols		Bidder has to provide solution as per requirement given in Tender specification
141	38	Section – F Deliverable and Service Level Agreements 2. Implementation Timelines & Penalties	Study of existing Setup and submission of plan of action with OEM	Request to make minimum 45 days to Study of existing Setup and submission of plan of action with OEM	Appointment of respective stake holders at Circle office, Site visit, Collating of Data, Preparation of AS-IS document and Plan of Action	As per RFP
142	38	Section – F Deliverable and Service Level Agreements 2. Implementation Timelines & Penalties	Supply, Installation, Configuration Commissioning , Within 90 Days from the issuance of LOA	Within 90 Days from the issuance of LOA supply of Devices is not possible	Due prevailing Semi conductor shortage situation supply within 90 days is not possible. Need to factor Minimum 180 days	As per RFP
143	49	5. Tender Fee and Earnest Deposit Money / Bid Security Deposit	The successful bidder shall at his own expenses deposit with MSEDCL an irrevocable Performance bank guarantee (PBG) ,for 10% of the contract value at the time of signing contract in the format given in Annexure 10 and should be valid for 66 months from the date of LOA. EMD will be returned to the successful bidder only after it submits the PBG .The indicative conditions in which the PBG of the selected vendor may be forfeited are:	As per Notification by Ministry of Finance Dated - 30th Dec 2021. Performance security is reduced to 3% till 31 March 2023	Kindly oblige	As per RFP
144	27	1. SD-WAN Controller / 13	SD-WAN controller should support dynamic routing protocols - OSPF, BGP. SD-WAN controller should be able to create FULL MESH topology with optimal routing	Please modify this clause to "SD-WAN controller should support dynamic routing protocols - OSPF, BGP. SD-WAN controller should be able to create FULL MESH / Partial Mesh topology with optimal routing"	In the SD-WAN setup all the resources will be in Data centre, if any branch to branch communication is required, then we will have partial Mesh capability in SDWAN solution.	As per RFP
145	27	1. SD-WAN Controller / 16	Should support NTP, SNMPv3, DHCP server & relay, syslog, SCP, SSH, NAT/PAT, 802.1Q VLAN tagging	Please modify this clause to "Should support NTP, SNMPv3, DHCP server & relay, syslog, SCP/SSH, NAT/PAT, 802.1Q VLAN tagging"	Currently SSH protocol is widely used for remote login. Accroding to open SSH developers in April 2019 SCP is now outdated.	As per RFP
146	27	1. SD-WAN Controller / 17	SD-WAN controller/HUB appliance support IPv6	Please modify this Clause to "SD-WAN controller/HUB appliance support IPv6 or IPV6 ready in future with patch update without any cost "	From Day one IPv6 feature will not implemented, whenever the feature will be required we will provide the IPV6 patch free of cost.	As per RFP
147	28	1. SD-WAN Controller / 26	If a link carrying application traffic fails, the application traffic must be moved from the failed link to a functioning link in milliseconds without any application timeouts and disconnects.	Please modify this Clause to "If a link carrying application traffic fails, the application traffic must be moved from the failed link to a functioning link in sub second without any application timeouts and disconnects."	All application is also having the resiliency feature. If one tunnel goes down then all the traffic will be shifted to other tunnel and that will be happen in sub-second time.	As per RFP
148	28	1. SD-WAN Controller/27	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify this Clause to "The proposed solution must have ability to reorder any packets that are retransmitted during a failover or support session based load balancing."	Different OEM is having different technology for load balancing. Most of the OEM is supporting session based load balancing instead of packet based load balancing. In session based load balancing packet reorder functionality is not required.	As per RFP
149	30	2. Remote Location SD-WAN Appliance/ 1	*Provide Dedicated WI-FI based SD-WAN appliance* **or SD-WAN appliance with external Access Point** *and have zero touch deployment features.*	Please modify this Clause to "Provide SD-WAN appliance with external Access Point and have zero touch deployment features."	Wi-Fi AP in SD-WAN appliance is security threat. Wi-fi attacks are different from wired attack and SDWAN is having Wired IPS not the Wireless IPS functionality. So if any hacker hack the Wi-Fi session then he can also hack the SW-WAN fabric as well.	Refer Corrigendum for Revised clause. (WI-FI based SD-WAN appliance with external Access points is required and having secure zero touch deployment features.)

150	31	2. Remote Location SD-WAN Appliance / 11	SD-WAN appliance Should have minimum 6 x 10/100/1000 Mbps RJ-45 Ethernet and 1 USB port for 3G or 4G Dongle connectivity. It is preferable that the SD-WAN devices has support for 3G/4G interface card	Please modify this Clause to "SD-WAN appliance Should have minimum 4 x 10/100/1000 Mbps RJ-45 Ethernet and 1 USB port for 3G or 4G Dongle connectivity. It is preferable that the SD-WAN devices has support for 3G/4G interface card"	In each Remote Location, there will be maximum two links. If other device needs to connect on the Remote Location, it should be connect to switch not on the SDWAN appliance. As per best practice design other devices should connect to switch and uplink to SD-WAN gateway Different OEM is having different architecture for SDWAN.	As per RFP, Out of the total requirement of 6 ports it is proposed to use 2 Ports for WAN link,3 Ports for Access Points and 1 Port for existing switch
151	31	2. Remote Location SD-WAN Appliance / 13	SD-WAN appliance should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology with optimal routing	Please modify this Clause to "SD-WAN appliance should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH/Partial MESH topology with optimal routing"	In the SD-WAN setup all the resources will be in Data centre, if any branch to branch communication is required, then we will have partial Mesh capability in SDWAN solution.	As per RFP
152	31	2. Remote Location SD-WAN Appliance / 16	Should support NTP, SNMPv3, DHCP server & relay, syslog, SCP, SSH, NAT/PAT, 802.1Q VLAN tagging	Please modify this clause to "Should support NTP, SNMPv3, DHCP server & relay, syslog, SCP/SSH, NAT/PAT, 802.1Q VLAN tagging"	Currently SSH protocol is used for remote login, SCP is now SCP is outdated and SSH is the widely used protocol.	As per RFP
153	31	2. Remote Location SD-WAN Appliance / 17	SD-WAN appliance support IPv6	Please modify this Clause to "SD-WAN appliance support IPv6 or IPV6 ready in future with patch update without any cost "	From Day one IPv6 feature will not implemented, whenever the feature will be required we will provide the IPV6 patch free of cost.	As per RFP
154	32	2. Remote Location SD-WAN Appliance / 24	The solution shall support network elements to be deployed in any kind of topologies such as any-to- any dynamically, Hub and Spoke, Partial Mesh, Full Mesh on a per segment basis	Please modify this Clause to "The solution shall support network elements to be deployed in any kind of topologies such as any-to- any dynamically/ Partial MESH, Hub and Spoke, Partial Mesh/Full Mesh on a per segment/role/VLAN basis"	In the SD-WAN setup all the resources will be in Data centre, if any branch to branch communication is required, then we will have partial Mesh capability in SDWAN solution. For MSCDCL at a single organisation, VLAN or role based segmentation is the most feasible solution.	As per RFP
155	33	2. Remote Location SD-WAN Appliance / 36	The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1	Please modify this Clause to "The Remote Location SD-WAN appliance should able to support minimum 15 Segments/VLANs/ROLE from day-1"	For MSCDCL at a single organisation, VLAN or role based segmentation is the most feasible solution.	As per RFP
156	56	Stage 1 - Technical Evaluation/Commercial Evaluation	The Technical bids of those bidders who qualify in the prequalification (QR) process only will be evaluated further against the Technical bid evaluation criteria specified in the RFP.	Kindly list the parameters of QR process		Refer Section-C Qualification Criteria of the Tender
157		Switches for Access Point	Switches for Access Point	Do we need to consider PoE switch or Do we need to factor Power Injectors		As per Tender bidder has to provide all the required component to implement the solution
158	18	Section D	Bidder has to provide the new wall mount rack,cable manager,jack panel with UPS sufficient for supplied devices along with industry standardized earthing for supplied equipment's.	Chemical Earthing or The Conventional method of Earthing		Industry standardized earthing.
159	43	4. Payment Terms	2. Installation & Commissioning of all SD-WAN solution hardware 40% of A1 of Price SDWAN Solution Charges	Installation & Commissioning payment should be released after site commissioned and signoff submission		As per RFP
160	43	4. Payment Terms	3. .Stabilization of all SD-WAN Solution hardware 30 % of SDWAN Solution Charges Upon successful stabilization certificate and training of SDWAN Solution	Kindly elobrate on stabilization period		Refer corrigendum for more clarity
161	15	Bidders Pre-Qualification Criteria S.No.ii	The Bidder should have average Annual turnover of minimum 2 Crs in the last 3 financial years (FY 18-19 ,19-20,20-21 or FY 19-20, 20-21,21-22).	As indicated in RFP 30% (approx) of the estimated project cost (6.5622 Cr) has been asked as annual turnover in Pre-Qualification Criteria and 80%, 100, and 120% (approx) of the estimated project cost as experience required by one order, two order and three order respectively. We request you kindly reduce the experience required to 50%, 70%, and 90% of the estimated project cost by one order, two orders, and three orders respectively. This increase the number of participants in the bid.		As per RFP

162	16	Bidders Pre-Qualification Criteria S.No. iv	Bidder should have experience for supply, installation and maintenance of IT networking and security infrastructure, during last 5 years from date of publishing of this tender. The Bidder should have executed similar works as follows : 1. One work order/Contract costing not less than Rs. 5.24 Crores OR 2. Two work orders/Contracts costing not less than Rs. 3.28 Crores each OR 3. Three work orders/Contracts costing not less than Rs. 2.62 Crores each.	As indicated in RFP 30% (approx) of the estimated project cost (6.5622 Cr) has been asked as annual turnover in Pre-Qualification Criteria and 80%, 100, and 120% (approx) of the estimated project cost as experience required by one order, two order and three order respectively. We request you kindly reduce the experience required to 50%, 70%, and 90% of the estimated project cost by one order, two orders, and three orders respectively. This increase the number of participants in the bid.		As per RFP
163	44	Payment Terms S.No. 5	To be paid on quarterly basis, on submission of Quarterly Reports	we request you to release the FMS payment on a monthly basis		As per RFP
164	49	Contract Performance Security S.No. 2	The Bidder should provide the contract performance guarantee for the sum of 10 % (ten percent) of the Contract Price for the due performance of a contract. This Contract Performance Security shall be valid till the expiry of 180 days after the end of the contract period	We request you to kindly reduce the performance guarantee from 10% to 3% as per the guideline issued by the Department of Expenditure, Ministry of Finance, Government of India in OM No. F. 9/4 /2020-PPD dated 30.12.2021.		As per RFP
165	18	Section 1	It is expected from the bidder to follow best suitable enterprise network topology for all offices & provide the better secured solution for the same. Also, the bidder must submit the final detailed diagrams for his/her proposed solution for all locations at the time of bid submission.	What is current network architecture and topology?	Physical visit to circle offices will not help understand the network architecture. Will need this information to work on solution designing; it can also have a operational as well as commercial impact.	It is requested to Refer Section – D Scope of Work and related subsections
166	18	Section 1 - iv.	Bidder has to provide WI-FI connectivity via wi-fi enabled SD-WAN device having 5G capability and supplied WI-FI access points to the respective offices .	How will MSEDCL check for 5G compatibility?	5G compatible devices are available. But 5G environment is not there to test the throughput; how to guarantee that?	Bidder has to provide solution as per tender requirement
167	18	Section 1 - x.	It is bidders responsibility to Install ,configure the SD-WAN controller at Centralized location (MSEDCL Cloud or Hosted Cloud Service) and Remote Office locations communicate with each other and forming the full MESH topology (Refer the Methodology under Section D Scope of Work 4 Methodology)	Are there any specific guidelines for hosting of the SD-WAN controller?	SD-WAN controller is normally hosted at the sedrvice provider's premises and not necessarily native to a public cloud. If there are any specific guidelines it might have an impact on solution designing as well as commercials.	As per Section – D Scope of Work 1. Scope of Work Sr No. xvi.It is joint responsibility of bidders and OEM to design, Install and configure the SD-WAN controller…..
168	18	Section 1 - x.	It is bidders responsibility to Install ,configure the SD-WAN controller at Centralized location (MSEDCL Cloud or Hosted Cloud Service) and Remote Office locations communicate with each other and forming the full MESH topology (Refer the Methodology under Section D Scope of Work 4 Methodology)	Is it required to have any controller instance at MSEDCL's AWS cloud space?	SD-WAN controller is normally hosted at the sedrvice provider's premises and not necessarily native to a public cloud. If there are any specific guidelines it might have an impact on solution designing as well as commercials.	Bidder need to provide requirement in Annexure 18
169	18	Section 1 - xii.	Bidders must provide Cyber Security compliant SD-WAN Solution	Kindly share required security compliances required	Solution design will be dependent on this compliance requirement	Refer RFP Section – D Scope of Work 1. Scope of Work Sr. No xxi. and specifications mentioned in the RFP
170	18	Section 1 - xiv.	Bidder should provide the Centralized Management (Configuration, Network Management, Backup ,Monitoring etc.) and Centralised Reporting tool for managing complete SD-WAN solution and should have the capacity to store the logs for minimum 12 months on MSEDCL Cloud OR those who are providing Centralized Management (Configuration, Network Management, Backup,Monitoring etc.) and Centralised Reporting tool for managing complete SD-WAN solution as a service in this case bidder will borne all cost associated with it to run smooth operation of solution.	Is the reporting tool access required for MSEDCL?	MSEDCL expects reports on the intervals asked or needs the access to the toll to extract the tools?	To be provided as per RFP

171	18	Section 1 - xiv.	Bidder should provide the Centralized Management (Configuration, Network Management, Backup ,Monitoring etc.) and Centralised Reporting tool for managing complete SD-WAN solution and should have the capacity to store the logs for minimum 12 months on MSEDCL Cloud OR those who are providing Centralized Management (Configuration, Network Management, Backup,Monitoring etc.) and Centralised Reporting tool for managing complete SD-WAN solution as a service in this case bidder will borne all cost associated with it to run smooth operation of solution.	What are the details required to be captured in the logs to be stored? OR What all logs are to be maintained?	These details will be required to follow the requirement from MSEDCL.	Details mentioned in the technical specifications requirement mentioned in the RFP
172	18	Section 1 - xvii.	It is bidders responsibility to avail Highest level of Support with Next Business Day replacement.	What is the total time expected to resolve in case of hardware failure?	This clause seems to talk about a hardware failure at MSEDCL's location. Firstly it will have to be figured out if it's a hardware problem.	Refer the RFP section 3. Service Level Agreements " The problem must be fixed within 6 hours for 99% of the calls in a month. For every fall of 1%, the penalty of 4% of quarterly AMC charges will be levied.If Problem not resolved, bidders shall provide replacement within 24 Hrs of logging complaint. If problem is not resolved in 24 Hrs after logging complaint additional 2000 Rs per week per device will be levied. "
173	24	Section 4.5 - III	Should maintain the Voice ,Video quality and support VOIP	How the quality of voice, video be checked?	The quality and performance will be dependant on the connectivity part as well. The underlay connectivity performance should not hamper the SD-WAN performance.	Appropriate QoS to be used for the same
174	22	Section 3	Hardware/Virtual Instance Requirements Details	Seek clarity on virtual instances in HA for SDWAN devices, Access Points, Reporting Tool.	Hardware device cannot have a virtual instance. Is it required to keep additional device at all 66 locations? Is it required to have a HA instances for Reporting Tool?	for clarity Refer Corrigendum
175	24	Section 4.5 - V-b	Latency mitigation techniques layer 3 and Layer 4 application optimization	Need to understrand what is expected here.	We are not able to understand this requirement.	As per RFP ,Bidder has to implement the SD-WAN solution in consultation and co-ordination with OEM .To be provided as per RFP
176	83	Annexture 2 - (A1) - 4	NMS ,Orchestration Tool for Ticketing, Logging , Reporting and Monitoring at MSEDCL Cloud or Cloud Hosted Service	Are there any specific guidelines for hosting of the Ticketing Tool?	If there are any specific guidelines it might have an impact on solution designing as well as commercials.	As per RFP ,Bidder may provide an ITSM compliant ticketing tool
177	19	Scope of Work-point No ix	All the required consumables, labor charges, active & passive components supply, installation & configurations, cabling, casing & capping, civil & electrical work, erection and laying of cables (CAT6, stacking cables, patch chords etc.), connectors, tagging of new cables and all other required components to implement the solution will be in the bidders scope and any damages while bidders work will have to be rectified by bidder.		What will be the location-wise Passive components scope of work? Passive work totally depends on the installation area, length of cable used and the no.of points at location.	Refer RFP section Section – D Scope of Work 1. Scope of Work wherein it is mentioned that bidder is asked to survey for understanding requirement .
178	19	Scope of Work-point No xii	Bidders must provide Cyber Security compliant SD-WAN Solution		Bidders must provide Cyber Security compliant SD-WAN Solution. looking for specific features in cyber security?	As per RFP Section – D Scope of Work 1. Scope of Work Sr. No xxi. and specifications mentioned in the RFP
179	21	On-site Support-point No iv	In this Bidder shall manage IT infra supplied by him along with existing Network equipment (Switches, Routers etc.) at all locations and other MSEDCL network related activities which may part of existing or future upcoming project.		for existing infra management, will MSEDCL provide support from existing OEM if required?	As per RFP.
180	22	4.1 Architecture point No II	Solution should be Amazon cloud ready with supported software image at MSEDCL Cloud (SD-WAN controller) i.e. MSEDCL Cloud or hosted cloud Service and Hardware based at remote location		In case of MSEDCL cloud usage, will that cost will be bare by MSEDCL or will be it in bidder account only?	If bidder proposes SD-WAN controller on MSEDCL cloud, Bidder must mention cloud infra requirement in Annexure 18. Cloud infra outside the MSEDCL cloud will have to borne by bidder.

181	23	4.3 Network Integration point No II	Hub location Cloud device should support in-path and out of path installation		Need More information	As per RFP ,Bidder has to implement the SD-WAN solution in consultation and co-ordination with OEM .To be provided as per RFP
182	26	Section – E Mandatory Technical Specifications Point 1	Section – E Mandatory Technical Specifications	SD-WAN controller must be MSEDCL cloud ready SD┐WAN virtual appliance and should be installed in MSEDCL Cloud with High Availability Or SD-WAN controller as a hosted cloud service and it should be configure in High Availability and no single point failure in any terms	1) Are you referring SD-WAN controller as a Head-end device/software which will be placed in HA at the Amazon cloud, where MSEDCL applications are hosted. 2) If bidder proposing SD-WAN controller as a hosted cloud service then is MSEDCL looking for the hosted cloud service hosted in India Only (POP should be India) as per the Government Guidelines (i.e. No data should go out of India)	Refer Corrigendum
183	27	Section – E Mandatory Technical Specifications Point 10	Section – E Mandatory Technical Specifications	SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall,IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL.	Are you referring 2 Gbps is a SD-WAN throughput. Is MSEDCL not looking for an critical security features like Antivirus, malware protection, BOTnet, Application control alongwith IPS, URL filter, Firewall. and hence request you to mention this features & Threat Protection throughput in the RFP.	As per RFP
184	30	Remote Location SD-WAN Appliance Point 1	Remote Location SD-WAN Appliance	Provide Dedicated WI-FI based SD-WAN appliance or SD┐WAN appliance with external Access Point and have zero touch deployment features. Bidders has to provide 3 wifi access at each location	as per the specifications need for 3 wifi access at each locations to provide a good WIFI coverage at the locations. Please note dedicated WIFI based SD-WAN appliance will not provide the coverage compared to 3 wifi access points. Hence kindly modify this clause as **"SD┐WAN appliance with external Access Point and have zero touch deployment features. Bidders has to provide 3 wifi access at each location"**	As per RFP,The 3 external access points have to be provided for extending the coverage of wifi enabled SD-WAN device
185	30	Remote Location SD-WAN Appliance Point 9	Remote Location SD-WAN Appliance	SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.)	are you refering 200Mbps throughput as a IPSEC encrypted throughput ? Why critical security functions like Antivirus, malware protection, BOTNET etc.not mention alongwith URL Filter, Firewall, IPS, SSL inspection/IPSEC. Is MSEDCL not looking for these security features ? If yes kindly modify this clause as **"SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide 600 Mbps or more threat protection throughput after enabling features like URL Filtering, Firewall, IPS, SSL inspection, Application control, Antivirus, malware protection, botnet.**	As per RFP
186	31	Remote Location SD-WAN Appliance Point 12	Remote Location SD-WAN Appliance	Out of 6 Ethernet port at least 2 or all port should be WAN ports & The proposed SD-WAN edge device should have minimum 8GB RAM and sufficient internal memory to ensure higher performance	Fortigate Solution can deliver higher performance (5 to 9 times more) with low memory. We strongly believe that adopting superior technology enables us to deliver higher throughput utilizing low resources and reduce carbon footprint. also network and network security devices are size based on Throughput, concurrent connections, sessions per seconds, number of IPSEC tunnel supports etc. not based on the RAM. Hence please remove the RAM clause from the specifications.	As per RFP
187	31	Remote Location SD-WAN Appliance Point 14	Remote Location SD-WAN Appliance	SD-WAN appliance should support minimum 250 SD┐WAN Nodes	are you referring 250 SD-WAN nodes means the users count at each Remote locations ? Kindly clarity.	1 SD-WAN device should be connect to 250 SD-WAN devices
188	32	Remote Location SD-WAN Appliance Point 33	Remote Location SD-WAN Appliance	he proposed SD-WAN solution should provide Active┐Active resource utilization at WAN edge and WAN link layers. The solution should support Active-Active dual router topology without using external upstream switches.	Page No 21, Hardware/Virtual Instance Requirements Details mention Remote Offices Requriement - 1 SDWAN Device at each location, 1) Then please let us know why there is an need for Active-Active dual router topology is needed with using an external upstream switches. 2) Also support for Active-Active dual router topology without using external upstream switches is an OEM specific and request to remove this clause so other OEM can also participate in the RFP.	As per RFP
189	32	Remote Location SD-WAN Appliance Point 36	Remote Location SD-WAN Appliance	The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1	are you refering 15 segments menas 15 VLANS ? Kindly clarify	As per RFP clause
190	35	NMS ,Orchestration, Administration, Management and Logging Tool Point 20	NMS ,Orchestration, Administration, Management and Logging Tool	Solution should able to support centralized single plane of management system to allow device configuration, Policy provisioning, Software updates and assurance capabilities.	is MSEDCL not looking to manage all remote locations WIFI-Access Points through a centralize single pane of management alongwith the SDWAN devices and DC SDWAN VM. Hence kindly modify this clause as **"Solution should able to support centralized single plane of management system to allow device configuration, Policy provisioning, Software updates and assurance capabilities for WIFI Access Points, SDWAN devices at remote locations and DC VM"**	As per RFP
191		new clarification	new clarification	can you please share the location wise Internet, MPLS and users counts.		Location details are shared in Annexure 14: Location Details.All location shall use Internet Broadband

192				can you please share the DC (Amazon) MPLS and Internet Bandwidth details.		Internet Service is provided by Cloud Service Provider ,Bandwidth details are not available.
193	15	2. Bidders Pre-Qualification Criteria, Point 4	Bidder should have experience for supply, installation and maintenance of IT networking and security infrastructure, during last 5 years from date of publishing of this tender. The Bidder should have executed similar works as follows : 1. One work order/Contract costing not less than Rs. 5.24 Crores OR 2. Two work orders/Contracts costing not less than Rs. 3.28 Crores each OR 3. Three work orders/Contracts costing not less than Rs. 2.62 Crores each. Note : All the projects submitted for above experience criteria should be completed projects only.	Please modify the clause as follows for wider participation of Bidder Bidder should have experience for supply, installation and maintenance of IT networking **or** security infrastructure, during last 5 years from date of publishing of this tender. The Bidder should have executed similar works as follows : 1. One work order/Contract costing not less than Rs. 5.24 Crores OR 2. Two work orders/Contracts costing not less than Rs. 3.28 Crores each OR 3. Three work orders/Contracts costing not less than Rs. 2.62 Crores each. Note : All the projects submitted for above experience criteria should be completed projects only.		Refer Corrigendum
194	15	2. Bidders Pre-Qualification Criteria, Point 4	Copies of Work order or LOA during the last 5 financial years AND Client certificate for each project mentioning scope of works and value of contract	Please modify the clause as follows for wider participation of Bidder Copies of Work order or LOA during the last 5 financial years AND Client certificate for each project mentioning scope of works and value of contract/**CA Certificate mentioning the Scope of Work and value of contract**		As per RFP
195	17	3. Qualification Criteria for OEM	OEM Must be present in Leaders or in Challengers of Latest Gartner Magic Quadrant (WAN Edge Infrastructure) reports (This clause is not applicable to OEM offering Make in India product as Per GOI guidelines)	**Please modify the clause as follow** **OEM Must be present in Leaders or in Challengers of Latest Gartner Magic Quadrant (WAN Edge Infrastructure) reports**	Gratner Reports represent the OEMs that they qualifed and capable to work on large scale projet. Hence allow OEMs only that are leader and challenger in the gartner.	As per RFP
196	39, 58	2. Implementation Timelines & Penalties Point 4 and 21. Completion Schedule Point	Will be for 5 years from date of LOA 5 Years from the issuance of stabilization certificate. Includes 1 year Warranty + 4 year AMC period.	Both the Clause of page 39 and 58 start date of O&M are different, Kindly clarify when 5 year of O&M will be applicable		Refer Corrigendum
197	42	3. Service Level Agreements, Note, Point 6	The total deduction per quarter shall not exceed 10% of the total QP value	Please modify the clause as follow The total deduction per quarter shall not exceed 5% of the total QP value		As per RFP
198	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS and Vulnerability management capabilties	Please modify the clause as follows for wider participation of OEMs: "SDWAN Controller must offer SD-WAN fucntionalities along with security features such as stateful inspection Firewall, App Aware Firewall, Web/URL Filtering for local internet and should be able to block infected and malicious domains also solution should support DDoS/Vulnerability management capabilties"	Please clarify if the specification ask for DDOS protection of SDWAN Controller and remote edge SDWAN devices? Also, as an OEM have a Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to our products and networks. Please confirm if this is what department is looking for or else please modify the clause as vulnerability management should not part of the SDWAN solution and this fucntionality should be met by third part dedicated solution.	As per RFP
199	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	Please modify the clause as follows for wider participation of OEMs: "SD-WAN controller must have functions like WAN/Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single/multiple tunnel"	Packet Duplication is an SD-WAN feature designed to overcome packet loss in network designs where a WAN edge router has multiple overlay tunnels to the next-hop router. The feature instructs a SDWAN edge router to transmit one copy of each packet over multiple IPsec tunnels. If a packet is lost over the transient path, the receiving SDWAN router can use another copy of the same packet received over another tunnel. If no packets are lost, all unnecessary duplicates are silently discarded.	Refer Corrigendum
200	27	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall, IPS, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL	Please modify the clause as follows for wider participation of OEMs: "SD-WAN controller instance must deliver at least 2 Gbps throughput. The SD-WAN device should provide no packet drops with no performance degradation after enabling all features on instance (Like Firewall, SSL inspection/IPSEC etc.) and even after increase in remote SD-WAN appliances (limited to tender specs) during contract period and without any additional cost implication to MSEDCL"	The virtual HUB SD-WAN edge appliance will be deployed in the AWS cloud where all the applications are hosted. The SD-WAN head end device will decrypt the traffic forward it to internal security infrastructure for traffic filtering. Hence request you to modify the clause for wider participation of OEMs.	As per RFP

201	27	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	SD-WAN controller should support dynamic routing protocols - OSPF, BGP. SD-WAN controller should be able to create FULL MESH topology with optimal routing	SD-WAN controller/head end device should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology or on-demand tunneling between branches for optimal routing	Our solution supports dynamic on-demand tunnels between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage.	As per RFP
202	28	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify the clause as follows for wider participation of OEMs: The proposed solution must have ability to reorder/re-transmit failed packets during the failover.	Different OEMs have different mechanisms to deal with Packet loss. Request you to modify the clause for wider participation of OEMs.	Refer Corrigendum
203	28	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links simultaneously for a single application.	Please modify the clause as follows for wider participation of OEMs: To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links for a single application.	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, we use application aware routing and use specific virtual path for traffic destined towards specifis application/ IP address. With this method, solution can use multiple links to load balance all the traffic and critical traffic gets high performance as those applications are running on specific virtual path which are having high SLA. In case of failover/ detorattion on the high sla path, traffic will switch over to another virtual path/tunnel.	As per RFP
204	26	Section – E Detail Technical Specifications 1. SD-WAN Controller at MSEDCL Cloud	Additional Clause	SD-WAN Controller can be hosted in MSEDCL Cloud or OEM Cloud where the OEM provides Day 0/1/2 support however the SD-WAN Head end device should be placed in MSEDCL Cloud as Virtual appliance. SD-WAN solution should provide Control, Data and Management plane separation on device.		As per RFP
205	30	2. Remote Location SD-WAN Appliance	Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Please modify the clause as follows for wider participation of OEMs: Provide Dedicated WI-FI based SD-WAN appliance or SDWAN appliance with external Access Point and the SDWAN solution should have zero touch deployment features. Bidders has to provide 3 wifi access at each location .	Wireless is not part of the SDWAN solution. The SDWAN Controller supports zero touch deplohyment of SDWAN devices only. Hence request you to modify the clause for wider participation of OEMs.	As per RFP
206	30	2. Remote Location SD-WAN Appliance	SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single tunnel.	Please modify the clause as follows for wider participation of OEMs: SD-WAN device must have functions like traffic Flow Optimization, Forward Error Correction or Packet Duplication with capability to send duplicate packets over a single/dual tunnel.	Packet duplication sends copies of packets on alternate available paths to reach SD-WAN devices. The feature instructs a WAN edge router to transmit one copy of each packet over multiple IPsec tunnels. If a packet is lost over the transient path, the receiving router can use another copy of the same packet received over another tunnel. If no packets are lost, all unnecessary duplicates are silently discarded. This feature requires atleast two tunnels to be configured between the sending the receiving SDWAN router.	Refer Corrigendum
207	30	2. Remote Location SD-WAN Appliance	SD-WAN edge device must deliver at least 200Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.)	Please modify the clause as follows for wider participation of OEMs: SD-WAN edge device must deliver at least 65 Mbps encrypted throughput .The SD-WAN device should provide no performance degradation and no packet drops after enabling all features (Like URL Filtering, Firewall, IPS, SSL inspection/ IPSEC etc.).	65 Mbps of SDWAN throughput with all the services turned ON is more than sufficient for remote branch locations. The amount of traffic that is going to be generated from branch locations will not exceed 50 Mbps (this includes rich media applications like video coferencing etc.)	As per RFP

208	30	2. Remote Location SD-WAN Appliance	SD-WAN controller must offer SD-WAN functionalities along with security features such as stateful inspection firewall, App Aware Firewall, Web/URL Filtering, IPS for local internet and should be able to block infected and malicious domains	Please modify the clause as follows: SD-WAN controller must offer SD-WAN functionalities along with security features such as stateful inspection firewall, App Aware Firewall, Web/URL Filtering, IPS for local internet and should be able to block infected and malicious domains, DNS Security, Advanced Malware Protection including following features: • File type blocking (e.g., block download of .exe files) • Full or selective SSL decryption to further protect the organization from hidden attacks and time-consuming infections • Granular app controls to block specific user activities in select apps (e.g., file uploads to Dropbox, attachments to Gmail, post/shares on Facebook) • Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address	Secure access service edge (SASE) combines networking and security functions in the cloud to deliver seamless, secure access to applications, anywhere users work. Since MSEDCL is already using AWS for hosting their applications and SAAS applications : -More workloads are running in the cloud than in the enterprise data center. -SaaS applications are used more frequently than locally installed ones. -More traffic is destined to public cloud services than to the enterprise data center. -More traffic from branch offices is heading to public clouds and will now require Direct Internet Access SASE is the right approach for MSEDCL as it will provide the following benefits: Reduced Complexity, Increased and Optimized performance, Consistent Security and Threat prevention with reduced risk, Centralized orchestration.	As per RFP. For inclusion of SASE architecture refer Corrigendum
209	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology with optimal routing	Please modify the clause as follows: SD-WAN branch end device should support dynamic routing protocols - OSPF, BGP. SD-WAN solution should be able to create FULL MESH topology and on-demand tunneling between branches for optimal routing. The on demand tunnels should be triggered to be set up only when there is traffic between the two devices. and after the flow of traffic between the devices stops the tunnel between the devices should tear down thereafter not using any network bandwidth and not affecting any device performance.	Our solution supports dynamic on-demand tunnels between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage.	As per RFP
210	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance should support minimum 250 SDWAN Nodes	Please modify the clause as follows for wider participation of OEMs: "SD-WAN appliance should support minimum 200 SDWAN Nodes"	We intent to deploy ON demand tunneling between any two SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices. After the flow of traffic between the devices stops, a user-configurable inactivity timer starts, and after the configured time, the tunnel between the devices is removed. The on-demand link between the two devices is then considered to be inactive. In this inactive state, it does not use network bandwidth and does not affect device performance. The advantages of on demand tunneling are: • Improved performance, especially for less-powerful platforms operating in a full-mesh network. • Improved latency in hub-and-spoke deployments when on-demand tunnels are used between spokes. • Reduced bandwidth use in the network because tunnels in Inactive state do not require Bidirectional Forwarding Detection (BFD) probes, so there is less BFD traffic produced in the network. • Direct tunnels between spokes, while also optimizing CPU and memory usage. As the number of locations are just 66 is nos. even with 100% scalibility and with ON demand tunneling turned ON, support for 200 tunnels should be more than enough.	As per RFP
211	32	2. Remote Location SD-WAN Appliance	The proposed solution must have ability to reorder any packets that are retransmitted during a failover.	Please modify the clause as follows for wider participation of OEMs: The proposed solution must have ability to reorder/re-transmit failed packets during the failover.	Different OEMs have different mechanisms to deal with Packet loss. Request you to modify the clause for wider participation of OEMs.	Refer Corrigendum

212	32	2. Remote Location SD-WAN Appliance	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links simultaneously for a single application.	Please modify the clause as follows for wider participation of OEMs: To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, and large file transfers, the solution should be able to leverage multiple links for a single application.	To ensure high application performance for bandwidth intensive applications such as Video, multi-media streaming, backups, we use application aware routing and use specific virtual path for traffic destined towards specifis application/ IP address. With this method, solution can use multiple links to load balance all the traffic and critical traffic gets high performance as those applications are running on specific virtual path which are having high SLA. In case of failover/ detorattion on the high sla path, traffic will switch over to another virtual path/tunnel.	As per RFP
213	32	2. Remote Location SD-WAN Appliance	The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1	Please modify the clause as follows: The Remote Location SD-WAN appliance should able to support minimum 15 Segments from day-1. SD-WAN branch device should support logical segmentation of WAN, LAN and Management interfaces.	This will ensure improved security and end to end segmentation. Hence request you to make the required change.	As per RFP
214	31	2. Remote Location SD-WAN Appliance	SD-WAN appliance Should have minimum 6 x 10/100/1000 Mbps RJ-45 Ethernet and 1 USB port for 4G/5G Dongle connectivity. It is preferable that the SDWAN devices has support for 4G/5G interface card	Please modify the clause as follows: SD-WAN appliance Should have minimum 2 x 10/100/1000 Mbps RJ-45 Ethernet WAN ports (Out of this one port should provide SFP support) and 8 x 10/100/1000 Mbps RJ-45 LAN ports (Out of this 4 port should provide POE or 2 ports should provide POE+ support) along with 4G/5G connectivity thru USB/Dongle or Interface card, preferred is card.	The SDWAN device should have the flexibility to terminate broadband link over fiber (many service providers provide broadband service over fiber - FTTH). The SDWAN device should also provide capability of PoE to power the access points at branch locations.	As per RFP
215	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN branch hardware should be a hardened appliance of OEM running SD-WAN firmware on top of it and all function, scale tests should be done along with hardware and software together	Please add this clause to ensure that the appliance provided can perform in MSEDCL's environment and has undergone performance and scale tests with hardware and software together.	As per RFP
216	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should provide local internet breakout from branches to access SAAS/IAAS applications directly. SD-WAN solution should have built in intelligence to find out the best optimized path from multiple paths to access SAAS applications like O365, webex, Salesforce, box etc.	MSEDCL will deploy direct internet access at its branch locations. Also, MSEDCL is/will be using SAAS applications like O365, MS Teams/Webex, Salesforce, box etc. Hence it is requested to add this clause which will benefit MSEDCL through improved performance of SAAS based applications.	As per RFP
217	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should have automation and guided worflows to configure Virtual edge devices hosted in multiple Cloud providers like AWS/AZURE/GCP to access customer applications within host VPC/VNET	This will ensure automated deployment of HUB devices in AWS cloud without any manual intervention.	As per RFP
218	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should support real-time network performance measurement and visibility for applications along with policy validations	This is an important feature which will ensure that the policies applied by MSEDCL are working properly and will also provide real time visibility into network performance.	As per RFP
219	30	2. Remote Location SD-WAN Appliance	Additional Clause	SD-WAN solution should support Geolocation-based firewall rules to configure firewall rules for allowing or denying network traffic based on the specified source and destination locations	This is a very important security feature especially when MSEDCL is going to deploy Direct internet Access at branch locations: Use-Case Scenario A client (192.168.11.10) in a local area network (LAN) initiates traffic over Dedicated Internet Access (DIA) to a destination IP addresses belonging to France (FRA) and China (CHN). As per the security firewall policy, traffic to France should be inspected and that to China should be dropped. Benefits of Geolocation-Based Firewall Rules: 1) You can restrict access to particular countries without needing to know the associated IP addresses for those countries. 2) A geolocation can be a country, a continent, or a list containing both continents and countries. 3) You can add multiple geolocation lists or geolocations using a single policy.	As per RFP

220	19	1. Scope of Work	Perform load balancing for improving the performance with reachability, jitter, latency , packet loss and bandwidth utilization.	Please modify the clause as follows for wider participation of OEMs: Perform load balancing for improving the performance with reachability, jitter, latency , packet loss and/or bandwidth utilization.	Bandwidth utilization is not the correct method to perform load balancing, it leads to challenges in packet forwarding method and unnecessary re-transmissions.	As per RFP