

**REPLY / CLARIFICATION TO BIDDERS QUERIES RAISED DURING PRE-BID MEETING  
OPEN ETENDER # 297918 FOR  
SDWAN SOLUTION**

**Open e-TENDER ID- 297918  
Tender Type- Open**

**Date / Time of  
Pre- Bid :  
05.05.2026; 15:30  
Hrs**

<b>Sr. No.</b>	<b>Tender Clause No. / Annexures</b>	<b>Page No.</b>	<b>Bidders Comments / Queries</b>	<b>GEL Reply / Clarifications to All Bidders</b>
--------------------	--	---------------------	-----------------------------------	--

1	Project Scope		<p>"GEL IT team should be able to manage network congestion by optimizing application-level traffic and should provide monitoring capabilities on an ongoing basis <b>and also be able to provide end user response time metrics on a GUI</b>"</p> <p>With regards to the above clause SD-WAN can help the IT team manage network congestion by optimizing application-level traffic through capabilities such as application-aware routing, QoS, traffic prioritization, SLA-based path selection, and continuous monitoring of WAN performance parameters such as link utilization, latency, packet loss, jitter, tunnel health, and application/path performance.</p> <p>SD-WAN can also provide GUI-based visibility into network and application path performance. However, actual end-user response time may depend on multiple factors beyond SD-WAN, including endpoint performance, client/browser behaviour, server/application processing, database response, and backend infrastructure.</p> <p>Kindly confirm whether the requirement is to provide SD-WAN-level application and network performance visibility as mentioned above. If the expectation is to measure full end-user transaction response time, please elaborate the exact use case , as this has a broader scope and requires additional solution/components.</p>	OK, We are elaborate the clause. Refer Revised RFP.
2	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #2		<p><b>Justificaton</b> - Individual port failure should not be mandated as a standalone HA failover trigger, as devices may have multiple ports and redundant WAN/LAN links. A single port failure may not make the device unavailable.</p> <p><b>Request to modify as follows</b> The proposed solution should be capable of HA (High Availability) Active/Passive or Active/Active for control-plane and data-plane components,and should support auto and manual failover in case of device failure, control-plane failure, data-plane failure, or connectivity failure impacting service availability.</p>	OK, We are change the clause. Refer Revised RFP.

3	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #8		<p><b>Justification-</b> Congestion is an indirect condition rather than a standard measurable SD-WAN SLA parameter. Its impact is reflected through latency, loss, and jitter, which are the typical metrics used for performance-based path selection.</p> <p><b>Request to modify as follows</b>  "The proposed solution appliance should be able to select the path based on the link quality ( latency, loss and jitter) must be taken into consideration when a data transfer is initiated."</p>	Tender terms prevails
4	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #13		<p><b>Justification-</b> The requirement requires integrations such as AD, NTP, TACACS, monitoring tools, and incident management tools are generally relevant for SD-WAN management, authentication, logging, monitoring, and operations.</p> <p>However please clarify the expected level of integration with Trend Micro Antivirus and XDR/EDR solution. Direct native integration between SD-WAN and endpoint security platforms such as Antivirus/EDR/XDR is not typically a standard SD-WAN capability.SD-WAN solutions can generally integrate with security and operations ecosystems through standard mechanisms such as syslog, SNMP, NetFlow/IPFIX, APIs etc Therefore, if the requirement is for event correlation, alerting, reporting between SD-WAN and Trend Micro AV/XDR/EDR, the same can be achieved through standard logging/API where supported. Kindly confirm whether this level of integration is acceptable, rather than mandating a direct native integration with a specific endpoint security vendor.</p>	Yes, Trend Micro AV/XDR/EDR, can be achieved and acceptable through standard logging/API where supported.
5	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #15		<p><b>Justification</b>  VLANs are typically used for LAN-side segmentation and are not a standard SD-WAN failover construct. SD-WAN failover should be defined based on WAN transport/link health and overlay path availability rather than generic failover between VLANs</p> <p><b>Request to modify as follows</b>  SD-WAN should be able to configure and failover on/between Physical WAN Interface and Virtual/Logical WAN Interface, based on WAN link and overlay path availability.</p>	Ok, This clause changed. Pls refer revised RFP.

6	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #20	<p><b>Justification -</b> Anti-Virus should be removed as it is typically an endpoint/security function and not directly applicable to sd-wan.</p> <p>“Zero Day Attack Protection” should be reworded as “Zero Day Threat Mitigation / Advanced Threat Protection capabilities,” since zero-day protection cannot be treated as an absolute guarantee by any single SD-WAN control. IPS signatures, AMP/file hash intelligence, URL/domain categorization, reputation feeds, and threat intelligence databases are regularly updated and help protect against known and emerging threats.</p> <p><b>Request to modify as follows :</b></p> <p>"The proposed Solution should support following Security Features : -</p> <ul style="list-style-type: none"> <li>a. IPS (Intrusion Prevention System),</li> <li>b. IDS (Intrusion Detection System)</li> <li>c. Advanced threat protection / zero-day threat mitigation capabilities</li> <li>d. Application base Control.</li> <li>e. Anti- Malware/ Spyware and Anti-Botnet protection,</li> <li>f. IP/URL Filtering Reputation and DDOS.</li> <li>g. All solution including the logging, central manager for SD-WAN nodes should be on-prem, cloud-based solution not acceptable." </li></ul>	OK, We will change the Clause. Pls refer revised RFP.
---	---	--	---

7	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #21	<p><b>Justification</b></p> <p>ISIS is generally not required for enterprise SD-WAN CPE deployments and is more commonly used in provider/core networks. Static routing, OSPF, BGP and EIGRP are sufficient for typical SD-WAN branch, hub, DC, and LAN integration use cases. Therefore, ISIS support may be removed to avoid making the clause unnecessarily restrictive.</p> <p>The requirement for “Multi-gigabit fabric for module-to-module communication” may be reconsidered, as this is specific to modular/chassis-based platforms where separate interface or service modules communicate through an internal fabric/backplane. For fixed-form-factor SD-WAN CPE devices, this may not be directly applicable or measurable as a standard SD-WAN feature.</p> <p><b>Request to modify as follows</b></p> <p>"The proposed SD_WAN solution must support following IP &amp; Routing Features: -</p> <ul style="list-style-type: none"> <li>a. b. c. IPv4 &amp; IPv6 routing support</li> <li>Static routes, Dynamic -OSPF, BGP and EIGRP</li> <li>Policy Based, Performance based routing,</li> <li>d. Must support either of VXLAN/NVGRE/GRE or IPSEC, DNS, DHCP.</li> <li>e. Bidirectional Forwarding detection (BFD) or similar features Network</li> <li>Address Translation (NAT),</li> <li>f. Access Control lists (ACLs) and VRRP</li> </ul>	OK, Pls refer revised RFP
8	Technical requirement -Software Defined Network Solution at DC , DR and office locations : SD-WAN Point #7	<p><b>7 Justification</b> - “Zero Day Attack Protection” should be reworded as “Zero Day Threat Mitigation / Advanced Threat Protection capabilities,” since zero-day protection cannot be treated as an absolute guarantee by any single SD-WAN control. IPS signatures, AMP/file hash intelligence, URL/domain categorization, reputation feeds, and threat intelligence databases are regularly updated and help protect against known and emerging threats.</p> <p><b>Request to modify as follows</b></p> <p>Appliance should support Threat Protection &amp; Throughput (FW + IPS + IDS + Application control + Malware Protection, URL Filtering, Zero Day Threat Mitigation / Advanced Threat Protection capabilities,)</p>	OK, We will change the Clause. Pls refer revised RFP.

9	<p>Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Management plane: - (control Plane &amp; Data Plane) Point #4</p>		<p>The SDWAN controller should be deployed in redundant (HA) mode at DC.</p> <p>Our understanding is that management-plane HA can be designed across DC and DR, while control-plane and data-plane HA has to be deployed within the DC and also extended across DR, based on the final resiliency design. Please clarify if otherwise.</p>	Tender terms prevails
10	<p>"Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>"Management plane: - (control Plane &amp; Data Plane) #12</p>		<p><b>Justification</b> - As per industry recommendations and SD-WAN standard practices, branch edges can operate in a disconnected mode from centralised controllers, but only for a limited time frame. This ensures continuity of operations during temporary outages. Survival of the branch edge without access to centralized controllers for an indefinite period is not recommended. Security keys used for data plane encryption require periodic refresh to maintain cryptographic integrity. Extended isolation also limits policy updates, threat intelligence, and visibility — all critical for secure and manageable SD-WAN operations.</p> <p><b>Request to modify as follows</b> There should be no impact on data plane if the centralized controller is not reachable during failure and should be configurable for upto 7 days.</p>	Tender terms prevails

11	<p>"Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Architectural Specification Point #13</p>		<p><b>Justification</b> -The current connectivity requirement is understood to be based on a Hub-Spoke topology, where branch/spoke locations primarily communicate with/via the Hub/DC. If spoke-to-spoke communication is required, the same can be managed through the Hub/DC or selectively enabled using Partial Mesh based on specific business/application requirements.</p> <p>The requirement for Any-to-Any architecture without dependency on tunnels should be removed, as this is not aligned with standard SD-WAN design principles. In SD-WAN, secure overlay connectivity over WAN is typically established using encrypted tunnels between SD-WAN nodes. This ensures that traffic transported over WAN/Internet links remains encrypted and secure. Mandating any-to-any connectivity without overlay tunnels may create ambiguity and could compromise the intended secure SD-WAN architecture.</p> <p><b>Request to modify as follows :</b> SD-WAN solution must support Hub-Spoke, Spoke-Hub-Hub-Spoke and Partial Mesh topologies. The solution should support policy-based spoke-to-spoke communication either via Hub/DC or through selective Partial Mesh connectivity, as per business/application requirements. Secure overlay connectivity over underlay transports should be established using encrypted tunnels as per standard SD-WAN architecture.</p>	Tender terms prevails
12	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Architectural Specification" Point#21</p>		<p><b>Justification</b> - Currently we understand no multicast services are being used, however it is desired to have the support to be made available in the same hardware whenever required</p> <p><b>Request to modify as follows</b> The SDWAN solution should support multicast if required in future by upgrading software / license without the need for change in SDWAN hardware</p>	Tender terms prevails
13	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Security features in SDWAN appliance" Point#9</p>		<p>The requirement stating that the "proposed solution is preferred to be PCI-DSS compliant" should be removed as PCI-DSS is specifically applicable to environments that store, process, or transmit payment card data and may not be applicable to the current network.</p>	Tender terms prevails

14	<p>"Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Branch and Hub Devices Hardware specification Point #1</p>		<p><b>Justification-</b> Majority service providers today provide last miles on fiber and prefers to deliver the hand-off on fiber and hence we request to have capability of terminating a fiber connectivity directly on the device. They have already migrated, or are in the process of migrating, last-mile connectivity to fiber and therefore prefer to deliver customer hand-offs on fiber interfaces.To align with this industry evolution and to reduce deployment complexity, eliminate the need for external media converters, and improve overall reliability and performance, we request that the proposed device should have provision to support direct termination of fiber connectivity</p> <p><b>Request to modify as follows</b> The Branch CPE should have total 6 Ports (1G) <b>out of which at least 1 or 2 port should be SFP-based.</b> It should have min 8 GB RAM and 8GB of Flash. Proposed solution must support at least 1 X 3G/4G/LTE interface in Active/Backup mode natively or via external ODU.</p>	Ok, Pls refer revised RFP.
15	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Branch and Hub Devices Hardware specification"</p> <p>Additional Point</p>		<p><b>Justification</b> The requirement is added to ensure that each Branch CPE has sufficient per-device IPsec tunnel scale to support hub/DC, DR, cloud, and selective partial-mesh connectivity. Since encrypted overlay tunnels are established at the device level, defining a minimum of 250 gateway-to-gateway IPsec tunnels helps ensure correct sizing, scalability, and future growth without platform limitation.</p> <p><b>Request to add this clause.</b> The Branch CPE device should support at least 250 gateway-gateway IPSEC tunnels.</p>	Ok, We will change Clause.
16	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Branch and Hub Devices Hardware specification"</p> <p>Additional Point</p>		<p><b>Justification</b> The requirement is added to align the DC CPE tunnel scale with asked scalability of upto 1000 sites in a fabric, each site may have 2–3 WAN links. Since the DC/Hub device terminates the majority of branch overlay tunnels, a minimum support of 3000 gateway-to-gateway IPsec tunnels is required to ensure scalability, correct sizing, and future growth without platform limitations.</p> <p><b>Request to add this clause.</b> The DC CPE device should support at least 3000 gateway-gateway IPSEC tunnels to support scalability for 1000 sites which can have minimum 2-3 WAN links.</p>	Ok, We will change Clause.



17	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Branch and Hub Devices Hardware specification" Point#2</p>		<p><b>Justification</b></p> <p>Since the DC CPE will function as the hub/aggregation device and should support higher tunnel scale, routing scale, policies, and future feature enhancements, it is recommended to specify a higher minimum memory requirement than Branch CPE. While 8 GB RAM may be sufficient for branch devices, the DC CPE should have at least minimum 16 GB RAM from Day-1 and scalable</p> <p><b>Request to modify as follows:</b></p> <p>The DC CPE should have min 8 GE Copper and 4 X 10 GE Fiber with minimum <b>16GB RAM from Day-1</b> scalable up to 32 GB.</p>	Tender terms prevails
18	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 2. Project Scope &gt;&gt;</p> <p>Bidder has to integrate SDWAN solution with existing AD, TACACS, NTP, Monitoring Tools Etc deployed at GEL and GSPC office.</p>	Page No 3	<p>TACACS is the propriety to specific OEM. Request to remove TACACS from this clause.</p> <p><b>Suggested Change for Qualify and participate:</b> Bidder has to integrate SDWAN solution with existing AD, NTP, Monitoring Tools, Etc deployed at GEL and GSPC office.</p>	ok, Updating the clause - Bidder has to integrate SDWAN solution with ADS, TACACS/RADIUS, NTP, Monitoring Tools Etc deployed at GEL and GSPC office.
19	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 3. Functional Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; The proposed devices/appliances should be able to interoperate with the existing products of different vendors. (eg: - Cisco, checkpoint, D-Link, Fortinet, WatchGuard, Dell, Array, etc.) deployed at Gujarat Gas Ltd.</p>	Page No 3	<p>This clause is too broad, no OEM can confirmed</p> <p><b>“interoperate with existing products of different vendors”</b></p> <p>without specifying protocols/use cases. FortiGate does interoperate in standards-based scenarios (e.g., IPsec/IKE, BGP), but your clause does not limit scope, so strict compliance to the clause wording cannot be guaranteed.</p> <p><b>Suggested Change for Qualify and participate:</b> The proposed devices/appliances shall support standards-based interoperability for integration with existing multi-vendor environments, including IPsec (IKEv1/IKEv2) VPN connectivity and standard routing (e.g., BGP/OSPF/static) subject to supported parameters.</p>	Tender terms prevails

20	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 3. Functional Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; The proposed Solution should support following Security Features :</p> <ul style="list-style-type: none"> <li>a. IPS (Intrusion Prevention System),</li> <li>b. IDS (Intrusion Detection System)</li> <li>c. Zero Day Attack Protection from Day one</li> <li>d. Application base Control.</li> <li>e. Anti- Malware/ Spyware and Anti-Botnet protection,</li> <li>f. IP Reputation and DDOS.</li> <li>g. Anti-Virus features from day One</li> <li>h. All solution including the logging, central manager for SD-WAN nodes should be onprem, cloud-based solution not acceptable.</li> </ul>	Page No 4	<p>Although the clause seems clear, our understanding is that from Day 1 both the branch and hub devices must have all required security services enabled, and these services must be delivered from the same SD-WAN hardware appliance, without any additional setup or separate devices. As this is not explicitly stated in the specifications, please confirm that this understanding is correct.</p>	Yes
----	--	-----------	---	-----

21	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 3. Functional Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; The proposed SD_WAN solution must support following IP &amp; Routing Features:</p> <ul style="list-style-type: none"> <li>- a. IPv4 &amp; IPv6 routing support</li> <li>b. Static routes, Dynamic -OSPF, BGP, EIGRP and ISIS.</li> <li>c. Policy Based, Performance based routing,</li> <li>d. Must support either of VXLAN/NVGRE/GRE or IPSEC, DNS, DHCP.</li> <li>e. Bidirectional Forwarding detection (BFD) or similar features</li> <li>f. Network Address Translation (NAT),</li> <li>g. Access Control lists (ACLs) and VRRP,</li> <li>h. Multi-gigabit fabric for module to module communication</li> </ul>	Page No 4	<p>b . <b>EIGRP</b> is a proprietary protocol favouring to specific OEM . Request for removal this protocol for level playing field.</p> <p>g. <b>Multi-gigabit fabric for module to module communication</b> - Router specific favouring specific OEM.</p> <p><b>Suggested Change for Qualify and participate:</b> Request the GEL IT team to remove the above proprietary specifications of a specific OEM to ensure fair competition and wider participation.</p>	Ok, We will change Clause.
22	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; SD-WAN &gt;&gt; The SDWAN solution should be software based and should be capable of running on general purpose X86 hardware.</p>	Page No 5	<p>As per best practices, a hardened hardware appliance from the same OEM should be considered. Such appliance ensures a long term investment protection and delivers committed performance as specified in the public datasheet. In contrast, x86-based platforms or third-party hardware running virtual images may not guarantee the required performance or OS / Firmware longterms compatibility due to different hardware and software vendors.</p> <p><b>Suggested Change for Qualify and participate:</b> The SDWAN appliance must be hardnded hardware with OS from the same OEM .</p>	Ok, We will change clause . Pls refer revised RFP.

23	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt;</p> <p>Management plane: - (control Plane &amp; Data Plane) &gt;&gt; The centralized SDWAN controller should be separate or in same (SD WAN Router) device from the Hub device and should provide complete orchestration and automation of SDWAN network.</p>	Page No 5	<p>Each OEM has its own architecture to deliver functionality. This clause appears to favor a specific OEM's design and may limit participation from other leading OEMs.</p> <p><b>Suggested Change for Qualify and participate:</b> The centralized SDWAN controller should be separate or in same (SD WAN Router) device from the Hub device and should provide complete orchestration and automation of SDWAN network <b>via Management / Controller.</b></p>	<p>Ok, We will change this clause - The centralized SDWAN controller should be separate or in same (SD WAN Router) device from the Hub device and should provide complete orchestration and automation of SDWAN network via Management / Controller.</p>
24	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt;</p> <p>Management plane: - (control Plane &amp; Data Plane) &gt;&gt; Management and control plane should be centralized with capability to be separated for each VRF/Tenant in such a way that management/control, and data traffic are not dropped.</p>	Page No 6	<p>Each OEM has its own architecture to deliver functionality. This clause appears to favor a specific OEM's design and may limit participation from other leading OEMs.</p> <p><b>Suggested Change for Qualify and participate:</b> Management and control plane should be centralized with capability to be separated for each VRF/Tenant in such a way that <b>management , Control &amp; data traffic are not dropped.</b></p>	<p>Ok, We will change the clause. Pls refer revised RFP.</p>

25	<p>Section II -B - SOW - Scope of Work_SDWAN  &gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt;  Management plane: - (control Plane &amp; Data Plane) &gt;&gt; Control plane/SDWAN controller must support single pane of glass for configuration management, security configuration and monitoring and must validate the configuration before apply it to running configuration.</p>	Page No 6	<p>Each OEM has its own architecture to deliver functionality. This clause appears to favor a specific OEM's design and may limit participation from other leading OEMs.</p> <p><b>Suggested Change for Qualify and participate: Management Plane / Control plane / SDWAN controller must support single pane of glass for configuration management, security configuration and monitoring and must validate the configuration before apply it to running configuration.</b></p>	Ok, We will change the clause. Pls refer revised RFP.
26	<p>Section II -B - SOW - Scope of Work_SDWAN  &gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt;  Management plane: - (control Plane &amp; Data Plane) &gt;&gt; The network should be implemented as true software defined network architecture with a centralized control plane residing in the Central Controller, also Data Plane and Control Plane should be separate end-to-end.</p>	Page No 6	<p>Each OEM has its own architecture to deliver functionality. This clause appears to favor a specific OEM's design and may limit participation from other leading OEMs.</p> <p><b>Suggested Change for Qualify and participate: The network should be implemented as true software defined network architecture with a Central Management / Controller and Data &amp; control Plane shall be separate end to end.</b></p>	Ok, We will change the clause. Pls refer revised RFP.
27	<p>Section II -B - SOW - Scope of Work_SDWAN  &gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt;  Management plane: - (control Plane &amp; Data Plane) &gt;&gt; There should be no impact on data plane if the centralized controller is not reachable during failure.</p>	Page No 6	<p>Each OEM has its own architecture to deliver functionality. This clause appears to favor a specific OEM's design and may limit participation from other leading OEMs.</p> <p><b>Suggested Change for Qualify and participate: There should be no impact on data plane if the centralized Management / controller is not reachable during failure.</b></p>	Ok, We will change the clause. Pls refer revised RFP.

28	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; Architectural Specification &gt;&gt; The data plane at the branch locations, data center should be programmable from the central software defined network controller and should provide single pane of glass form complete WAN network.</p>	Page No 6	<p>Each OEM has its own architecture to deliver functionality. This clause appears to favor a specific OEM's design and may limit participation from other leading OEMs.</p> <p><b>Suggested Change for Qualify and participate:</b> The data plane at the branch locations, data center should be programmable from the central software defined network <b>controller / Manager</b> and should provide single pane of glass form complete WAN network.</p>	Ok, We will change the clause. Pls refer revised RFP.
29	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; Architectural Specification &gt;&gt; The system should be able to retrieve the network information without any peering protocols like BGP, OSPF or any other routing protocol over WAN.</p>	Page No 8	<p>This clause favouring specific OEM functionality and restricting other OEM participation. Request for removal this clause for level playing field.</p> <p><b>Suggested Change for Qualify and participate:</b> Request the GEL IT team to remove the this proprietary Clause of a specific OEM to ensure fair competition and wider participation.</p>	Ok, We will change this clause - The solution should support centralized network discovery, topology learning, and path intelligence with minimal dependency on dynamic routing protocol peering across WAN links
30	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; Security features in SDWAN appliance &gt;&gt; The Proposed SDWAN CPE solution should support Intrusion detection and prevention for local breakout internet traffic.</p>	Page No 8	<p>As mentioned in the functional specification it is highly recommended to ask the complete security stack not only IPS functionality.</p> <p><b>Suggested Change for Qualify and participate:</b>The Proposed SDWAN HUB and Edge devices shall support IPS , IDS , Application, control , Malware Protection, Zero Day Attack protection , Bot Protection within same hardware.</p>	Ok, We will change the clause. Pls refer revised RFP.

31	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; Branch and Hub Devices Hardware specification</p> <p>&gt;&gt; The Branch CPE should have total 6 Copper Ports (1G) either any combination of SFP or on board from day 1. It should have min 8 GB RAM and 8GB of Flash. Proposed solution must support at least 1 X 3G/4G/LTE interface in Active/Backup mode.</p>	Page no 9	<p>ASIC-based hardware does not require high memory to achieve the desired throughput. The current memory clause appears to favor x86-based platforms; hence, we request its removal to ensure fair competition.</p> <p>Also, the requirement of at least one 3G/4G/LTE interface in active/backup mode seems to favor specific OEM hardware. This functionality can be provided through an ISP's external ODU, so we request removal of this clause as well.</p> <p><b>Suggested Change for Qualify and participate:</b> The Branch CPE should have total 6 Copper Ports (1G) either any combination of SFP or on board from day 1.</p>	Ok, We will change the clause. Pls refer revised RFP.
32	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; Branch and Hub Devices Hardware specification</p> <p>&gt;&gt; The DC CPE should have min 8 GE Copper and 4 X 10 GE Fiber with 8GB scalable up to 32 GB</p>	Page No 9	<p>SD-WAN devices should be evaluated based on throughput performance, not solely on memory or compute specifications. Memory-based scaling is a legacy router approach; Hardened hardware appliances do not allow configuration changes.</p> <p>Hence including strict memory clauses appears to favor specific x86-based OEMs and may restrict other leading OEMs to participate.</p> <p><b>Suggested Change for Qualify and participate:</b> The DC CPE should have min 8 GE Copper and 4 X 10 GE Fiber ports from day 1.</p>	Tender terms prevails
33	<p>Section II -B - SOW - Scope of Work_SDWAN</p> <p>&gt;&gt; 4. Technical Specifications of SD-WAN (DC,DR, Tier-1/2/3, Remote branch Location) &gt;&gt; Branch and Hub Devices Hardware specification</p> <p>&gt;&gt; Software defined network Appliance should be supplied with minimum 6Gbps of throughput with services like SD-WAN, IP-Sec, NAT features enabled from day one.</p>	Page No 10	<p>It is highly recommended to ask the Secure SD WAN throughput where all the security services are enabled and measure the appliance throughput to protect your investment.</p> <p><b>Suggested Change:</b> Suggested to ask security enabled throughput which helps GEL to implement the security enabled SD-WAN solution.</p>	Tender terms prevails

34	Proposed solution should be in the form of Virtual Appliance or hardware appliance from same OEM or approved 3rd party hardware for OEM software and should be able to support High-Availability Central Location as per the requirement.	6	<p>Kindly delete this clause.</p> <p><b>Justification:</b> Proposed solution should be in the form of Virtual Appliance or hardware appliance from same OEM or approved 3rd party hardware for OEM software and should be able to support High-Availability Central Location as per the requirement.</p>	Tender terms prevails
35	The Branch CPE should have total 6 Copper Ports (1G) either any combination of SFP or on board from day 1. It should have min 8 GB RAM and 8GB of Flash. Proposed solution must support at least 1 X 3G/4G/LTE interface in Active/Backup mode.	9	<p>Kindly relax this clause so that other OEM solutions can also qualify.</p> <p>ASIC-based architectures typically do not require higher memory to achieve the desired performance. Also, SIM-based functionality may be available only in higher-end models.</p> <p><b>Suggestion:</b> The Branch CPE should have total 4 Copper Ports (1G) either any combination of SFP or on board from day 1.</p>	Tender terms prevails
36	The DC CPE should have min 8 GE Copper and 4 X 10 GE Fiber with 8GB scalable up to 32 GB	9	<p>Request you to kindly remove this clause.</p> <p>Network devices shall be evaluated and selected based on their published performance parameters, not solely on memory or compute specifications. Therefore, we request removal of this clause so that ASIC-based vendor solutions can also participate."</p>	Tender terms prevails
37	Payment Details - Support for 2nd , 3rd ,4th and 5th Year: Quarterly advance payment.	13	Request you to kindly change the AMC support payment "Yearly Advance".	Ok, We will change the clause. Pls refer revised RFP.
38	Buyback requirement. The successful bidder has to buy back the existing devices/equipment (e.g. CISCO 1900 routers etc.) as mentioned in commercial bid (Refer Annexure – 1 List of IT Device for Buyback).	13	request you to remove the buyback clause.	Tender terms prevails
39	Section III - Schedule of Rates	1	For Warranty Support, do we need to mention Unit rate (1 no.) or Rate of Total Quantity?	Tender terms prevails



40	<b>Section V - Delivery Period</b> The BIDDER must deliver and install the complete hardware and software solution at the DC (Gandhinagar), DR (Surat), or an alternate site designated by GEL within 24 weeks from the date of Contract awarded.	2	<p>Need clarity whether 16 weeks or 24 weeks. Please confirm if 24 weeks delivery timeline is for DC &amp; DR?</p>	Total Timeline for delivery + installation is 24 weeks.
41	<b>Section II B: UPTIME and Service Level Agreement</b>	11	Please clarify whether WAN link outages caused by ISP/service provider shall be excluded from SD-WAN appliance uptime SLA calculations.	Yes
42	<b>Section II B:</b> The proposed SDWAN solution should support Multicast.	8	Please clarify the multicast applications and protocols currently in use within GEL network for proper solution sizing and validation.	Yes, Application such as VC, CCTV and in future SCADA and other business application will be added.
43	In the solution, the tunnel/VRF creation should be automatic & dynamic without any manual configuration on the edges and the controller	3	<p>Clarification Required:  Our understanding from this clause is Post onboarding , overlay tunnels and VRFs/segments shall be provisioned automatically by the centralized controller / orchestrator with no manual per-site configuration. And Recommended for automation If branch-to-hub connectivity fails, the solution shall auto-create secure spoke-to-spoke tunnels and reroute traffic per policy, and shall automatically remove/tear down such temporary tunnels and withdraw routes when hub connectivity is restored (configurable SLA/health checks with hysteresis)</p> <p><b>Our Suggestion:</b>  1. The solution shall provide controller/orchestrator-driven, zero-touch automation for overlay tunnel and VRF/segment provisioning with no manual per-site configuration after onboarding shall be done from template.  2. If any branch loses hub connectivity or miss SLA , the solution shall automatically form secure branch-to-branch tunnels and reroute traffic per policy, and shall automatically withdraw routes and tear down those temporary tunnels when hub connectivity is restored</p>	Yes, as suggested understanding is correct.

44	The proposed devices/appliances should be able to interoperate with the existing products of different vendors. (eg: - Cisco, checkpoint, D-Link, Fortinet, WatchGuard, Dell, Array, etc. )deployed at Gujarat Gas Ltd.	3	<p><b>Clarification required:</b> The clause is too broad/absolute: no vendor can guarantee “interoperate with existing products of different vendors” without specifying protocols/use cases. FortiGate does interoperate in standards-based scenarios (e.g., IPsec/IKE, BGP), but your clause does not limit scope, so strict compliance to the clause wording cannot be guaranteed</p> <p><b>Suggestion:</b> The proposed devices/appliances shall support standards-based interoperability for integration with existing multi-vendor environments, including IPsec (IKEv1/IKEv2) VPN connectivity and standard routing (e.g., BGP/OSPF/static) subject to supported parameters</p>	Tender terms prevails
45	<p>The proposed Solution should support following Security Features : -</p> <ul style="list-style-type: none"> <li>a. IPS (Intrusion Prevention System),</li> <li>b. IDS (Intrusion Detection System)</li> <li>c. Zero Day Attack Protection from Day one</li> <li>d. Application base Control.</li> <li>e. Anti- Malware/ Spyware and Anti- Botnet protection,</li> <li>f. IP Reputation and DDOS.</li> <li>g. Anti-Virus features from day One</li> <li>h. All solution including the logging, central manager for SD-WAN nodes should be onprem, cloud-based solution not acceptable.</li> </ul>	4	<p><b>Clarification Required:</b> Although the clause appears self-explanatory, our understanding is that, from Day 1, both the branch and hub devices must be enabled with all security services specified in the functional specifications and all the security services shall be delivered from same hardware appliance. Since this is not explicitly mentioned in the device specifications, kindly confirm.</p>	Yes

46	The SDWAN solution should be software based and should be capable of running on general purpose X86 hardware.	5	<p><b>Clarification required:</b> Our understanding from the clause is that the proposed controller and edge devices shall be supplied as hardened appliances from the OEM solution, whereas the orchestration and reporting tools shall be software-based and may be deployed on x86 platforms or on any standard server hardware</p> <p><b>Our Suggestion:</b> The orchestrator/reporting platform shall be software-based, deployable on general-purpose x86 hardware. The edge and hub controller devices must be same OEM hardened hardware appliances.</p>	OK, We will change the Clause. Pls refer revised RFP.
47	The SDWAN solution should provide capability to be hosted on cloud-based and on premise deployment.	5	<p><b>Clarification required:</b> This clause appears to be designed for the future cloud roadmap. However, Clause No. 6 (Page No 5) asks for a complete on-premises solution, which requires clarification and contradicts the current clause. Therefore, please suggest the required changes. As per our understanding for the proposed deployment, the solution should be fully on-premises.</p>	It is only fully on-premises.
48	Appliance should support Threat Protection & Throughput (FW + IPS + IDS + Application control + Malware Protection, Zero Day Attack protection)	5	<p>Please clarify the required throughput values after enabling the security service. GEL to update on throughput requirement for hub and edge devices as there is no clarification in the clause.</p>	The Throughput for SD WAN device at DC/DR, Branch location is inclusive of all security licence /services. Refer RFP – (Software defined network Appliance specifications)
49	The network should be implemented as true software defined network architecture with a centralized control plane residing in the Central Controller, also Data Plane and Control Plane should be separate end-to-end.	6	<p>clause is not clear to understand. Data plane and the management plane shall be separate as per the solution therefore, please amend the clause. The network should be implemented as true software defined network architecture with a centralized management and control Plane should be separate end-to-end.</p>	Ok, We will change This clause - The centralized SDWAN controller should be separate or in same (SD WAN Router) device from the Hub device and should provide complete orchestration and automation of SDWAN network via Management / Controller.

50	<p>3.Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location)</p> <p>The proposed SD_WAN solution must support following IP &amp; Routing Features: -</p> <p>b. Static routes, Dynamic -OSPF, BGP, EIGRP and ISIS.</p>	page-4	Request to remove EIGRP as its vendor proprietary	OK, We will remove this Protocaol.
51	<p>4. Technical requirement -Software Defined Network Solution at DC , DR and office locations</p> <p>Management plane: - (control Plane &amp; Data Plane) point-1</p>	page-5	<p>Request to rephrase the clause as follows:</p> <p>The centralized SDWAN controller should be separate device from the Hub device and should provide complete orchestration and automation of SDWAN network</p>	Ok, We will change This clause - The centralized SDWAN controller should be separate or in same (SD WAN Router) device from the Hub device and should provide complete orchestration and automation of SDWAN network via Management / Controller.
52	<p>4. Technical requirement -Software Defined Network Solution at DC , DR and office locations</p> <p>Security features in SDWAN appliance</p>	Page-8	<p>Request to addition for better solution coverage</p> <p>The solution must support 5000 applications from day-1 and additionally support custom applications and use such parameters for traffic forwarding, QOS, security policies and reporting</p>	Tender terms prevails
53	<p>4. Technical requirement -Software Defined Network Solution at DC , DR and office locations</p> <p>Security features in SDWAN appliance</p>	Page-8	<p>Request to addition for better solution coverage</p> <p>The solution must support DNS based traffic inspection and traffic enforcement by blocking DNS based vulnerabilities like DNS tunneling</p>	The solution should cater all DNS protection attacks.

54	4. Technical requirement -Software Defined Network Solution at DC , DR and office locations  Security features in SDWAN appliance	Page-8	Request to addition for better solution coverage  The solution must support Geo-location based, botnet, c&c's, phishing IP's using dynamic security policies.	Yes, This is part of scope with respect to Security licence at DC/DR, Branch Offices.
55	4. Technical requirement -Software Defined Network Solution at DC , DR and office locations  Reporting in SDWAN	Page-9	Request to addition for better solution coverage  The solution must Support deailed reports for WAN link usage, performance (Latency, Jitter, loss), application discovered, security events for URL, IP, DNS, IPS and Anti-virus and Zero-day protection analysis from sandbox from day-1	Tender terms prevails
56	4. Technical requirement -Software Defined Network Solution at DC , DR and office locations  Branch and Hub Devices Hardware specification  point-1	Page-9	Request to Separate the Interface specifications for Branch and DC/DR locations, to ensure the solutioning is done differently	Tender terms prevails
57	4. Technical requirement -Software Defined Network Solution at DC , DR and office locations  Branch and Hub Devices Hardware specification  point-7	Page-10	Request to change the branch bandwidth based on current bandwidth and 1.5x to accommodate for future growth.  Category - B - 100 Mbps Cateogory-C - 50 Mbps	Tender terms prevails

58	Project Scope		<p>"GEL IT team should be able to manage network congestion by optimizing application-level traffic and should provide monitoring capabilities on an ongoing basis <b>and also be able to provide end user response time metrics on a GUI</b>"</p> <p>With regards to the above clause SD-WAN can help the IT team manage network congestion by optimizing application-level traffic through capabilities such as application-aware routing, QoS, traffic prioritization, SLA-based path selection, and continuous monitoring of WAN performance parameters such as link utilization, latency, packet loss, jitter, tunnel health, and application/path performance.</p> <p>SD-WAN can also provide GUI-based visibility into network and application path performance. However, actual end-user response time may depend on multiple factors beyond SD-WAN, including endpoint performance, client/browser behavior, server/application processing, database response, and backend infrastructure.</p> <p>Kindly confirm whether the requirement is to provide SD-WAN-level application and network performance visibility as mentioned above. If the expectation is to measure full end-user transaction response time, please elaborate the exact use case , as this has a broader scope and requires additional solution/components.</p>	<p>OK, We are elaborate the clause. Refer Revised RFP.</p>
59	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #2		<p><b>Justificaton</b> - Individual port failure should not be mandated as a standalone HA failover trigger, as devices may have multiple ports and redundant WAN/LAN links. A single port failure may not make the device unavailable.</p> <p><b>Request to modify as follows</b> The proposed solution should be capable of HA (High Availability) Active/Passive or Active/Active for control-plane and data-plane components,and should support auto and manual failover in case of device failure, control-plane failure, data-plane failure, or connectivity failure impacting service availability.</p>	<p>Ok, We will change Clause.</p>

60	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #8		<p><b>Justification-</b> Congestion is an indirect condition rather than a standard measurable SD-WAN SLA parameter. Its impact is reflected through latency, loss, and jitter, which are the typical metrics used for performance-based path selection.</p> <p><b>Request to modify as follows</b>  "The proposed solution appliance should be able to select the path based on the link quality ( latency, loss and jitter) must be taken into consideration when a data transfer is initiated."</p>	Tender terms prevails
61	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #13		<p><b>Justification-</b> The requirement requires integrations such as AD, NTP, TACACS, monitoring tools, and incident management tools are generally relevant for SD-WAN management, authentication, logging, monitoring, and operations.</p> <p>However please clarify the expected level of integration with Trend Micro Antivirus and XDR/EDR solution. Direct native integration between SD-WAN and endpoint security platforms such as Antivirus/EDR/XDR is not typically a standard SD-WAN capability.SD-WAN solutions can generally integrate with security and operations ecosystems through standard mechanisms such as syslog, SNMP, NetFlow/IPFIX, APIs etc Therefore, if the requirement is for event correlation, alerting, reporting between SD-WAN and Trend Micro AV/XDR/EDR, the same can be achieved through standard logging/API where supported. Kindly confirm whether this level of integration is acceptable, rather than mandating a direct native integration with a specific endpoint security vendor.</p>	Yes, Acceptable.
62	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #15		<p><b>Justification</b>  VLANs are typically used for LAN-side segmentation and are not a standard SD-WAN failover construct. SD-WAN failover should be defined based on WAN transport/link health and overlay path availability rather than generic failover between VLANs</p> <p><b>Request to modify as follows</b>  SD-WAN should be able to configure and failover on/between Physical WAN Interface and Virtual/Logical WAN Interface, based on WAN link and overlay path availability.</p>	Ok, We will change Clause.

63	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #20	<p><b>Justification -</b> Anti-Virus should be removed as it is typically an endpoint/security function and not directly applicable to sd-wan.</p> <p>“Zero Day Attack Protection” should be reworded as “Zero Day Threat Mitigation / Advanced Threat Protection capabilities,” since zero-day protection cannot be treated as an absolute guarantee by any single SD-WAN control. IPS signatures, AMP/file hash intelligence, URL/domain categorization, reputation feeds, and threat intelligence databases are regularly updated and help protect against known and emerging threats.</p> <p><b>Request to modify as follows :</b></p> <p>"The proposed Solution should support following Security Features : -</p> <ul style="list-style-type: none"> <li>a. IPS (Intrusion Prevention System),</li> <li>b. IDS (Intrusion Detection System)</li> <li>c. Advanced threat protection / zero-day threat mitigation capabilities</li> <li>d. Application base Control.</li> <li>e. Anti- Malware/ Spyware and Anti-Botnet protection,</li> <li>f. IP/URL Filtering Reputation and DDOS.</li> <li>g. All solution including the logging, central manager for SD-WAN nodes should be on-prem, cloud-based solution not acceptable." </li></ul>	OK, We will change the Clause. Pls refer revised RFP.
----	---	--	---



64	Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location) Point #21		<p><b>Justification</b></p> <p>ISIS is generally not required for enterprise SD-WAN CPE deployments and is more commonly used in provider/core networks. Static routing, OSPF, BGP and EIGRP are sufficient for typical SD-WAN branch, hub, DC, and LAN integration use cases. Therefore, ISIS support may be removed to avoid making the clause unnecessarily restrictive.</p> <p>The requirement for “Multi-gigabit fabric for module-to-module communication” may be reconsidered, as this is specific to modular/chassis-based platforms where separate interface or service modules communicate through an internal fabric/backplane. For fixed-form-factor SD-WAN CPE devices, this may not be directly applicable or measurable as a standard SD-WAN feature.</p> <p><b>Request to modify as follows</b></p> <p>"The proposed SD_WAN solution must support following IP &amp; Routing Features: -</p> <ul style="list-style-type: none"> <li>a. b. c. IPv4 &amp; IPv6 routing support</li> <li>Static routes, Dynamic -OSPF, BGP and EIGRP</li> <li>Policy Based, Performance based routing,</li> <li>d. Must support either of VXLAN/NVGRE/GRE or IPSEC, DNS, DHCP.</li> <li>e. Bidirectional Forwarding detection (BFD) or similar features Network</li> <li>Address Translation (NAT),</li> <li>f. Access Control lists (ACLs) and VRRP</li> </ul>	Ok, Pls refer Revised RFP.
65	Technical requirement -Software Defined Network Solution at DC , DR and office locations : SD-WAN Point #7		<p><b>7 Justification</b> - “Zero Day Attack Protection” should be reworded as “Zero Day Threat Mitigation / Advanced Threat Protection capabilities,” since zero-day protection cannot be treated as an absolute guarantee by any single SD-WAN control. IPS signatures, AMP/file hash intelligence, URL/domain categorization, reputation feeds, and threat intelligence databases are regularly updated and help protect against known and emerging threats.</p> <p><b>Request to modify as follows</b></p> <p>Appliance should support Threat Protection &amp; Throughput (FW + IPS + IDS + Application control + Malware Protection, URL Filtering, Zero Day Threat Mitigation / Advanced Threat Protection capabilities,)</p>	OK, We will change the Clause. Pls refer revised RFP.

66	<p>Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Management plane: - (control Plane &amp; Data Plane) Point #4</p>		<p>The SDWAN controller should be deployed in redundant (HA) mode at DC.</p> <p>Our understanding is that management-plane HA can be designed across DC and DR, while control-plane and data-plane HA has to be deployed within the DC and also extended across DR, based on the final resiliency design. Please clarify if otherwise.</p>	Tender terms prevails
67	<p>"Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>"Management plane: - (control Plane &amp; Data Plane) #12</p>		<p><b>Justification</b> - As per industry recommendations and SD-WAN standard practices, branch edges can operate in a disconnected mode from centralised controllers, but only for a limited time frame. This ensures continuity of operations during temporary outages. Survival of the branch edge without access to centralized controllers for an indefinite period is not recommended. Security keys used for data plane encryption require periodic refresh to maintain cryptographic integrity. Extended isolation also limits policy updates, threat intelligence, and visibility — all critical for secure and manageable SD-WAN operations.</p> <p><b>Request to modify as follows</b> There should be no impact on data plane if the centralized controller is not reachable during failure and should be configurable for upto 7 days.</p>	Tender terms prevails

68	<p>"Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Architectural Specification Point #13</p>		<p><b>Justification</b> -The current connectivity requirement is understood to be based on a Hub-Spoke topology, where branch/spoke locations primarily communicate with/via the Hub/DC. If spoke-to-spoke communication is required, the same can be managed through the Hub/DC or selectively enabled using Partial Mesh based on specific business/application requirements.</p> <p>The requirement for Any-to-Any architecture without dependency on tunnels should be removed, as this is not aligned with standard SD-WAN design principles. In SD-WAN, secure overlay connectivity over WAN is typically established using encrypted tunnels between SD-WAN nodes. This ensures that traffic transported over WAN/Internet links remains encrypted and secure. Mandating any-to-any connectivity without overlay tunnels may create ambiguity and could compromise the intended secure SD-WAN architecture.</p> <p><b>Request to modify as follows :</b> SD-WAN solution must support Hub-Spoke, Spoke-Hub-Hub-Spoke and Partial Mesh topologies. The solution should support policy-based spoke-to-spoke communication either via Hub/DC or through selective Partial Mesh connectivity, as per business/application requirements. Secure overlay connectivity over underlay transports should be established using encrypted tunnels as per standard SD-WAN architecture.</p>	Tender prevails	terms
69	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Architectural Specification" Point#21</p>		<p><b>Justification</b> - Currently we understand no multicast services are being used, however it is desired to have the support to be made available in the same hardware whenever required</p> <p><b>Request to modify as follows</b> The SDWAN solution should support multicast if required in future by upgrading software / license without the need for change in SDWAN hardware</p>	Tender prevails	terms
70	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Security features in SDWAN appliance" Point#9</p>		<p>The requirement stating that the "proposed solution is preferred to be PCI-DSS compliant" should be removed as PCI-DSS is specifically applicable to environments that store, process, or transmit payment card data and may not be applicable to the current network.</p>	Tender prevails	terms

71	<p>"Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Branch and Hub Devices Hardware specification Point #1</p>		<p><b>Justification-</b> Majority service providers today provide last miles on fiber and prefers to deliver the hand-off on fiber and hence we request to have capability of terminating a fiber connectivity directly on the device. They have already migrated, or are in the process of migrating, last-mile connectivity to fiber and therefore prefer to deliver customer hand-offs on fiber interfaces.To align with this industry evolution and to reduce deployment complexity, eliminate the need for external media converters, and improve overall reliability and performance, we request that the proposed device should have provision to support direct termination of fiber connectivity</p> <p><b>Request to modify as follows</b> The Branch CPE should have total 6 Ports (1G) <b>out of which at least 1 or 2 port should be SFP-based.</b> It should have min 8 GB RAM and 8GB of Flash. Proposed solution must support at least 1 X 3G/4G/LTE interface in Active/Backup mode natively or via external ODU.</p>	OK, We will change the Clause. Pls refer revised RFP.
72	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Branch and Hub Devices Hardware specification"</p> <p>Additional Point</p>		<p><b>Justification</b> The requirement is added to ensure that each Branch CPE has sufficient per-device IPsec tunnel scale to support hub/DC, DR, cloud, and selective partial-mesh connectivity. Since encrypted overlay tunnels are established at the device level, defining a minimum of 250 gateway-to-gateway IPsec tunnels helps ensure correct sizing, scalability, and future growth without platform limitation.</p> <p><b>Request to add this clause.</b> The Branch CPE device should support at least 250 gateway-gateway IPSEC tunnels.</p>	Ok, we will add this clause.
73	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Branch and Hub Devices Hardware specification"</p> <p>Additional Point</p>		<p><b>Justification</b> The requirement is added to align the DC CPE tunnel scale with asked scalability of upto 1000 sites in a fabric, each site may have 2–3 WAN links. Since the DC/Hub device terminates the majority of branch overlay tunnels, a minimum support of 3000 gateway-to-gateway IPsec tunnels is required to ensure scalability, correct sizing, and future growth without platform limitations.</p> <p><b>Request to add this clause.</b> The DC CPE device should support at least 3000 gateway-gateway IPSEC tunnels to support scalability for 1000 sites which can have minimum 2-3 WAN links.</p>	Ok, we will add this clause.

74	<p>""Technical requirement -Software Defined Network Solution at DC , DR and office locations :</p> <p>Branch and Hub Devices Hardware specification" Point#2</p>		<p><b>Justification</b> Since the DC CPE will function as the hub/aggregation device and should support higher tunnel scale, routing scale, policies, and future feature enhancements, it is recommended to specify a higher minimum memory requirement than Branch CPE. While 8 GB RAM may be sufficient for branch devices, the DC CPE should have at least minimum 16 GB RAM from Day-1 and scalable</p> <p><b>Request to modify as follows:</b> The DC CPE should have min 8 GE Copper and 4 X 10 GE Fiber with minimum <b>16GB RAM from Day-1</b> scalable up to 32 GB.</p>	Tender terms prevails
75	Section-2-B-SOW Scope of Work Page no -2		<p>De-installation of the existing router at the branch along with power cables and replacing with new SD-WAN device and power cables (rack mounting). Reconnecting all uplinks and other cables in proper manner. Asset tagging to be done on the new network equipment. Same will be supplied by GEL.</p> <p>Clarity: Kindly clarify the scope of GEL in the clause.Is it related to all the equipments along with cables.</p>	GEL will provide Power , Space and Downtime Only.
76	Section-2-B-SOW Scope of Work Page no -4		<p>All network wide configuration &amp; application routing policies shall be from the Centralized policy management and SDWAN controller.</p> <p>Clarity: Confirm if the controllers will be on prem or should be hosted on cloud.</p>	ON Prem only
77	Section-2-B-SOW 5. Delivery & Installation Page no 10		<p>Bidder shall be responsible for delivery and installation of the complete solution (hardware &amp; software both) ordered at both DC &amp; DR (currently in Gandhinagar &amp; Surat respectively) or any other alternate site as per GEL requirement within 16 weeks from the date of issuance /award of Purchase order.</p> <p>Page 12- Hardware delivery timelines- 16 weeks &amp; implementation and go live-8 weeks from hardware delivery.</p> <p>Clarity: Both clauses contradicting each other and hence need clarity. Delivery timeline mentioned in penalty clause is ok to go ahead with.</p>	Total Timeline for delivery + installation is 24 weeks.

78	Section-2-B-SOW 9. Payment Details Page no 13		<ul style="list-style-type: none"> <li>• 30% of payment on successful installation and commissioning of all Hardware and submission of installation report duly signed /certified by GEL Network SME</li> </ul> <p>Please confirm if the acceptance of locations will be link wise or phase wise/lot of 10 or 20. We request for site wise acceptance for providing troublefree operations and maintenance.</p>	OK, Site wise device invoice can be raised post successful installation and acceptance of commissioning report.
79	STC- SDWAN Solution		<p>4. DELIVERY PERIOD / INSTALLATION: 4.1 The BIDDER must deliver and install the complete hardware and software solution at the DC (Gandhinagar), DR (Surat), or an alternate site designated by GEL within 24 weeks from the date of Contract awarded.</p> <p>Query: We request GEL to amend the delivery timelines to 28-32 weeks.</p>	Tender terms prevails
80	Architectural Specification: Clause No.15	8	<p>The default behaviour of router needs routing for LAN advertisement. Once a VPN tunnel is created, routing protocols like BGP, OSPF, RIP, static etc are needed over the tunnel for LAN advertisement. There could be some proprietary solution that might be using the same at router software level and abstracted from dashboard users. Hence requesting you to remove this clause for better participation of other OEMs who uses standard routing process.</p>	Ok, We will change Clause.
81	Security features in SDWAN appliance: Clause No.1	8	<p>Zero trust security architecture is not the scope of any SD-WAN solution. It supports only those OEMs who converges several solutions like gateway router, gateway security and end point protection solution into one. Hence requesting you to remove this point to allow SD-WAN players who doesn't provide endpoint solutions.</p>	Tender terms prevails
82	Security features in SDWAN appliance: Clause No.2	8	<p>In the tender document on Page No.2 it is mentioned "<i>Bidder has to plan the central SDWAN devices for DC and DR, to support for approximately 100+ edge devices from day 1 and also support scalability up to 200 edge devices at any point of time.</i>" This point contradicts the referred clause. Therefore please provide clarity on whether the solution should support 200 edge devices or 1000 edge devices.</p>	Tender terms prevails
83	Branch and Hub Devices Hardware specification: Clause No.1	9	<p>It is mentioned that the branch device needs to support min 8GB RAM and 8 GB flash. Kindly make it generic as min 8 GB RAM and 8GB SSD. It is also mentioned that the device should support at least 1 X 3G/4G/LTE interface in Active/Backup mode. Can we use USB slots to support 3G/4G/5G USB dongle.</p>	Yes, Use of USB slot with support USB dongle accepted.

84	Branch and Hub Devices Hardware specification: Clause No.2	9	It is mentioned that the hub device needs to support 8GB scalable to 32GB. Are you referring to RAM or storage? If it is RAM, then the storage value is missing. Kindly add the same.	Ok, Pls refer revised RFP.
85	Branch and Hub Devices Hardware specification: Clause No.7	10	The throughput values of Type A,B,C are with SD-WAN services only. The throughput after enabling the security services is not mentioned. Kindly provide these values. Moreover 6 Gbps throughput mentioned for the hub appliance seems to be an overkill and therefore requesting you to align the same with the aggregated bandwidth at the hub location or reduce is to 4 Gbps or less	Tender terms prevails
86	Management plane: - (control Plane & Data Plane): Clause No.1	5	The control plane and the data plane needs to be separate and not converged to comply with points No. 3, 11, 12 mentioned under the same section. Hence allow only SD-WAN solutions that have their control plane and data plane decoupled.	Ok, We will change This clause - The centralized SDWAN controller should be separate or in same (SD WAN Router) device from the Hub device and should provide complete orchestration and automation of SDWAN network via Management / Controller.
87	Section II -A- BIDDER QUALIFICATION CRITERIA_SDWAN Solution, The Bidder shall have at least ANY of the following experience of having successfully carried out supply and installation of software defined network appliance during the last 3 years reckoned from the month in which this tender is published:	1	Request you to accept the purchase orders that are currently in progress.	BQC criteria can not be change.

88	Section V - STC - SDWAN Solution RATE VALIDITY 3.1 The RATES specified in the RATE CONTRACT shall remain firm & fixed till Completion of Work including the WARRANTY/EXTENDED WARRANTY PERIOD i.e. 05 (Five) years	2	We request you to please remove the word “Rate Contract.” In view of ongoing price fluctuations, executing a rate contract is not feasible at this stage. This should be treated as a one-time purchase, with price validity of 30 days from the RA date.	Tender terms prevails
89	CONTRACT-CUM-PERFORMANCE BANK GUARANTEE (CPBG): 10% of the basic Callout Order Value and valid up-to Callout Order validity end date + 3 months claim lodgement period.	2	We request you to kindly consider reducing the CPBG from 10% to 5% of the basic Callout Order value, in line with prevailing industry standards and to ease financial constraints.	Tender terms prevails
90	Section II -B - SOW - Scope of Work_SDWAN Solution -- Branch and Hub Devices Hardware specification -- Point 1	9	Request customer to kindly confirm whether the Branch CPE should mandatorily support minimum 6 x 1G Copper RJ45 interfaces from day one, since the current clause mentions “any combination of SFP or onboard interfaces,” which is open to interpretation.	Tender terms prevails
91	Section II -B - SOW - Scope of Work_SDWAN Solution -- Branch and Hub Devices Hardware specification -- Point 1	9	The RFP clause specifies support for 3G/4G/LTE connectivity in Active/Backup mode but does not mandate an inbuilt LTE interface. Industry-standard SD-WAN devices support LTE failover through external USB dongles/interfaces or ODU-based connectivity with equivalent functionality. Hence, request customer to confirm that support for 3G/4G/LTE connectivity through external USB interfaces/dongles or ODU shall also be considered compliant.	OK, We will change the Clause. Pls refer revised RFP.
92	Section II -B - SOW - Scope of Work_SDWAN Solution -- Branch and Hub Devices Hardware specification -- Point 7	10	All C category locations have bandwidth requirements below 30 Mbps and even after considering 3x future scalability, the effective bandwidth requirement remains below 100 Mbps. Hence, requesting higher throughput specifications may result in over-sizing of the solution and additional cost without practical utilization. Therefore, request customer to kindly consider minimum throughput of 100 Mbps with all security features enabled for C category locations.	Tender terms prevails
93	Section - IIB	3	Server and storage hardware infra for controllers are under customer scope or they need to be provided by the bidder.	Pls refer revised RFP.



94	Section - IIB	3	The successful bidder has to buy back the existing Network devices/equipment (Refer -Annexure -2 List of IT network device for Buyback .) Can this point be removed and how the value of buyback will be considered as an factor in the evaluation process. Kindly share the valuation method	Tender terms prevails
95	Section - IIB	11	While calculating penalty, kindly confirm the outage due to link non-funcational will not be considered as the link is not part of this RFP.	Yes
96	Section - IIB	14	QHSE REQUIREMENTS - Provide more details scope on it.	Tender terms prevails
97	Section - IIB	2	RFP mentions support for ~100 edge devices scalable to 200. Please confirm Expected growth timeline Whether licenses should be procured upfront for 200 nodes or phased	Tender terms prevails
98	Section - IIB	Across Page3 and Page7	Please confirm threshold values and detailed scope for:  Latency Jitter Packet Loss for dynamic path selection policies	Tender terms prevails
99	Section - IIB	3	Please confirm interoperability expectations with existing OEM devices (Cisco, Fortinet, etc.) and specific use cases.	Tender terms prevails
100	Section - IIB	3	Is HA (dual appliance) required at branch locations or only at DC/DR?	DC & DR Only
101	Section - IIB	4	Please clarify definition of “Zero-Day Protection” and acceptable OEM technologies (sandboxing, AI-based detection, etc.)	Pls refer revised RFP.
102	Section - IIB	9	Please clarify whether DDoS mitigation responsibility lies entirely with the SD-WAN solution or partially with upstream ISPs.	Tender terms prevails
103	Section - IIB	9	The RFP specifies DDoS protection at every SD-WAN CPE. Please clarify whether DDoS protection is expected:  Inline at each branch device Centrally at DC/DR locations Or via upstream ISP/cloud-based scrubbing services	DC,DR and Branch Devices.
104	Section - IIB	9	Please clarify whether DDoS protection requirement is limited to:  L3/L4 volumetric attacks (SYN flood, UDP flood, ICMP flood) or Advanced L7 application-layer attacks (HTTP flood, DNS amplification, etc.)	The solution should cater all DDoS protection attacks.

105	Section - IIB	2	<p>The solution should be primarily able to provide aggregation of network links , load balancing of traffic, prioritizing of application over the network links, implementation of QoS per tunnel on the fly, discover network traffic with application-level insight with deep packet visibility and analyse and report on application usage and anomalies and prioritizing a specific application traffic over a link. Provide detailed scope on it.</p>	Pls refer revised RFP.
106	Section - IIB	8	<p>The system should be able to support multiple internet break out points based on the application (e.g. The system should do a direct internet break out at the branch location for internet traffic while rest of the internet traffic should be egressed through a centralized security infrastructure in the data center or the cloud). As per Annexure-1 there are all MPLS given at the branch location but on page 8 it is asking for local internet break out, kindly clarify on it.</p>	It is for DC and DR links and future upcoming branch link also.
107	Section II -B - SOW - Scope of Work_SDWAN Solution	Page 2	<p>Bidder has to plan the central SDWAN devices for DC and DR, to support for approximately 100+ edge devices from day 1 and also support scalability up to 200 edge devices at any point of time.</p> <p>We presume that the collocation space, power &amp; access to the DC &amp; DR site will be provided by GEL. Please confirm.</p>	Yes
108	Section II -B - SOW - Scope of Work_SDWAN Solution	Page 3	<p>Successful bidder shall provide all technical specifications, all necessary entitlements, papers of license, etc. for both hardware and software of all equipment covered in this RFP to the GEL.</p> <p>OEMs provide SDWAN licenses in subscription model only. Hope GEL is in understanding for subscription-based licenses of SDWAN solution.</p>	Yes
109	Section II -B - SOW - Scope of Work_SDWAN Solution	Page 3	<p>The proposed solution should be capable of HA (High Availability) Active/Passive or Active/Active and should be capable of auto &amp; manual failover in case active device fails (Port/Controller etc) and also incase connectivity fails.</p> <p>Is HA required across all locations or only at DC, DR, HQ, CO type of sites?</p>	DC & DR Only

110	Section II -B - SOW - Scope of Work_SDWAN Solution	Page 4	<p>The proposed solution to be able to Integrate with AD, Trend micro antivirus and XDR/EDR solution,NTP Server, TACACS, PIM, Monitoring tool, incident management tool etc.</p> <p>Request to clarify on the level of integration required with XDR/EDR, Trendmicro AV.</p>	Pls refer revised RFP
111	Section II -B - SOW - Scope of Work_SDWAN Solution	Page 10	<p>Bidder shall be responsible for delivery and installation of the complete solution (hardware &amp; software both) ordered at both DC &amp; DR (currently in Gandhinagar &amp; Surat respectively) or any other alternate site as per GEL requirement within 16 weeks from the date of issuance /award of Purchase order.</p> <p>Request to change to 24 weeks delivery &amp; installation considering the current logistics challenges in equipment shipment &amp; implementation of controllers at DC &amp; DR, Hub devices &amp; branch devices.</p>	Total Timeline for delivery + installation is 24 weeks.
112	Section II -B - SOW - Scope of Work_SDWAN Solution	Page 10	<p>Note The date on which the complete system is installed will be taken as the date of installation. In case of part installation of the system, the date of last items installed will be taken as the date of installation.</p> <p>Request to consider partial implementation as when the SDWAN devices are installed at site &amp; site is migrated to SDWAN, user services will be operational on the SDWAN solution.</p>	Tender terms prevails
113	Section II -B - SOW - Scope of Work_SDWAN Solution	Page 17	<p>15. Annexure – 1 List of GEL and GSPC Locations MPLS Bandwidth (Mbps)</p> <p>Please clarify whether the bandwidth mentioned in this column is the "per link" bandwidth or "aggregate" bandwidth at site.</p>	It is an aggregate bandwidth
114	Section - III SOR- Schedule of Rates- SDWAN Solution	Page 1	<p>Part:A: Supply and Installation</p> <p>Schedule lists only the SDWAN CPE cost line items. Please include the line item for SDWAN Controllers at DC &amp; DR</p>	Tender terms prevails

115	BQC - Criteria Sr No 2 Section II -A- BIDDER QUALIFICATION CRITERIA_SDWAN Solution, Page No 1	Section II -A- BIDDER QUALIFICATION CRITERIA _SDWAN Solution, Page No 1	<p>We request you to amend the below clause as :</p> <p>1. The Bidder shall have at least ANY of the following experience of having successfully carried out supply and installation of software defined network appliance during the last <b>5 years</b> reckoned from the month in which this tender is published.</p> <p>2. Additionally requesting you to kindly elaborate on the term “software-defined network appliance” and clarify exactly what scope or type of solution/equipment GEL is referring to.</p>	BQC criteria Prevails
116	<p>3.Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location)</p> <p>h. All solution including the logging, central manager for SD-WAN nodes should be on-prem, cloud-based solution not acceptable.</p>	page-4	<p>Request to change the clause for point "H", as follows:</p> <p>All solution including the logging, central manager for SD-WAN nodes should be on-prem, cloud-based solution not acceptable. However, Zero day protection can be made available through cloud instance hosted in India.</p>	Pls refer revised RFP
117	<p>3.Functional Specifications of Software Defined network Appliance (DC,DR, Tier-1/2/3, Remote branch Location)</p> <p>The proposed SD_WAN solution must support following IP &amp; Routing Features: -</p> <p>b. Static routes, Dynamic -OSPF, BGP, EIGRP and ISIS.</p>	page-4	<p>Request to modify the clause to avoid proprietary protocols.</p> <p>The proposed SD_WAN solution must support following IP &amp; Routing Features: -</p> <p>b. Static routes, Dynamic -OSPF, BGP and ISIS.</p>	Ok, Pls refer revised RFP
118	<p>4. Technical requirement -Software Defined Network Solution at DC , DR and office locations</p> <p>Requirements and specifications "SDWAN"</p> <p>Point-6 network protocols and architectures.</p> <p>All Component of SD WAN should be on</p>	page-5	<p>Request to modify and remove the clause as follows:</p> <p>All components of SDWAN should be on premises meeting the end user requirements. However, the Zero day protection solution/ATP can be cloud hosted for enhanced coverage within India.</p>	Pls refer revised RFP

	premise meeting the end user requirements			
119	<p>4. Technical requirement -Software Defined Network Solution at DC , DR and office locations</p> <p>Management plane: - (control Plane &amp; Data Plane) point-1</p>	page-5	<p>Request to rephrase the clause as follows:</p> <p>The centralized SDWAN controller should be separate device from the Hub device and should provide complete orchestration and automation of SDWAN network</p>	<p>Ok, We will change This clause - The centralized SDWAN controller should be separate or in same (SD WAN Router) device from the Hub device and should provide complete orchestration and automation of SDWAN network via Management / Controller.</p>
120	<p>4. Technical requirement -Software Defined Network Solution at DC , DR and office locations</p> <p>Security features in SDWAN appliance</p>	Page-8	<p>Request to addition for better solution coverage</p> <p>The solution must support 5000 applications from day-1 and additionally support custom applications and use such parameters for traffic forwarding, QOS, security policies and reporting</p>	<p>Tender terms prevails</p>
121	<p>4. Technical requirement -Software Defined Network Solution at DC , DR and office locations</p> <p>Security features in SDWAN appliance</p>	Page-8	<p>Request to addition for better solution coverage</p> <p>The solution must support DNS based traffic inspection and traffic enforcement by blocking DNS based vulnerabilities like DNS tunneling</p>	<p>The solution should cater all DNS protection attacks.</p>

122	4. Technical requirement -Software Defined Network Solution at DC , DR and office locations  Security features in SDWAN appliance	Page-8	Request to addition for better solution coverage  The solution must support Geo-location based, botnet, c&c's, phishing IP's using dynamic security policies.	The solution should cater all Geo location based attacks Protection.
123	4. Technical requirement -Software Defined Network Solution at DC , DR and office locations  Reporting in SDWAN	Page-9	Request to addition for better solution coverage  The solution must Support deailed reports for WAN link usage, performance (Latency, Jitter, loss), application discovered, security events for URL, IP, DNS, IPS and Anti-virus and Zero-day protection analysis from sandbox from day-1	The solution should cater all attacks protection.
124	4. Technical requirement -Software Defined Network Solution at DC , DR and office locations  Branch and Hub Devices Hardware specification  point-1	Page-9	Request to Separate the Interface specifications for Branch and DC/DR locations, to ensure the solutioning is done differently	Pls refer revised RFP
125	4. Technical requirement -Software Defined Network Solution at DC , DR and office locations  Branch and Hub Devices Hardware specification  point-7	Page-10	Request to change the branch bandwidth based on current bandwidth and 1.5x to accommodate for future growth.  Category - B - 100 Mbps Cateogory-C - 50 Mbps	Tender terms prevails