परीक्षण मार्गदर्शिका

टीईसी ४९१६१:२०२६

(पूर्व सं: टीईसी/टीजी/आई टी/एस डी डब्लू-३०१/०१/दिसंबर-१९)

TEST GUIDE

TEC 49161:2026

(Earlier No. : TEC/TG/IT/SDW-301/01/DEC-19)

for

सॉफ्टवेयर डिफाइंड वाइड एरिया नेटवर्क

SOFTWARE DEFINED WIDE AREA NETWORK

[SDWAN]

(जीआर सं: टीईसी ४९१६०: २०२५)

(Standard No.: TEC 49160:2025)

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलालभवन, जनपथ, नई दिल्ली-११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHID LAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Release 03: Apr, 2026

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This Test Guide of testing pertains to Test Schedule and Test procedures for Software Defined Wide Area Network.

CONTENTS

A. HISTORY SHEET

Sl. No.	Standard / document No.	Title	Remarks
1.	TEC/TG/IT/SDW-301/01/DEC-19	TSTP for SDWAN Solution	Issue No. 1
2.	TEC 49161:2025	TSTP for SDWAN Solution	Conversion of TSTP to Test Guide
3.	TEC 49162:2026	TSTP for SDWAN Solution	

B. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance/functionality/ requirements/ performance of the **Software Defined Wide Area Networks (SDWAN)** solution to be deployed-in or implemented through Indian Telecom Network.

C. General information:

Sl. No.	General Information	Details (to be filled by testing team)	
1	Name and Address of the Applicant		
2	Date of Registration		
3	Name and No. of GR/IR/Applicant's Spec. against which the approval sought		
4	Details of Equipment		
	Type of Equipment	Model No.	Serial No.
(i)			
(ii)			
5	Any other relevant Information:-		

D. Testing team*: (to be filled by testing team)*

S No.	Name	Designation	Organization	Signature
1.				
2.				

E. List of the Test Instruments:

S No.	Name of the test instrument	Make /Model *(to be filled by testing team)*	Validity of calibration *(to be filled by testing team)*
1.			*dd/mm/yyy*
2			
3			
4			
5			
6			
7			
8			

F. Equipment Configuration Offered: (*to be filled by testing team)*

(a) <Equipment/product name> Configuration:

S No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

(b) <Other equipment name> Configuration:

S No.	Item	Details	Remarks

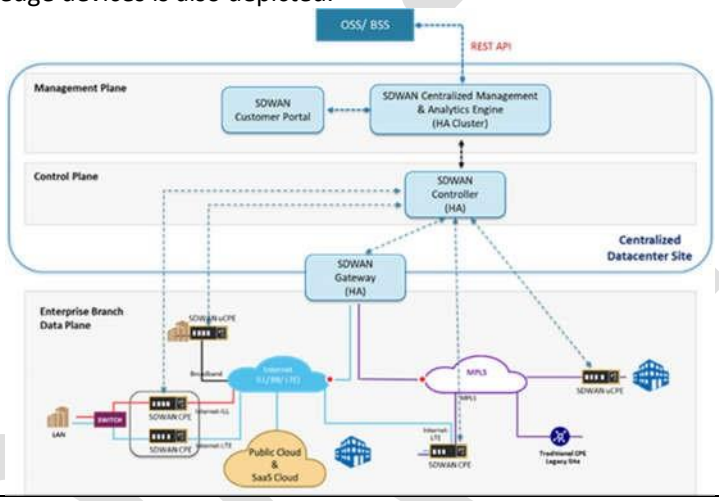
Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

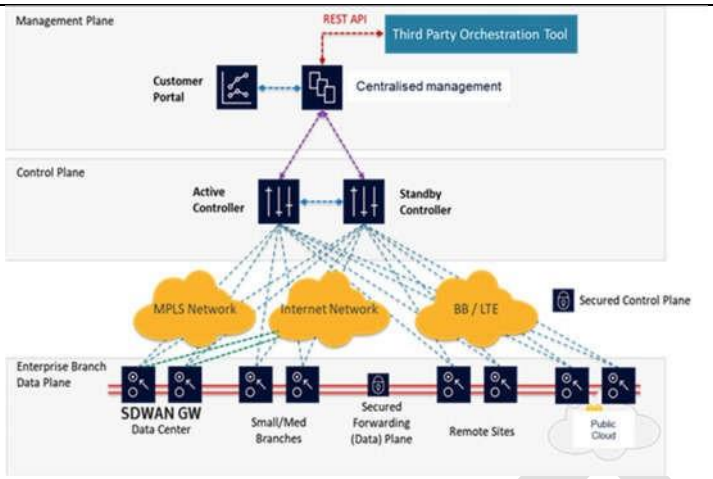
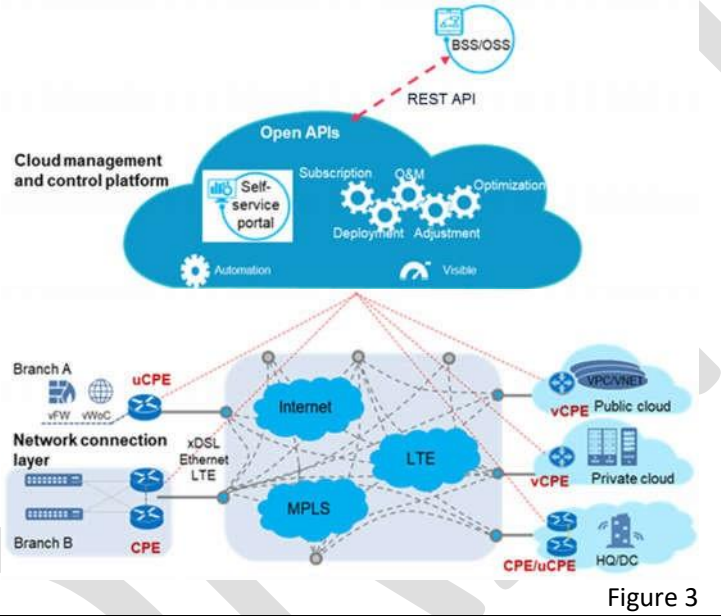
G. Equipment/System Manuals: *(to be filled by testing team)*

Availability of Maintenance manuals, Installation manual, Repair manual & User Manual etc. **(Y/N)**

H. Clause-wise Test Type and Test No.: -

Cl. No	Sub Cl.	Clause	Type of Test	Compliance
			Physical Check / Declaration / Documentation / Report from Accredited Test Lab / Functional Verification / Information / Lab Test (Test Reference)	**Complie d / Not Complie d / Submitte d / Not Submitte d / Not Applicabl e (Indicate Annexur e No for Test Results)**
1.0		Introduction:	Information	
		SD-WAN is the new trend for enterprise branch network architecture, which provides simplified and flexible branch interconnection. It enables the broader goal of enterprises connecting branch users to applications in a cost-effective WAN topology. It can reduce the bandwidth costs of WAN links through hybrid links viz MPLS link, Ethernet link, internet bandwidth link, broadband link, cable link, LTE/4G link. It is independent of the type of network – wireless or wireline networks, the public internet or leased line, whether the applications are hosted in data centers or on public clouds. This will also help enterprises' branch offices to route & distribute traffic to the internet whereby a more expensive MPLS line is not necessary.	Information	
1.1		Plug-and-play and automatic deployment technologies can reduce the service provisioning time. Intelligent scheduling with application detection ensures high-quality experience of key applications, and cloud-based management reduces O&M costs.	Information	
1.2		**SD-WAN solution features:** • Reduce WAN traffic • Route traffic on the fastest available paths between any two points • Provide better quality of service (QoS) for high-priority applications • Improve network security • Simplify administration for remote and branch offices • Allow enterprises to leverage low-cost and flexible	Information	

		Internet and 4G network connections in place of MPLS links. • Provide visibility into WAN paths to help administrators troubleshoot performance issues		
1.3		This GR pertains to controller, Management plane, Gateway and cost-effective SDWAN edge devices such as customer premises equipment (CPE), universal CPEs (uCPEs), virtual CPEs (vCPEs) and value added services (VAS). CPE is a dedicated appliance with dedicated hardware and software. uCPE utilises x86 based hardware as CPE. vCPE is a application/VNF running on a public or private cloud infrastructure.	Information	
1.4		An architecture diagram of SD-WAN is given in Figure-1 below. The diagram depicts the connectivity of the SDWAN edge devices with the controller via broadband (Wireline), LTE (Wireless) and MPLS. The interconnectivity between traditional CPEs connected on MPLS and controller/SDWAN edge devices is also depicted. 	Information	
1.5		SD-WAN architecture applies the principles of SDN onto the wide area network environment by clearly separating Management, control and data plane functions thereby providing the benefits of improved bandwidth economics, application prioritization and ease of centralized management. SDWAN provides dynamic policy based application path selection across any combination of transport. These three functions are depicted below in fig 2. The control plane is centralised and incorporated as a central controller. The deployment of various types of SDWAN edge devices (CPE, uCPE, vCPE) and their deployment is as shown in fig 3.	Information	

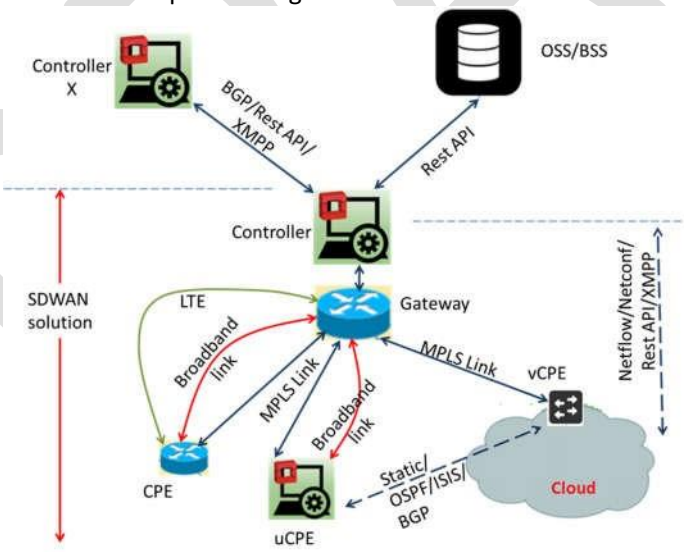
		 Figure 2  Figure 3		
1.6		**Management Plane :** The Centralized Policy Management is a programmable policy and analytics engine that provides following major functions and services:	Information	
1.6.1		It provides a flexible and hierarchical network policy framework that enables administrators to define and enforce resource policies in a user-friendly manner.	Information	
1.6.2		Network configuration including moves, adds and changes are centrally managed via an intuitive graphical user interface.	Information	
1.6.3		It supports open northbound ReSTful API interface to send and receive all information.	Information	
1.6.4		Centralized Analytics Engine collects and stores network statistics from the overlay networks it has provisioned. Statistics are aggregated over hours, days and months.	Information	
1.6.5		Certificate Authority that issues and verifies digital certificates	Information	
1.6.6		It manages and distributes the keys used by SDWAN edge	Information	

		devices for data-plane communication encryption		
1.7		**Control Plane:** The controller is the SDN controller and serves as the robust network control plane for the network services, maintaining a full view of the network and service topologies. Controller is managed by Policy Engine and serves below mentioned functions:	Information	
	1.7.1	Resilient SDN controllers.	Information	
	1.7.2	Full view of the network topology	Information	
	1.7.3	Utilizes open, standard and scalable BGP peering and federation for scaling wherever required. This includes REST/BGP/XMPP.	Information	
	1.7.4	Auto-discovery of CPEs, vCPE's & uCPE's	Information	
	1.7.5	Programs the data-plane forwarding on the CPEs, vCPE's & uCPE's	Information	
1.8		**SD-WAN edge device:**	Information	
	1.8.1	The SD-WAN edge device (CPE, vCPE or uCPE) constitute the network-forwarding (data) plane for network services at the central and remote business locations. CPE performs below mentioned functions: -	Information	
	a)	Network services demarcation and data forwarding from the branch	Information	
	b)	Securely deployed via bootstrapping process	Information	
	c)	Programmed via OpenFlow/Netconf/REST API/XMPP by the Controller	Information	
	d)	L2-L4 switching and routing with advanced network functions	Information	
	e)	Encryption services	Information	
	f)	Encapsulates traffic to/from the network (VXLAN/ VXLAN over IPsec/GRE/IPSec/MPLS over UDP)	Information	
	g)	Physical or Virtual form-factors	Information	
1.9		**SDWAN Self-Service Portal:**	Information	
	1.9.1	Self Service Portal is an overlay application on the SDN Controller platform which provides self-service management of VPNs and branches along with value added features such as analytics, reports and CPE ordering. .	Information	

	1.9.2	Self Service Portal is a web-based application designed specifically for users without expertise in the network technologies. The Self-Service Portal enables self-service management by the end-customers.	Information	

	1.9.3	The use of the portal allows the end user to easily expand the services by adding more branch CPEs, or more connections. It also provides visibility in the state of the services through the dashboard. It allows access to service and application level trends and define reporting schedule and Threshold Crossing Alerts(TCAs) per user basis.	Information	
2.0		**DESCRIPTION**	Information	
2.1		**Application layer** The application layer shall support integration to a third-party BSS/OSS, service portal using REST API/XMPP/NETCONF.	Information	
2.2		**Cloud management and control platform** The SDWAN solution shall manage the entire process of providing enterprise interconnection services. The controller centrally manages devices such as the CPEs, uCPEs, and vCPEs. This helps achieve mapping from CPEs to the VPN network topology configuration and orchestration, lightweight management & service chain orchestration of VNFs on the uCPE/vCPE, network service policy management & delivery and implementation of automatic network deployment and configuration, automatic policy delivery, inter-site routing information transmission, and inter-zone network interconnection & interoperability.	Information	
2.3		**Network connection layer** Leveraging cost-effective devices such as CPEs, uCPEs, and vCPEs, as overlay technologies, the solution uses various links such as the Internet, MPLS, LTE and traditional leased lines to provide interconnection between enterprise headquarters, branches, public clouds, and private clouds, enabling on-demand, dynamic and reliable - all-network connections. SDWAN shall be compatible with both IPv4 and IPv6, ensuring seamless connectivity across modern network infrastructures.	Information	
3.0		**FUNCTIONAL REQUIREMENTS:**		
3.1		**Functional Requirements for the Centralised Policy Management and SD-WAN Controllers:**		
	a)	The Centralized policy management and SD-WAN controller must provide a single, unified platform for network service provisioning, policy management, change and compliance management.	REFER ANNEXURE TEST SERIAL NO. 1	
	b)	The SD-WAN controller instances shall support High Availability (HA) redundant configurations.	REFER ANNEXURE TEST SERIAL NO. 2	
	c)	The SDWAN solution shall be centrally managed by web based GUI.	REFER ANNEXURE TEST SERIAL NO. 3	

	d)	The SDWAN centralized policy management and SDWAN controller shall be multi-tenant/enterprise supporting multiple enterprise customers.	REFER ANNEXURE TEST SERIAL NO. 4	
	e)	The solution must support zero-touch provisioning/plug-n-play for new branches, which entails on-site branch personnel having to make physical (i.e., cabling) changes only and centralised administrators not having to make configuration changes to bring new branches (which are connected) online.	REFER ANNEXURE TEST SERIAL NO. 5	
	f)	The solution must provide either manual or guided workflows for deployment and management of SDWAN infrastructure.	Declaration	
	g)	The solution must support real time flow analytics dashboard capabilities for identifying issues and taking corrective actions in application paths**.**	REFER ANNEXURE TEST SERIAL 6	
	h)	All network-wide configurations shall be from the Centralized policy management and SD-WAN controller.	REFER ANNEXURE TEST SERIAL NO. 7	
	i)	All application forwarding policies shall be configured from the Centralized policy management and SD-WAN controller.	REFER ANNEXURE TEST SERIAL NO. 8	
	j)	All control functions, including the policy engine and controller shall be deployed in redundant configurations	REFER ANNEXURE TEST SERIAL NO. 9	
	k)	All communications between the CPEs, vCPE's & uCPE's and SDWAN controller shall be encrypted with industry standard strong encryption.	REFER ANNEXURE TEST SERIAL NO. 10	
	l)	After successful installation, configuration of the CPEs, vCPE's & uCPE's shall be conducted via the SD-WAN management plane/controller.	REFER ANNEXURE TEST SERIAL NO. 11	
	m)	When using multiple underlays with different WAN addressing, the solution must support management over any WAN address. If any or multiple of the WAN links fail, it must be possible to operate / manage the solution over any remaining interface(s).	REFER ANNEXURE TEST SERIAL NO. 12	
	n)	The Solution should provide secure connectivity to Public Cloud Service Providers.	REFER ANNEXURE TEST SERIAL NO. 13	
	o)	The Management Policy Engine and controller shall support High Availability deployment	REFER ANNEXURE TEST SERIAL NO. 14	

	p)	The Management Policy Engine and controller shall support geographic redundancy.	REFER ANNEXURE TEST SERIAL NO. 14	
	q)	The Management Policy Engine and controller shall support capacity expansion.	REFER ANNEXURE TEST SERIAL NO. 15	
	r)	The controller shall support cluster deployment.	REFER ANNEXURE TEST SERIAL NO. 14	
3.1.1		**Interface/Protocol Support**		
	a)	SDN Management/controller shall support open protocols / Interfaces like NETCONF / YANG / XMPP/ OPENFLOW/REST API etc to centrally manage devices such as CPE's, uCPE's and vCPE's.	REFER ANNEXURE TEST SERIAL NO. 16	
	b)	The SDN Management/controller shall support Northbound REST API / NETCONF / YANG / XMPP/ OPENFLOW etc for integration with third party Orchestrator and Enterprise own Self-Service portal.	REFER ANNEXURE TEST SERIAL NO. 17	
	c)	The solution must support carrier grade scalable protocols like BGP/REST API/XMPP to share forwarding information between controllers. Various protocols supported by the SDWAN solution are depicted in figure-4 below: 	REFER ANNEXURE TEST SERIAL NO. 18	
	d)	The solution must support forwarding tunneling mechanism using open standard protocols like Vxlan/VXLAN over IPsec/GRE/IPSec/MPLS over UDP.	REFER ANNEXURE TEST SERIAL NO. 19	

	e)	The overlay paths established amongst the edge devices must support the ability to run routing protocols: static or dynamic (BGP/EGP). (Note: IGP (Interior Gateway Protocol) not be supported on overlay paths between different type of CPEs i.e between different autonomous systems, for which EGP(Exterior Gateway Protocol) is used.	REFER ANNEXURE TEST SERIAL NO. 20	
	f)	**The solution must support IPv6 for all interfaces and protocols, ensuring seamless connectivity in both IPv4 and IPv6 networks.**	Functional test check	
	g)	**The solution must support secure communication mechanisms, such as TLS/SSL, for all protocol interfaces to ensure data integrity and prevent unauthorized access.**	Functional test check	
3.1.2		**Account Management:**		
3.1.2.1		The solution shall allow administrators to create, modify, delete, and query accounts.	REFER ANNEXURE TEST SERIAL NO. 21	
3.1.2.2		The solution shall allow administrators to create accounts for the local tenant and specify the user name, description, role, authorized object, and other information when creating an account.	REFER ANNEXURE TEST SERIAL NO. 22	
3.1.2.3		The solution shall allow administrators to modify other accounts with lower authority levels, including authorization and role information.	REFER ANNEXURE TEST SERIAL NO. 23	
3.1.2.4		The solution shall allow administrators to change their own passwords.	REFER ANNEXURE TEST SERIAL NO. 24	
3.1.2.5		The solution shall support integration with LDAP/AAA..	REFER ANNEXURE TEST SERIAL NO. 25	
3.1.2.6		The Solution shall support local RBAC (Role Based Access Control	REFER ANNEXURE TEST SERIAL NO. 26	
3.1.2.7		The solution shall allow administrators to view the list of online administrators, including the following information: user name, role, login IP address, and login time.	REFER ANNEXURE TEST SERIAL NO. 27	
3.1.2.8		Allows administrators to set the idle timeout interval for web login. If an administrator does not perform any operations within this period of time after login, the administrator account will be automatically logged out.	REFER ANNEXURE TEST SERIAL NO. 28	
3.1.3		**System logs:**		

3.1.3.1		The solution should support integration with the centralised Syslog server for monitoring and audit trail.	REFER ANNEXURE TEST SERIAL NO. 29	
3.1.3.2		The solution shall support records information such as user creation, modification, and deletion and administrator login, account change, and password change.	REFER ANNEXURE TEST SERIAL NO. 30	
3.1.3.3		The solution shall allow administrators to query logs generated within 90 days and export selected logs or all logs. The purchaser may specify the exact log period.	REFER ANNEXURE TEST SERIAL NO. 31	
3.1.3.4		The solution shall support records logs for add, modify, and delete operations instead of the query operation.	REFER ANNEXURE TEST SERIAL NO. 31	
3.1.3.5		The solution shall allow administrators to query operation logs by account, operation object, time, log level, client IP address, operation result, and details. Operation logs shall be exported.	REFER ANNEXURE TEST SERIAL NO. 32	
3.1.3.6		The solution shall allow administrators to query security logs by tenant, account, operation object, time, log level, client IP address, operation result, and details. Security logs shall be exported.	REFER ANNEXURE TEST SERIAL NO. 32	
3.1.3.7		The solution shall support records or events such as patch loading, upgrade, node status changes in the Controller.	REFER ANNEXURE TEST SERIAL NO. 33	
3.1.4		**Openness:**		
3.1.4.1		The solution shall allow the CPEs to report performance data to the Controller through HTTP2.0/REST API/HTTPS for displaying the data in self-service portal.	REFER ANNEXURE TEST SERIAL NO. 34	
3.1.4.2		The solution shall support importing CA certificates of external systems for interconnection verification with the external systems.	REFER ANNEXURE TEST SERIAL NO. 35	
3.1.4.3		The solution shall support unified identity authentication for each integrated system, and provides the integrated login page and RESTful interface for Single Sign On (SSO) login.	REFER ANNEXURE TEST SERIAL NO. 36	
3.1.4.4		The solution should support administrators to define basic operations based on a YANG or XMPP or OPENFLOW or REST API or Netconf interfaces module, including configuration operations, status data, and remote procedure call (RPC), and notification mechanism.	REFER ANNEXURE TEST SERIAL NO. 37	

3.1.4.5		The Solution should support administrators to configure and query network services, collect alarms, and issue commands to devices through open protocols/interfaces NETCONF/ OPENFLOW/ XMPP/ SNMP/REST API etc. The CPEs report alarms through standard and open interfaces such as NETCONF, ReST API, SNMP.	REFER ANNEXURE TEST SERIAL NO. 37	
3.1.4.6		The Solution shall support enabling SSH (Secure Shell) key management by administrators to ensure channel security.	REFER ANNEXURE TEST SERIAL NO. 38	
3.1.4.7		The Solution support using TLS 1.2 or higher for encryption to ensure data transmission security.	REFER ANNEXURE TEST SERIAL NO. 39	
3.1.4.8		The Solution shall support integration with RADIUS, LDAP/AD or Local Authentication based RBAC (Role Based Access Control)	REFER ANNEXURE TEST SERIAL NO. 25	
3.1.5		**SDWAN Gateway:**		
3.1.5.1		The SDWAN gateway shall support gateway function between the legacy, non-SD-WAN brownfield network and the new/Green field SD-WAN network.	REFER ANNEXURE TEST SERIAL NO. 40	
3.1.5.2		The SDWAN Gateway shall be Multi-Tenant/enterprise supporting multiple enterprise customers.	REFER ANNEXURE TEST SERIAL NO. 41	
3.1.5.3		The SDWAN gateway shall support traffic flow between different WANs (Internet to MPLS etc).	REFER ANNEXURE TEST SERIAL NO. 42	
3.2		**Management Platform- Network and Service Assurance**		
	a)	The assurance platform shall have dashboard capability for on-demand realtime overlay service topology analysis**.**	REFER ANNEXURE TEST SERIAL NO. 43	
	b)	The assurance platform shall provide Overlay Root Cause Analysis i.e. tools to debug Configuration/connectivity problems between SDN Controller and SD-WAN Edge As well as within the overlay network i.e. between traditional CPEs & non traditional CPEs(SDWAN CPEs, uCPEs, vCPEs).	REFER TO TEST SERIAL NO. 44	
	c)	The assurance platform shall support automatic Inventory Discovery for SD edge devices.	REFER ANNEXURE TEST SERIAL NO. 45	

	d)	The assurance platform shall support advanced Service Inventory Visualization	REFER ANNEXURE TEST SERIAL NO. 45	
	e)	The solution shall provide tools to do Configuration Audit i.e. Validate SD-WAN Edge configuration against configuration in SD-WAN Controller	REFER ANNEXURE TEST SERIAL NO. 46	
	f)	The solution shall provide tools to monitor the Health of overlay components i.e. dashboard showing Top Unhealthy Overlays, Top Problems/ Alarms etc.	REFER ANNEXURE TEST SERIAL NO. 47	
	g)	The assurance platform shall provide Historical impact analysis. i.e the new SDWAN solution should be backward compatible with erstwhile enterprise network solution thereby ensuring inter operability & integration with existing SDWAN(s) solution to provide a unified SDWAN solution.	REFER ANNEXURE TEST SERIAL NO. 48	
	h)	The solution shall support communication between traditional CPEs & non traditional CPEs(SDWAN CPE/uCPE/vCPE) based on i) single configuration, provisioning and validation mechanism ii) a single assurance management entity.	Functional Test	

3.3		**SDWAN Self-Service Portal**		
	a)	The Self-Service portal shall be web based application and shall provide customization flexibility or a customizable dashboard with feature-specific widgets.	REFER ANNEXURE TEST SERIAL NO. 49	
	b)	The Self-Service portal shall support multi-tenancy & RBAC (Role based Access Control) capabilities that shall be used by the service provider, Enterprises, Wholesalers, End customers for self-service management of VPNs	REFER ANNEXURE TEST SERIAL NO. 50	
	c)	Self-Service Portal shall support monitor and configure a SD-WAN setup	REFER ANNEXURE TEST SERIAL NO. 51	
	d)	The Self-Service portal shall provide each Enterprise to generate a very comprehensive branch site to branch site and global network traffic/throughput report.	REFER ANNEXURE TEST SERIAL NO. 52	
	e)	The Self-Service portal shall provide reports such as Security Audit Report, User Activity Reports, per VPN traffic report, Application Aware Routing reports on a per VPN basis, trigger real-time and on demand traffic reports.	REFER ANNEXURE TEST SERIAL NO. 52	
	f)	The Self-Service portal shall provide real-time monitoring capabilities to include KPIs, TCAs and SLA reports.	REFER ANNEXURE TEST SERIAL NO. 52	

	g)	The Self-Service portal shall support following functional modules which shall expose to enterprises and end users 1 Service Fulfilment Network Service: a Create/Update/Delete L2 and L3 Domains b Value Add functions c Network Service Dashboard 2 Branch Enablement a Create/Update/Delete a Branch/Site b SD-WAN Edge Template Control c VPN Management: VPN lifecycle Create/Read/Update/Delete (CRUD), ACL Policies Control, Flexible Subnet Addressing, Assigned predefined policies to enterprise, PAT/IPsec, QoS, DHCP etc. d Activation and management which includes: Branch life cycle, zero or single factor or two factor authentications, specify branch CPE installer, Notify Installer for branch activation using notification app. 3 Visualization ○ Dashboard: a) Service Provider Dashboard View b) Enterprise Dashboard View c) Customizable on a per user basis d) Drilldown to detail view ○ Reports a) Traffic Throughput b) Application Discovery c) Application SLA Violations d) Network Performance e) Security Audit ○ Administration ○ Enterprise Management: a. Create/Update/Delete Enterprise/Organization b. Hierarchical enterprise support c. Customer profile template ○ User/ Access Control a) Users Management & fine grain access control for Service Provider as well as for end customers b) Use action logging	REFER ANNEXURE TEST SERIAL NO. 53	

	h)	**The customer portal shall support following:** • Service Provider Dashboard View • Customer Dashboard View • Branches Widget on a geographical map/Dashboard • Network Summary • SDWAN edge device view (on geographical map/dashboard) • Users Activity • Traffic Summary • Events & Statistics • User Activity • CPE health	REFER ANNEXURE TEST SERIAL NO. 54	
3.4		**Functional Requirements for the Network**		
3.4.1		**Service network**		
3.4.1.1		The SDWAN solution to support all Branches only on MPLS.	REFER ANNEXURE TEST SERIAL NO. 55	
3.4.1.2		SDWAN solution to support all Branches only on Internet.	REFER ANNEXURE TEST SERIAL NO. 56	
3.4.1.3		SDWAN solution to support Branches on both MPLS & Internet (on same CPE).	REFER ANNEXURE TEST SERIAL NO. 57	
3.4.1.4		SDWAN solution to support a few Branches on MPLS & other Branches on Internet.	REFER ANNEXURE TEST SERIAL NO. 58	
3.4.1.5		SDWAN solution to support a few Branches on MPLS & Internet (Ethernet/DSL/LTE) on same CPE & other Branches only on Internet.	REFER ANNEXURE TEST SERIAL NO. 59	
3.4.1.6		SDWAN solution to support a few Branches on MPLS only & other branches on MPLS+ Internet (Ethernet/DSL/LTE) on same CPE.	REFER ANNEXURE TEST SERIAL NO. 60	
3.4.1.7		The CPE device both in DC and Branches should support HA through Clustering of multiple CPE devices in DC, Active-Active and Active-Standby deployments	REFER ANNEXURE TEST SERIAL NO. 61	

3.4.1.8		Enterprise site to site connectivity： i. Support full mesh networking for direct communication. ii. Support hub-spoke networking for centralized communication iii. Support partial mesh networking, some spokes shall directly communicate with each other, and some communicate with each other through the hub.	REFER ANNEXURE TEST SERIAL NO. 62	
3.4.1.9		Enterprise site connectivity i. Support local mode：A branch site shall access the Internet / MPLS using local breakout. ii. Support centralized mode：A hub site, an aggregation site, or a branch site shall function as the centralized Internet access site. iii. Support Internet access in local mode (default) and centralized mode (backup), By default, a branch site accesses the Internet in local mode. When the Internet link for local access fails, the traffic is transmitted to the Internet by a centralized Internet access site.	REFER ANNEXURE TEST SERIAL NO. 63	
3.4.1.10		Support SD-WAN Site to MPLS legacy Site i. Local mode: An SD-WAN site shall directly access a traditional MPLS VPN in local Breakout mode. The CPE at the site functions as a CE and connects to the remote MPLS PE using a routing protocol such as BGP, OSPF, or a static routing protocol. ii. Centralized mode: An SD-WAN site shall communicate with a traditional site through a centralized site. Hub sites, aggregation sites, and branch sites shall be used as centralized access points.	REFER ANNEXURE TEST SERIAL NO. 64	
3.4.1.11		Support multi–virtual network: each virtual network supports differentiated configuration of traffic policies, including Site to Site (S2S), site-to-legacy network, QoS, ACL, and path selection.	REFER ANNEXURE TEST SERIAL NO. 65	
3.4.1.12		Routing:: ✓ Overlay(Peering between the SDWAN edge and LAN device)：BGP/OSPF/ static routing shall be supported. ✓ Underlay(Peering between the SDWAN edge and PE): The routes shall be BGP routes/ OSPF routes/ static routes. ✓ Routing policy: The blacklist or whitelist shall be configured to filter overlay BGP routes. The blacklist or whitelist shall be configured to filter underlay BGP/ OSPF routes. ✓ Adjustment of the priority of a routing protocol: The priority of an underlay BGP route, OSPF route, or static route shall be specified.	REFER ANNEXURE TEST SERIAL NO. 66, 67, 68 & 69	
3.5		**Functional Requirement for CPE**		

3.5.1		**WAN-side networking**		
3.5.1.1		Single-site single-CPE (hub site or aggregation site) : The CPE supports two or more physical links.	REFER ANNEXURE TEST SERIAL NO. 70	
3.5.1.2		Single-site dual-CPE (hub site or aggregation site) : Each CPE supports two or more physical links. In the single-site dual-CPE scenario, a maximum of six physical links are supported.	REFER ANNEXURE TEST SERIAL NO. 71	
3.5.1.3		Dual-hub : In the dual-hub scenario, one or two CPEs shall be deployed at each hub site. Two hub sites work in active/standby mode.	REFER ANNEXURE TEST SERIAL NO. 72	
3.5.1.4		Hierarchical VPN : branch-aggregation-hub mode is supported.	REFER ANNEXURE TEST SERIAL NO. 73	
3.5.1.5		The SDWAN solution shall support hybrid links : Multiple access link combinations are supported: MPLS + MPLS, MPLS + Internet, and Internet + Internet, MPLS+LTE, etc.	REFER ANNEXURE TEST SERIAL NO. 74	
3.5.1.6		The hub/CPE devices should be able to aggregate the bandwidth across multiple links e.g. in the event of a bulk transfer multiple links can be leveraged to provide more bandwidth and faster downloads.	REFER ANNEXURE TEST SERIAL NO. 75	
3.5.1.7		The WAN path selection at the branch site should failover/switch over/ shift over to the back up path in near real time to real-time so as to maintain high availability of SDWAN solution. Path selection should support be guided by an SLA matrix, considering factors such as latency, jitter, and packet loss, and should support dynamically evaluation of link health.	Functional test check	
3.5.2		**Basic Routing**		
	a)	The SD-WAN CPEs, vCPE's & uCPE's shall support: • 802.1Q on LAN and WAN interfaces • BGP/OSPF on both LAN (for learning customer addresses) and WAN (for learning underlay addresses) interfaces □ Local IP breakout to underlay network, be it Internet or IPVPN	REFER ANNEXURE TEST SERIAL NO. 77	
	b)	SDWAN Edges (CPEs, vCPE's & uCPE's) shall support configurable IPv4 NAPT for traffic breaking out to the underlay on WAN interfaces	REFER ANNEXURE TEST SERIAL NO. 78	

	c)	Edges shall support configurable Ipv4 1:1 NAT on WAN interfaces for traffic breaking in / out to the underlay on WAN interfaces	REFER ANNEXURE TEST SERIAL NO. 79	
	d)	Edges shall support configurable Ipv4 inbound port forwarding for traffic breaking in to the underlay on WAN interfaces	REFER ANNEXURE TEST SERIAL NO. 80	
	e)	DSCP marking of traffic based upon at least 5 tuple policy	REFER ANNEXURE TEST SERIAL NO. 81	
	f)	The edge devices shall support classification of traffic into 8 forwarding classes.	REFER ANNEXURE TEST SERIAL NO. 82	
	g)	The edge devices shall support at least 4 queues.	REFER ANNEXURE TEST SERIAL NO. 82	
	h)	The edge devices shall support shaping of WAN/LAN egress traffic.	REFER ANNEXURE TEST SERIAL NO. 83	
	i)	The edge devices shall support policing and packet filtering of ingress/egress traffic.	REFER ANNEXURE TEST SERIAL NO. 84	
	j)	The SD-WAN CPEs, vCPEs, and uCPEs shall support IPSEC and/or GRE tunneling for secure communication between SD-WAN edges or over untrusted networks."	Functional test check	
3.5.3		**WAN**		
	a)	Dual CPE redundancy shall be supported using VRRP or BFD on LAN side of the network.	REFER ANNEXURE TEST SERIAL NO. 85	
	b)	The solution shall support using LTE links as the active and standby links for applications, if applicable.	REFER ANNEXURE TEST SERIAL NO. 86	
	c)	CPE Uplink shall support Broadband as uplink with IpoE and PPPoE.	REFER ANNEXURE TEST SERIAL NO. 87	

	d)	The CPE shall support Ipv6 uplink with static or dynamic address allocation	REFER ANNEXURE TEST SERIAL NO. 88	
	e)	The solution shall support IPSEC and/or GRE tunnels for secure communication between SD-WAN devices across the WAN, especially for branch-to-branch or branch-to-hub connections	Functional test	
3.5.4	a)	**Interface Types**: WAN interface type shall be supported by the CPE: • Ethernet interfaces (XGE/GE/FE) • Ethernet sub-interfaces shall be used as WAN links. • 3G/ 5G LTE interfaces (Optional for the purchaser) • xDSL interfaces (ADSL, VDSL, or G.SHDSL) (Optional for the purchaser)	REFER ANNEXURE TEST SERIAL NO. 89	
3.5.5		**LAN**		
	3.5.5.1	**Wired network** :		
	a)	Support wired network with Layer 3 devices connected, Layer 3 devices shall connect to the network using BGP routes, OSPF routes, or static routes.	REFER ANNEXURE TEST SERIAL NO. 66	
	b)	Support wired network with Layer 2 devices connected, Layer 2 devices shall connect to the network through VLAN, VRRP or any other redundancy mechanism like Redundant Group configuration with failure detected by BFD.	REFER ANNEXURE TEST SERIAL NO. 90	
	c)	Supports DHCP Server or DHCP relay.	REFER ANNEXURE TEST SERIAL NO. 91	
	d)	Ethernet interfaces (GE/FE) support.	REFER ANNEXURE TEST SERIAL NO. 92	
	3.5.5.2	Support VLAN Tagging – 802.1 Q, 802.1 ad,	REFER ANNEXURE TEST SERIAL NO. 92	
3.5.5.3		**Wi-Fi network (optional to the purchaser)**		
	a)	The Integrated AP function shall be enable on CPEs to allow terminal users to access networks through Wi-Fi.	REFER ANNEXURE TEST SERIAL NO. 93	

	b)	CPE shall support at-least 4 SSID and around 10-30 users	REFER ANNEXURE TEST SERIAL NO. 94	
	c)	The DHCP or DHCP relay function shall be enable to assign IP addresses to Wi-Fi users.	REFER ANNEXURE TEST SERIAL NO. 94	
	d)	Standard wireless securityWPA2 authentication modes should be supported.	REFER ANNEXURE TEST SERIAL NO. 94	
	e)	The CPE shall support enterprise specific Dual Band, Omni-Directional, External / internal Antenna options	REFER ANNEXURE TEST SERIAL NO. 95	
	f)	Advanced Wi-Fi configuration shall be supported: (optional to the purchaser) • Wi-Fi AP configuration and Operations (Alarms & Stats) management using same management plane • Support click through captive portal for use case like display a webpage with use policy and Accept. • Public and Private SSID with Internal captive portal and Pre-Shared Key respectively	REFER ANNEXURE TEST SERIAL NO. 96	
3.5.6		**VNF Support (applicable for Universal CPE/vCPE)**		
	a)	The solution shall support onboarding third party VNF on to the host CPE	REFER ANNEXURE TEST SERIAL NO. 97	
	b)	VNF on boarding should be fully integrated automated management and provisioning	REFER ANNEXURE TEST SERIAL NO. 97	
	c)	The solution shall support service chaining using L2-L4 based policies through these VNF	REFER ANNEXURE TEST SERIAL NO. 98	

3.6		**CPE Categories**		
3.6.1		CPE Type 1 Specifications:		
	a)	At least 4x100/1000 Ethernet interface (RJ45)	REFER ANNEXURE TEST SERIAL NO. 99	

	b)	Full Duplex 10Mbps throughput expandable to 100Mbps with IPSec	REFER ANNEXURE TEST SERIAL NO. 99	
	c)	1x AC / DC PSU: 220V AC ±20% or –48 V DC Nominal (negative 48 V DC) with a voltage variation –40 V to –57 V DC.,	REFER ANNEXURE TEST SERIAL NO. 99	
	d)	LTE Uplink: 1 LTE support – On board SIM (with inbuilt omni directional antenna) or USB for LTE dongle (Optional to the purchaser)	REFER ANNEXURE TEST SERIAL NO. 99	
3.6.2		**CPE Type 2 Specifications:**		
	a)	4x100/1000 Ethernet interface (RJ45) + 2x1G SFP port.	REFER ANNEXURE TEST SERIAL NO. 100	
	b)	Full Duplex 50Mbps throughput expandable to 500Mbps with Ipsec	REFER ANNEXURE TEST SERIAL NO. 100	
	c)	LTE Uplink: 1 LTE support – On board SIM (with inbuilt omni directional antenna) or USB for LTE dongle(optional to purchaser)	REFER ANNEXURE TEST SERIAL NO. 100	
	d)	1x AC PSU	REFER ANNEXURE TEST SERIAL NO. 100	

3.6.3		**CPE Type 3 Specifications:**		
	a)	4x100/1000 Ethernet interface (RJ45) + 2x1G SFP port	REFER ANNEXURE TEST SERIAL NO. 101	
	b)	Full Duplex 100Mbps throughput expandable to 1000Mbps with Ipsec	REFER ANNEXURE TEST SERIAL NO. 101	
	c)	LTE Uplink: 1 LTE support – On board SIM (with inbuilt omni directional antenna) or USB for LTE dongle (optional to purchaser)	REFER ANNEXURE TEST SERIAL NO. 101	
	d)	2x AC PSU	REFER ANNEXURE TEST SERIAL NO. 101	
3.6.4		**CPE Type 4 Specifications:**		
	a)	2x SFP+ 10GbE, 4 x1G SFP/Electrical ports	REFER ANNEXURE TEST SERIAL NO. 102	
	b)	Full Duplex 500Mbps throughput expandable to 5000Mbps with IPsec	REFER ANNEXURE TEST SERIAL NO. 102	
	c)	2x AC PSU	REFER ANNEXURE TEST SERIAL NO. 102	
3.7		**Functional Requirements for Deployment**		
3.7.1		The solution shall support Zero touch Provisioning, the method could be one of the following: ✓ Email based ✓ USB based ✓ DHCP based ✓ Mobile App based	REFER ANNEXURE TEST SERIAL NO. 103	
3.7.2		Deployment terminal type : PCs and mobile terminals (such as mobile phones and tablets) shall connect to CPEs through wired or wireless connections to deploy the CPEs.	REFER ANNEXURE TEST SERIAL NO. 103	
3.7.3		If multiple links are available, a CPE shall selects the link that first goes Up to connect to the Controller. (Management path selection is not supported.)	REFER ANNEXURE TEST SERIAL NO. 103	

3.7.4		The Controller and site devices shall synchronize time from an external NTP server. Spoke nodes shall synchronize time from an NTP server or the hub site/management plane.	REFER ANNEXURE TEST SERIAL NO. 103	
3.7.5		Self-installation and Activation (auto configuration) SD-WAN Edges shall support low / zero touch customer selfinstall where:	Information	
	a)	WAN link is provided with an IP address, netmask, default gateway and DNS server via DHCP, PPPoE, 3G/LTE or Static configuration	REFER ANNEXURE TEST SERIAL NO. 104	
	b)	The solution shall not require any off-site customer specific prestaging / pre-configuration	REFER ANNEXURE TEST SERIAL NO. 105	
	c)	The auto configuration system shall require secure mutual authentication of the SD-WAN controller and specific SD-WAN Edge.	REFER ANNEXURE TEST SERIAL NO. 105	
	d)	Individual SD-WAN Edges shall be identified by a unique key / certificate which is installed on to the Edge by the trusted installer at installation time by some simple but secure method requiring no or minimal manual data input.	REFER ANNEXURE TEST SERIAL NO. 106	
	e)	The SD-WAN Edges shall have a number of trusted third party certificate authority certificates (root Cas) pre-installed for use when authenticating the SD-WAN controller.	REFER ANNEXURE TEST SERIAL NO. 106	
	f)	There shall be a secure, industry recognised mechanism for checking and revoking root CA certificates.	REFER ANNEXURE TEST SERIAL NO. 107	
	g)	The URL of the SD-WAN controller shall not be pre-installed in the Edge and shall be provided at installation time by the trusted installer. The URL of the SD-WAN controller can be preinstalled in the Edge if mutual recognition is possible as per clause (c) above.	REFER ANNEXURE TEST SERIAL NO. 108	
	h)	The SD-WAN Edge shall support seamless bootstrap using USB stick with activation details if applicable.	REFER ANNEXURE TEST SERIAL NO. 105	
	i)	The solution shall allow for one (1) and two (2) factor of activation of SD-WAN Edge and Gateway devices	Functional Verification	

	j)	The solution shall operate when the Edge devices are behind NAT (NAT-T).	REFER ANNEXURE TEST SERIAL NO. 109	
	k)	The solution shall support hybrid branches which have a WAN connection to an MPLS IP VPN and a second WAN connection to the internet,	REFER ANNEXURE TEST SERIAL NO. 110	
	l)	When deployed with a mix of hybrid Edges, IP VPN connect Edges and Internet connected Edges, Edges will continue to be able to communicate under asymmetric break conditions as long as all sites have at least one active connection.	REFER ANNEXURE TEST SERIAL NO. 111	
	m)	The solution shall support secure firmware updates during the installation process, ensuring devices are running the latest security patches.	Functional test check/ Undertaking	
3.7.6		**Transport Independent Overlay Services**		
	a)	Each SD-WAN edge device shall dynamically establish fully meshed encrypted overlay paths to every other edge device, across multiple different WAN services: L3VPN MPLS, Internet and Cellular Data connectivity (3G/4G/5G).	REFER ANNEXURE TEST SERIAL NO. 112	
	b)	The solution shall support site-site remote routing via the primary WAN-aggregation site hub-and-spoke model).	REFER ANNEXURE TEST SERIAL NO. 62	
	c)	The solution shall support dynamic optimal direct site-to-site remote routing (spoke-to-spoke model).	REFER ANNEXURE TEST SERIAL NO 62.	
	d)	The overlay paths established amongst the edge devices shall support: * Transport of unicast, multicast, and broadcast traffic	REFER ANNEXURE TEST SERIAL NO. 113	
	e)	The ability to run routing protocols towards LAN: OSPF/BGP	REFER ANNEXURE TEST SERIAL NO. 62	
	f)	The local users in each of the branch offices must be able to access Internet directly without going through the HO.	REFER ANNEXURE TEST SERIAL NO. 114	
	g)	The solution must use Ethernet as standard media type for WAN transport.	REFER ANNEXURE TEST SERIAL NO. 89	

	h)	The overlay services shall support both encrypted and nonencrypted modes of operation for all overlay types	REFER ANNEXURE TEST SERIAL NO. 112	
	i)	The overlay services layer3 VPN/L2 VPN and Ethernet Services – P2P layer2 VPNs, P2MP layer2VPNs, MP2MP layer2VPNs. (optional to the purchaser)	REFER ANNEXURE TEST SERIAL NO. 113	
	j)	The solution shall support Multiple independent overlay services per Edge, with independent routing tables (allowing overlapping addressing) separated on the LAN side via different ports or different port + VLAN combinations e.g.	REFER ANNEXURE TEST SERIAL NO. 113	
	k)	The solution may support controller less operation for atleast 24 hours in case the connectivity to SDN controller is lost. This capability is required to maintain high availability(HA) of SDWAN solution	Functional Test	
	l)	Overlay services must be configurable and continue to operate if the IP addresses assigned to one or more WAN interfaces are dynamic.	REFER ANNEXURE TEST SERIAL NO 112	
	m)	The solution shall support multiple Tenant networks isolated from one another	REFER ANNEXURE TEST SERIAL NO. 116	
	n)	The solution shall support a set of distinct networks for a single Tenant.	REFER ANNEXURE TEST SERIAL NO. 113	
	o)	The solution shall support integration with MPLS PE Router.	REFER ANNEXURE TEST SERIAL NO. 112	
	p)	The solution shall allow to dynamically add and remove services as required	REFER ANNEXURE TEST SERIAL NO. 113	
	q)	Edge devices must be able to load-balance traffic across multiple WAN paths based on load balancing algorithms efficiently using all available WAN bandwidth.	REFER ANNEXURE TEST SERIAL NO. 117	
	r)	The solution must be able to monitor the network performance—jitter, packet loss, and delay—and make decisions to forward critical applications over the best-performing path based on the defined application policy.	REFER ANNEXURE TEST SERIAL NO. 52	

	s)	The solution must respond to measured performance changes (degradation) in addition to link and node state changes (up/down) and adjust application forwarding accordingly.	REFER ANNEXURE TEST SERIAL NO. 52	
	t)	The solution must be able to prioritize real time traffic over other traffic.	REFER ANNEXURE TEST SERIAL NO. 118	
3.8		**Application Identification and Application Aware Routing (AAR)(Optional to the purchaser)**		
3.8.1		DPI functionalities – The solution must have application awareness with capability of deep packet inspection of traffic in order to identify and monitor applications' performance to determine what traffic is running across the network in order to tune the network routing for business critical services and to help ensure that critical applications are properly prioritized across the network.	REFER ANNEXURE TEST SERIAL NO. 119	
3.8.2		The solution shall support to Identify and classify network traffic coming into the access ports of a NSG on a per application basis using • Signature-based L7 classification e.g ○ ERP ○ O365 full suite ○ VoIP ○ H.323 & SIP ○ Web based applications ○ Web traffic • Custom classification based on source/destination IP address, source/ destination L4 ports, L4 Protocol (TCP/UDP) • The Solution may also support nested application identification to detect applications hidden within other protocols or encrypted traffic, such as HTTPS or VPN tunnels.	REFER ANNEXURE TEST SERIAL NO. 119	
3.8.3		The solution shall support Application-Aware Routing (AAR) enables policy-driven application performance management in a multi-path network	REFER ANNEXURE TEST SERIAL NO. 120	
3.8.4		App signatures of DPI engine must update regularly	REFER ANNEXURE TEST SERIAL NO. 120	
3.8.5		CPEs support application identification and various applicationbased policies, including intelligent path selection and QoS.	REFER ANNEXURE TEST SERIAL NO. 120	

3.8.6		Application identification using the first packet is supported. The first packet shall be defined based on the triplet information (destination port number, destination IP address, and protocol type).	REFER ANNEXURE TEST SERIAL NO. 120	
3.8.7		When quality of the active and standby links meets requirements, the active and standby links are selected based on policies. (If the quality of the active link meets requirements, it will not be compared with that of the standby link.)	REFER ANNEXURE TEST SERIAL NO. 120	
3.8.8		When the preceding condition is not met, the link has the higher quality is selected. (If the quality of the active link does not meet requirements, it will be compared with that of the standby link. If the standby link has higher quality, traffic will be switched to the standby link; otherwise, traffic will be retained on the current link.)	REFER ANNEXURE TEST SERIAL NO. 120	
3.8.9		Load balancing shall be implemented based on the link bandwidth, namely, the link load. Active and standby links and Active-Active links shall be configured based on the application. When a link becomes busy, the traffic of an application that has been generated is still forwarded by the link, and another link is selected to forward new traffic of the application.	REFER ANNEXURE TEST SERIAL NO. 120	
3.8.10		**SLA Aware Routing**		
a)		The solution shall provide information / metrics on the current and historic overall traffic utilization (total egress, ingress bandwidth), WAN side and LAN side on a per site basis with a resolution of 5 minutes or less.	REFER ANNEXURE TEST SERIAL NO. 120	
b)		It shall be possible for customers to define policies to permit or deny applications on a domain wide and per site basis.	REFER ANNEXURE TEST SERIAL NO. 120	
c)		It shall be possible to define application performance requirements including: maximum acceptable latency and maximum acceptable packet loss.	REFER ANNEXURE TEST SERIAL NO. 120	
d)		Solution to alert if the application is receiving an acceptable service from the underlay.	REFER ANNEXURE TEST SERIAL NO. 120	
e)		The solution must be able to dynamically control data packet forwarding decisions by looking at application type, performance, policies, and path status.	REFER ANNEXURE TEST SERIAL NO. 120	

		The solution shall support application flows to be switched to another path, if the performance (RTT/One-way Latency, Jitter, and Packet Loss) of an uplink degrades beyond the thresholds specified in the Application's policy.	Functional test check	
3.9		**Security**		
3.9.1		The Controller authenticates CPEs using certificates	REFER ANNEXURE TEST SERIAL NO. 106	
3.9.2		The Controller shall upgrade CPEs' certificates.	REFER ANNEXURE TEST SERIAL NO. 106	
3.9.3		SSH for Security of the channel for the Controller to configure and manage CPEs should be supported.	REFER ANNEXURE TEST SERIAL NO. 38	
3.9.4		SSL for HTTP//HTTPS of Security of the channel for CPEs to report data to the Controller should be supported.	REFER ANNEXURE TEST SERIAL NO. 34	
3.9.5		URL blacklist and URL whitelist are supported	REFER ANNEXURE TEST SERIAL NO. 121	
3.9.6		By default, if the firewall function is enabled, traffic shall be forwarded from a trust zone to an untrusted zone but not from an untrusted zone to a trust zone.	Functional Verification	
3.9.7		The solution shall support Embedded Software Defined Security	REFER ANNEXURE TEST SERIAL NO. 122	
3.9.8		All remote-site traffic must be encrypted when transported over WAN transport links: MPLS, Internet and LTE network protecting Data Confidentiality and Integrity.	REFER ANNEXURE TEST SERIAL NO. 122	
3.9.9		The solution shall support scalable IPSec for full mesh networking.	REFER ANNEXURE TEST SERIAL NO. 122	
3.9.10		Encryption shall be supported for all overlay services, both L2 or L3.	REFER ANNEXURE TEST SERIAL NO. 122	

3.9.11		It should be possible to set a key-rotation timer defining a maximum duration any particular key or set of keys shall be used for data plane encryption (not applicable in case of external PKI).	REFER ANNEXURE TEST SERIAL NO. 124	
3.9.12		The solution shall support flexible combination of hub-spoke and full-mesh topologies	REFER ANNEXURE TEST SERIAL NO. 62	
3.9.13		The solution shall support Interop with IKEv2 platforms	REFER ANNEXURE TEST SERIAL NO. 123	
3.9.14		The encryption shall be done as per Ipsec standards using AES with 128-bit keys or higher coupled with Internet Key Exchange Version 2 (IKEv2).	REFER ANNEXURE TEST SERIAL NO. 125	
3.9.15		The use of encryption should not limit the performance or availability of a remote-site applications and should be transparent to end users.	REFER ANNEXURE TEST SERIAL NO. 125	
3.9.16		The solution must support L7 application firewall and VRFs to allow for network isolation.	REFER ANNEXURE TEST SERIAL NO. 126	
3.9.17		The solution shall support Stateful ACL/Firewall.	REFER ANNEXURE TEST SERIAL NO. 127	
3.9.18		The solution shall support Security analytics for SD-WAN through Traffic Visibility, Analytics and Dynamic Security Automation. The solution shall support at least below security features: • Real-time alerts of traffic analytics • Automatic policy reconfiguration Alert creation and logging of malicious traffic or activate mirroring of the end point and redirect traffic to a perimeter Security Device.	REFER ANNEXURE TEST SERIAL NO. 128	
3.9.19		The solution shall support multiple user accounts per customer with individual user logins	REFER ANNEXURE TEST SERIAL NO. 53	
3.9.20		The solution shall support multiple levels of user permission, specifically a read only.	REFER ANNEXURE TEST SERIAL NO. 53	

3.9.21		Digital certificates, or an alternative form of strong authentication, must be supported for northbound interfaces. The signed certificate must come from a trusted source.	REFER ANNEXURE TEST SERIAL NO. 31	
3.9.22		The solution shall support configuration history and change control.	REFER ANNEXURE TEST SERIAL NO. 11	
3.9.23		The solution shall support rollback of configuration changes.	REFER ANNEXURE TEST SERIAL NO. 11	
3.9.24		Mirroring select traffic from suspicious end points	Functional Verification	
3.9.25		Reports & raise alerts based on ACL allow/deny hits vs. Time	REFER ANNEXURE TEST SERIAL NO. 129	
3.9.26		Reports & raise alerts based on ACL allow/deny hits by source	REFER ANNEXURE TEST SERIAL NO. 129	
3.9.27		Reports & raise alerts based on ACL allow/deny hits by destination	REFER ANNEXURE TEST SERIAL NO. 129	
3.9.28		Reports & raise alerts based TCP conn vs. Time	REFER ANNEXURE TEST SERIAL NO. 129	
3.9.29		The solution shall support integration with Cloud Security Platform like Zscaler to provide cloud-based security stack to secure internet breakout traffic	REFER ANNEXURE TEST SERIAL NO. 130	
3.9.30		The solution shall support software defined policies to selectively send traffic Cloud Security platform	REFER ANNEXURE TEST SERIAL NO. 130	
3.9.31		The Solution shall provide reports such as security audit report, user activities report, per VPN Traffic Report, application aware routing report on a per VPN basis as well as should trigger real time & on demand traffic reports.	Functional test check	
3.10		**Qos Policy**		
3.10.1		QoS shall be configured for traffic between multiple virtual networks. (The percentage of the overlay tunnel bandwidth shall be specified for each site based on the virtual network.)	REFER ANNEXURE TEST SERIAL NO. 118	

3.10.2		QoS for local breakout and overlay traffic (percentage-based configuration)	REFER ANNEXURE TEST SERIAL NO. 118	
3.10.3		QoS policies shall be configured based on the application or traffic classifier.	REFER ANNEXURE TEST SERIAL NO. 118	
3.10.4		The service priority (highest, high, medium, or low) shall be defined, and the guaranteed bandwidth shall be set to a specific value.	REFER ANNEXURE TEST SERIAL NO. 82	
3.10.5		The service priority (highest, high, medium, or low) shall be defined, and the guaranteed bandwidth shall be set to a percentage value.	REFER ANNEXURE TEST SERIAL NO. 82	
3.10.6		Traffic shaping shall be set to a specific value.	REFER ANNEXURE TEST SERIAL NO. 84	
3.10.7		Traffic policing (CAR) shall be set to a specific value.	REFER ANNEXURE TEST SERIAL NO. 84	
3.10.8		DSCP based re-marking shall be supported.	REFER ANNEXURE TEST SERIAL NO. 84	
3.10.9		The solution shall support below Quality of Service feature allows traffic classification, prioritization, and shaping to ensure that performance-sensitive applications are prioritized, fairness is maintained, and packet loss is minimized.	REFER ANNEXURE TEST SERIAL NO. 84	
3.10.10		The solution shall support Ingress classification for traffic is mapped to one of eight forwarding classes based on the Ipv4 DSCP or CoS value in the customer packet.	REFER ANNEXURE TEST SERIAL NO. 82	
3.10.11		The solution shall support DSCP and CoS remarking for the uplink outer tunnel header are modified based on Remarking Policies to allow you to redefine forwarding class assignments per uplink based on a user-defined mapping table.	REFER ANNEXURE TEST SERIAL NO. 131	
3.10.12		The solution shall support Inner packet markings from the LAN side are not modified.	REFER ANNEXURE TEST SERIAL NO. 131	

3.10.13		The solution shall support Egress queuing, traffic is assigned to four egress queues based on its forwarding class with one queue is based on strict priority queuing and three are based.	REFER ANNEXURE TEST SERIAL NO. 132	
3.10.14		**On-demand Remediation** for various traffic types should be available for the event where link performance is degraded as below: i) Real-time applications – For Real time applications such as voice and video FEC (Forward Error Correction) during periods of packet loss should be supported. ii) Jitter buffer on CPE devices shall be supported when WAN links experience jitters. iii) TCP Application – TCP Applications such as File Transfer, Negative Acknowledgment (NACK) must be supported to deliver high TCP throughput during lossy condition	Functional Verification	
3.11		**Monitoring and Visualization**		
3.11.1		Link quality detection：Link jitter, delay, and packet loss ratio shall be measured.	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.2		Link quality visualization：Link quality support be visualized on the Controller, which displays the link quality indicators including the jitter, delay, and packet loss ratio. The information shall be displayed and sorted by intra-site link or inter-site link.	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.3		If a link quality threshold is exceeded, the Controller should be generating and displays an alarm.	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.4		TCP application connections by measuring the WAN delay, server delay, and packet loss ratio of each application shall be display.	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.5		The Controller visually should display and sorts information about the application quality by intra-site application or inter-site application.	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.6		Link quality measurement (LQM) rates the quality of applications shall be display.	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.7		If an application quality threshold is exceeded, the Controller should generate and displays an alarm.	REFER ANNEXURE TEST SERIAL NO. 52	

3.11.8		NetStream/IPFix/Sflow/Jflow/Netflow shall be used to analyze network traffic for integrating with the third party analytics tool.	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.9		The Controller should display traffic statistics by site, link, or application	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.10		Link-based traffic data shall be collected and displayed by intra-site link or inter-site link.	REFER ANNEXURE TEST SERIAL NO. 89	
3.11.11		The link bandwidth usage shall be calculated.	REFER ANNEXURE TEST SERIAL NO. 52	
3.11.12		Application-based traffic data shall be collected and displayed by site, link, or terminal IP address.	REFER ANNEXURE TEST SERIAL NO. 53	
3.11.13		Statistics of all traffic at a site shall be calculated and displayed.	REFER ANNEXURE TEST SERIAL NO. 53	
3.11.14		Statistics of all traffic between sites shall be calculated and displayed, and a list of top N sites sorted by traffic volume is also displayed.	REFER ANNEXURE TEST SERIAL NO. 54	
3.11.15		Statistics of underlay traffic, local breakout traffic, and application traffic shall be calculated.	REFER ANNEXURE TEST SERIAL NO. 53	
3.11.16		A device reports the link or application quality data every 1 minute and traffic information every 5 minutes. You need to manually refresh the page of the Controller.	REFER ANNEXURE TEST SERIAL NO. 53	
3.11.17		Application usage related data over time should be available and it should provide an option to filter it down to things like Source Devices, Applications, Destination IP etc.	REFER ANNEXURE TEST SERIAL NO. 53	
3.11.18		Link performance and quality data should be available for at least 1 year. There should be an option to go back in time and check for things like average throughput of the link, latency, jitter, packet loss etc.	Functional Verification	
3.11.19		It should have the capability to capture real time traffic like TCP, UDP, ICMP and display the statistics in the orchestrator itself.	Functional Verification	
3.12		**Reliability**		

3.12.1		Multiple links of a single CPE are required to provide back up to each other.	REFER ANNEXURE TEST SERIAL NO. 133	
3.12.2		Multiple links of the two CPEs are required to provide back up to each other.	REFER ANNEXURE TEST SERIAL NO. 133	
3.12.3		In the dual-CPE scenario, the CPEs (at a hub site, an aggregation site, or a spoke site) use the VRRP or equivalent protocol towards WAN shall be supported	REFER ANNEXURE TEST SERIAL NO. 134	
3.12.4		In the dual-CPE scenario, the CPEs (at a hub site, an aggregation site, or a spoke site) function as the active and standby gateways for the intranet through OSPF.	REFER ANNEXURE TEST SERIAL NO. 135	
3.12.5		Two CPEs shall be deployed at a hub site to improve reliability.	REFER ANNEXURE TEST SERIAL NO. 62	
3.12.6		The two hubs work in both active/active and active/standby mode.	REFER ANNEXURE TEST SERIAL NO. 134	
3.12.7		A Controller shall be deployed in cluster mode. If a node is faulty, the Controller shall still work properly.	REFER ANNEXURE TEST SERIAL NO. 2	
3.12.8		If the Controller is faulty, existing services shall be forwarded without interruption.	REFER ANNEXURE TEST SERIAL NO. 2	

3.13		**O&M**		
3.13.1		The site topology shall be displayed based on GIS.	REFER ANNEXURE TEST SERIAL NO. 54	
3.13.2		The solution should support on-demand real time overlay topology analysis.	REFER ANNEXURE TEST SERIAL NO. 43	
3.13.3		Management of device alarms shall be supported.	REFER ANNEXURE TEST SERIAL NO. 47	
3.13.4		Unauthorized registration logs and operation logs shall be supported.	REFER ANNEXURE TEST SERIAL NO. 31	
3.13.5		Configure CPEs to report logs to the log server shall be supported. Parameters such as the IP address, port number, encryption policy, and log format of the log server are configurable.	REFER ANNEXURE TEST SERIAL NO. 29	
3.13.6		CPEs shall be upgraded in batches.	REFER ANNEXURE TEST SERIAL NO. 33	
3.13.7		Patches shall be installed on CPEs in batches.	REFER ANNEXURE TEST SERIAL NO. 33	
3.13.8		On the Controller, multiple sites and devices at the sites be selected for an upgrade and patch installation task.	REFER ANNEXURE TEST SERIAL NO. 33	
3.13.9		the solution shall support schedule upgrade and patch installation tasks for offline CPEs. When the CPEs go online, they are automatically upgraded, and automatically load and activate patches.	REFER ANNEXURE TEST SERIAL NO. 33	
3.13.10		The Controller shall display the upgrade or patch installation status of each CPE.	REFER ANNEXURE TEST SERIAL NO. 33	
3.13.11		Rollback is supported.	REFER ANNEXURE TEST SERIAL NO. 33	

3.13.12		The Controller should support multi-tenant management.	REFER ANNEXURE TEST SERIAL NO. 4	
3.13.13		A device shall be remotely reset.	REFER ANNEXURE TEST SERIAL NO. 87	
3.13.14		The site configuration shall be saved.	REFER ANNEXURE TEST SERIAL NO. 1	
3.13.15		The Controller should provide the ping function to diagnose the connectivity of overlay and underlay networks	REFER ANNEXURE TEST SERIAL NO. 136	
3.13.16		The Controller provides the trace route function.	Functional Verification	
3.13.17		The Controller shall collect fault information.	REFER ANNEXURE TEST SERIAL NO. 47	
3.13.18		Users shall log in to the CPE through SSH to view CPE configurations.	REFER ANNEXURE TEST SERIAL NO. 38	
3.13.19		The Controller shall display information about CPEs' CPU usage, memory usage, and flash/hard disk usage.	REFER ANNEXURE TEST SERIAL NO. 54	
3.13.20		vCPE's shall be provisioned through centralized SDWAN Controller to send all syslog message to a remote secure syslog server	REFER ANNEXURE TEST SERIAL NO. 29	
3.13.21		Syslog messages may transit an un-secured WAN network hence all syslog messages should be sent and protected with TLS using client certificates	REFER ANNEXURE TEST SERIAL NO. 29	
3.13.22		System should also support forwarding syslog messages to end Enterprise hosted primary and optionally secondary Syslog server	REFER ANNEXURE TEST SERIAL NO. 137	
3.13.23		The Orchestrator/management should provide capability of remote diagnostics like Ping, trace route, testing VPN connectivity, list active flows, paths, flush active flows etc	REFER ANNEXURE TEST SERIAL NO. 136	

3.13.24		The SD-WAN solution should be able to provide interface capture of CPE devices to mirror the traffic to remote server for troubleshooting.	Functional Verification	
3.13.25		The Orchestrator/management should provide ARP table dump, Route table dump, tech support logs for the CPE device without the requirement of logging into the CLI of device	REFER ANNEXURE TEST SERIAL NO. 138	
3.14		**Scalability**		
		SDWAN solution shall support Standalone & High Availability features along with support of Sinde PE & Dual CPE Setup. However the actual scalability features required shall be specifled by the purchaser in tendering requirements.	Functional test check	
	a)	The SDWAN solution shall support at least 100 Tenants/ Enterprises	REFER ANNEXURE TEST SERIAL NO. 139	
	b)	The SDWAN solution shall support at least 10K SDWAN CPEs	REFER ANNEXURE TEST SERIAL NO. 139	
	c)	The SDWAN solution shall support at least 15K VRFs	REFER ANNEXURE TEST SERIAL NO. 140	
	d)	The solution shall support 10 VRFs (Micro-VPNs) per SDWAN CPE	REFER ANNEXURE TEST SERIAL NO. 141	
	e)	The solution shall support at least 1K SDWAN CPEs in a single VRF	REFER ANNEXURE TEST SERIAL NO. 139	
	f)	The SDWAN CPE shall support at least 1K IPSec tunnels simultaneously	REFER ANNEXURE TEST SERIAL NO. 139	
	g)	The SDWAN CPE shall support at least 10K Routes	REFER ANNEXURE TEST SERIAL NO. 142	
	h)	The SDWAN Gateway shall be multi-tenant and support at least 50 Tenants / Enterprises	REFER ANNEXURE TEST SERIAL NO. 143	
	i)	The SDWAN Gateway shall support at least 5K SDWAN CPEs simultaneously	REFER ANNEXURE TEST SERIAL NO. 143	

	j)	The SDWAN Gateway shall support at least 32K Routes	REFER ANNEXURE TEST SERIAL NO. 143	
	k)	The SDWAN Gateway shall be available as a software function with throughout upto 1Gbps	REFER ANNEXURE TEST SERIAL NO. 143	
	l)	To support individual real-time dashboards for respective enterprise customers	REFER ANNEXURE TEST SERIAL NO. 47	
	m)	SDWAN solution shall support minimum (specified by purchaser) concurrent site to site VPN tunnels and user sessions per SDWAN CPE.	Functional test check	
	n)	The SDWAN solution shall support automatic resource allocation & load balancing based on traffic conditions, link performance & SLAs	Functional test check	
4.0		**QUALITY REQUIREMENTS**		
	4.1	The manufacturer shall furnish the MTBF value. Minimum value of MTBF shall be specified by the purchaser. The calculations shall be based on the guidelines given in either QA document No. QM-115 {January 1997} "Reliability Methods and Predictions" or any other international standards	Declaration	
	4.2	The equipment shall be manufactured in accordance with international quality management system ISO 9001:2015 or any other equivalent ISO certificate for which the manufacturer should be duly accredited. A quality plan describing the quality assurance system followed by the manufacturer would be required to be submitted.	Declaration	
	4.3	The equipment shall conform to the requirements for Environment specified in TEC QA standards QM-333 {Issue-March, 2010} (TEC 14016:2010) "Standard for Environmental testing of Telecommunication Equipment" or any other equivalent international standard, for operation, transportation and storage. The applicable environmental category A or B to be decided by the purchaser based on the use case.	Declaration	
5.0		**EMI/EMC Requirements**		

	5.1	**General Electromagnetic Compatibility (EMC) Requirements:** The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from an accredited test agency.	Information	
	a)	**Conducted and radiated emission (applicable to telecom equipment):** **Name of EMC Standard:** "CISPR 32 (2015) with amendments - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment". **Limits:-** i) To comply with Class B of CISPR 32 (2015) with amendments for indoor deployments and Class A of CISPR 32 (2015) with amendments with amendments for outdoor deployments.	Report from Accredited Test Lab	
	b)	**Immunity to Electrostatic discharge:** **Name of EMC Standard:** IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test". **Limits: -** i. Contact discharge level 2 {± 4 kV} or higher voltage; ii. Air discharge level 3 {± 8 kV} or higher voltage;	Report from Accredited Test Lab	

	c)	**Immunity to radiated RF:** **Name of EMC Standard:** IEC 61000-4-3 (2010) "Testing and measurement techniques -Radiated RF Electromagnetic Field Immunity test" **Limits:-** **For Telecom Terminal Equipment without Voice interface (s)** Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.	Report from Accredited Test Lab	
	d)	**Immunity to fast transients (burst):** **Name of EMC Standard: IEC** 61000- 4- 4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test" **Limits:-** Test Level 2 i.e. a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal / control / data / telecom lines;	Report from Accredited Test Lab	
	e)	**Immunity to surges:** **Name of EMC Standard:** IEC 61000-4-5 (2014) "Testing & Measurement techniques for Surge immunity test" **Limits:-** i. For mains power input ports: (a)2 kV peak open circuit voltage for line to ground coupling (b) 1 kV peak open circuit voltage for line to line coupling ii. For telecom ports: (a) 2 kV peak open circuit voltage for line to ground (b)2 kV peak open circuit voltage for line to line coupling.	Report from Accredited Test Lab	

	f)	**Immunity to conducted disturbance induced by Radio frequency fields:**	Report from Accredited Test Lab	

		Name of EMC Standard: IEC 61000-4-6 (2013) with amendments "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields”. **Limits:-** Under the test level 2 {3 V r.m.s.}in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.		
	g)	**Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):** **Name of EMC Standard:** IEC 61000-4-11 (2004) “Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests”. **Limits:-** i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e. 70 % supply voltage for 500 ms) ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s. iv) a voltage interruption corresponding to a reduction of supply voltage of >95% for 10ms.	Report from Accredited Test Lab	

	h)	**Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any):** **Name of EMC Standard:** IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) – Part 4-29: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests **Limits:-** i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B. ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C. iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B. iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000ms. Applicable Performance Criteria shall be C. v. Voltage variations corresponding to 80% and 120%of supply for 100 ms to10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B.		

Note: - For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16 (TEC 11016:2016) and the referenced base standards i.e. IEC and CISPR standards and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (h) and TEC Standard TEC/SD/DD/EMC-221/05/OCT-16 (TEC 11016:2016). The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	Euro Norm
CISPR 11	EN 55011

		CISPR 32 / EN 55032 IEC 61000-4-2 / EN 61000-4-2 IEC 61000-4-3 / EN 61000-4-3 IEC 61000-4-4 / EN 61000-4-4 IEC 61000-4-5 / EN 61000-4-5 IEC 61000-4-6 / EN 61000-4-6 IEC 61000-4-11 / EN 61000-4-11 IEC 61000-4-29 / EN 61000-4-29		
6.0		**Safety Requirements**		
	6.1	The equipment shall conform to relevant safety requirements as per IS/IEC 62368-1:2018) or Latest as prescribed under Table no. 1 of the TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT": TEC10009: 2024. The manufacturer/supplier shall submit a certificate in respect of compliance to these requirements.	Report from Accredited Test Lab	
7.0		**Security Requirements**	Information	
	7.1	The security requirements are as covered under respective functional requirements.	Information	
	7.2	The SDWAN solution shall be subjected to Indian Telecom licensing and regulatory requirements.	Declaration	
		CHAPTER-2		
8.0		**INFORMATION FOR THE PROCURER OF PRODUCT** This chapter describes the desirable requirements for the SDWAN solution and will depend upon the requirement of the purchaser. Hence the tendering authority may choose out of the clauses mentioned below as per requirement.	Information	
8.1		All technical documents shall be in English language both in CD-ROM and in hard copy. The documents shall comprise of: i. System description documents ii. Installation, Operation and Maintenance documents iii. Training documents Repair manual	Documentation	

	8.1.1	**System description documents:** The following system description documents shall be supplied along with the system: i. Over-all system specification and description of hardware and software ii. Equipment layout drawings iii. Cabling and wiring diagrams iv. Schematic drawings of all circuits in the	Documentation	

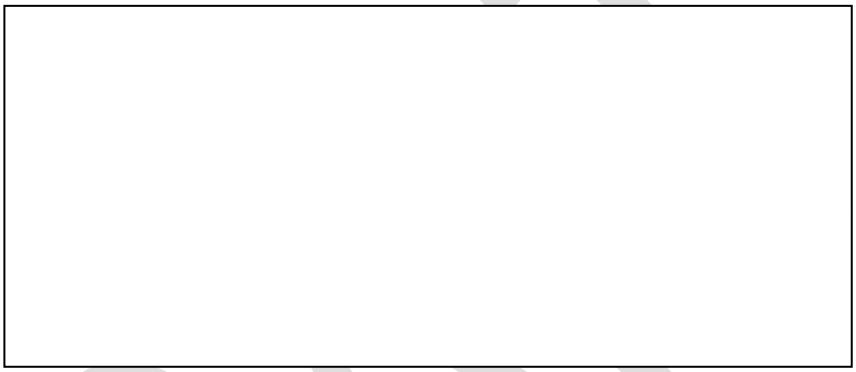
		system with timing diagrams wherever necessary v. Detailed specification and description of all Input / Output devices vi. Adjustment procedures, if there are any field adjustable units. vii. Detailed description of software describing the principles, functions and interactions with hardware, structure of the program and data viii. Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data ix. Program and data listings x. Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification		
	8.1.2	**System operation documents:** The following system operation documents shall be available: i. Installation manuals and testing procedures ii. Precautions for installation, operations and maintenance iii. Operating and Maintenance manual of the system iv. Safety measures to be observed in handling the equipment v. Man-machine language manual vi. Fault location and troubleshooting instructions including fault dictionary vii. Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement. viii. Emergency action procedures and alarm dictionary	Documentation	

	8.1.3	**Training Documents:** i. Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available. ii. Any provisional document, if supplied, shall be clearly indicated. The updates of all provisional documents shall be provided immediately following the issue of such updates.	Documentation	

		iii. The structure and scope of each document shall be clearly described. iv. The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information. v. All diagrams, illustrations and tables shall be consistent with the relevant text		
	8.1.4	**Repair Manual:** i. Procedure for trouble shooting and subassembly replacement ii. Test fixtures and accessories for repair iii. Systematic trouble shooting charts (fault tree) for all the probable faults with their remedial actions	Documentation	
8.2	8.2.1	**Additional Installation Requirements** All necessary interfaces, connectors, connecting cables and accessories required for satisfactory installation and convenient operations shall be supplied. Type of connectors, adopters to be used shall be in conformity with the interfaces defined in this GR.	Declaration	
	8.2.2	It shall be ensured that all testers, tools and support required for carrying out the stage by stage testing of the equipment before final commissioning of the network shall be supplied along with the equipment.	Information	
	8.2.3	All literature and instructions required for installation of the equipment, testing and bringing it to service shall be made available in English language.	Information	

	8.2.4	For the installations to be carried out by the supplier, the time frames shall be furnished by the supplier including the important milestones of the installation process well before commencing the installations.	Information	
	8.2.5	The supplier shall have maintenance/repair facility in India.	Declaration	
	8.2.6	All the software updates shall be provided on continuous basis for a minimum period of 7 years from the date of induction of system in the telecom network. These updates shall include new features and services and other maintenance updates	Declaration	
8.3		**Guidelines for the tendering authority** The following	Information	
		information shall be specified by the purchaser while tendering the items: a) The purchaser may decide the exact specification based on their use case deployment. b) For optional features, the requirement if any may be stipulated by tendering/purchasing authority		

I. TEST SETUP & PROCEDURES:

1. Test No.	
2. Test Details	*Name and Other relevant details*
3. Test Instruments Required	1. <Name> 2.
4. Test Setup	
5. Test Procedure	*Testing Steps may be written here…..* 1. …….. 2. …….. 3. ……..
6. Test Limits	(*if any*)
7. Expected Results	1. ……..<values>…… 2. ……..<values>…… 3.

J. SUMMARY OF TEST RESULTS

GR/IR No.: TEC 49160:2025
TSTP No.: TEC 49161:2026

Equipment name & Model No._____

ClauseNo.	Compliance (Complied/Not Complied/ Submitted/Not Submitted/Not Applicable)	Remarks / Test Report Annexure No.

Date:
Place: **Signature & Name of TEC testing Officer /**

***** **Signature of Applicant / Authorized Signatory**

***** ***Section J as given above is also to be submitted by the Applicant/Authorised signatory as part of in-house test results alongwith Form-A. The Authorised signatory shall be the same as the one for Form 'A'***.

S. No.	1
TEST CASE NO.	3.1.a, 3.13.14
TEST PURPOSE	To verify the Centralized policy management and SD-WAN controller must provide a single, unified platform for network service provisioning, policy management, change and compliance management.
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy Management engine, Controller and CPE must be deployed. Procedure: 1. Configure a Tenant and service configuration from the management plane and verify respective service is getting created on controller as well as CPE. 2. Configure a specific policy from the same management plane and verify same is getting applied on the CPE. 3. Perform changes on policy configuration and verify changes are getting applied on CPE.
EXPECTED RESULT	Service provisioning, policy configuration and changes should be done by single management plane.
TEST RESULT	
REMARKS	

S.No.	2
TEST CASE NO.	3.1.b, 3.12.7
TEST PURPOSE	To Verify SD-WAN controller instances shall support High Availability (HA) redundant configurations
TESTING DETAILS	
PROCEDURE	Perquisite: 1. Policy management engine must be deployed Procedure: 1. Deploy minimum two SDWAN controllers. 2. CPE shall be connected to both controllers. 3. Configure services/policies from management plane and shall be reflected on both controllers. 4. Shutdown one controller and verify configurations are still present on other controller and CPE is still connected to second controller.
EXPECTED RESULT	SD WAN controller instances should support High availability redundancy configuration.
TEST RESULT	
REMARKS	

S.No.	3
TEST CASE NO.	3.1. c
TEST PURPOSE	To verify SDWAN solution shall be centrally managed by web based GUI
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy Management engine, Controller and CPE must be deployed. Procedure: 1. Open the policy management on web browser. 2. Configure a Tenant/ service/policy from the management plane on GUI.
EXPECTED RESULT	SDWAN centralized management engine should be web GUI based.
TEST RESULT	
REMARKS	

S.No.	4
TEST CASE NO.	3.1.d, 3.13.12
TEST PURPOSE	To Verify SDWAN centralized policy management and SDWAN controller shall be multi-tenant/enterprise supporting multiple enterprise customers.
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy Management engine, Controller and CPE must be deployed. Procedure: 1. Create at least 2 enterprise tenant or organisations on policy management plane and verify same is getting reflected on SDWAN controller. 2. Verify both organisations are isolated from each other.
EXPECTED RESULT	SDWAN Policy management engine and controller should be multi-tenant. Multiple tenants/enterprise organisations should be created isolated from each other.
TEST RESULT	
REMARKS	

S.No.	5
TEST CASE NO.	3.1. e
TEST PURPOSE	The solution must support zero-touch provisioning/plug-n-play for new branches, which entails on-site branch personnel having to make physical (i.e., cabling) changes only.
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy Management engine, Controller deployed. Procedure: 1. Configure the tenant and respective parameters from the policy management plane. 2. Plug in the CPE with power cable and physical links only. 3. Power on the CPE and verify same is getting discovered on controller and management plane.
EXPECTED RESULT	SDWAN should support zero-touch provisioning of CPEs.
TEST RESULT	
REMARKS	

S.No.	6
TEST CASE NO.	3.1. g
TEST PURPOSE	The solution must support end-to-end real-time flow visualization for the application paths for identifying issues and taking corrective actions
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy Management engine, Controller and CPEs must be deployed. Procedure: 1. Configure the tenant and respective parameters from the policy management plane. 2. Send flows from LAN side. 3. Verify flows visualisation.
EXPECTED RESULT	Flows visualisation shall be available.
TEST RESULT	
REMARKS	

S.No.	7
TEST CASE NO.	3.1.h
TEST PURPOSE	All network-wide configurations shall be from the Centralized policy management and SD-WAN controller.
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy Management engine, Controller and CPE must be deployed. Procedure: 1. Configure a Tenant and service configuration from the management plane and verify respective service is getting created on controller as well as CPE. 2. Configure a specific policy from the same management plane and verify same is getting applied on the CPE.
EXPECTED RESULT	All network configuration should be done by centralized policy engine
TEST RESULT	
REMARKS	

S.No.	8
TEST CASE NO.	3.1.i
TEST PURPOSE	All application forwarding policies shall be configured from the Centralized policy management and SD-WAN controller
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy Management engine, Controller and CPE must be deployed. Procedure: 1. Configure a Tenant and service configuration from the management plane and verify respective service is getting created on controller as well as CPE. 2. Configure a specific policy from the same management plane and verify same is getting applied on the CPE.
EXPECTED RESULT	All forwarding policies should be configured from centralized policy engine
TEST RESULT	
REMARKS	

S.No.	9
TEST CASE NO.	3.1.j
TEST PURPOSE	All control functions, including the policy engine and controller shall be deployed in redundant configurations
TESTING DETAILS	
PROCEDURE	Procedure: 1. Deploy policy engine in redundant mode and verify status 2. Deploy controller in redundant mode and verify status. 3. Shutdown one policy engine and verify controller is still connected to second policy engine of same cluster. 4. Shutdown one controller and verify services are still up and connected with single controller and policy engine.
EXPECTED RESULT	Policy engine and controller should be deployed in redundant configuration.
TEST RESULT	
REMARKS	

S.No.	10
TEST CASE NO.	3.1.k
TEST PURPOSE	All communications between the CPEs, vCPE's & uCPE's and SD-WAN controller shall be encrypted with industry standard strong encryption
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Management policy engine, controller and CPE must be deployed. Procedure: 1. Provision the vCPE and uCPE and establish connection with controller. 2. Verify communication between controller and CPE is encrypted.
EXPECTED RESULT	Communication between CPE and controller should be encrypted.
TEST RESULT	
REMARKS	

S. No.	11
TEST CASE NO.	3.1.L, 3.9.22, 3.9.23
TEST PURPOSE	After successful installation, configuration of the CPEs, vCPE's & uCPE's shall be conducted via the SD-WAN management plane/controller
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Management policy engine, controller and CPE must be deployed. Procedure: 1. Provision the vCPE and uCPE and establish connection with controller. 2. Configure the networking parameters and services from the SDWAN management plane. 3. Verify services are getting reflected at CPE via management plane / controller. check the configuration, the configuration roll back function and the configuration history.
EXPECTED RESULT	Configuration of CPEs should be done by management plane/controller.
TEST RESULT	
REMARKS	

S.No.	12
TEST CASE NO.	3.1.M
TEST PURPOSE	When using multiple underlays with different WAN addressing, the solution must support management over any WAN address. If any or multiple of the WAN links fail, it must be possible to operate / manage the solution over any remaining interface(s).
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Management policy engine, controller and CPE must be deployed. Procedure: 1. Connect the CPE with two disjoint underlays. Underlays should be isolated from each other. 2. Verify controllers are connected to CPE via disjoint underlays. 3. Disconnect one uplink of CPE and verify CPE is still managed by controller using remaining uplink. 4. Perform changes from the policy management engine and verify same is getting reflected at CPE.
EXPECTED RESULT	CPE is connected to controller with disjoint underlays uplink and failure of any uplink should not affect the operations.
TEST RESULT	
REMARKS	

S.No.	13
TEST CASE NO.	3.1.N
TEST PURPOSE	The Solution should provide secure connectivity to Public Cloud Service Providers
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Management policy engine, controller and CPE must be deployed at one branch. 2. A workload should be available on any public cloud service providers (e.g Google cloud platform, AWS, Microsoft Azure) Procedure: 1. Device on LAN side of branch CPE should be able to reach to public cloud service providers. 2. Verify communication between branch CPE and public cloud service is encrypted.
EXPECTED RESULT	Communication with public cloud service providers are encrypted.
TEST RESULT	
REMARKS	

S.No.	14
TEST CASE NO.	3.1.O, 3.1.P, 3.1.R
TEST PURPOSE	The Management Policy Engine and controller shall support High Availability deployment The Management Policy Engine and controller shall support geographic redundancy
TESTING DETAILS	
PROCEDURE	Procedure: 1. Deploy management policy engine and SDWAN controller in geographically dispersed location for redundancy.
EXPECTED RESULT	Management plane and controller should support Geo redundancy and high availability.
TEST RESULT	
REMARKS	

S.No.	15
TEST CASE NO.	3.1.Q
TEST PURPOSE	The Management Policy Engine and controller shall support capacity expansion
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. management policy engine and SDWAN controller must be deployed. 2. A CPE should be connected to the SDWAN controller. Procedure : 1. Deploy an additional controller and connect the CPE to new controller only. 2. Verify CPEs are able to communicate each other.
EXPECTED RESULT	Management plane and controller should capacity expansion.
TEST RESULT	
REMARKS	

S. No.	16
TEST CASE NO.	3.1.1.A
TEST PURPOSE	SDN Management/controller shall support open protocols / Interfaces like NETCONF / YANG / XMPP/ OPENFLOW/REST API etc to centrally manage devices such as CPE's, uCPE's and vCPE's
TESTING DETAILS	
PROCEDURE	Procedure : 1. Verify connectivity between management engine and controller is using open protocols. 2. Verify connectivity between controller and CPE is using open protocols.
EXPECTED RESULT	Management plane /controller should support open protocols/interfaces
TEST RESULT	
REMARKS	

S.No.	17
TEST CASE NO.	3.1.1.B
TEST PURPOSE	The SDN Management/controller shall support Northbound REST API / NETCONF / YANG / XMPP/ OPENFLOW etc for integration with third party Orchestrator and Enterprise own Self-Service portal.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify policy management engine/controller provides the open northbound interface for integration.
EXPECTED RESULT	Management plane /controller should support open northbound interface for integration with 3rd party orchestrator.
TEST RESULT	
REMARKS	

S. No.	18
TEST CASE NO.	3.1.1.C
TEST PURPOSE	The solution must support carrier grade scalable protocols like BGP/REST API/XMPP to share forwarding information between controllers.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify communication/federation between SDWAN controllers is using MPBGP/REST API/XMPP. 2. Verify routing information is exchanged between controllers.
EXPECTED RESULT	SDWAN controller should support BGP or REST API or XMPP protocols for routing information exchange between them.
TEST RESULT	
REMARKS	

S. No.	19
TEST CASE NO.	3.1.1.D
TEST PURPOSE	The solution must support forwarding tunnelling mechanism using open standard protocols like Vxlan/Vxlan over IPsec/GRE/IPSec/MPLS over UDP.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect at least two CPEs at two branches. 2. Send the overlay traffic from branch-1 Lan to Branch-2 lan. 3. Verify traffic is encapsulated over Vxlan/Vxlan over IPsec/GRE/IPSec/MPLS over UDP.
EXPECTED RESULT	Branch to branch traffic should be forwarded using Vxlan/VXLAN over IPsec/GRE/IPSec/MPLS over UDP tunnelling.
TEST RESULT	
REMARKS	

S. No.	20
TEST CASE NO.	3.1.1.E
TEST PURPOSE	The overlay paths established amongst the edge devices must support the ability to run routing protocols: static or dynamic (OSPF/ISIS and BGP).
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a CPE at branch location. 2. Create an overlay service from the policy engine to branch. 3. Configure static route or dynamic protocol OSPF/ISIS and BGP on overlay with LAN. 4. Verify static route is installed. If dynamic protocol is used verify neighborship is established.
EXPECTED RESULT	Static route or dynamic protocol neighborship is established in overlay.
TEST RESULT	
REMARKS	

S. No.	21
TEST CASE NO.	3.1.2.1
TEST PURPOSE	The solution shall allow administrators to create, modify, delete, and query accounts.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Login to management policy engine using administrator credentials. 2. Create a new user with specific rights for eg view only. 3. Login using new user and verify only specific actions can be performed. 4. Login via admin user again and modify user access. 5. Delete user and verify same has been deleted.
EXPECTED RESULT	Administrator are allowed to create, modify, delete accounts.
TEST RESULT	
REMARKS	

S. No.	22
TEST CASE NO.	3.1.2.2
TEST PURPOSE	The solution shall allow administrators shall to create accounts for the local tenant and specify the user name, description, role, authorized object, and other information when creating an account
TESTING DETAILS	
PROCEDURE	Procedure: 1. Login to management policy engine using administrator credentials. 2. Create a tenant/organisation and create a new user with specific rights/roles. 3. Login using new user and verify only specific actions can be performed within its tenant only. 4. New user should have visibility of its local tenant only.
EXPECTED RESULT	Administrator should be able to create tenant specific users with specific roles.
TEST RESULT	
REMARKS	

S. No.	23
TEST CASE NO.	3.1.2.3
TEST PURPOSE	The solution shall allow administrators to modify other accounts with lower authority levels, including authorization and role information
TESTING DETAILS	
PROCEDURE	Procedure: 1. Login to management policy engine using administrator credentials. 2. Create atleast two tenant/organisation and create new users in respective tenant with specific rights/roles. 3. Login using new user and verify only specific actions can be performed within its tenant only. 4. Login with administrator user and modify each tenant user with different role.
EXPECTED RESULT	Administrator should be able to modify other accounts users roles.
TEST RESULT	
REMARKS	

S. No.	24
TEST CASE NO.	3.1.2.4
TEST PURPOSE	The solution shall allow administrators to change their own passwords
TESTING DETAILS	
PROCEDURE	Procedure: 1. Login to management policy engine using administrator credentials. 2. Modify the administrator user password. 3. Logout and login using new password.
EXPECTED RESULT	Administrator should be able to change its own password
TEST RESULT	
REMARKS	

S. No.	25
TEST CASE NO.	3.1.2.5, 3.1.4.8
TEST PURPOSE	The solution shall support integration with LDAP/AAA
TESTING DETAILS	
PROCEDURE	Procedure: 1. Integrate policy management engine with LDAP or AAA.
EXPECTED RESULT	Policy management engine should be integrated with LDAP/AAA
TEST RESULT	
REMARKS	

S.No.	26
TEST CASE NO.	3.1.2.6
TEST PURPOSE	The Solution shall support local RBAC (Role Based Access Control)
TESTING DETAILS	
PROCEDURE	Procedure: 1. Create local users on Policy management engine with different roles. 2. Verify respective users
EXPECTED RESULT	Role based access control should be supported on SDWAN.
TEST RESULT	
REMARKS	

S. No.	27
TEST CASE NO.	3.1.2.7
TEST PURPOSE	The solution shall allow administrators to view the list of online administrators, including the following information: user name, role, login IP address, and login time
TESTING DETAILS	
PROCEDURE	Procedure: 1. Login to controller or policy engine with specific user. 2. Check the current user logged in details with IP address, login time, username in respective system.
EXPECTED RESULT	Should be able to view the list of line users with username, role, login IP, Address and login time.
TEST RESULT	
REMARKS	

S. No.	28
TEST CASE NO.	3.1.2.8
TEST PURPOSE	Allow administrators to set the idle timeout interval for web login. If an administrator does not perform any operations within this period of time after login, the administrator account will be automatically logged out
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure idle timeout interval. 2. Login with specific user and keep the system idle for stipulated time. 3. Verify UI is automatically logged out post expiry of idle timeout.
EXPECTED RESULT	Administrator can set idle timeout interval for web login and UI should be logged out automatically after expiry of idle timeout interval
TEST RESULT	
REMARKS	

S. No.	29
TEST CASE NO.	3.1.3.1, 3.13.5, 3.13.20,3.13.21
TEST PURPOSE	The solution should support integration with the centralised Syslog server for monitoring and audit trail vCPE's shall be provisioned through centralized SDWAN Controller to send all syslog message to a remote secure syslog server
TESTING DETAILS	
PROCEDURE	Procedure: 1. Bootstrap a vCPE. 2. Integrate centralised syslog server with policy management engine/controller/CPE. 3. Verify logs messages are sent to syslog server. 4. Verify syslog messages are encrypted with TLS certificate. For eg. https.
EXPECTED RESULT	SDWAN solution should send messages to centralized syslog server.
TEST RESULT	
REMARKS	

S. No.	30
TEST CASE NO.	3.1.3.2
TEST PURPOSE	The solution shall support records information such as user creation, modification, and deletion and administrator login, account change, and password change.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Create / modify /delete a user. 2. Verify logs are generated for each specific action performed.
EXPECTED RESULT	Records related to user creation/modification/deletions should be available.
TEST RESULT	
REMARKS	

S.No.	31
TEST CASE NO.	3.1.3.3, 3.1.3.4
TEST PURPOSE	The solution shall allow administrators to query logs generated within 90 days and export selected logs or all logs. The purchaser may specify the exact log period. The solution shall support records logs for add, modify, and delete operations in addition to the query operation
TESTING DETAILS	
PROCEDURE	Procedure: 1. Create / modify /delete an entity or perform any operational task. 2. Verify logs are generated for specific action performed. 3. Query the logs from logger.
EXPECTED RESULT	Records related to creation/modification/deletions of entities should be available in respective logging system.
TEST RESULT	
REMARKS	

S.No.	32
TEST CASE NO.	3.1.3.5, 3.1.3.6
TEST PURPOSE	The solution shall allow administrators to query operation logs by account, operation object, time, log level, client IP address, operation result, and details. Operation logs shall be exported
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify syslogs logs are generated for any operational activity.
EXPECTED RESULT	Logs should be available to administrators with relevant fields and should be exported to external system.
TEST RESULT	
REMARKS	

S.No.	33
TEST CASE NO.	3.1.3.7, 3.13.6, 3.13.7,3.13.8,3.13.9, 3.13.10,3.10.11
TEST PURPOSE	The solution shall support records or events such as patch loading, upgrade, node status changes in the policy management engine/controller. CPE shall be upgraded in batches Multiple CPE upgrade in single go. The Controller shall display the upgrade or patch installation status of each CPE.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Note the current version of CPE. 2. Perform CPE upgrade from the policy management engine/controller. 3. Verify the status of patch download and upgrade. 4. Verify new software release update on policy management engine/controller. 5. Upgrade another CPE in same sequence. 6. Upgrade multiple CPEs in one go. 7. Schedule upgrade to CPE to a specific time. 8. Verify upgrade status on policy engine.
EXPECTED RESULT	Events should be available for patch loading, upgrade and node status change.
TEST RESULT	
REMARKS	

S. No.	34
TEST CASE NO.	3.1.4.1, 3.9.4
TEST PURPOSE	The solution shall allow the CPEs to report performance data to the Controller through HTTP2.0/REST API/HTTPS for displaying the data in selfservice portal
TESTING DETAILS	
PROCEDURE	Procedure: 1. Send flows from the LAN side between branches. 2. Verify stats are being exported to centralized core using HTTP2.0/RESTAPI/HTTPS. 3. Verify stats and reports on self service portal
EXPECTED RESULT	CPE should be able to send stats to centralized Policy engine/Controller. Reports should be available in self service portal.
TEST RESULT	
REMARKS	

S.No.	35
TEST CASE NO.	3.1.4.2, 3..9.21
TEST PURPOSE	The solution shall support importing CA certificates of external systems for interconnection verification with the external systems.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Generate certificates from CA. 2. Verify certificates are downloaded to CPE. 3. Verify https/tls connection is established using the correct certificates.
EXPECTED RESULT	CPE connection with management policy engine/controller should be established using correct certificates.
TEST RESULT	
REMARKS	

S.No.	36
TEST CASE NO.	3.1.4.3
TEST PURPOSE	The solution shall support unified identity authentication for each integrated system, and provides the integrated login page and RESTful interface for Single Sign On (SSO) login
TESTING DETAILS	
PROCEDURE	Procedure: 1. Integrate system for SSO login. 2. Perform and verify SSO login to respective portal.
EXPECTED RESULT	SSO should be supported.
TEST RESULT	
REMARKS	

S.No.	37
TEST CASE NO.	3.1.4.4, 3.1.4.5
TEST PURPOSE	The solution should support administrators to define basic operations based on a YANG or XMPP or OPENFLOW or REST API or Netconf interfaces module, including configuration operations, status data, and remote procedure call (RPC), and notification mechanism The Solution should support administrators to configure and query network services, collect alarms, and issue commands to devices through open protocols/interfaces NETCONF/ OPENFLOW/ XMPP/ SNMP/REST API etc. The CPEs report alarms through standard and open interfaces such as NETCONF, ReST API, SNMP
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure a new service/network on CPE from the policy management engine and verify same is getting reflected to CPE using open protocols / interfaces. 2. Generate alarm on CPE and verify same is notified using open protocols.
EXPECTED RESULT	Policy management engine/controller should use YANG or XMPP or OPENFLOW or REST API or NETCONF or SNMP for configuration of CPE, alarms notification mechanism.
TEST RESULT	
REMARKS	

S.No.	38
TEST CASE NO.	3.1.4.6, 3.9.3, 3.13.18
TEST PURPOSE	The Solution support using SSH to ensure channel security. Users shall log in to the CPE through SSH to view CPE configurations
TESTING DETAILS	
PROCEDURE	Procedure: 1. SSH to policy management engine/controller. 2. SSH to CPE.
EXPECTED RESULT	Login via SSH should be supported.
TEST RESULT	
REMARKS	

S.No.	39
TEST CASE NO.	3.1.4.7
TEST PURPOSE	The Solution support using TLS 1.2 or higher for encryption to ensure data transmission security.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify TLS 1.2 or higher is supported between controller/ CPE for encryption.
EXPECTED RESULT	SDWAN should support TLS 1.2 or higher encryption.
TEST RESULT	
REMARKS	

S.No.	40
TEST CASE NO.	3.1.5.1
TEST PURPOSE	The SDWAN gateway shall support gateway function between the legacy, non-SD-WAN brownfield network and the new/Green field SD-WAN network.
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine, Controller and atleast 2 SDWAN CPEs must be deployed. 2. a legacy branch (non SDWAN) CPE must be deployed. 3. SDWAN gateway must be deployed Procedure: 1. Send traffic from Lan side of SDWAN branch to legacy side via gateway. 2. Verify traffic flow between SDWAN branch and non SDWAN branch is via gateway.
EXPECTED RESULT	SDWAN gateway should provide reachability between non SDWAN legacy network and SD WAN enabled branches.
TEST RESULT	
REMARKS	

S.No.	41
TEST CASE NO.	3.1.5.2
TEST PURPOSE	The SDWAN Gateway shall be Multi-Tenant/enterprise supporting multiple enterprise customers.
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine, Controller and SDWAN CPEs must be deployed. 2. A SDWAN gateway must deployed. Procedure: 1. Create atleast two or more tenants/enterprise organisations on policy management plane. 2. Extend the new created tenants to SD WAN gateway and verify they are isolated from each other. 3. Send the traffic in each tenants via gateway to verify the reachability and multi tenancy.
EXPECTED RESULT	SDWAN gateway should be able to support atleast two or more Tenant/enterprises.
TEST RESULT	
REMARKS	

S. No.	42
TEST CASE NO.	3.1.5.3
TEST PURPOSE	The SDWAN gateway shall support traffic flow between different WANs (Internet to MPLS etc).
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine, Controller and atleast 2 SDWAN CPEs must be deployed. 2. A SDWAN gateway must deployed. Procedure: 1. Connect 2 CPEs with disjoint underlay. One branch over internet and another over MPLS. 2. Connect SDWAN gateway with both underlays. 3. Send overlay traffic between branch-1 and branch-2 and verify traffic is flowing through gateway.
EXPECTED RESULT	SDWAN gateway should support traffic flow between disjoint underlays.
TEST RESULT	
REMARKS	

S.No.	43
TEST CASE NO.	3.2.A, 3.13.2
TEST PURPOSE	The assurance platform shall provide overlay service topology and view. The overlay network topology shall be displayed
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure service for a tenant between multiple branches from policy management engine. 2. Verify service topology is shown on assurance platform.
EXPECTED RESULT	Assurance platform should provide overlay service topology.
TEST RESULT	
REMARKS	

S.No.	44
TEST CASE NO.	3.2.B
TEST PURPOSE	The assurance platform shall provide Overlay Root Cause Analysis i.e. tools to debug Configuration/connectivity problems between SDN Controller and SD-WAN Edge
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure service for a tenant between multiple branches from policy management engine. 2. Verify service topology is shown on assurance platform. 3. Perform network failures or disconnect one branch. 4. Verify overlay root cause is shown.
EXPECTED RESULT	Mechanism for overlay root cause analysis should be shown.
TEST RESULT	
REMARKS	

S.No.	45
TEST CASE NO.	3.2.C, 3.2. D
TEST PURPOSE	The assurance platform shall support automatic Inventory Discovery for SD edge devices. The assurance platform shall support advanced Service Inventory Visualization
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect multiple branches to a tenant. 2. Configure service for a tenant between multiple branches from policy management engine. 3. Verify services/branches are automatically discovered in platform. 4. Verify service topology is shown on assurance platform.
EXPECTED RESULT	CPEs should be automatically discovered in assurance platform and services should be visible.
TEST RESULT	
REMARKS	

S.No.	46
TEST CASE NO.	3.2.E
TEST PURPOSE	The solution shall provide tools to do Configuration Audit i.e. Validate SD-WAN Edge configuration against configuration in SD-WAN Controller
TESTING DETAILS	
PROCEDURE	Procedure: 1. Perform a CPE configuration audit using appropriate tools to validate configuration with controller.
EXPECTED RESULT	Audit tools to validate CPE configuration against the SDWAN controller config should be available.
TEST RESULT	
REMARKS	

S. No.	47
TEST CASE NO.	3.2.F, 3.13.3,3.13.17,3.14.L
TEST PURPOSE	The solution shall provide tools to monitor the Health of overlay components i.e. dashboard showing Top Unhealthy Overlays, Top Problems/ Alarms etc. Management of device alarms shall be supported
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect multiple CPE branches and configure overlay services on branches. 2. Verify dashboard and health status. 3. Disconnect 1 or 2 branches multiple times or perform overlay network failures. 4. Verify dashboard shows top unhealthy overlays and alarms.
EXPECTED RESULT	Health of overlay network should be shown on dashboard.
TEST RESULT	
REMARKS	

S. No.	48
TEST CASE NO.	3.2.G
TEST PURPOSE	The assurance platform shall provide Historical impact analysis.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Check impact analysis in assurance platform.
EXPECTED RESULT	Assurance platform should provide historical impact analysis
TEST RESULT	
REMARKS	

S. No.	49
TEST CASE NO.	3.3.A
TEST PURPOSE	The Self-Service portal shall be web-based application and shall provide a customizable dashboard with feature-specific widgets
TESTING DETAILS	
PROCEDURE	Procedure: 1. Open self-service portal on web browser. 2. Verify enterprise/organisation dashboard provide feature specific widgets.
EXPECTED RESULT	The Self-Service portal should be web-based application and should provide a dashboard with feature-specific widgets
TEST RESULT	
REMARKS	

S.No.	50
TEST CASE NO.	3.3.B
TEST PURPOSE	The Self-Service portal shall support multi-tenancy & RBAC (Role based Access Control) capabilities that shall be used by the service provider, Enterprises, Wholesalers, End customers for self-service management of VPNs
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify Self-service portal supports multiple organisations and are isolated from each other. 2. Create admin and view only users in each of the organisation. Verify user is able to access the contents based on roles defined.
EXPECTED RESULT	The Self-service portal should be multi tenant and should have user based on roles with admin/view only rights.
TEST RESULT	
REMARKS	

S.No.	51
TEST CASE NO.	3.3.C
TEST PURPOSE	Self-Service Portal shall support monitor and configure a SD-WAN setup
TESTING DETAILS	
PROCEDURE	Procedure: 1. Deploy a SDWAN branch site using self-service portal. 2. Configure the overlay IP/rules from the portal. 3. Generate a alarm and verify the alarm is displayed on self-service portal. 4. Verify branch level reports are available in portal
EXPECTED RESULT	The Self-service portal should provide configuration knobs for self-service configuration and portal should show details alarms of network.
TEST RESULT	
REMARKS	

S.No.	52
TEST CASE NO.	3.3.D, 3.3.E, 3.3.F, 3.9.31, 3.11.1, 3.11.2, 3.11.4,3.11.6,3.11.9,3.11.11, 3.7.6 q,r
TEST PURPOSE	The Self-Service portal shall provide each Enterprise to generate a very comprehensive branch site to branch site and global network traffic/throughput report. The Self-Service portal shall provide reports such as Security Audit Report, User Activity Reports, per VPN traffic report, Application Aware Routing reports on a per VPN basis, trigger real-time and on demand traffic reports. The Self-Service portal shall provide real-time monitoring capabilities to include KPIs, TCAs and SLA reports Link quality detection：Link jitter, delay, and packet loss ratio shall be measured. Link quality visualization：Link quality support be visualized on the Controller, which displays the link quality indicators including the jitter, delay, and packet loss ratio. The information shall be displayed and sorted by intra-site link or inter-site link The Controller should display traffic statistics by site, link, or application. The link bandwidth usage shall be calculated.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify branch throughput. 2. Verify network /VPN level throughput report. 3. Verify AAR traffic report 4. Verify KPI for network sla based on jitter latency and packet loss between branches.
EXPECTED RESULT	The Self-service portal should provide comprehensive reports on branch leve as well as per VPN level.
TEST RESULT	
REMARKS	

S.No.	53
TEST CASE NO.	3.3.G, 3.9.13, 3.9.20, 3.11.[12-18]
TEST PURPOSE	The Self-Service portal shall support following functional modules which shall expose to enterprises and end users: 1. Network services 2. Branch enablement 3. Visualisation 4. User/access control Application-based traffic data shall be collected and displayed by site, link, or terminal IP address. Statistics of all traffic at a site shall be calculated and displayed. Statistics of underlay traffic, local breakout traffic, and application traffic shall be calculated. A device reports the link or application quality data every 1 minute and traffic information every 5 minutes. You need to manually refresh the page of the Controller
TESTING DETAILS	
PROCEDURE	Procedure: 1. Create /update/delete a branch site using self-service portal. 2. Add the installer for branch for site activation based on single/two factor authentication. 3. Send mail to installer from portal 4. Configure and delete L2/L3 VPN service from self-service portal to branch site create above. 5. Configure subnets, ACL rules, QoS, PAT to underlay, DHCP , Encryption from the portal. 6. Verify self-service portal dashboard at service provider level and individual enterprise level. 7. Dashboard should provide option to drill down to more detailed view. 8. Reports for a. DPI b. Traffic throughput. c. Network performance. d. Application performance. e. Sla violations. 9. Create user with specific role-based groups. Such as admin and view only users. Verify admin user is able to do provisioning whereas read only user is not able to configure anything.
EXPECTED RESULT	The Self-Service portal should support following functional modules which shall expose to enterprises and end users: 1. Network services 2. Branch enablement 3. Visualisation 4. User/access control.
TEST RESULT	
REMARKS	

S. No.	54
TEST CASE NO.	3.3.H, 3.11.14, 3.13.1, 3.13.19
TEST PURPOSE	The customer portal shall support following: 1. Service Provider Dashboard View 2. Customer Dashboard View 3. Branches Widget on a geographical map/Dashboard 4. Network Summary 5. SDWAN edge device view (on geographical map/dashboard) 6. Users Activity 7. Traffic Summary 8. Events & Statistics 9. CPE Health Statistics of all traffic between sites shall be calculated and displayed, and a list of top N sites sorted by traffic volume is also displayed The site topology shall be displayed based on GIS. The Controller shall displays information about CPEs' CPU usage, memory usage, and flash/hard disk usage
TESTING DETAILS	
PROCEDURE	Procedure: 1. Open self-service portal as root/ service provider user and check the dashboards of individual enterprises. 2. Login to self-service portal from enterprise user and verify customer specific dashboard. 3. Verify branches are visible in Geo MAP. 4. Network summary throughput , top branches, DPI traffic network wise. 5. Top users based on upload/download. 6. Events for alarms node level wise and verify traffic reports for DPI, Network SLAs, throughput. 7. CPE health status like uptime, alarms, CPU, Memory, software version.
EXPECTED RESULT	The customer portal shall support following: 1. Service Provider Dashboard View 2. Customer Dashboard View 3. Branches Widget on a geographical map/Dashboard 4. Network Summary 5. SDWAN edge device view (on geographical map/dashboard) 6. Users Activity 7. Traffic Summary 8. Events & Statistics
	9. CPE Health
TEST RESULT	
REMARKS	

S.No.	55
TEST CASE NO.	3.4.1.1
TEST PURPOSE	SDWAN solution to support all Branches only on MPLS
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine/controller must be deployed. Procedure: 8. Connect multiple CPE branches on common MPLS underlay uplink. 9. Connect CPE with centralized controller using MPLS underlay. 10. Send traffic between branches.
EXPECTED RESULT	All branches on common MPLs underlay should be able to send overlay traffic flows with each other.
TEST RESULT	
REMARKS	

S.No.	56
TEST CASE NO.	3.4.1.2
TEST PURPOSE	SDWAN solution to support all Branches only on Internet
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine/controller must be deployed. Procedure: 1. Connect multiple CPE branches on internet underlay uplink. 2. Connect CPE with centralized controller using internet underlay. 3. Send traffic between branches.
EXPECTED RESULT	All branches on internet underlay should be able to send overlay traffic flows with each other.
TEST RESULT	
REMARKS	

S.No.	57
TEST CASE NO.	3.4.1.3
TEST PURPOSE	SDWAN solution to support Branches on both MPLS & Internet (on same CPE).
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine/controller must be deployed. Procedure: 1. Connect CPE branches on dual disjoint underlay uplinks. MPLS and internet 2. Verify CPE is connected to controllers using disjoint underlays.
EXPECTED RESULT	Disjoint dual uplink underlays on same CPE should be supported.
TEST RESULT	
REMARKS	

S.No.	58
TEST CASE NO.	3.4.1.4
TEST PURPOSE	SDWAN solution to support a few Branches on MPLS & other Branches on Internet
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine/controller must be deployed. Procedure: 1. Connect atleast 2 CPE branches only on MPLS underlay uplink and another few branches only on internet underlay uplink. 2. Verify CPEs are connected to respective controllers. 3. Send traffic between branches using gateway.
EXPECTED RESULT	Branches only on internet should be able to send traffic to sites only on MPLS
TEST RESULT	
REMARKS	

S. No.	59
TEST CASE NO.	3.4.1.5
TEST PURPOSE	SDWAN solution to support a few Branches on MPLS & Internet (Ethernet/DSL/LTE) on same CPE & other Branches only on Internet.
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine/controller must be deployed. Procedure: 1. Connect atleast 2 CPE branch only on internet underlay uplink and another few branches on dual uplink on internet and MPLS. 2. Verify CPEs are connected to respective controllers. 3. Send traffic between branches.
EXPECTED RESULT	All branches should be able to send flows with each other.
TEST RESULT	
REMARKS	

S. No.	60
TEST CASE NO.	3.4.1.6
TEST PURPOSE	SDWAN solution to support a few Branches on MPLS only & other branches on MPLS+ Internet (Ethernet/DSL/LTE) on same CPE
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine/controller must be deployed. Procedure: 1. Connect atleast 2 CPE branch only on MPLS underlay uplink and another few branches on dual uplink on internet and MPLS. 2. Verify CPEs are connected to respective controllers. 3. Send traffic between branches.
EXPECTED RESULT	All branches should be able to send flows with each other.
TEST RESULT	
REMARKS	

S. No.	61
TEST CASE NO.	3.4.1.7
TEST PURPOSE	The CPE device both in DC and Branches should support HA through Clustering of multiple CPE devices in DC, Active-Active and Active-Standby deployments
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy management engine/controller must be deployed. Procedure: 1. Configure 2 SDWAN Gateway CPEs deployed in DC in active/active mode. 2. Connect 2 CPEs at a branch-1 in active/active mode. 3. Connect a branch-2 standalone. 4. Send traffic flows between branch 1 and branch 2. 5. Perform branch-1 CPE-1 / Uplink failure and verify traffic flow is sent via branch-1 CPE-2. 6. Perform all the above steps in Active/standby mode as well.
EXPECTED RESULT	Clustering of multiple CPE devices in active/active and active/standby mode should be supported.
TEST RESULT	
REMARKS	

S. No.	62
TEST CASE NO.	3.4.1.8, 3.7.6.B, 3.7.6.C, 3.9.12
TEST PURPOSE	Enterprise site to site connectivity I. Support full mesh networking for direct communication. II. Support hub-spoke networking for centralized communication III. Support partial mesh networking, some spokes shall directly communicate with each other, and some communicate with each other through the hub.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 3 Spoke and 1 Hub sites. 2. Send traffic between all sites in full mesh. 3. Set the configuration to restrict traffic between spoke-1 with spoke2 and spoke-3 but between hub and spokes it should be allowed. 4. Verify traffic between spoke-1 to spoke-2 and spoke-1 & 2 to Hub site. 5. Set the configuration to restrict direct traffic between spoke-1 and spoke-2 only but direct communication between spoke-1 and spoke-3 is allowed. 6. Traffic between spoke-1 and spoke-2 should be through the Hub site.
EXPECTED RESULT	1. All sites should be able to send flows directly in full mesh. 2. Only flows between spoke and hub site is allowed. Direct Spoke to spoke communication is not allowed. 3. Partial mesh networking, selective spoke to spoke sites communication should be allowed and some spoke to spoke is allowed through the Hub site.
TEST RESULT	
REMARKS	

S. No.	63
TEST CASE NO.	3.4.1.9
TEST PURPOSE	Enterprise site connectivity I. Support local mode : A branch site shall access the Internet / MPLS using local breakout. II. Support centralized mode : A hub site, an aggregation site, or a branch site shall function as the centralized Internet access site. III. Support Internet access in local mode (default) and centralized mode (backup), By default, a branch site accesses the Internet in local mode. When the Internet link for local access fails, the traffic is transmitted to the Internet by a centralized Internet access site.
TESTING DETAILS	
PROCEDURE	Proced ıre: 1. Connect atleast 1 access branch and 1 Hub/Aggregation sites each with internet and MPLS uplink 2. Configure local breakout at branch and verify internet/MPLS reachability for overlay traffic. 3. Disable local breakout at branch and configure central breakout related configuration. 4. Verify overlay traffic is sent to central hub/aggregation branch for internet access. 5. Enable local breakout configuration 6. Verify traffic by default is using respective uplink at access branch for internet access and perform uplink failure. 7. Enable central breakout options. 8. Verify traffic is now sent to central hub/aggregation site for central breakout.
EXPECTED RESULT	1. Traffic should be sent to underlay using local breakout to internet/MPLS uplink. 2. Traffic from access branch should be sent to central hub branch or site or aggregation site for centralized internet access. 3. Post failure of local internet uplink on access site, traffic should be sent to central hub/aggregation site for internet breakout.
TEST RESULT	
REMARKS	

S. No.	64
TEST CASE NO.	3.4.1.10, 3.7.6.O
TEST PURPOSE	Support SD-WAN Site to MPLS legacy Site I. Local mode: An SD-WAN site shall directly access a traditional MPLS VPN in local Breakout mode. The CPE at the site functions as a CE and connects to the remote MPLS PE using a routing protocol such as BGP, OSPF, or a static routing protocol. II. Centralized mode: An SD-WAN site shall communicate with a traditional site through a centralized site. Hub sites, aggregation sites, and branch sites shall be used as centralized access points
TESTING DETAILS	
PROCEDURE	Proced re: 1. Connect a legacy non SDWAN site on traditional VPN. 2. Connect SDWAN branch on MPLS uplink and enable static route or dynamic protocol BGP/OSPF with MPLS PE. 3. Verify route to non SDWAN site is received from the PE or static route on CPE is installed. 4. Enable local mode on SD-WAN branch and send traffic between branches. 5. Disable local mode and connect a SDWAN gateway/Hub branch at centralized location. 6. Ensure connectivity of gateway/hub site with SDWAN and legacy branch both. 7. Send traffic between branches via centralized hub/aggregation/gateway site.
EXPECTED RESULT	1. Traffic between non SDWAN on traditional VPN and SDWAN site on same MPLS uplink should be allowed. Static or dynamic protocol on uplink should be configure to provide the reachability with traditional site in local mode 2. Traffic between non SDWAN on traditional VPN and SDWAN site on same MPLS uplink should be sent via centralized hub/aggregation/gateway site in centralized mode of deployment.
TEST RESULT	
REMARKS	

S. No.	65
TEST CASE NO.	3.4.1.11
TEST PURPOSE	Support multi–virtual network: each virtual network supports differentiated configuration of traffic policies, including Site to Site (S2S), site-to-legacy network, QoS, ACL, and path selection.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure a tenant/organisation on policy management engine. 2. Create atleast 2 VPNs in same tenant/organisation. 3. Create networks in VPNs. 4. Create unique policies, QoS, ACL and path selection rules in individual VPNs. 5. Verify networks and configurations are isolated from each other. 6. Verify configuration on controller and CPE.
EXPECTED RESULT	For an Enterprise/Tenant/organization multiple virtual networks should be supported and should be isolated from each other. Each VPN should have its own policies, Network, QoS, ACL and path selection configurations isolated from other.
TEST RESULT	
REMARKS	

S. No.	66
TEST CASE NO.	3.4.1.12.1, 3.5.5.1.A, 3.7.6.E
TEST PURPOSE	Overlay(Peering between the SDWAN edge and LAN device) : BGP/OSPF/ static routing shall be supported
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure a tenant/organisation on policy management engine. 2. Configure a overlay VPN service and respective network. 3. Connect a router on the LAN port of CPE. 4. Configure static or dynamic protocol with LAN router, BGP/OSPF. 5. Verify neighborship is up when dynamic protocol is used. 6. Advertise LAN routes from the router to CPE and verify routes are installed at CPE overlay. 7. Verify CPE overlay routes are advertised to LAN router.
EXPECTED RESULT	Routing on overlay with LAN router with BGP/OSPF/Static protocol should be supported. Routes received from Lan should be installed in overlay service.
TEST RESULT	
REMARKS	

S.No.	67
TEST CASE NO.	3.4.1.12.2
TEST PURPOSE	Underlay(Peering between the SDWAN edge and PE): The routes shall be BGP routes/ OSPF routes/ static routes
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure a tenant/organisation on policy management engine. 2. Configure a overlay VPN service and respective network. 3. Configure static or dynamic protocol on underlay uplink with PE router. 4. Verify neighborship is up when dynamic protocol is used. 5. Verify CPE overlay routes are advertised to underlay peering and further can be advertised to PE router.
EXPECTED RESULT	Routing on underlay with PE router using BGP/OSPF/Static protocol should be supported. Overlay Routes received of Lan should be advertised in underlay peering.
TEST RESULT	
REMARKS	

S.No.	68
TEST CASE NO.	3.4.1.12.3
TEST PURPOSE	Routing policy: The blacklist or whitelist shall be configured to filter overlay BGP routes. The blacklist or whitelist shall be configured to filter underlay BGP/ OSPF routes
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure a tenant/organisation on policy management engine. 2. Configure a overlay VPN service and respective network. 3. Connect a router on overlay LAN port and configure dynamic protocol BGP/OSPF with LAN router. 4. Configure static or dynamic protocol on underlay uplink with PE router. 5. Verify neighborship is up when dynamic protocol is used. 6. Configure and apply routing policies for selective route advertisement or to install selective route.
EXPECTED RESULT	Routing policies for selective route advertisement or to filter selective route in overlay as well as underlay should be supported. Route whitelisted in policies should only be installed or advertised.
TEST RESULT	
REMARKS	

S.No.	69
TEST CASE NO.	3.4.1.12.4
TEST PURPOSE	Adjustment of the priority of a routing protocol: The priority of an underlay BGP route, OSPF route, or static route shall be specified.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure a tenant/organisation on policy management engine. 2. Configure a overlay VPN service and respective network. 3. Configure dynamic protocol on underlay uplink with PE router. 4. Verify neighborship is up when dynamic protocol is used. 5. Configure option or policy to advertise routes with selective BGP attributes or OSPF metric. 6. Verify received routes at PE router un underlay.
EXPECTED RESULT	Adjustment of BGP attributes or OSPF metric should be supported.
TEST RESULT	
REMARKS	

S.No.	70
TEST CASE NO.	3.5.1.1
TEST PURPOSE	Single-site single-CPE (hub site or aggregation site) : The CPE supports two or more physical links.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a CPE with two or more physical links. 2. Atleast 2 uplinks ports should be available on CPE. 3. Verify connectivity with controllers are up.
EXPECTED RESULT	CPE should be connected to atleast two uplink ports and should be connected to controllers.
TEST RESULT	
REMARKS	

S.No.	71
TEST CASE NO.	3.5.1.2
TEST PURPOSE	Single-site dual-CPE (hub site or aggregation site) ： Each CPE supports two or more physical links. In the single-site dual-CPE scenario, a maximum of six physical links are supported
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect two CPEs on same branch each with its respective uplinks.
EXPECTED RESULT	Dual CPEs at a branch should support atleast 6 physical links.
TEST RESULT	
REMARKS	

S.No.	72
TEST CASE NO.	3.5.1.3
TEST PURPOSE	Dual-hub：In the dual-hub scenario, one or two CPEs shall be deployed at each hub site. Two hub sites work in active/standby mode
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 1 CPE at two hub sites. 2. Create network for respective hub sites on policy management engine. 3. Configure one hub site as active site and another as standby site. 4. Send traffic via active hub site and perform active hub failure. 5. Verify traffic is now sent via standby Hub site.
EXPECTED RESULT	Dual Hub sites should work in active/standby mode.
TEST RESULT	
REMARKS	

S.No.	73
TEST CASE NO.	3.5.1.4
TEST PURPOSE	Hierarchical VPN： branch-aggregation-hub mode is supported
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 2 Spoke and 1 Hub/Aggregation site. 2. Set the configuration to restrict direct traffic between spoke-1 with spoke-2 but between hub/Aggregation and spokes it should be allowed. 3. Verify traffic between spoke-1 to spoke-2 and spoke-1 & 2 to Hub/Aggregation site. 4. Traffic between spoke-1 and spoke-2 should be through the Hub/Aggregation site.
EXPECTED RESULT	Traffic between spoke to spoke should be via hub/aggregation.
TEST RESULT	
REMARKS	

S.No.	74
TEST CASE NO.	3.5.1.5
TEST PURPOSE	The SDWAN solution shall support hybrid links: Multiple access link combinations are supported: MPLS + MPLS, MPLS + Internet, and Internet + Internet, MPLS+LTE, etc
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a CPE with dual uplinks with below options: a. Link-1 = MPLS, Link-2 = MPLS b. Link-1 = MPLS, Link-2 = Internet c. Link-1 = Internet, Link-2 = Internet d. Link-1 = MPLS, Link-2 = LTE 2. Verify connectivity with controller in all scenarios.
EXPECTED RESULT	SDWAN should support hybrid uplinks and disjoint underlays. A combination of MPLS / Internet / LTE should be supported as uplink.
TEST RESULT	
REMARKS	

S.No.	75
TEST CASE NO.	3.5.1.6
TEST PURPOSE	The hub/CPE devices should be able to aggregate the bandwidth across multiple links e.g. in the event of a bulk transfer multiple links can be leveraged to provide more bandwidth and faster downloads
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a CPE with dual uplinks in Active/Active mode. 2. Configure ECMP mode to enable load balancing across multiple links. 3. Send multiple traffic flows between branches and verify flows are load balanced across multiple uplinks.
EXPECTED RESULT	Multiple flows should be load balanced across multiple uplinks.
TEST RESULT	
REMARKS	

S.No.	76
TEST CASE NO.	3.5.1.7
TEST PURPOSE	The WAN path selection at the branch site should failover/switch over/ shift over to the back up in near real time so as to maintain high availability of SDWAN solution
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a CPE with dual uplinks . 2. Send a traffic flow between branches and verify flow on WAN-1 3. Perform a failure of WAN-1 and verify traffic is shifted to WAN-2 automatically.
EXPECTED RESULT	Verify traffic is shifted to WAN-2 upon the failure of WAN-1
TEST RESULT	
REMARKS	

S.No.	77
TEST CASE NO.	3.5.2.A
TEST PURPOSE	The SD-WAN CPEs, vCPE's & uCPE's shall support 802.1Q on LAN and WAN interfaces BGP/OSPF on both LAN (for learning customer addresses) and WAN (for learning underlay addresses) interfaces Local IP breakout to underlay network, be it Internet or IPVPN
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. At least a Internet WAN uplink or IPVPN uplink. Procedure: 1. Configure SDWAN CPE WAN port and LAN port with 802.1Q encapsulation from policy management engine. 2. verify point to point IPs are reachable on LAN port as well as on WAN port with correct 802.1Q VLAN. 3. Connect a router on the LAN port of CPE. 4. Configure dynamic protocol with LAN router, BGP/OSPF. 5. Verify neighborship is up when dynamic protocol is used. 6. Verify CPE overlay routes are advertised to LAN router. 7. Configure local breakout at branch with NAT for forward the traffic to underlay. 8. Send traffic flow from overlay towards a destination in underlay. 9. Verify SRC-IP is NATTED with WAN interface IPs and routed through underlay
EXPECTED RESULT	Point to point IP on LAN and WAN interface should be reachable using correct 802.1Q VLAN. BGP / OSPF neighborship should be up on LAN side interface. Local IP breakout to underlay should be supported.
TEST RESULT	
REMARKS	

S.No.	78
TEST CASE NO.	3.5.2.B
TEST PURPOSE	SDWAN Edges (CPEs, vCPE's & uCPE's) shall support configurable IPv4 NAPT for traffic breaking out to the underlay on WAN interfaces.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure SDWAN CPE WAN port and LAN port with 802.1Q encapsulation from policy management engine. 2. verify point to point IPs are reachable on LAN port as well as on WAN port with correct 802.1Q VLAN.
EXPECTED RESULT	Point to point IP on LAN and WAN interface should be reachable using correct 802.1Q VLAN.
TEST RESULT	
REMARKS	

S.No.	79
TEST CASE NO.	3.5.2.C
TEST PURPOSE	Edges shall support configurable Ipv4 1:1 NAT on WAN interfaces for traffic breaking in / out to the underlay on WAN interfaces
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch with WAN interface. 2. Configure local breakout at branch with NAT for forward the traffic to underlay. 3. Send traffic flow from overlay towards a destination in underlay. 4. Verify SRC-IP is NATTED with WAN interface IPs and routed through underlay
EXPECTED RESULT	Traffic from overlay should be 1:1 Natted to underlay WAN interface and end to end reachable.
TEST RESULT	
REMARKS	

S.No.	80
TEST CASE NO.	3.5.2.D
TEST PURPOSE	Edges shall support configurable Ipv4 inbound port forwarding for traffic breaking in to the underlay on WAN interfaces.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch with WAN interface. 2. Configure local breakout at branch with NAT static port forward to map the specific port and private IP hosted in LAN to be reachable from internet/WAN. 3. Send traffic flow from Internet/WAN IP towards specific port and verify session to overlay host is getting opened. 4. Port forwarding is used to map traffic destined to public IP and port from remote location is NATTED and forwarded to private IP and respective port.
EXPECTED RESULT	Traffic from underlay should be Natted using static port forwarding to overlay.
TEST RESULT	
REMARKS	

S.No.	81
TEST CASE NO.	3.5.2.E, 3.10.8,
TEST PURPOSE	DSCP marking of traffic based upon at least 5 tuple policy
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch and create an overlay service. 2. Configure a QoS policy to mark the traffic flow on overlay service to selective DSCP value. 3. DSCP value marking should be done based on atleast 5 tuples i.e SRC PORT, DST PORT, SRC-IP, DST-IP, Protocol. 4. Apply QoS configuration. 5. Send overlay traffic between two branches and verify traffic flow is marked with respective DSCP value by CPE.
EXPECTED RESULT	DSCP marking should be done based on SRC-IP, DST-IP, SRC-PORT, DSTPORT, Protocol.
TEST RESULT	
REMARKS	

S. No.	82
TEST CASE NO.	3.5.2.F, 3.5.2.G, 3.10.10, 3.10.4, 3.10.9
TEST PURPOSE	The edge devices shall support classification of traffic into 8 forwarding classes The edge devices shall support at least 4 queues
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch and create an overlay service. 2. Configure a QoS policy to mark the traffic flow on overlay service to selective Forwarding class based on DSCP value or 5 tuples. 3. Map each traffic type with 8 Forwarding classes. 4. Configure 4 queues and respective rates of each individual queue. 5. Map 8 forwarding classes to 4 queues. 6. Send multiple traffic flows for each class and verify traffic is getting mapped to respective queues.
EXPECTED RESULT	Traffic should mapped to 8 forwarding classes and 4 queues.
TEST RESULT	
REMARKS	

S.No.	83
TEST CASE NO.	3.5.2.H, 3.10.6, 3.10.9
TEST PURPOSE	The edge devices shall support shaping of WAN/LAN egress traffic
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch and create an overlay service. 2. Configure a QoS policy to mark the traffic flow on overlay service to selective Forwarding class based on DSCP value or 5 tuples. 3. Map each traffic type with 8 Forwarding classes. 4. Configure 4 queues and respective rates of each individual queue. 5. Configure burst size for each individual queue. 6. Map 8 forwarding classes to 4 queues. 7. Apply QoS configuration on LAN and WAN egress port. 8. Send multiple traffic flows bursty in nature for each class and verify traffic is getting mapped to respective queues.
EXPECTED RESULT	Traffic should mapped to respective forwarding classes and queues and burst should be incorporated based on configured values.
TEST RESULT	
REMARKS	

S. No.	84
TEST CASE NO.	3.5.2.I, 3.10.7, 3.10.9
TEST PURPOSE	The edge devices shall support policing and packet filtering of ingress/egress traffic.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch and create an overlay service. 2. Configure QoS policy and rate limiter for queues. 3. Configure rate limiting/policing on LAN ingress port. 4. Map fc to respective queue and rate limit the queue. 5. Configure QoS/Queue/policer on egress port or WAN port. 6. Send excess traffic from LAN to WAN and verify respective policing is taken into effect. i.e no more than configured value should be forwarded.
EXPECTED RESULT	Traffic flows should be policed / filtered on ingress and egress ports.
TEST RESULT	
REMARKS	

S.No.	85
TEST CASE NO.	3.5.3.a
TEST PURPOSE	Dual CPE redundancy shall be supported using VRRP or BFD on LAN side of the network.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect two CPEs and respective uplinks on CPE. 2. Connect two CPEs to a switch on LAN side. 3. Create Master and Backup CPEs out of the dual CPE. 4. Verify one CPE is master and another is standby. 5. BFD or VRRP heartbeat is used between CPEs on LAN side for redundancy.
EXPECTED RESULT	Dual CPE supports redundancy using VRRP or BFD.
TEST RESULT	
REMARKS	

S.No.	86
TEST CASE NO.	3.5.3.B
TEST PURPOSE	The solution shall support using LTE links as the active and standby links for applications, if applicable
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect CPE using LTE uplink as primary. 2. Verify CPE is connected to controller using LTE uplink.
EXPECTED RESULT	CPE should support LTE uplink.
TEST RESULT	
REMARKS	

S.No.	87
TEST CASE NO.	3.5.3.C, 3.7.6.L, 3.13.13
TEST PURPOSE	CPE Uplink shall support Broadband as uplink with IpoE and PPPoE
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect the CPE with Broadband uplink. 2. Setting of uplink should be DHCP/Dynamic. 3. Verify CPE is connected to controller using Broadband uplink. 4. Reset the CPE from policy engine remotely and connect with broadband uplink of PPPoE dialer. 5. Set the username/password in settings/templates for PPPoE dialer. 6. Verify CPE is connected to controller using PPPoE Broadband uplink.
EXPECTED RESULT	CPE should support Broadband IPOE or PPPoE as uplink.
TEST RESULT	
REMARKS	

S.No.	88
TEST CASE NO.	3.5.3.D
TEST PURPOSE	The CPE shall support Ipv6 uplink with static or dynamic address allocation
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure the CPE uplink with static IPv6 address and gateway in template or keep the addressing as dynamic. 2. Connect the CPE uplink respectively. 3. Verify CPE is connected to controller using Ipv6 static or Dynamic addressing.
EXPECTED RESULT	CPE should support static or dynamic IPv6 on uplink.
TEST RESULT	
REMARKS	

S. No.	89
TEST CASE NO.	3.5.4.A, 3.7.6.G
TEST PURPOSE	Following WAN interface type shall be supported by the CPE: 1. Ethernet interfaces (XGE/GE/FE) 2. Ethernet sub-interfaces shall be used as WAN links. 3. 3G/LTE interfaces (3G or LTE) 4. xDSL interfaces (ADSL, VDSL, or G.SHDSL) (Optional for the purchaser)
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure CPE uplink with dot1q trunk VLAN on WAN interface in template. 2. Verify CPE is connected to controller using sub-interface / dot1q WAN interface.
EXPECTED RESULT	CPE should support ethernet interface of 10GE/GE/FE. CPE should be capable of setting up dot1q on WAN ethernet interface. CPE should be able to support 3G/LTE interface on uplink. xDSL interface (optional to test)
TEST RESULT	
REMARKS	

S. No.	90
TEST CASE NO.	3.5.5.1.B
TEST PURPOSE	Support wired network with Layer 2 devices connected, Layer 2 devices shall connect to the network through VLAN, VRRP or any other redundancy mechanism like Redundant Group configuration with failure detected by BFD
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect two CPEs and respective uplinks on CPE. 2. Connect two CPEs to a switch on LAN side. 3. Configure LAN port as dot1q and create VLAN for control/data traffic. 4. Create Master and Backup CPEs out of the dual CPE. 5. Verify one CPE is master and another is standby. 6. BFD or VRRP heartbeat is used between CPEs on LAN side for redundancy. 7. Perform failure and verify backup CPE becomes master.
EXPECTED RESULT	CPE should be connected to Layer-2 device using VLAN and VRRP or BFD heartbeat are passed through the switch for redundancy mechanism. One CPE should be master and another should be backup.
TEST RESULT	
REMARKS	

S. No.	91
TEST CASE NO.	3.5.5.1.C
TEST PURPOSE	Supports DHCP Server or DHCP relay.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure a LAN subnet and add the address range in subnet/DHCP server configuration on the policy engine. 2. Configure DHCP options optionally to provide DNS server etc. 3. Connect a laptop / DHCP client on the CPE LAN port and verify client is getting the dynamic IP from the local DHCP server of CPE and from the respective address range. 4. Disable the local DHCP configuration and configure a DHCP relay to external server in overlay. 5. Connect the laptop / DHCP client on CPE and verify client DHCP discover is relayed to external DHCP server. 6. Client is able to get the IP from external DHCP server.
EXPECTED RESULT	CPE should support local DHCP server or DHCP relay to external DHCP server for dynamic address allocation on LAN device.
TEST RESULT	
REMARKS	

S. No.	92
TEST CASE NO.	3.5.5.1. D, 3.5.5.1.E
TEST PURPOSE	Ethernet interfaces (GE/FE) support Support VLAN Tagging – 802.1 Q, 802.1 ad, QinQ (0x8100), QinQ and native
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify CPE Lan port is GE/FE. 2. Connect a device on LAN side with dot1Q VLAN and verify point to point ip is reachable. 3. Connect a device on Lan side with Null encapsulation and verify point to point IP is reachable.
EXPECTED RESULT	CPE should support GE or FE port on LAN.
TEST RESULT	
REMARKS	

S. No.	93
TEST CASE NO.	3.5.5.2. A
TEST PURPOSE	The Integrated AP function shall be enable on CPEs to allow terminal users to access networks through Wi-Fi
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect the WIFI capable CPE. 2. Create a overlay subnet for WIFI. 3. Connect a laptop on WIFI SSID and verify laptop is getting the dynamic IP. 4. Verify user is able to ping remote overlay subnet using WIFI on LAN side.
EXPECTED RESULT	CPE should support integrated AP function and user should be able to reach overlay remote subnet using wifi.
TEST RESULT	
REMARKS	

S. No.	94
TEST CASE NO.	3.5.5.2. B, C , D
TEST PURPOSE	CPE shall support at-least 4 SSID and around 10-30 users. Standard wireless securityWPA2 authentication modes should be supported The DHCP or DHCP relay function shall be enabled to assign IP addresses to Wi-Fi users
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure at-least 4 SSID on the policy engine for the CPE. 2. Standard wireless security WPA2 authentication modes should be supported. 3. Verify 4 SSIDs advertised and are available for connection. 4. Create a local subnet and address range for dynamic address allocation. 5. Optionally DHCP relay can be configured for IP address assignment on Lan side. 6. Connect a 10 to 30 laptop or wifi capable devices on any of the SSID and verify laptop is getting the dynamic IP. 7. Verify users can ping remote overlay subnet using WIFI on LAN side.
EXPECTED RESULT	CPE should support atleast 4 SSID and users should be able to reach remote overlay subnet using wifi. Standard authentication method WPA2 should be supported to authenticate LAN users.
TEST RESULT	
REMARKS	

S. No.	95
TEST CASE NO.	3.5.5.2. E
TEST PURPOSE	The CPE shall support enterprise specific Dual Band, Omni-Directional, External / internal Antenna options
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify CPE supports internal or external antenna for WiFi. 2. Configure the transmission @ 2.4 Ghz and 5 Ghz frequency.
EXPECTED RESULT	The CPE should support 2.4 Ghz and 5 Ghz Band. Antenna options should be internal or external to CPE
TEST RESULT	
REMARKS	

S. No.	96
TEST CASE NO.	3.5.5.2. F
TEST PURPOSE	Advanced Wi-Fi configuration shall be supported: (optional to the purchaser) • Wi-Fi AP configuration and Operations (Alarms & Stats) management using same management plane • Support click through captive portal for use case like display a webpage with use policy and Accept • Public and Private SSID with Internal captive portal and Pre-Shared Key respectively
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure at-least SSID on the policy engine for the CPE. 2. Configure captive portal and right to use policy. 3. Connect a user to WIFI SSID respectively and verify Captive portal page is displayed. 4. Once user accepts the policy then only he is able to browse.
EXPECTED RESULT	User should be displayed a captive portal webpage with right to use policy and accept button. Public and private SSID should be available.
TEST RESULT	
REMARKS	

S. No.	97
TEST CASE NO.	3.5.6. A, B, D, E
TEST PURPOSE	The solution shall support onboarding third party VNF on to the host CPE based on same SDWAN Management plane. VNF onboarding should be fully integrated automated management and provisioning The solution shall support lightweight VNF lifecycle management for instantiation/deletion of VM The solution shall support same management plane to provide resource monitoring and VNF health checkup
TESTING DETAILS	
PROCEDURE	Procedure: 1. Create VNF related parameters for resource eg image location/ VNF interfaces / CPU/ MEMORY etc from the management plane. 2. Select and map the VNF to the CPE on which the VNF to be onboarded. 3. Execute the VNF onboarding process from the management plane. 4. Verify VNF is up and running as virtual machine on the CPE. 5. Stop the VNF from the management plane and verify VNF is stopped on the CPE. 6. Restart the VNF from the management plane and verify VNF is restarted. 7. Verify VNF resources from the management plane.
EXPECTED RESULT	A third party VNF should be on boarded on the CPE from the management plane. VNF deletion, re-instantiation, start, stop should be supported from the management plane. VNF current status and resource usage from the management plane.
TEST RESULT	
REMARKS	

S. No.	98
TEST CASE NO.	3.5.6. C
TEST PURPOSE	The solution shall support service chaining using L2-L4 based policies through these VNF
TESTING DETAILS	
PROCEDURE	Procedure: 1. Create service chaining rules on the management plane using specific port or layer-3 subnet or layer-4 ports as match criteria. 2. Define service chaining end-points or targets towards firewall. 3. Send the selective traffic flow from the LAN side and verify traffic is sent form VNF. 4. Verify all other non-matching flows are not sent to VNF.
EXPECTED RESULT	Service chaining of traffic flow towards VNF should be supported based on defined polices.
TEST RESULT	
REMARKS	

S. No.	99
TEST CASE NO.	3.6.1
TEST PURPOSE	CPE Type 1 Specifications: 1. At least 4x100/1000 Ethernet interface (RJ45) 2. Full Duplex 10Mbps throughput expandable to 100Mbps with IPSec 3. 1x AC PSU, 4. LTE Uplink: 1 LTE support – On board SIM or USB for LTE dongle (Optional to the purchaser)
TESTING DETAILS	
PROCEDURE	Parameters to be verified: 1. CPE Type 1 Specifications: 2. At least 4x100/1000 Ethernet interface (RJ45) 3. Full Duplex 10Mbps throughput expandable to 100Mbps with IPSec 4. 1x AC PSU, 5. LTE Uplink: 1 LTE support – On board SIM or USB for LTE dongle (Optional to the purchaser).
EXPECTED RESULT	CPE Type-1 specs should be supported.
TEST RESULT	
REMARKS	

S. No.	100
TEST CASE NO.	3.6.2
TEST PURPOSE	CPE Type 2 Specifications: 1. 4x100/1000 Ethernet interface (RJ45) + 2x1G SFP port . 2. Full Duplex 50Mbps throughput expandable to 500Mbps with Ipsec 3. LTE Uplink: 1 LTE support – On board SIM or USB for LTE dongle(optional to purchaser) 4. 1x AC PSU
TESTING DETAILS	
PROCEDURE	Parameters to be verified: 1. 4x100/1000 Ethernet interface (RJ45) + 2x1G SFP port . 2. Full Duplex 50Mbps throughput expandable to 500Mbps with Ipsec 3. LTE Uplink: 1 LTE support – On board SIM or USB for LTE dongle(optional to purchaser) 4. 1x AC PSU
EXPECTED RESULT	CPE Type-2 specs should be supported.
TEST RESULT	
REMARKS	

S. No.	101
TEST CASE NO.	3.6.3
TEST PURPOSE	CPE Type 3 Specifications: 1. 4x100/1000 Ethernet interface (RJ45) + 2x1G SFP port . 2. Full Duplex 100Mbps throughput expandable to 1000Mbps with Ipsec 3. LTE Uplink: 1 LTE support – On board SIM or USB for LTE dongle(optional to purchaser) 4. 2x AC PSU
TESTING DETAILS	
PROCEDURE	Parameters to be verified: 1. 4x100/1000 Ethernet interface (RJ45) + 2x1G SFP port . 2. Full Duplex 100Mbps throughput expandable to 1000Mbps with Ipsec 3. LTE Uplink: 1 LTE support – On board SIM or USB for LTE dongle(optional to purchaser) 4. 2x AC PSU
EXPECTED RESULT	CPE Type-3 specs should be supported.
TEST RESULT	
REMARKS	

S. No.	102
TEST CASE NO.	3.6.4
TEST PURPOSE	CPE Type 4 Specifications: 1. 2x SFP+ 10GbE, 4 x1G SFP/Electrical ports 2. Full Duplex 500Mbps throughput expandable to 5000Mbps with Ipsec 3. 2x AC PSU,
TESTING DETAILS	
PROCEDURE	Parameters to be verified: 1. 2x SFP+ 10GbE, 4 x1G SFP/Electrical ports 2. Full Duplex 500Mbps throughput expandable to 5000Mbps with Ipsec 3. 2x AC PSU,
EXPECTED RESULT	CPE Type-4 specs should be supported.
TEST RESULT	
REMARKS	

S. No.	103
TEST CASE NO.	3.7.1 , 3.7.2, 3.7.3, 3.7.4, 3.7.5.H,3.7.5.I
TEST PURPOSE	The solution shall support Zero touch Provisioning the method could be one of the following: Email based, USB based, DHCP based. Deployment terminal type: PCs and mobile terminals (such as mobile phones and tablets) shall connect to CPEs through wired or wireless connections to deploy the CPEs. If multiple links are available, a CPE shall select the link that first goes Up to connect to the Controller. The Controller and site devices shall synchronize time from an external NTP server. Spoke nodes shall synchronize time from an NTP server or the hub site/management plane
TESTING DETAILS	
PROCEDURE	Procedure: 1. Provision templates on management plane and underlay parameters. 2. Send the information using email or download the same using USB. 3. Connect a laptop or PC to CPE Lan port with wire connection or wireless connection. Verify laptop gets the IP from CPE. 4. Connect dual uplinks on CPE. Ensure link-1 is primary and Link-2 is secondary. 5. Ensure both links are physically up but link-1 GW is unreachable. 6. Provision the CPE using the mail or USB data and verify CPE is connected to controller using secondary link. 7. CPE should be NTP sync with external server or controller or management plane.
EXPECTED RESULT	CPE should be provisioning using email or USB or DHCP. CPE should be able to connect to controller with available link/secondary link. CPE should be NTP sync.
TEST RESULT	
REMARKS	

S. No.	104
TEST CASE NO.	3.7.5.A
TEST PURPOSE	The Edge WAN link is provided with an IP address, netmask, default gateway and DNS server via DHCP, PPPoE, 3G/LTE or Static configuration
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect the CPE with Broadband uplink. 2. Setting of uplink should be DHCP/Dynamic. 3. Verify CPE is connected to controller using Broadband uplink. 4. Reset the CPE and connect with broadband uplink of PPPoE dialer. 5. Set the username/password in settings/templates for PPPoE dialer. 6. Verify CPE is connected to controller using PPPoE Broadband uplink. 7. Reset the CPE and connect with LTE sim or dongle on uplink. 8. Verify CPE is able to connect to controller using LTE uplink.
EXPECTED RESULT	The Edge WAN link bootstrapped with an IP address, netmask, default gateway and DNS server via DHCP, PPPoE, 3G/LTE or Static configuration on WAN side.
TEST RESULT	
REMARKS	

S. No.	105
TEST CASE NO.	3.7.5.B, 3.7.5.C, 3.7.5.h
TEST PURPOSE	The solution shall not require any off-site customer specific pre-staging / pre-configuration. The auto configuration system shall require secure mutual authentication of the SD-WAN controller and specific SD-WAN Edge
TESTING DETAILS	
PROCEDURE	Procedure: 1. Provision templates on central management plane and underlay parameters. 2. Send the information using email or download the same using USB. 3. Connect a laptop or PC to CPE Lan port with wire connection or wireless connection. Verify laptop gets the IP from CPE. 4. Connect CPE with uplink. 5. Provision the CPE using the mail or USB data and verify CPE is connected to controller. 6. Verify connection protocol between CPE and controller is encrypted.
EXPECTED RESULT	CPE should be able to connect to controller without any pre-staging or preconfiguration on CPE. CPE and controller connection should be encrypted.
TEST RESULT	
REMARKS	

S. No.	106
TEST CASE NO.	3.7.5.D 3.7.5.E, 3.9.1, 3.9.2
TEST PURPOSE	Individual SD-WAN Edges shall be identified by a unique key / certificate which is installed on to the Edge by the trusted installer at installation time by some simple but secure method requiring no or minimal manual data input. The SD-WAN Edges shall have a number of trusted third party certificate authority certificates (root Cas) pre-installed for use when authenticating the SD-WAN controller
TESTING DETAILS	
PROCEDURE	Procedure: 1. Generate certificates from CA. 2. Verify certificates are downloaded to CPE. 3. Verify openflow-tls connection is established using the correct certificates with controller.
EXPECTED RESULT	There should be pre-installed CA which should update the certificates on SDWAN edge for authentication with controller.
TEST RESULT	
REMARKS	

S. No.	107
TEST CASE NO.	3.7.5.F
TEST PURPOSE	There shall be a secure, industry recognized mechanism for checking and revoking root CA certificates.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Generate certificate from CA. 2. Revoke certificate from CA and verify revoked certificates used by CPE/Controller is authenticated. 3. Verify communication between CA and CPE/Controller is encrypted.
EXPECTED RESULT	CPE certificate authentication should be done over secure channel using standard protocols. Certificate authority should be able to revoke certificates.
TEST RESULT	
REMARKS	

S. No.	108
TEST CASE NO.	3.7.5.G
TEST PURPOSE	The URL of the SD-WAN controller shall not be pre-installed in the Edge and shall be provided at installation time by the trusted installer.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Ensure two controllers are present. 2. Provision templates on central management plane and Controller-1 details. 3. Send the information using email or download the same using USB. 4. Connect a laptop or PC to CPE Lan port with wire connection or wireless connection. Verify laptop gets the IP from CPE. 5. Connect CPE with uplink. 6. Verify no CPE is managed by controllers. 7. Provision the CPE using the mail or USB data and verify CPE is connected to controller-1 only.
EXPECTED RESULT	CPE should be able to connect to controller-1 only after the correct information provided by installer.
TEST RESULT	
REMARKS	

S. No.	109
TEST CASE NO.	3.7.5.J
TEST PURPOSE	The solution shall operate when the Edge devices are behind NAT (NAT-T).
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect minimum two CPEs behind a NAT device. 2. Provision templates on central management plane. 3. Send the information using email or download the same using USB. 4. Connect a laptop or PC to CPE Lan port with wire connection or wireless connection. Verify laptop gets the IP from CPE. 5. Connect CPEs with uplink (behind NAT) 6. Provision the CPE using the mail or USB data and verify CPE is connected to controller. 7. verify CPEs can send data plane traffic between each other.
EXPECTED RESULT	CPEs should be able to connect to controller and send traffic between each other.
TEST RESULT	
REMARKS	

S. No.	110
TEST CASE NO.	3.7.5.K
TEST PURPOSE	The solution shall support hybrid branches which have a WAN connection to an MPLS IP VPN and a second WAN connection to the internet.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 2 CPE branches with dual uplinks on MPLS underlay uplink and internet underlay uplink respectively. 2. Verify CPEs are connected to respective controllers. 3. Send traffic between branches.
EXPECTED RESULT	Traffic between branches are sent using
TEST RESULT	
REMARKS	

S. No.	111
TEST CASE NO.	3.7.5.I
TEST PURPOSE	When deployed with a mix of hybrid Edges, IP VPN connect Edges and Internet connected Edges, Edges will continue to be able to communicate under asymmetric break conditions as long as all sites have at least one active connection
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 2 CPE branches only on MPLS underlay uplink and another few branches only on internet underlay uplink. 2. Verify CPEs are connected to respective controllers. 3. Send traffic between branches using gateway.
EXPECTED RESULT	Branches only on internet should be able to send traffic to sites only on MPLS
TEST RESULT	
REMARKS	

S. No.	112
TEST CASE NO.	3.7.6 A, 3.7.6.H, 3.7.6.K, 3.7.6.N, 3.9.9, 3.9.10
TEST PURPOSE	The each SD-WAN edge device shall dynamically establish fully meshed encrypted overlay paths to every other edge device, across multiple different WAN services: L3VPN MPLS, Internet and Cellular Data connectivity (3G/4G).
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 2 CPE branches only on MPLS underlay uplink and internet uplink. 2. Verify CPEs are connected to respective controllers. 3. Configure a Layer-3 VRF between sites. 4. Send traffic without encryption. 5. Enable encryption on layer-3 VRF 6. Send traffic between branches with encryption.
EXPECTED RESULT	Full mesh traffic between CPEs should be IPSEC encrypted.
TEST RESULT	
REMARKS	

S. No.	113
TEST CASE NO.	3.7.6.D, 3.7.6.I, 3.7.6,J, 3.7.6.N, 3.7.6.P
TEST PURPOSE	The overlay services layer3 VPN/L2 VPN and Ethernet Services – P2P layer2 VPNs, P2MP layer2VPNs, MP2MP layer2VPNs. (optional to the purchaser) The solution shall support Multiple independent overlay services per Edge, with independent routing tables (allowing overlapping addressing) separated on the LAN side via different ports or different port + VLAN combinations The overlay paths established amongst the edge devices shall support: Transport of unicast, multicast, and broadcast traffic The solution shall support a set of distinct networks for a single Tenant. The solution shall allow to dynamically add and remove services as required
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 2 CPE branches 2. Verify CPEs are connected to respective controllers. 3. Configure atleast two Layer-3 VRF between sites. 4. Configure atleast two layer-2 VPNs between sites. 5. Configure overlapping IPs in different VPNs. 6. Verify each VRF routing table is separated from each other and overlapping up address can be used. 7. Configure unique IP network with a single layer-3 VPN and verify overlapping IP address is not allowed within same VPN. 8. Send unicast, broadcast and multicast traffic between sites. 9. Remove a layer-2 and a layer-3 VPN service from the policy engine. Verify services are removed dynamically from the CPE.
EXPECTED RESULT	Layer-2 and Layer-3 VPN services should be configured on edge device and overlapping address space should be allowed in each VRF. VRF routing table should be sperate. Overlapping IP address should not be allowed in same Layer-3 VRF. Overlay services should be dynamically removed from the policy engine.
TEST RESULT	
REMARKS	

S. No.	114
TEST CASE NO.	3.7.6.F
TEST PURPOSE	The local users in each of the branch offices must be able to access Internet directly without going through the HO.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect CPE with internet uplink. 2. Provision the CPE and ensure connectivity with controller. 3. Enable Network Address translation. 4. Verify Internet access and traffic is sent to internet from the CPE directly.
EXPECTED RESULT	Local User should be able to access internet from the CPE internet uplink.
TEST RESULT	
REMARKS	

S. No.	115
TEST CASE NO.	3.7.6. K, 3.12.8
TEST PURPOSE	The solution may support controller less operation for atleast 24 hours in case the connectivity to SDN controller is lost. This capability is required to maintain high availability(HA) of SDWAN solution
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast two CPEs with atleast one uplink. 2. Configure a controller less operation from the policy engine for atleast 24 hours or to a test value. 3. Disconnect the CPE from controller by simulating network failure. 4. Verify traffic between CPEs are still forwarded and CPE is now running in controller mode operation.
EXPECTED RESULT	CPE should continue forwarding of traffic in case of disconnection with controller to a configured time period.
TEST RESULT	
REMARKS	

S. No.	116
TEST CASE NO.	3.7.6.M
TEST PURPOSE	The solution shall support multiple Tenant networks isolated from one another.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Create at least 2 enterprise tenant or organisations on policy management plane and verify same is getting reflected on SDWAN controller. 2. Verify both organisations are isolated from each other. 3. Connect CPEs on respective organisations and verify they are not able to reach each other. 4. Remove Services from the management plane and verify same is removed from controller as well as CPE.
EXPECTED RESULT	Both CPEs should not be able to communicate to each other.
TEST RESULT	
REMARKS	

S. No.	117
TEST CASE NO.	3.7.6. Q
TEST PURPOSE	Edge devices must be able to load-balance traffic across multiple WAN paths based on load balancing algorithms efficiently using all available WAN bandwidth.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast two CPEs with dual uplinks. 2. Configure both uplinks are Active/Active. 3. Send multiple different flows from Lan. 4. Verify flows are load balanced on dual uplinks.
EXPECTED RESULT	CPE should load balance traffic on multiple uplinks.
TEST RESULT	
REMARKS	

S. No.	118
TEST CASE NO.	3.7.6. T, 3.10.3
TEST PURPOSE	The solution must be able to prioritize real time traffic over other traffic
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch and create an overlay service. 2. Configure a QoS policy to mark the traffic flow on overlay service to selective Forwarding class based on DSCP value or 5 tuples. 3. Map each traffic type with priority FC and queue. 4. configure queue Rates. 6. send a high priority traffic and a Best effort traffic flow and verify real time traffic flow is prioritized over best effort traffic.
EXPECTED RESULT	Real time traffic should be prioritized and drops should be seen on best effort traffic only.
TEST RESULT	
REMARKS	

S. No.	119
TEST CASE NO.	3.8.1, 3.8.2
TEST PURPOSE	DPI Functionality. Application identification based on Layer-7 signatures. Custom application identification based on L3-L4 and TCP/UDP parameters.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect CPE with internet uplink and enable network address translations. 2. Enable DPI and browse internet from laptop on LAN. 3. Verify Applications are detected and displayed in reports. 4. Create custom application using L3 to L4 parameters and verify traffic is identified in custom application.
EXPECTED RESULT	Internet Application should be identified using L7 signatures and Custom application based on L3-L4 parameters. Reports should show the DPI traffic.
TEST RESULT	
REMARKS	

S. No.	120
TEST CASE NO.	3.8.(3-10) 3.7.6.R, 3.7.6.S
TEST PURPOSE	Application Aware routing with Sla Aware Routing.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect two CPEs with dual uplinks with Active/Standby respectively. 2. configure custom policies/rules to define at least two applications. 3. Configure atleast two applications between branches. 4. Define primary path for each individual application. 5. Define acceptable SLA parameters: Latency, Jitter and packet loss. 6. In normal condition verify APP-1 is going through link-1 and APP-2 is going through link-2 7. Insert Latency on link-1 and verify application is shifted to other link-2. 8. Remove latency and verify traffic is shifted back to link-1 9. Repeat step 7 and 8 for jitter and packet loss as well. 10. Repeat step-7-9 for Link-2 as well.
EXPECTED RESULT	Overlay traffic APP-1 traffic should be sent via Link-1 and APP-2 traffic should be sent via Link-2. Traffic should be shifted from link-1 to link-2 based on SLA violation and vice versa.
TEST RESULT	
REMARKS	

S. No.	121
TEST CASE NO.	3.9.5
TEST PURPOSE	URL blacklist and URL whitelist are to be supported.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify a url is getting opened to user behind CPE. 2. Configure a policy to block web domain/url. 3. Verify web domain is getting blocked. 4. Whitelist the url or remove the policy. 5. Verify web domain is getting opened.
EXPECTED RESULT	URL blacklist and whitelist should be supported.
TEST RESULT	
REMARKS	

S. No.	122
TEST CASE NO.	3.9.7, 3.9.8,3.9.9, 3.9.10
TEST PURPOSE	Encryption for Layer-3 and Layer-2 Overlay Services.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 3 CPE branches. 2. Verify CPEs are connected to respective controllers. 3. Configure a Layer-3 VRF between sites. 4. Send traffic without encryption. 5. Enable encryption on layer-3 VRF 6. Send traffic between branches with encryption. 7. Configure a layer-2 service between sites. 8. Send traffic without encryption. 9. Enable encryption on layer-2 service and verify traffic is encrypted between sites.
EXPECTED RESULT	Full mesh Layer-2 and layer-3 overlay traffic between CPEs should be IPSEC encrypted.
TEST RESULT	
REMARKS	

S. No.	123
TEST CASE NO.	3.9.13
TEST PURPOSE	The solution shall support Interop with IKEv2 platforms
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a CPE at one branch. 2. Connect a router which supports ipsec IKEv2 3. Configure IKEv2 between CPE and router. 4. Verify tunnel is established.
EXPECTED RESULT	IKEv2 tunnel should be established with router.
TEST RESULT	
REMARKS	

S. No.	124
TEST CASE NO.	3.9.11
TEST PURPOSE	It should be possible to set a key-rotation timer defining a maximum duration any particular key or set of keys shall be used for data plane encryption (not applicable in case of external PKI).
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 3 CPE branches. 2. Verify CPEs are connected to respective controllers. 3. Configure a Layer-3 VRF between sites. 4. Send traffic without encryption. 5. Enable encryption on layer-3 VRF 6. Send traffic between branches with encryption. 7. Set the refresh timer for keys used for encryption.
EXPECTED RESULT	Keys should be refreshed based on timer expiry.
TEST RESULT	
REMARKS	

S. No.	125
TEST CASE NO.	3.9.14
TEST PURPOSE	The encryption shall be done as per Ipsec standards using AES with 128-bit keys or higher coupled with Internet Key Exchange Version 2 (IKEv2).
TESTING DETAILS	
PROCEDURE	Procedure: 1. Verify IPSEC encryption supports AES 128 bit or higher.
EXPECTED RESULT	IPSEC encryption should use AES 128 bit or higher.
TEST RESULT	
REMARKS	

S. No.	126
TEST CASE NO.	3.9.16
TEST PURPOSE	The solution must support L7 application firewall and VRFs to allow for network isolation
TESTING DETAILS	
PROCEDURE	Procedure: 1. Create atleast 2 VRFs within same enterprise. 2. Create layer-3 subnets in each VRFs. 3. Create 2 VRFs on same CPE. 4. Verify subnets are isolated form each other and have different routing table on controller as well as CPE. 5. Configure a policy rule to drop an application based on layer-7 signature. 6. Configure a policy rule to drop GMAIL traffic but allow all other internet traffic on VRF-1. 7. All traffic in VRF-2 should be allowed.
EXPECTED RESULT	VRF-1 and VRF-2 should be isolated from each other and should have separate routing table. Layer-7 filtering capabilities should be supported on CPE and per VRF
TEST RESULT	
REMARKS	

S. No.	127
TEST CASE NO.	3.9.17
TEST PURPOSE	The solution shall support Stateful ACL/Firewall
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect atleast 2 CPEs. 2. Create a stateful ACL/Firewall rule. 3. Send traffic between branches and verify specific state is maintained on CPE.
EXPECTED RESULT	Stateful ACL/Firewall should be supported.
TEST RESULT	
REMARKS	

S. No.	128
TEST CASE NO.	3.9.18
TEST PURPOSE	The solution shall support Security analytics for SD-WAN through Traffic Visibility, Analytics and Dynamic Security Automation. The solution shall support at least below security features: • Real-time alerts of traffic analytics • Automatic policy reconfiguration • Automatic action when crossing monitoring thresholds like Quarantine an end-point. Redirect Traffic to a perimeter IDS/IPS
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Connect atleast 2 CPEs. 2. Management plane and analytics engine should be configured. Procedure: 1. Send multiple flows / traffic between branches. 2. Verify flows can be seen on analytics engine/portal. 3. Configure Threshold alerts / parameters for specific bytes/packets. 4. Send traffic higher then the threshold set and verify alert is generated. 5. Configure rule to quarantine the end-point based on threshold breached. 6. Configure rule to redirect traffic to a firewall.
EXPECTED RESULT	Near Real time analytics should be supported. Automatic policy configuration based on monitoring threshold should be supported. Traffic should be redirected to FW based on threshold breech.
TEST RESULT	
REMARKS	

S. No.	129
TEST CASE NO.	3.9.25, 3.9.26, 3.9.27, 3.9.28
TEST PURPOSE	1. Reports & raise alerts based on ACL allow/deny hits vs. Time 2. Reports & raise alerts based on ACL allow/deny hits by source 3. Reports & raise alerts based on ACL allow/deny hits by destination 4. Reports & raise alerts based TCP conn vs. Time
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Connect atleast 2 CPEs. 2. Management plane and analytics engine should be configured. Procedure: 1. Send multiple flows / traffic between branches. 2. Verify flows can be seen on analytics engine/portal. 3. Configure ACL to allow or deny traffic based on source. 4. Configure another ACL to allow or deny traffic based on destination. 5. Send TCP flow using specified source. 6. Verify reports of ACL hits. 7. Send TCP flow using specified destination. 8. Verify reports of ACL hits.
EXPECTED RESULT	Reports should be available based on allow/deny rule for a ACL entry. Reports should be available based on specific ACL rule to allow/deny by source. Reports should be available based on specific ACL rule to allow/deny by destination. Reports should be available based on TCP vs Time.
TEST RESULT	
REMARKS	

S. No.	130
TEST CASE NO.	3.9.29, 3.9.30
TEST PURPOSE	The solution shall support integration with Cloud Security Platform like Zscaler to provide cloud-based security stack to secure internet breakout traffic The solution shall support software defined policies to selectively send traffic Cloud Security platform.
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Zscaler subscription should be available. Procedure: 1. Configure CPE and establish IPSEC with Zscaler gateway node. 2. Configure policy to send traffic to internet via Zscaler gateway. 3. Verify traffic is sent via Zscaler. 4. Configure policy to specify specific office365 application via Zscalar and remaining internet traffic should go directly. 5. Verify only office 365 traffic is sent by Zscalar GW.
EXPECTED RESULT	Selective traffic should be sent by Zscalar gateway node.
TEST RESULT	
REMARKS	

S. No.	131
TEST CASE NO.	3.10.11, 3.10.12
TEST PURPOSE	The solution shall support DSCP and CoS remarking for the uplink outer tunnel header are modified based on Remarking Policies to allow you to redefine forwarding class assignments per uplink based on a user-defined mapping table. The solution shall support Inner packet markings from the LAN side are not modified.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch and create an overlay service. 2. Configure a QoS policy to classify the traffic by DSCP value to a specific forwarding class. 3. Configure egress qos policy to remark the tunnel encapsulation header with specific DSCP /COS value. 4. Apply QoS configuration. 5. Send overlay traffic between two branches and verify tunnel header of flow is marked with respective DSCP value by CPE. However inner head marking is untouched.
EXPECTED RESULT	DSCP and COS remarking for outer tunnel header should be supported. Inner packet header DSCP values are not modified.
TEST RESULT	
REMARKS	

S. No.	132
TEST CASE NO.	3.10.13
TEST PURPOSE	The solution shall support Egress queuing, traffic is assigned to four egress queues based on its forwarding class with one queue is based on strict priority queuing and three are based
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a branch and create an overlay service. 2. Configure a QoS policy to mark the traffic flow on overlay service to selective Forwarding class based on DSCP value or 5 tuples. 3. Map each traffic type with 8 Forwarding classes. 4. Configure 4 queues and respective rates of each individual queue. 5. Configure one queue with strict priority and remaining 3 queues as WRR. 6. Map 8 forwarding classes to 4 queues. 7. Send multiple traffic flows for each class and verify traffic is getting mapped to respective queues.
EXPECTED RESULT	Traffic should mapped to 8 forwarding classes and 4 queues. One queue should be strict priority and other three should be WRR
TEST RESULT	
REMARKS	

S. No.	133
TEST CASE NO.	3.12.1, 3.12.2
TEST PURPOSE	Multiple links of a single CPE are required to provide back up to each other.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect two CPEs with dual uplinks active/standby respectively. 2. Perform a failure of link-1 and verify traffic between branches are sent using link-2
EXPECTED RESULT	CPE should support link level reundnacy.
TEST RESULT	
REMARKS	

S. No.	134
TEST CASE NO.	3.12.3, 3.12.6
TEST PURPOSE	Dual CPE redundancy
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a CPE as branch01 with respective uplink and user on LAN. 2. Connect dual CPEs as branch02 on same site and respective uplinks on CPE. 3. Connect two CPEs to a switch on LAN side. 4. Create Master and Backup CPEs out of the dual CPE. 5. Verify one CPE is master and another is standby. 6. Send traffic between branch01 and branch02 and verify traffic is sent only via uplink of branch-01. 7. Perform failure of CPE01 of branch-02 uplink and verify traffic is sent via uplink of CPE02 branch-02. 8. Restore failure 9. Configure both CPEs for Active/Active uplinks. 10. Send multiple flows and verify flows are load balanced on CPE-01 uplink and CPE-02 uplink of Branch-02.
EXPECTED RESULT	Dual CPE redundancy with active/standby uplink and active/active uplink.
TEST RESULT	
REMARKS	

S. No.	135
TEST CASE NO.	3.12.4
TEST PURPOSE	In the dual-CPE scenario, the CPEs (at a hub site, an aggregation site, or a spoke site) function as the active and standby gateways for the intranet through OSPF.
TESTING DETAILS	
PROCEDURE	Procedure: 1. Connect a CPE as branch01 with respective uplink and user on LAN. 2. Connect dual CPEs as branch02 on same site and respective uplinks on CPE. 3. Connect two CPEs to a switch on LAN side. 4. Create Master and Backup CPEs out of the dual CPE. 5. Verify one CPE is master and another is standby. 6. Connect a router to lan switch and establish OSPF between router and CPE. 7. Send and receive routes from OSPF in overlay.
EXPECTED RESULT	OSPF should be established with Lan router and routes should be learned.
TEST RESULT	
REMARKS	

S. No.	136
TEST CASE NO.	3.13.15,3.13.23
TEST PURPOSE	The Controller should provide the ping function to diagnose the connectivity of overlay and underlay networks.
TESTING DETAILS	
PROCEDURE	Procedure. 1. Configure a overlay ping configuration from the policy engine/ controller. 2. Execute overlay service ping from the policy engine and verify response. 3.
EXPECTED RESULT	Overlay Ping should be supported from centralized policy engine.
TEST RESULT	
REMARKS	

S. No.	137
TEST CASE NO.	3.13.22
TEST PURPOSE	System should also support forwarding syslog messages to end Enterprise hosted primary and optionally secondary Syslog server
TESTING DETAILS	
PROCEDURE	Procedure. 1. Configure syslog servers to specific enterprise. 2. Ensure syslog servers are reachable in overlay VRF to specific organisation only. 3. Send traps and verify logs are sent to syslog server.
EXPECTED RESULT	Overlay syslog server configuration should be supported for specific organization.
TEST RESULT	
REMARKS	

S. No.	138
TEST CASE NO.	3.13.25
TEST PURPOSE	The Orchestrator/management should provide ARP table dump, Route table dump, tech support logs for the CPE device without the requirement of logging into the CLI of device
TESTING DETAILS	
PROCEDURE	Procedure. 1. Execute route-table command from controller to verify routing table of CPE. 2. Execute ARP/mac-table commands from controller to verify arp table of CPE. 3. Verify all commands are executed from controller/policy engine without logging in to the CPE.
EXPECTED RESULT	CPE logs and route-table should be executed from central policy engine/controller without logging into the CPE.
TEST RESULT	
REMARKS	

S. No.	139
TEST CASE NO.	3.14.A,B,E,F
TEST PURPOSE	The SDWAN solution shall support at least 100 Tenants/ Enterprises The SDWAN solution shall support at least 10K SDWAN CPEs The solution shall support at least 1K SDWAN CPEs in a single VRF. The SDWAN CPE shall support at least 1K IPSec tunnels simultaneously
TESTING DETAILS	
PROCEDURE	Prerequisite: 1. Policy Management engine, Controller must be deployed. Procedure: 1. Configure 100 Organisation/Enterprises on policy management engine. 2. Connect 1K CPE in a single organisation in single VRF. 3. Configure 10K CPEs in total combined all organisations/enterprise. 4. Verify VRF on CPE and Controller as well 5. enable full mesh IPSEC between a organisation which has 1K CPEs. 6. Verify random encrypted traffic flow between sites.
EXPECTED RESULT	The SDWAN solution shall support at least 100 Tenants/ Enterprises The SDWAN solution shall support at least 10K SDWAN CPEs The solution shall support at least 1K SDWAN CPEs in a single VRF The SDWAN CPE shall support at least 1K IPSec tunnels simultaneously
TEST RESULT	
REMARKS	

S. No.	140
TEST CASE NO.	3.14.C
TEST PURPOSE	The SDWAN solution shall support at least 15K VRFs
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure organisations and configure multiple VRFs in each organisation with a total sum of 15K VRFs
EXPECTED RESULT	The SDWAN solution shall support at least 15K VRFs
TEST RESULT	
REMARKS	

S. No.	141
TEST CASE NO.	3.14.D
TEST PURPOSE	The solution shall support 10 VRFs (Micro-VPNs) per SDWAN CPE
TESTING DETAILS	
PROCEDURE	Procedure: 1. Configure a Organisation and create 10 VRFs in same organisation. 2. Map the VRFs to a CPE. 3. Verify VRFs are created on CPE
EXPECTED RESULT	The solution shall support 10 VRFs (Micro-VPNs) per SDWAN CPE
TEST RESULT	
REMARKS	

S. No.	142
TEST CASE NO.	3.14.G
TEST PURPOSE	The SDWAN CPE shall support at least 10K Routes
TESTING DETAILS	
PROCEDURE	Procedure: 1. Bootstrap CPEs 2. Generate 10K routes in overlay domain. 3. Verify 10K routes are installed on CPE as well as on controller.
EXPECTED RESULT	The SDWAN CPE shall support at least 10K Routes
TEST RESULT	
REMARKS	

S. No.	143
TEST CASE NO.	3.14.H,I,J,K
TEST PURPOSE	The SDWAN Gateway shall be multi-tenant and support at least 50 Tenants / Enterprises The SDWAN Gateway shall support at least 5K SDWAN CPEs simultaneously The SDWAN Gateway shall support at least 32K Routes The SDWAN Gateway shall be available as a software function with throughout upto 1Gbps
TESTING DETAILS	
PROCEDURE	Procedure: 1. Bootstrap a SDWAN gateway device and connect it with 50 organisations. 2. Connect 5K CPEs with SDWAN gateway. 3. Generate 32K routes in total for SDWAN gateway and verify routes are installed on Gateway and controller. 4. Send traffic from SDWAN gateway to CPE of 1Gbps.
EXPECTED RESULT	The SDWAN Gateway shall be multi-tenant and support at least 50 Tenants / Enterprises The SDWAN Gateway shall support at least 5K SDWAN CPEs simultaneously The SDWAN Gateway shall support at least 32K Routes The SDWAN Gateway shall be available as a software function with throughout upto 1Gbps
TEST RESULT	
REMARKS	

Template for submitting Comments on draft Test Guide "Software Defined Wide Area Network"

(Draft Test Guide No. TEC 49161:2026)

Name of Manufacturer/Stakeholder:

Organization:

Contact details:

Clause No.	Clause	Comments	Justification for Proposed change

The comments in above format may be submitted via Email to diri.tec@nic.in and adic1.tec@gov.in