Test Results Summary for IOS XE SD-WAN for Japan (Release Version 20.13.1/17.13.1)

First Published: 2023-12-21

Last Modified: 2023-12-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Overview

Cisco IOS XE SD-WAN

Cisco SD-WAN IOS XE test , an integral part of the enterprise solution, is a program that validates various Cisco IOS XE SD-WAN devices. This is achieved by testing the latest versions of Cisco IOS XE SD-WAN devices.

Cisco IOS XE SD-WAN devices for Japan , in turn is an add-on testing at the solution level, where the requirements gathered are specific to Japanese usage and market.

The requirements are derived based on the following:

- New features in SDWAN 20.13.1 - IOS XE 17.13.1
- High priority scenarios and basic regression features

The test execution is carried out on selected Cisco IOS XE SD-WAN devices, which affect the Japanese segment that are prioritized by Cisco Japan team.

The following Products and Applications are covered in the test execution:

- Cisco vManage,vBond,vSmart
- ESXi Host 7.0
- Cisco Catalyst 8300
- Cisco Catalyst 8200
- Cisco Catalyst 8500L
- Cisco Catalyst 8500
- Cisco ISR 4461
- Cisco Catalyst 9K PoE Switch
- Cisco Catalyst 1111-8P

Acronyms

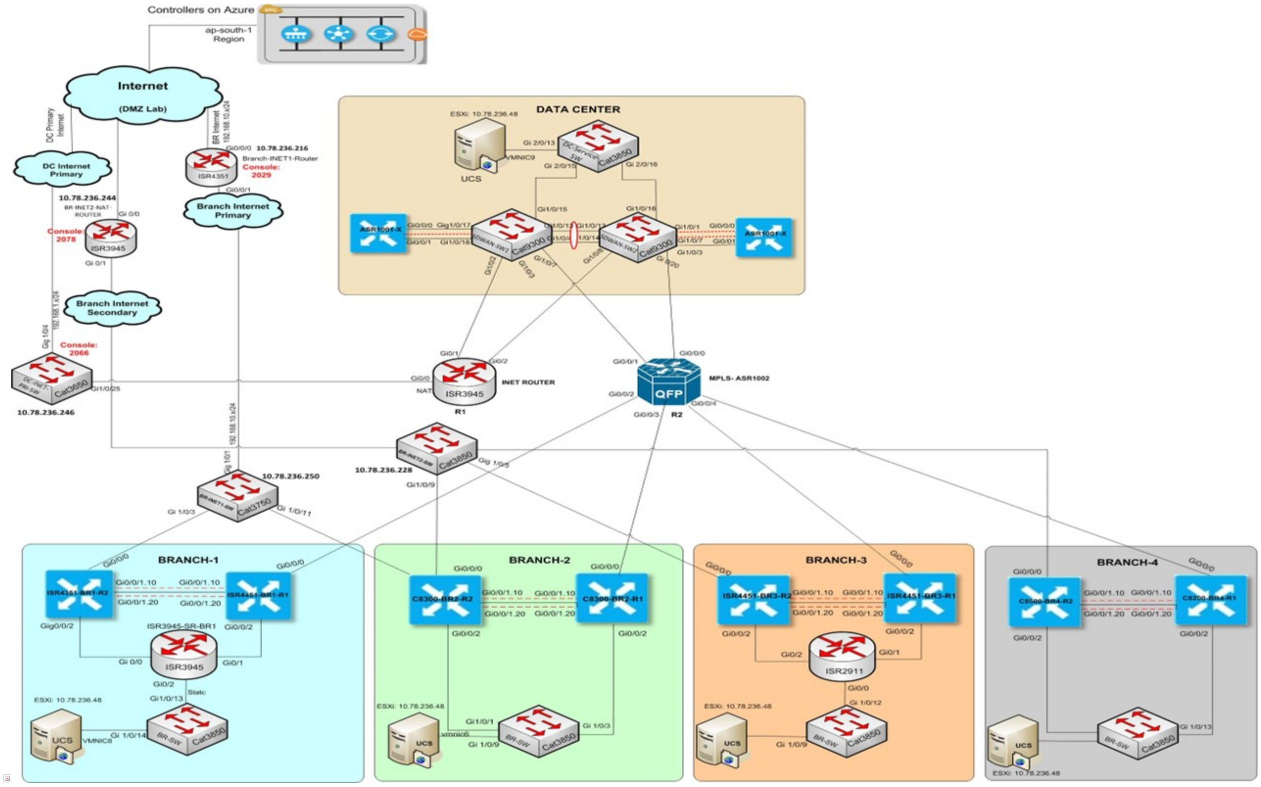
Acronym	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Address-family
API	Application Programming Interface
ASN	Autonomous System Number
ASR	Aggregation Services Routers
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BR	Branch

BR Site	Branch Site
CA	Certificate Authority
CDF	Cloud Delivered Firewall
cEdge Router	Cisco Edge Router
Cisco DNA	Cisco Digital Network Architecture
Config	Configuration
Config-t	Configuration-transaction
COM Port	Communication Port
CoR	Cloud on Ramp
CLI	Command Line
CSP	Cisco Cloud Services Platform
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
DIA	Direct Internet Access
DR	Disaster Recovery
DSCP	Differentiated Services Code Point
Dst	Destination
EF	Expedited Forwarding
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
FW	Firewall
GUI	Graphical User Interface
GW Site	Gate Way Site
GRE	Generic Routing Encapsulation
HA	High Availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IMIX	Internet Mix
INET	Internet
IOS	Internetworking Operating System
IPS	Intrusion prevention system

ISR	Integrated Services Routers
LAN	Local Area Network
MAN	Metropolitan Area Network
MPLS	Multi-Protocol Label Switching
ISE	Identity Services Engine
MTU	Maximum transmission unit
NA	Not Applicable
NAT	Network Address Translation
NTP	Network Time Protocol
NIC	Network Interface Card
OMP	Overlay Management Protocol
OSPF	Open Shortest Path First
O365	Office 365
PAT	Port Address Translation
PnP	Plug and Play

Test topology and Environment Matrix

Test Topology



Component Matrix

Applications	Category	Component	Version
Controller Network	Virtual Network	vBond	20.13.1
		vManage	20.13.1
		vSmart	20.13.1
	Switch	Cat 9K PoE	17.3
Communications Infrastructure	IOS XE SDWAN	C8300, C8200,C8500 & C8500L	17.13.1
		ISR4461	17.13.1
UCS	UCSC-C240-M5SX	ESXi Host	7.0, 7.5
Client	Operating System	End point	Windows 11
	Browsers	Mozilla	122.0.1
		Chrome	122.0.6261.29

What's New ?

SDWAN 20.13.1 - IOS XE 17.13.1 Solution testing

- ICMP Endpoint Tracker for NAT DIA for IPv4 or IPv6 Interfaces
- Support for the TLS 1.3 Protocol for Cisco Catalyst SD-WAN Control Connections
- vManage support for autonomus mode: Phase2
- Support for Centralized Data Policy for NAT66 DIA
- IPv6 Support in Cisco SD-WAN Manager UI Troubleshooting
- Dataplane serviceability Improvements(EPC,packet-trace) fro IPsec running(Crypto OFFLOAD)
- Port-channel support on transport side for link redundance and BW aggregation
- Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager
- SR CFD

Open Caveats

CDETS ID	TITLE
CSCwh398647	Credentials for Cisco Smart Account Save Button is Not working.
CSCwh42373	Smart Account Credentials When I Enabled its throwing error like "Client timed out " its take 60 ses.
CSCwh43416	When we Enabled PMT Credential by proper credential its showing "Client timed out" its take 60sec
CSCwh74524	vManage page is getting hung while user trying to review the device cli configuration
CSCwh89180	ISR4461 Platform can't able to download the PKI Certificates from vManage
CSCwh92524	Can't Able to Attach Service Chain Configuration due to vManage loading issue.
CSCwh66772	Unable to generated link for JSON and CSV File format when we Export.
CSCwh75845	Tunnel status showing up but unable to ping the tunnel ip address
CSCwh89503	Unable to Enabled Cloud Services in Vmanage Due to Error occurred while connecting Analytics server
CSCwh90585	Cloud Services Setting its Shows Save Successfully While Analytics Disabled ,But its not Enabled
CSCwh76837	SDWAN ipsec - Not able to change the ipsec transform set encryption algorithm from ah to esp
CSCwh75756	Unable to generate Admin-tech file in vmanage
CSCwh92610	Troubleshooting options drop-down is persisting on other page.
CSCwh68229	show run int Tunnel is not showing the tunnel mode ipsec ipv4/v6
CSCwh48420	Enabled Data Stream for transport in Hostname text taken Ip address only its accepted 0.0.0.0
CSCwh51955	SD-WAN Router Interface Details under Service Chain Configurations is accepting Junk characters
CSCwh69794	Router Details were not Retrieved and displaying as no data available.
CSCwh71151	Menu options were overlaid on the Previewing Device CLI Configurations

CSCwh62891	Log are not generating after shutdown the wan interface with tracker
CSCwh62921	Getting incorrect log message for adding tracker in the loopback interface.
CSCwh44587	Option missing from drop down under service chain definition.
CSCwh51728	Wrong "User Name" & password accepted for UTD Snort Subscriber Signature for Download
CSCwh48560	Cancel Button is working like reset button its not Canceled all panel in Administrator settings.
CSCwh56248	Enablement of the Controller-managed mode facilitates with the sd-routing
CSCwh89692	Menu Labelling are not visible
CSCwh64505	Overlapping of ipv6 address occurring in traceroute.
CSCwh64494	In Speedtest, Up bandwidth option is missing under table setting.
CSCwh64590	Accepting invalid value for count in Advanced options for ping.
CSCwh63006	Unable to Configure maximum payload size in ipv6 troubleshooting as per given hint
CSCwh92804	Path is invisible while navigating into troubleshooting page
CSCwh92905	Troubleshooting drop-down is misleading the page by greying out the Incorrect options.
CSCwh92929	Options(Yes/No) were merged while Dissociating a Profile under Configuration Group.
CSCwh89127	Having issue with UI dashboard - Not showing the report and explore name
CSCwh73967	Ipsec reply window size is not changeable for site to site vpn in cat8k platform
CSCwh37584	No Options were displayed in Menu, If created a new custom user access.
CSCwh47134	Unable to Save application priority & SLA for interface drop-down list
CSCwh89671	Can't Able to Dissociate any of the Profile's under Configuration Group
CSCwh49676	Navigation Menu is overlaid on the Config Page and causing inconvenience to the user.
CSCwh68093	IPV4 Subnet Mask drop-down options are floating and vManage is getting feezed in Firefox Browser

Resolved Caveats

CDETS ID	TITLE
CSCwh29887	Can't Able to set custom time to retrieve the DPI Stats at specific time.
CSCwh51819	Service Chain Configurations under Service Fabric UI page behaviour is faulty.
CSCwh35820	Users and Access Page options under Administration are Misleading.
CSCwh68229	show run int Tunnel is not showing the tunnel mode ipsec ipv4/v6
CSCwh51167	Feature Profiles header page under Configuration is misleading.

New Features

ICMP Endpoint Tracker for NAT DIA for IPv4 or IPv6 Interfaces

Logical ID	Title	Description	Status	Defect ID
ENJ.NAT.20.13.1_17.13.1_N01	To configure the ipv4 interface-icmp endpoint-ip tracker and check the CLI.	To create ipv4 icmp endpoint tracker and check the cli status+C4:C28	Passed	
ENJ.NAT.20.13.1_17.13.1_N02	To configure the ipv6 interface-icmp endpoint-ip tracker and check the CLI.	To create ipv6 icmp endpoint tracker and check the cli status	Passed	
ENJ.NAT.20.13.1_17.13.1_N03	To configure the ipv4 interface-icmp endpoint-dns and check the CLI.	To create ipv4 icmp endpoint tracker with dns and check the cli status	Passed	
ENJ.NAT.20.13.1_17.13.1_N04	To configure the ipv6 interface-icmp endpoint-dns and check the CLI.	To create ipv6 icmp endpoint tracker with dns and check the cli status	Passed	
ENJ.NAT.20.13.1_17.13.1_N05	To configure the endpoint tracker group for mixed ipv4(icmp and http) and check the status.	Create mixed ipv4 endpoint tracker group and check the status	Passed	
ENJ.NAT.20.13.1_17.13.1_N06	To configure the endpoint tracker group for mixed ipv4 and check the CLI.	Create mixed ipv4 endpoint tracker group and check the status	Passed	
ENJ.NAT.20.13.1_17.13.1_N07	To configure the endpoint tracker group for mixed ipv6(icmp and http) and check the status.	Create mixed ipv6 endpoint tracker group and check the status	Passed	

ENJ.NAT.20.13.1_17.13.1_N08	To configure the endpoint tracker group for mixed ipv6 and check the CLI.	Create mixed ipv4 endpoint tracker group and check the status for ipv6 interface	Passed	
ENJ.NAT.20.13.1_17.13.1_N09	To flap the interface and check the functionality of tracker for endpoint-ip(ipv4).	Shut and un shut the ipv4 interface when icmp tracker is attached	Failed	CSCwh62891
ENJ.NAT.20.13.1_17.13.1_N10	Reboot the cEdge device and check the tracker functionality.	Create the endpoint tracker and check the status after reboot the device	Passed	
ENJ.NAT.20.13.1_17.13.1_N11	To view and check the sla summary after attaching the icmp and http tracker to interface.	To create ipv4 icmp endpoint tracker and check the sla summary in the cli	Passed	
ENJ.NAT.20.13.1_17.13.1_N12	To apply both ipv6 and ipv4 tracker for dual stack DIA interface and check status.	To configure dual stack DIA interface for both ipv6 and ipv4 and check status	Passed	
ENJ.NAT.20.13.1_17.13.1_N13	To configure the ipv4 interface-icmp endpoint-ip tracker and check the CLI-add on template.	To create ipv4 icmp endpoint tracker and check the cli status	Passed	
ENJ.NAT.20.13.1_17.13.1_N14	To configure the ipv4 interface-icmp endpoint-dns tracker and check the CLI-add on template.	To create ipv4 icmp endpoint tracker and check the cli status	Passed	

ENJ.NAT.20.13.1_17.13.1_N15	To configure the endpoint tracker group for mixed ipv4(icmp and http) with Boolean AND check the status.	To create endpoint tracker group with Boolean and for icmp ipv4	Passed	
ENJ.NAT.20.13.1_17.13.1_N16	To configure the endpoint tracker group for mixed ipv6(icmp and http) with Boolean AND check the status.	To create endpoint tracker group with Boolean and for icmp ipv6	Passed	
ENJ.NAT.20.13.1_17.13.1_N17	To Configure the interval period to icmp prob tracker and check the failover times.	To Configure the interval period to icmp prob tracker and check the failover times.	Passed	
ENJ.NAT.20.13.1_17.13.1_N18	To check and verify the tracker timeout latency threshold configuration using cli.	To check and verify the tracker timeout latency threshold configuration using cli.	Passed	
ENJ.NAT.20.13.1_17.13.1_N19	To configure the ipv4 interface-icmp endpoint-ip tracker using vManage configuration group.	To configure the ipv4 interface-icmp endpoint-ip tracker using vManage configuration group.	Passed	
ENJ.NAT.20.13.1_17.13.1_N20	To configure the ipv4 interface-icmp endpoint-dns tracker using vManage configuration group	To configure the ipv4 interface-icmp endpoint-dns tracker using vManage configuration group	Passed	

ENJ.NAT.20.13.1_17.13.1_N21	To configure the endpoint tracker group for mixed ipv4(icmp and http) and check the status using vManage configuration group.	To configure the endpoint tracker group for mixed ipv4(icmp and http) and check the status using vManage configuration group.	Passed	
ENJ.NAT.20.13.1_17.13.1_N22	To configure the ipv4 interface-icmp endpoint-ip tracker and check tracker status in vManage.	To configure the ipv4 interface-icmp endpoint-ip tracker and check tracker status in vManage.	Passed	
ENJ.NAT.20.13.1_17.13.1_N23	To configure the ipv6 interface-icmp endpoint-ip tracker using vManage configuration group.	To configure the ipv6 interface-icmp endpoint-ip tracker using vManage configuration group.	Passed	
ENJ.NAT.20.13.1_17.13.1_N24	Attach the ipv4 endpoint-ip tracker to the loopback interface and check the behaviors.	Attach the ipv4 endpoint-ip tracker to the loopback interface and check the behaviour.	Failed	CSCwh62921
ENJ.NAT.20.13.1_17.13.1_N25	To configure the ipv4 interface-icmp endpoint-ip tracker and check the CLI.	To create ipv4 icmp endpoint tracker and check the cli status	Passed	

Support for the TLS 1.3 Protocol for Cisco Catalyst SD-WAN Control Connections

Logical ID	Title	Description	Status	Defect ID
ENJ.TLS.20.13.1_17.13.1_N01	To verify that the TLS handshake and encryption mechanisms are functioning correctly in the SD-WAN environment.	To test the TLS Handshake and Encryption	passed	
ENJ.TLS.20.13.1_17.13.1_N02	To Verify that the TLS cipher suits mechanisms are functioning correctly in the SDWAN Environment.	To test the TLS cipher suits	passed	
ENJ.TLS.20.13.1_17.13.1_N03	To validate the Certificate of vSmarts and vManage, during the TLS handshake process	To test the Certificate Validation	passed	
ENJ.TLS.20.13.1_17.13.1_N04	To ensure proper validation of TLS certificate in the SDWAN environment.	To test the Certificate Validation	passed	
ENJ.TLS.20.13.1_17.13.1_N05	Fresh bring up using new TLS 1.3 Cipher. verify the new ciphers are present and control connections, bfd and OMP are all up	To test the TLS 1.3 Cipher on the fresh set up and verify logs	passed	
ENJ.TLS.20.13.1_17.13.1_N06	Check the time taken for the controls to come back up when rebooting the vSmart	To test session resumption functionality to optimize TLS connection establishment.	passed	

ENJ.TLS.20.13.1_17.13.1_N07	To verify that load balancing and failover mechanisms work seamlessly with TLS connections.	To verify that load balancing and failover mechanisms work seamlessly with TLS connections.	passed	
ENJ.TLS.20.13.1_17.13.1_N08	To ensure compatibility with various TLS 1.3 & TLS 1.2 Respectively	To verify support for different TLS protocol versions.	passed	
ENJ.TLS.20.13.1_17.13.1_N09	To ensure that TLS connections recover gracefully after network disruptions and outages.	To ensure that TLS connections recover gracefully after network disruptions and outages.	passed	
ENJ.TLS.20.13.1_17.13.1_N010	To verify that TLS 1.3 connections adhere to the SD-WAN's defined policies with respect to QOS.	To verify the pushing the data policy from vManage to cEdge for QOS.	passed	
ENJ.TLS.20.13.1_17.13.1_N011	To verify that TLS 1.3 connections adhere to the SD-WAN's defined policies with respect to DPI.	To verify the pushing the data policy from vManage to cEdge for DPI.	passed	
ENJ.TLS.20.13.1_17.13.1_N012	To verify the SDWAN system's ability to handle certificate revocation.	To verify the SD-WAN system's ability to handle certificate renewal and revocation.	passed	
ENJ.TLS.20.13.1_17.13.1_N013	To verify the SDWAN system's ability to handle certificate renewal.	To verify the SD-WAN system's ability to handle certificate renewal	passed	

ENJ.TLS.20.13.1_17.13.1_N014	To ensure that proper logs and monitoring mechanisms are in place for TLS related activity.	To ensure that proper logs and monitoring mechanisms are in place for TLS-related activities.	passed	
ENJ.TLS.20.13.1_17.13.1_N015	To evaluate the behavior of TLS connections under stress and over extended periods	To evaluate the behaviour of TLS connections under stress and over extended periods.	passed	
ENJ.TLS.20.13.1_17.13.1_N016	To evaluate the behavior of TLS connections under stress and over extended periods	To evaluate the behaviour of TLS connections under stress and over extended periods.	passed	
ENJ.TLS.20.13.1_17.13.1_N017	To test the SD-WAN's ability to gracefully terminate active TLS connections during an emergency shutdown.	To test the SD-WAN's ability to gracefully terminate active TLS connections during an emergency shutdown.	passed	
ENJ.TLS.20.13.1_17.13.1_N018	To validate that the SD-WAN system handles TLS-related errors gracefully and provides appropriate notifications.	To validate that the SD-WAN system handles TLS-related errors gracefully and provides appropriate notifications.	passed	
ENJ.TLS.20.13.1_17.13.1_N019	To verify the proper Termination and clean up of TLS session.	To validate session termination works as expected.	passed	
ENJ.TLS.20.13.1_17.13.1_N020	Shutdown vManage and check the logs	To validate session termination works as expected.	passed	

vManage support for autonomous mode: Phase2

Logical ID	Title	Description	Status	Defect ID
ENJ.Aut.20.13.1_17.13.1_N01	Configure the control connections in autonomous mode whether the devices are behind NAT	Check the control connections in autonomous mode whether the devices are behind NAT	Failed	CSCwh48560
ENJ.Aut.20.13.1_17.13.1_N02	Configure and enable autonomous mode in vManage check the site health and application health	Check the autonomous mode in vManage check the site health and application health	Passed	
ENJ.Aut.20.13.1_17.13.1_N03	Check and verify the Tunnel health in autonomous mode using Vmanage	Check the Tunnel health in autonomous mode using Vmanage	Passed	
ENJ.Aut.20.13.1_17.13.1_N04	Check and verify the BFD session and control connection using Vmanage	verify the BFD session and control connection using Vmanage	Passed	
ENJ.Aut.20.13.1_17.13.1_N05	Configure the Tunnel health and verify in Vmanage autonomous mode without BFD Sessions	verify the BFD session and control connection using Vmanage with Tunnel health	Passed	
ENJ.Aut.20.13.1_17.13.1_N06	Check and verify the top application widget when NetFlow is supported in autonomous	verify the top application widget when NetFlow is supported in autonomous	Passed	
ENJ.Aut.20.13.1_17.13.1_N07	Configure the Control connection in autonomous and check the BFD session	verify the BFD session and control connection using Vmanage	Passed	

ENJ.Aut.20.13.1_17.13.1_N08	Check and verify the Packet Capture via Ping the internet using vManage in non sdwan device	verify Packet Capture via Ping the internet using Vmanage in non sdwan device	Passed	
ENJ.Aut.20.13.1_17.13.1_N09	Check and verify the Speed test using vManage in non sdwan device	verify Speed test using vManage in non sdwan device	Passed	
ENJ.Aut.20.13.1_17.13.1_N10	Check and verify the Trace route using vManage in non sdwan device	verify Trace route using vManage in non sdwan device	Passed	
ENJ.Aut.20.13.1_17.13.1_N11	Configure the autonomous mode in devices check and verify the security page with no changes in vmanage.	verify the Configure the autonomous mode in devices and verify the security page with no changes in vmanage.	Passed	
ENJ.Aut.20.13.1_17.13.1_N12	Check and verify the Real Time operational support in phase 2	Verify the the Real Time operational support in phase 2	Passed	
ENJ.Aut.20.13.1_17.13.1_N13	Configure the required certificates verify the notification in autonomous mode in supported dives	Verify the Real Time operational support in phase 2	Passed	
ENJ.Aut.20.13.1_17.13.1_N14	Check control connection with information from data packets or through Only transport IP addresses	Verify the control connection with information from data packets or through Only transport IP addresses	Passed	
ENJ.Aut.20.13.1_17.13.1_N15	Check the interface connectivity whether it will be notification.	Verify the interface connectivity whether it will be notification.	Passed	

ENJ.Aut.20.13.1_17.13.1_N16	Verify the behavior of a router by Disabling & Enabling Controller-Managed.	Verify the router by Disabling & Enabling Controller-Managed.	Passed	
ENJ.Aut.20.13.1_17.13.1_N17	User MUST be able to retrieve logs, core-file, admin-tech for C8KV devices from vManage	Verify the router by Disabling & Enabling Controller-Managed.	Passed	
ENJ.Aut.20.13.1_17.13.1_N18	Verify installed image detail via vManage	Verify installed image detail via vManage	Passed	
ENJ.Aut.20.13.1_17.13.1_N19	To Verify control connections should come up after validating router in vManage GUI.	Check control connections should come up after validating router in vManage GUI.	Passed	
ENJ.Aut.20.13.1_17.13.1_N20	Configure and verify the autonomous mode in C8500 device in sdwan router	Check and verify the autonomous mode in C8500 device in sdwan router	Passed	
ENJ.Aut.20.13.1_17.13.1_N21	Configure and verify the autonomous mode in ISR1k device in sdwan router	Check and verify the autonomous mode in ISR1k device in sdwan router	Passed	
ENJ.Aut.20.13.1_17.13.1_N22	Configure the multiple WAN interface and check the control connection in vmanage and devices	Check the multiple WAN interface and check the control connection in vmanage and devices	Passed	
ENJ.Aut.20.13.1_17.13.1_N23	Check and verify the NetFlow will be support in vmanage with autonomous mode	Check and verify the NetFlow will be support in vmanage with autonomous mode	Passed	

ENJ.Aut.20.13.1_17.13.1_N24	Check and verify the management widget will be supported with autonomous mode in vManage	Check the management widget will be supported with autonomous mode in vManage	Passed	

Support for Centralized Data Policy for NAT66 DIA

Logical ID	Title	Description	Status	Defect ID
ENJ.NAT66.20.13.1_17.13.1_N001	Configure Edge router connected to Single DIA for IPv6 internet access with SLAAC	To Configure Single DIA using SLAAC	passed	
ENJ.NAT66.20.13.1_17.13.1_N002	Configure Edge router connected to two/multiple DIA for IPv6 internet access with SLAAC	To Configure two/multiple DIA using SLAAC	passed	
ENJ.NAT66.20.13.1_17.13.1_N003	Configure NAT66 with inside source prefix will be supported for single interfaces for RA SLACC	To Configure NAT66 with inside source prefix and verify	passed	
ENJ.NAT66.20.13.1_17.13.1_N004	Configure NAT66 with inside source prefix will be supported for multiple interfaces for RA SLACC	To Configure NAT66 with inside source prefix and verify	passed	
ENJ.NAT66.20.13.1_17.13.1_N005	Configure NAT66 for the VPN interface template using Feature template in vManage	To Configure NAT66 with inside source prefix and verify with vManage Feature template	passed	
ENJ.NAT66.20.13.1_17.13.1_N006	Configure NAT66 for the VPN interface template using ux2.0(Configuration Group) vManage	To Configure NAT66 with inside source prefix and verify with vManage ux2.0 template	passed	
ENJ.NAT66.20.13.1_17.13.1_N007	Verify the SLAAC EUI-64 addressing on service side hosts - Extended Unique Identifier	To Configure SLAAC EUI-64 address on service side host	passed	

ENJ.NAT66.20.13.1_17.13.1_N008	Verify the nat66 ipv6 DIA for non sdwan Vrf -aware software infrastructure (vasi) with bgp	To Configure Nat66 with no sdwan using vasi with bgp	passed	
ENJ.NAT66.20.13.1_17.13.1_N009	Verify the nat66 ipv6 DIA using static route for non sdwan	To Configure Nat66 with no sdwan using static route	passed	
ENJ.NAT66.20.13.1_17.13.1_N010	configure NAT66 IPv6 DIA Flow stickiness support for data policy and try to enable(by default)/disable	To Configure NAT66 IPv6 DIA Flow stickiness to to record the flow level state of the NAT path	passed	
ENJ.NAT66.20.13.1_17.13.1_N011	Configure data policy for IPV6 NAT66 DIA with Source data prefix using vManage	To Configure NAT66 IPv6 DIA with source data prefix	passed	
ENJ.NAT66.20.13.1_17.13.1_N012	Configure data policy for IPV6 NAT66 DIA with Destination data prefix using vManage	To Configure NAT66 IPv6 DIA with Destination data prefix	passed	
ENJ.NAT66.20.13.1_17.13.1_N013	Configure data policy for IPV6 NAT66 DIA with Source data prefix & Destination port using vManage	To Configure NAT66 IPv6 DIA with Source data prefix & Destination port	passed	
ENJ.NAT66.20.13.1_17.13.1_N014	Configure data policy for IPV6 NAT66 DIA with Destination data prefix & Source port using vManage	To Configure NAT66 IPv6 DIA with Destination data prefix & Source port	passed	

ENJ.NAT66.20.13.1_17.13.1_N015	Configure data policy for IPV6 NAT66 DIA with Custom application Source data prefix using vManage	To Configure NAT66 IPv6 DIA with Custom application Source data prefix	passed	
ENJ.NAT66.20.13.1_17.13.1_N016	Configure data policy for IPV6 NAT66 DIA with Application & Destination data prefix using vManage	To Configure NAT66 IPv6 DIA with Application & Destination data prefix	passed	
ENJ.NAT66.20.13.1_17.13.1_N017	Configure data policy for IPV6 NAT66 DIA with Application family & Destination data prefix using vManage	To Configure NAT66 IPv6 DIA with Application family & Destination data prefix	passed	
ENJ.NAT66.20.13.1_17.13.1_N018	Configure data policy for IPV6 NAT66 DIA with Application family & Destination/Source data & port number prefix using CLI	To Configure NAT66 IPv6 DIA with Application family & Destination/Source data & port number prefix using CLI	passed	
ENJ.NAT66.20.13.1_17.13.1_N019	Configure data policy for IPV4/IPV6 NAT66 DIA with Custom application Source data prefix using vManage with dual stack enabled	To Configure NAT66 IPv6 DIA with source data Custom application Source data prefix using vManage with dual stack enabled	passed	

ENJ.NAT66.20.13.1_17.13.1_N020	Configure data policy for IPV4/IPV6 NAT66 DIA with Application & Destination data prefix using vManage with dual stack enabled	To Configure NAT66 IPv6 DIA with Application & Destination data prefix using vManage with dual stack enabled	passed	
ENJ.NAT66.20.13.1_17.13.1_N021	Configure data policy for IPV4/IPV6 NAT66 DIA with Application family & Destination data prefix using vManage with dual stack enabled	To Configure NAT66 IPv6 DIA with Application family & Destination data prefix using vManage with dual stack enabled	passed	
ENJ.NAT66.20.13.1_17.13.1_N022	Configure data policy for IPV4/IPV6 NAT66 DIA with Application family & Destination/Source data & port number prefix using CLI with dual stack enabled	To Configure NAT66 IPv6 DIA with Application family & Destination/Source data & port number prefix using CLI with dual stack enabled	passed	
ENJ.NAT66.20.13.1_17.13.1_N023	Configure data policy for IPV6 NAT66 DIA with Source data prefix using vManage with NAT Fallback	To Configure NAT66 IPv6 DIA with Source data prefix using vManage with NAT Fallback	passed	
ENJ.NAT66.20.13.1_17.13.1_N024	Configure data policy for IPV6 NAT66 DIA with Destination data prefix using vManage with NAT Fallback	To Configure NAT66 IPv6 DIA with Destination data prefix using vManage with NAT Fallback	passed	

ENJ.NAT66.20.13.1_17.13.1_N025	Configure data policy for IPV6 NAT66 DIA with Source data prefix & Destination port using vManage with NAT Fallback	To Configure NAT66 IPv6 DIA with source data prefix & Destination port using vManage with NAT Fallback	passed	
ENJ.NAT66.20.13.1_17.13.1_N026	Configure data policy for IPV6 NAT66 DIA with Destination data prefix & Source port using vManage with NAT Fallback	To Configure NAT66 IPv6 DIA with Destination data prefix & Source port using vManage with NAT Fallback	passed	
ENJ.NAT66.20.13.1_17.13.1_N027	Configure data policy for IPV6 NAT66 DIA with Custom application Source data prefix using vManage with NAT Fallback	To Configure NAT66 IPv6 DIA with Custom application Source data prefix using vManage with NAT Fallback	passed	
ENJ.NAT66.20.13.1_17.13.1_N028	Configure data policy for IPV6 NAT66 DIA with Application & Destination data prefix using vManage with NAT Fallback	To Configure NAT66 IPv6 DIA with Application & Destination data prefix using vManage with NAT Fallback	passed	
ENJ.NAT66.20.13.1_17.13.1_N029	Configure data policy for IPV6 NAT66 DIA with Application family & Destination data prefix using vManage with NAT Fallback	To Configure NAT66 IPv6 DIA with Application family & Destination data prefix using vManage with NAT Fallback	passed	

ENJ.NAT66.20.13.1_17.13.1_N030	Configure data policy for IPV6 NAT66 DIA with Application family & Destination/Source data & port number prefix using CLI with NAT Fallback	To Configure NAT66 IPv6 DIA with Application family & Destination/Source data & port number prefix using CLI with NAT Fallback	passed	

IPv6 Support in Cisco SD-WAN Manager UI Troubleshooting

Logical ID	Title	Description	Status	Defect ID
ENJ. IPV6.20.13.1_17.13.1_ N.01	To create an IPv6 Ping on cEdge with VPN 0	Creating a ping for cEdge using ipv6 ping with vpn 0	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.02	To check the packet summary for ipv6 ping on cEdge when destination is unreachable.	To verify the packet summary ,when the destination used for ipv6 ping on cEdge is unreachable.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.03	To check the packet summary for IPv6 Ping on cEdge in service VPN.	To verify the packet summary ,when performed an ipv6 ping on cEdge with service VPN	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.04	To perform the IPv6 Ping for local address on cEdge in VPN 0	To verify the packet summary ,when performed an ipv6 ping on cEdge in VPN 0 using local address .	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.05	To perform the IPv6 Ping for local address on cEdge in Service VPN.	To verify the packet summary ,when performed an ipv6 ping on cEdge in VPN 1 using local address .	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.06	To create IPv6 Ping with TCP/UDP probe on cEdge in VPN 0	To check the working of ipv6 ping on cEdge in VPN 0 with TCP/UDP probe in vManage.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.07	To create IPv6 Ping with TCP/UDP probe on cEdge in Service VPN .	To check the working of ipv6 ping on cEdge in Service VPN with TCP/UDP probe in vManage.	passed	

ENJ. IPV6.20.13.1_17.13.1_ N.08	To verify IPv6 Ping with advanced options on cEdge in VPN 0	To check IPv6 ping with advanced options and to verify the packet summary on cEdge with VPN 0.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.09	To verify IPv6 Ping with advanced options on cEdge in Service VPN .	To check IPv6 ping with advanced options and to verify the packet summary on cEdge with VPN 1.	Failed	CSCwh64590 ,CSCwh63660
ENJ. IPV6.20.13.1_17.13.1_ N.10	To monitor IPv6 traceroute on cEdge in VPN 0	To create an IPv6 traceroute on cEdge in VPN0 and check whether the trace path obtained is correct or not.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.11	To monitor IPv6 traceroute on cEdge in Service VPN .	To create an IPv6 traceroute on cEdge in VPN1 and check whether the trace path obtained is correct or not.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.12	To monitor IPv6 traceroute local address on cEdge in VPN 0	To create an an IPv6 traceroute with local address on cEdge in VPN0 and check whether the trace path obtained is correct or not.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.13	IPv6 traceroute with advanced options on cEdge in VPN 0	To create an IPv6 traceroute for vpn1 with advanced options and check the trace path.	Failed	CSCwh64505
ENJ. IPV6.20.13.1_17.13.1_ N.14	IPv6 traceroute with advanced options on cEdge in Service VPN	To create an IPv6 traceroute for service vpn with advanced options and check the trace path.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.15	To perform IPv6 packet capture and Speed test cEdge in VPN 0	To check the packet capture on cEdge in VPN0 with IPv6 Troubleshooting.	Failed	CSCwh64494

ENJ. IPV6.20.13.1_17.13.1_ N.16	To perform IPv6 packet capture on cEdge in Service VPN.	To check the packet capture on cEdge in VPN1 with IPv6 Troubleshooting.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.17	Packet capture for IPv6 with filter on cEdge in VPN 0.	To check the packet capture on cEdge in VPN1 with IPv6 by using filter in Troubleshooting.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.18	To configure IPv6 Radius/TACACS configuration on cEdge	To check and verify the configuration of IPv6 Radius/TACACS configuration on cEdge	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.19	To Ping IPv6 on controllers	To check and verify the ping results performed with ipv6 on controllers.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.20	To Ping IPv6 local address on controllers	To create a Ping IPv6 local address on controllers	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.21	To create IPv6 Ping with TCP/UDP probe on controllers	To check and verify the ping results on controllers with TCP/UDP probe type.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.22	To perform IPv6 Ping with advanced options on controllers	To check IPv6 ping with advanced options and to verify the packet summary on controllers.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.23	IPv6 traceroute on controllers	To check and verify the trace path for the controllers while performing the trace route in troubleshooting.	passed	
ENJ. IPV6.20.13.1_17.13.1_ N.24	IPv6 traceroute with advanced options on controllers	To check and verify the IPv6 traceroute with advanced options on controllers	passed	

ENJ. IPV6.20.13.1_17.13.1_N.25	To check the simulate flows on cEdge in VPN0 with IPv6 Troubleshooting.	To configure IPv6 Radius/TACACS configuration on controllers	passed	

Data plane serviceability Improvements(EPC,packet-trace) fro IPsec running(Crypto OFFLOAD)

Logical ID	Title	Description	Status	Defect ID
ENJ.DP.20.13.1_17.13.1_N001	Configure ipsec with Basic traffic encryption and decryption - ipv4 & verify with EPC	To Configure ipsec with ipv4 address and verify with EPC	Failed	CSCwh75845
ENJ.DP.20.13.1_17.13.1_N002	Configure ipsec with Basic traffic encryption and decryption - ipv4 & Verify with packet capture	To Configure ipsec with ipv4 address and verify with packet capture	Passed	CSCwh68229
ENJ.DP.20.13.1_17.13.1_N003	Configure the reply window size 512 and capture using EPC	To Configure the reply window size 512 and capture using EPC	Passed	
ENJ.DP.20.13.1_17.13.1_N004	Configure the reply window size 256 and capture using EPC	To Configure the reply window size 256 and capture using EPC	Failed	CSCwh73967
ENJ.DP.20.13.1_17.13.1_N005	Configure the reply window size 512 and capture using packet capture	To Configure the reply window size 512 and capture using packet capture	Passed	
ENJ.DP.20.13.1_17.13.1_N006	Configure the reply window size 256 and capture using packet capture	To Configure the reply window size 256 and capture using packet capture	Passed	
ENJ.DP.20.13.1_17.13.1_N007	Configure the same pre-share key for ipsec using ipv4 address and capture it using packet capture	To Configure ipsec with same preshare key	Passed	

ENJ.DP.20.13.1_17.13.1_N008	Configure the different pre-share key for ipsec using ipv4 address and capture it using packet capture	To Configure ipsec with different preshare key	Passed	
ENJ.DP.20.13.1_17.13.1_N009	Configure the same pre-share key for ipsec using ipv4 address and capture it using EPC	To Configure ipsec with same preshare key	Passed	
ENJ.DP.20.13.1_17.13.1_N010	Configure the different pre-share key for ipsec using ipv4 address and capture it using EPC	To Configure ipsec with different preshare key	Passed	
ENJ.DP.20.13.1_17.13.1_N011	Configure the ipsec using Encapsulation protocol with ESP (Encryption and Authentication Algorithm) using EPC	To Configure Ipsec with Encapsulation protocol with ESP	Failed	CSCwh76837
ENJ.DP.20.13.1_17.13.1_N012	Configure the ipsec using Encapsulation protocol with AH (Authentication Algorithm) using Packet trace	To Configure ipsec with Encapsulation protocol with AH	Passed	
ENJ.DP.20.13.1_17.13.1_N013	Configure ipsec using 3DES Encryption Algorithm and monitor using EPC	To Configure ipsec with 3DES Encryption Algorithm	Passed	
ENJ.DP.20.13.1_17.13.1_N014	Configure ipsec using AES Encryption Algorithm and monitor using packet trace	To Configure ipsec with AES Encryption Algorithm	Passed	

ENJ.DP.20.13.1_17.13.1_N015	Configure ipsec using hmac-sha Authentication Algorithm and monitor using EPC	To Configure IPSEC with hmac-sha Authentication Algorithm	Passed	
ENJ.DP.20.13.1_17.13.1_N016	Configure ipsec using hmac-MD5 Authentication Algorithm and monitor using packet trace	To Configure IPSEC with hmac-MD5 Authentication Algorithm	Passed	
ENJ.DP.20.13.1_17.13.1_N017	Configure ipsec using same DH group and monitor using packet trace without pfs using EPC	To Configure IPSEC with same DH group	Passed	
ENJ.DP.20.13.1_17.13.1_N018	Configure ipsec using different DH group and monitor using packet trace without pfs using packet trace	To Configure IPSEC with using different DH group	Passed	
ENJ.DP.20.13.1_17.13.1_N019	Configure ipsec using same DH group and monitor using packet trace with pfs using EPC	To Configure IPSEC with same DH group	Passed	
ENJ.DP.20.13.1_17.13.1_N020	Configure ipsec using different DH group and monitor using packet trace with pfs using packet trace	To Configure IPSEC different DH group	Passed	

Port-channel support on transport side for link redundance and BW aggregation

Logical ID	Title	Description	Status	Defect ID
ENJ.Port.20.13.1_17.13.1_N01	Configure Lag on the transport side and verify its Successfully configured or not	Configure Lag on the transport side and verify its Successfully configured or not	Passed	
ENJ.Port.20.13.1_17.13.1_N02	Configure Port-channel on the transport side and check port channel load-balancing the traffic or not	Configure Port-channel on the transport side and check port channel load-balancing the traffic or not	Passed	
ENJ.Port.20.13.1_17.13.1_N03	Configure Lag on transport interface distribution for port channel or not	Configure Lag on transport interface distribution for port channel or not	Passed	
ENJ.Port.20.13.1_17.13.1_N04	Configure Port-channel on the transport side and check platform hardware qfp active summery	Configure Port-channel on the transport side and check platform hardware qfp active summery	Passed	
ENJ.Port.20.13.1_17.13.1_N05	Configure Port-channel on the transport side and verify Forward Error Correction (FEC)	Configure Port-channel on the transport side and verify Forward Error Correction (FEC)	Passed	
ENJ.Port.20.13.1_17.13.1_N06	Configure the port-channel1 and port-channel2 transport side and Verify the port-channel connections	Configure the port-channel1 and port-channel2 transport side and Verify the port-channel connections	Passed	

ENJ.Port.20.13.1_17.13.1_N07	Configuring Lag on the transport side Verify control tunnel bring up or not	Configuring Lag on the transport side Verify control tunnel bring up or not	Passed	
ENJ.Port.20.13.1_17.13.1_N08	Lag Configuration After checking the data tunnel bring-up with BFD for IPSEC	Lag Configuration After checking the data tunnel bring-up with BFD for IPSEC	Passed	
ENJ.Port.20.13.1_17.13.1_N09	Lag Configuration After checking the data tunnel bring-up with BFD for GRE	Lag Configuration After checking the data tunnel bring-up with BFD for GRE		
ENJ.Port.20.13.1_17.13.1_N10	Configuring Lag with enable tun-Qos-spoke and check downstream bandwidth on spoke	Configuring Lag with enable tun-qos-spoke and check downstream bandwidth on spoke	Passed	
ENJ.Port.20.13.1_17.13.1_N11	Configuring Lag and Checking the routes and the next-hop table	Configuring Lag and Checking the routes and the next-hop table	Passed	
ENJ.Port.20.13.1_17.13.1_N12	Configure Lacp with SLA Policy and verify SLA measurements with traffic	Configure Lacp with SLA Policy and verify SLA measurements with traffic	Passed	
ENJ.Port.20.13.1_17.13.1_N13	Configuring Lacp on Multiple Transport Side and checking its load-balancing with traffic or not	Configuring Lacp on Multiple Transport Side and checking its load-balancing with traffic or not	Passed	
ENJ.Port.20.13.1_17.13.1_N14	Configuring Lacp and Verify bandwidth aggregation traffic	Configuring Lacp and Verify bandwidth aggregation traffic	Passed	
ENJ.Port.20.13.1_17.13.1_N15	Verify tloc-extension with WAN side LAG TLOC	Verify tloc-extension with WAN side LAG TLOC	Passed	

ENJ.Port.20.13.1_17.13.1_N16	Configure Lacp on the transport side On Active-Active mode and check the traffic	Configure Lacp on the transport side On Active-Active mode and check the traffic	Passed	
ENJ.Port.20.13.1_17.13.1_N17	Configure Lacp on the transport side On Active-Passive mode and check the traffic	Configure Lacp on the transport side On Active-Passive mode and check the traffic	Passed	
ENJ.Port.20.13.1_17.13.1_N18	Configure Lacp on the transport side On Passive-Active mode and check the traffic	Configure Lacp on the transport side On Passive-Active mode and check the traffic	Passed	
ENJ.Port.20.13.1_17.13.1_N19	Configure Lacp on the transport side On Passive-Passive mode and check the traffic	Configure Lacp on the transport side On Passive-Passive mode and check the traffic	Passed	
ENJ.Port.20.13.1_17.13.1_N20	Configuring Lacp with QOS policy and checking QOS is Working based on policy or not	Configuring Lacp with QOS policy and checking QOS is Working based on policy or not	Passed	
ENJ.Port.20.13.1_17.13.1_N21	Configuring Lacp with ACL policy and checking ACL is Working based on policy or not.	Configuring Lacp with ACL policy and checking ACL is Working based on policy or not	Passed	
ENJ.Port.20.13.1_17.13.1_N22	Configuring Lacp with enabled tun-qos-hub on HUB and check downstream bandwidth on spoke	Configuring Lacp with enabled tun-qos-hub on HUB and check downstream bandwidth on spoke	Passed	

ENJ.Port.20.13.1_17.13.1_N23	Configuring Lacp with enable tun-qos-spoke and check downstream bandwidth on spoke	Configuring Lacp with enable tun-qos-spoke and check downstream bandwidth on spoke	Passed	
ENJ.Port.20.13.1_17.13.1_N24	Configuring Lacp and Send the traffic and verify through FIA on which next-hop traffic takes	Configuring Lacp and Send the traffic and verify through FIA on which next-hop traffic takes	Passed	
ENJ.Port.20.13.1_17.13.1_N25	Configuring Lacp and Shut down the interface which traffic is taking and check the failover	Configuring Lacp and Shut down the interface which traffic is taking and check the failover	Passed	
ENJ.Port.20.13.1_17.13.1_N26	Transport address update/renew/withdraw	Verify port-channels comes up fine after Transport address update/deletes		
ENJ.Port.20.13.1_17.13.1_N27	BFD/TLOC/control-connection/omp session flapping	Verify port-channel comes up fine after clearing BFD/TLOC/Control-connection/omp session	Passed	
ENJ.Port.20.13.1_17.13.1_N28	Router reload	Verify port-channel comes up fine after router reload		
ENJ.Port.20.13.1_17.13.1_N29	Port-channel interface flapping when dual stack is configured	Verify port-channel interface flapping	Passed	
ENJ.Port.20.13.1_17.13.1_N30	Scale number of port-channel sub-interfaces x 2 member links	Verify basic forwarding with aggr port-channel sub-interfaces with 2 member links	Passed	

Configure Third-party CA Certificates to Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager

Logical ID	Title	Description	Pass/Fail	Defect ID
ENJ.3rd PCE.20.13.1_17.13.1_ N.01	Try to Add a CA Certificate in vManage.	Adding a new CA Certificate in the vManage under Certificates.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_ N.02	Try to Add Multiple CA Certificates in vManage.	Adding multiple new CA Certificates in the vManage under Certificates.	Passed	CSCwh49676, CSCwh51167
ENJ.3rd PCE.20.13.1_17.13.1_ N.03	Create a configuration group under system profile and add a CA Certificate parcel.	User will be creating a configuration group under system profile and will add a CA Certificate Parcel under the System Profile	Passed	CSCwh89180
ENJ.3rd PCE.20.13.1_17.13.1_ N.04	Try Adding CA Certificate parcel and pushing it to ISR Edge Device.	User will be Associating devices to the created system profile under configuration group and push the CA Certificate.	Failed	CSCwh89180
ENJ.3rd PCE.20.13.1_17.13.1_ N.05	Edit the CA Certificate parcel and Re-push it to ISR Edge Device	Editing the CA Certificate Parcel and Re-Pushing it to the ISR Edge Devices of the Configuration Group.	Failed	CSCwh89180
ENJ.3rd PCE.20.13.1_17.13.1_ N.06	Delete the CA Certificate parcel and Re-push it to ISR Edge Device.	Deleting the CA Certificate Parcel and Re-Pushing it to the ISR Edge Devices of the Configuration Group.	Failed	CSCwh89180

ENJ.3rd PCE.20.13.1_17.13.1_N.07	Monitor the logs after Successful installation of CA Certificate for ISR Device.	Navigate to Monitor > Logs > Alarms and check whether the Alarm logs are displayed after successful installation of CA Certificate.	Failed	CSCwh89180
ENJ.3rd PCE.20.13.1_17.13.1_N.08	Verify the PKI Trustpoints are displayed under the ISR Devices > Real Time.	Navigate to Devices > Real Time and verify the PKI Trustpoints are displayed or not.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.09	Try Adding CA Certificate parcel and pushing it to C8KV Edge Device.	User will be Associating C8KV devices to the created system profile under configuration group and push the CA Certificate.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.10	Edit the CA Certificate parcel and Re-push it to C8KV Edge Device.	Editing the CA Certificate Parcel and Re-Pushing it to the C8KV Devices of the Configuration Group.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.11	Delete the CA Certificate parcel and Re-push it to C8KV Edge Device.	Deleting the CA Certificate Parcel and Re-Pushing it to the C8KV Devices of the Configuration Group.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.12	Monitor the logs after Successful installation of CA Certificate for C8KV Device.	Navigate to Monitor > Logs > Alarms and check whether the Alarm logs are displayed after successful installation of CA Certificate.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.13	Verify the PKI Trustpoints are displayed under the C8KV Devices > Real Time.	Navigate to Devices > Real Time and verify the PKI Trustpoints are displayed or not.	Passed	CSCwh68093

ENJ.3rd PCE.20.13.1_17.13.1_N.14	Try Adding CA Certificate parcel and pushing it to Catalyst Edge Device.	User will be Associating Catalyst devices to the created system profile under configuration group and push the CA Certificate.	Failed	CSCwf01763
ENJ.3rd PCE.20.13.1_17.13.1_N.15	Edit the CA Certificate parcel and Re-push it to Catalyst Edge Device.	Editing the CA Certificate Parcel and Re-Pushing it to the Catalyst Devices of the Configuration Group.	Passed	CSCwh69794
ENJ.3rd PCE.20.13.1_17.13.1_N.16	Delete the CA Certificate parcel and Re-push it to Catalyst Edge Device.	Deleting the CA Certificate Parcel and Re-Pushing it to the Catalyst Devices of the Configuration Group.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.17	Monitor the logs after Successful installation of CA Certificate for Catalyst Device.	Navigate to Monitor > Logs > Alarms and check whether the Alarm logs are displayed after successful installation of CA Certificate.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.18	Verify the PKI Trustpoints are displayed under the Catalyst Devices > Real Time.	Navigate to Devices > Real Time and verify the PKI Trustpoints are displayed or not.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.19	Execute GET API Read Permission for System Profile in vManage API.	Executing the GET API read Permission for the created system profile under configuration group.	Passed	CSCwh35820,CSCwh37584
ENJ.3rd PCE.20.13.1_17.13.1_N.20	Create a new user access and add a CA Certificate in vManage.	Creating a new user access and adding a new CA Certificate in the vManage under Certificates	Failed	CSCwh92929

ENJ.3rd PCE.20.13.1_17.13.1_N.21	Create a configuration group under system profile and add a CA Certificate parcel under newly created user.	User will be creating a configuration group under system profile and will add a CA Certificate Parcel under the System Profile under newly created user.	Passed	CSCwh71151, CSCwh74524
ENJ.3rd PCE.20.13.1_17.13.1_N.22	Edit the CA Certificate parcel and Re-push it to Edge Device under newly created user.	Editing the CA Certificate Parcel and Re-Pushing it to the Devices of the Configuration Group under newly created user.	Failed	CSCwh89671
ENJ.3rd PCE.20.13.1_17.13.1_N.23	Delete the CA Certificate parcel and Re-push it to Edge Device under newly created user.	Deleting the CA Certificate Parcel and Re-Pushing it to the Devices of the Configuration Group under newly created user	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.24	Create a new user access & verify the PKI Trustpoints are displayed under the Devices > Real Time.	Creating a new user access to verify the PKI Trustpoints of the certificates are displayed or not.	Passed	
ENJ.3rd PCE.20.13.1_17.13.1_N.25	Create a new user access Execute GET API Read Permission for System Profile in vManage.	Creating a new user access and execute the GET API read Permission for the created system profile under configuration group.	Passed	

SR/CFD

Logical ID	Title	Description	Pass/Fail	Defect ID
ENJ.SRCFD.20.12.1_17.12.1_N01	Check and verify the troubleshooting in packet capture.	Check and verify the troubleshooting in packet capture.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N02	Configure the packet capture with vpn 1001 with port channel.	Configure the packet capture with vpn 1001 with port channel.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N03	Check and verify the WAN interface with ipv4 address and capture the packets after 10 secs	Check and verify the WAN interface with ipv4 address and capture the packets after 10 secs	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N04	Check and verify the sub interface with ipv4 address and capture the packets after 10 secs.	Check and verify the sub interface with ipv4 address and capture the packets after 10 secs.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N05	Configure the WAN interface with vpn 100 verify the capture	Configure the WAN interface with vpn 100 verify the capture	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N06	Configure and verify the Transport interface with BFD Session	Configure and verify the Transport interface with BFD Session	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N07	Check and verify the platform and summary session after interface flaps	Check and verify the platform and summary session after interface flaps	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N08	Check and verify the BFD session after interface shutdown	Check and verify the BFD session after interface shutdown	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N09	Configure the BFD session with WAN interaface and verify the summary and status	Configure the BFD session with WAN interaface and verify the summary and status	Passed	

ENJ.SRCFD.20.12.1_17.12.1_N10	Check and verify the BFD session when data plane status is not active state.	Check and verify the BFD session when data plane status is not active state.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N11	clear the omp routes and check the bfd session.	clear the omp routes and check the bfd session.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N12	clear the control connections and check the bfd session states.	clear the control connections and check the bfd session states.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N13	To check the packet drops with different cause code associated with the BFD session down through CLI	To check the packet drops with different cause code associated with the BFD session down through CLI	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N14	To Flap the WAN Interface and check the bfd states	To Flap the WAN Interface and check the bfd states	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N15	To clear the omp routes and check the bfd session in ISR Devices.	To clear the omp routes and check the bfd session in ISR Devices.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N16	To Verify that the ICMP-echo probe is failing when the configured source interface doesn't have a valid source address.	To Verify that the ICMP-echo probe is failing when the configured source interface doesn't have a valid source address.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N17	To Verify that the ICMP-echo probe is success when configured with the valid source interface.	To Verify that the ICMP-echo probe is success when configured with the valid source interface.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N18	To restart the configure SLA and check the status.	To restart the configure SLA and check the status.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N19	To flap the source interface	To flap the source interface	Passed	

ENJ.SRCFD.20.12.1_17.12.1_N20	To configure the icmp probe and check the sla statistics	To configure the icmp probe and check the sla statistics	Passed	

Regression Features

SIG

Logical ID	Title	Status	Defect ID
ENJ.Sig.20.13.1_17.13.1_N.01	Sig Integration improvement (source-only load sharing).	Passed	
ENJ.Sig.20.13.1_17.13.1_N.02	Failover Manual SIG Tunnel with Source-Only Load Sharing via Templates.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.03	Failover and Bring-up Manual SIG Tunnel with Source-Only Load Sharing via Templates.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.04	Manual SIG Tunnel with Source-Only Load Sharing and Policy for Custom application.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.05	Manual SIG Tunnel with Source-Only Load Sharing and Policy for Allowing and blocking the sites based on the Destination lists.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.06	Check whether performance improvement due to Source-only load sharing.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.07	Source-Only Load Sharing with Automatic SIG Tunnels.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.08	SIG Active-Active Source-Only Load Sharing.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.09	Failover and Bring-up SIG Active-Active Source-Only Load Sharing via CLI.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.10	Weighted SIG Active-Active Source-Only Load Sharing via Vmanage.	Passed	

ENJ.Sig.20.13.1_17.13.1_N.11	Failover and Bring-up with Weighted SIG Active-Active Source-Only Load Sharing via CLI.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.12	SIG Active-Backup Source-Only Load Sharing via CLI.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.13	Failover and Bring-up with SIG Active-Backup Source-Only Load Sharing via CLI.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.14	Manual SIG Tunnel without and with Redirect Traffic to SIG and Source-Only Load Sharing via Templates.	Passed	
ENJ.Sig.20.13.1_17.13.1_N.15	Create and User-Defined Tracker in Cli to Monitor the Endpoint.	Passed	

OMP

Logical ID	Title	Status	Defect ID
ENJ.omp.20.13.1_17.13.1_N.01	OMP IPv4 Advertised Routes in CSV Format.	Passed	
ENJ.omp.20.13.1_17.13.1_N.02	OMP IPv4 Advertised Routes in JSON Format.	Passed	
ENJ.omp.20.13.1_17.13.1_N.03	Cancelling OMP IPv4 Advertised Routes in CSV Format.	Passed	
ENJ.omp.20.13.1_17.13.1_N.04	Cancelling OMP IPv4 Advertised Routes in JSON Format.	Passed	
ENJ.omp.20.13.1_17.13.1_N.05	OMP IPv4 Received Routes in CSV Format.	Passed	
ENJ.omp.20.13.1_17.13.1_N.06	OMP IPv4 Received Routes in JSON Format.	Passed	
ENJ.omp.20.13.1_17.13.1_N.07	Cancelling OMP IPv4 Received Routes in CSV Format.	Passed	
ENJ.omp.20.13.1_17.13.1_N.08	Cancelling OMP IPv4 Received Routes in JSON Format.	Passed	
ENJ.omp.20.13.1_17.13.1_N.09	OMP IPv4 Advertised Routes in CSV Format after removing routes.	Passed	
ENJ.omp.20.13.1_17.13.1_N.10	OMP IPv4 Advertised Routes in JSON Format after removing routes.	Passed	
ENJ.omp.20.13.1_17.13.1_N.11	Cancelling OMP IPv4 Advertised Routes in CSV Format after removing routes.	Passed	
ENJ.omp.20.13.1_17.13.1_N.12	Cancelling OMP IPv4 Advertised Routes in JSON Format after removing routes.	Passed	
ENJ.omp.20.13.1_17.13.1_N.13	OMP IPv4 Received Routes in CSV Format after removing routes.	Passed	

ENJ.omp.20.13.1_17.13.1_N.14	OMP IPv4 Received Routes in JSON Format after removing routes.	Passed	
ENJ.omp.20.13.1_17.13.1_N.15	Cancelling OMP IPv4 Received Routes in CSV Format after removing routes.	Passed	

OSPF

Logical ID	Title	Status	Defect ID
ENJ.OSPF.20.13.1_17.13.1_N.01	To enable the OSPF between cEdge and Service side router.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.02	To establish OSPF neighbour From Wan Edge to Service Routers and Specify the authentication and authentication key MD5 on the interface to allow OSPF to exchange routing update information securely.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.03	To Establish OSPF Peer between Wan edge and the service router with BFD Session between peers	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.04	To enable OSPF b/w Wan and Service router with DR and BDR selection on Service side.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.05	Advertising ospf routes into omp with advertise network ospf.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.06	Allowing x.x.x.x/x network in OSPF using route maps.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.07	Redistribute Ospf Routes into BGP.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.08	To configure the dual OSPF neighbour between Service router and WAN edge router and verify the failure of one of the neighbours.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.09	Denying x.x.x.x/x network in OSPF using route maps.	Passed	

ENJ.OSPF.20.13.1_17.13.1_N.10	To Redistribute OMP routes into the OSPF VRF 100 topology.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.11	To establish an OSPF neighbour relationship between wan edge and the Service router and specify how often the router sends OSPF hello packets, set hello & hold interval.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.12	Advertise OSPF External into OMP.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.13	Redistribute OMP into VRF 100 OSPF.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.14	To Advertise ospfv3 routes into OMP.	Passed	
ENJ.OSPF.20.13.1_17.13.1_N.15	To Re-distributed OMP routes into the OSPFV3 routing table.	Passed	

EIGRP

Logical ID	Title	Status	Defect ID
ENJ.EIGRP.20.13.1_17.13.1_N.01	Redistrubute OMP into EIGRP.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.02	Eigrp Convergence test.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.03	Adding networks.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.04	EIGRP Stub routing.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.05	EIGRP graceful Shutdown.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.06	EIGRP Key Authentication.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.07	Allowing 33.1.1.0/24 networking in Eigrp using route maps.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.08	Denying 55.1.1.0/24 networking in Eigrp using route maps.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.09	Configuring Administrative Distance value in EIGRP.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.10	Advertise 100.100.100.0/24 Network in omp routes.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.11	To Enable EIGRP on the Wan edge router	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.12	To modify hold timers on eigrp neighbours	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.13	EIGRP Test with different AS Number	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.14	EIGRP changing the routing id.	Passed	
ENJ.EIGRP.20.13.1_17.13.1_N.15	EIGRP route auto summarizations.	Passed	

BGP

Logical ID	Title	Status	Defect ID
ENJ.BGP.20.13.1_17.13.1_N.01	EBGP configs on the transport side.	Passed	
ENJ.BGP.20.13.1_17.13.1_N.02	EBGP with WEIGHT attribute	Passed	
ENJ.BGP.20.13.1_17.13.1_N.03	Configure BGP using keepalive and holdtime	Passed	
ENJ.BGP.20.13.1_17.13.1_N.04	EBGP with local preference attribute and AS path pretend attribute	Passed	
ENJ.BGP.20.13.1_17.13.1_N.05	Redistribution of OMP and BGP routes	Passed	
ENJ.BGP.20.13.1_17.13.1_N.06	IP SLA tracking for ipv4 static service side routes	Passed	
ENJ.BGP.20.13.1_17.13.1_N.07	IBGP configs on the service side	Passed	
ENJ.BGP.20.13.1_17.13.1_N.08	Establish connections of IBGP on the service side	Passed	
ENJ.BGP.20.13.1_17.13.1_N.09	Configure IBGP using VRF on the service side	Passed	
ENJ.BGP.20.13.1_17.13.1_N.10	. Configure IBGP with-out using VRF on the service side	Passed	
ENJ.BGP.20.13.1_17.13.1_N.11	Verify IBGP next hop origan and AS path	Passed	
ENJ.BGP.20.13.1_17.13.1_N.12	EBGP with Local Preference attribute and AS Path Prepend attribute (failover on link)	Passed	
ENJ.BGP.20.13.1_17.13.1_N.13	Decreasing Convergence by BDF configuration for EBGP	Passed	
ENJ.BGP.20.13.1_17.13.1_N.14	Verify IBGP next hop origan and AS path	Passed	
ENJ.BGP.20.13.1_17.13.1_N.15	Configure Bgp between br1 to dc using Vrf 100 via INET	Passed	

AAR

Logical ID	Title	Status	Defect ID
ENJ.aar.17.13.1_20.13.1_No.01	Basic Policy with Custom Application.	Passed	
ENJ.aar.17.13.1_20.13.1_No.02	Policy with Custom Application with Server name, IP.	Passed	
ENJ.aar.17.13.1_20.13.1_No.03	Policy with Custom Application with specified source IP and Port.	Passed	
ENJ.aar.17.13.1_20.13.1_No.04	Policy with Custom Application with specified Server name and Ports.	Passed	
ENJ.aar.17.13.1_20.13.1_No.05	Policy with Custom Application with specified source Ports and transport protocol(TCP/UDP).	Passed	
ENJ.aar.17.13.1_20.13.1_No.06	Color Preference and Count with Custom Application.	Passed	
ENJ.aar.17.13.1_20.13.1_No.07	Basic Policy to drop and use counter for a DPI application family using vmanage.	Passed	
ENJ.aar.17.13.1_20.13.1_No.08	Basic Policy to accept and use counter for a DPI application using vManage.	Passed	CSCwh29887
ENJ.aar.17.13.1_20.13.1_No.09	Policy to forward to a Next hop for the application family using vManage.	Passed	
ENJ.aar.17.13.1_20.13.1_No.10	Policy to forward to a TLOC colour for the application family with failover using vmanage.	Passed	

ENJ.aar.17.13.1_20.13.1_No.11	Policy to forward to a TLOC colour for the application family without failover using v-Manage.	Passed	
ENJ.aar.17.13.1_20.13.1_No.12	Basic Policy to drop and use counter for a DPI application family using CLI.	Passed	
ENJ.aar.17.13.1_20.13.1_No.13	Basic Policy to accept and use counter for a DPI application using CLI.	Passed	
ENJ.aar.17.13.1_20.13.1_No.14	Policy with Custom Application with specified source Ports and transport protocol.	Passed	
ENJ.aar.17.13.1_20.13.1_No.15	Policy to forward to a TLOC colour for the application family with out failover using vmanage.	Passed	

ACL

Logical ID	Title	Status	Defect ID
ENJ.ACL.20.13.1_17.13.1_N.01	Standard ACL to permit all incoming LAN traffic.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.02	Extended ACL to permit all incoming WAN traffic.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.03	Extended ACL permitting outbound https WAN traffic.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.04	Extended ACL permitting SSH LAN traffic with a following deny entry for the IP traffic.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.05	To deny the host via Standard access list applied on LAN interface in inbound direction.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.06	Extended ACL to deny ICMP traffic alone on WAN interface.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.07	Configure extended ACL on LAN interface to allow all traffic except SSH.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.08	Configure extended access list on WAN interface to deny remote device using FTP and Allow all other protocols.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.09	Extended ACL permitting SSH WAN traffic with a following deny entry for the same traffic.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.10	Changing entry of Standard ACL from denying to permitting all incoming LAN traffic.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.11	Standard SNMP_acl to deny all WAN traffic.	Passed	
ENJ.ACL.20.13.1_17.13.1_N.12	Extended ACL to allow BGP traffic and deny other traffic.	Passed	

NAT

Logical ID	Title	Status	Defect ID
ENJ.NAT.20.13.1_17.13.1_N.01	To configure the destination Inside NAT and check the NAT Translation.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.02	To configure the NAT DIA Tracker and the check the translation and tracker status.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.03	To configure the inside static NAT using an Inside Nat pool using centralized policy.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.04	To configure the static inside NAT and static outside Nat mapped inside Nat address pool.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.05	To configure a service side PAT port forwarding with inside tcp traffic(http-80) via CLI.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.06	To configure a service side static Nat port forwarding with inside tcp traffic(telnet-23) via CLI.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.07	To configure the intra vpn service side Nat and generate the traffic and check the translation.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.08	To configure the service side conditional static Nat with data policy using CLI.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.09	To configure the service side conditional Dynamic Nat with data policy using CLI.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.10	To configure the service side Network Nat with data policy using CLI.	Passed	

ENJ.NAT.20.13.1_17.13.1_N.11	To configure the service side static Nat object tracker with Data policy using cli.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.12	To configure the service side static Nat object tracker with Data policy using cli addon Template.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.13	To configure the intra vpn service side Nat and generate the traffic using cli add on template.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.14	To configure the service side conditional static Nat with matched and unmatched data policy and check the translation.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.15	To configure the service side static NAT using feature template and check the Nat translation.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.16	To configure Source Port Preservation for DIA Interface Overload Using a CLI Template.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.17	To configure the Source Port Preservation for DIA Pool Overload Using a CLI Template.	Passed	
ENJ.NAT.20.13.1_17.13.1_N.18	To configure the NAT DIA DUAL Tracker (Boolean OR) and the check the translation and tracker status.	Passed	

TLOC

Logical ID	Title	Status	Defect ID
ENJ.TLOC.20.13.1_17.13.1_N.01	INET TLOC to MPLS through Device CLI Template - Sub int.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.02	MPLS TLOC to INET through Device CLI Template - Sub int .	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.03	INET TLOC to MPLS config through vmanage CLI Template - Sub Int.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.04	MPLS TLOC to INET config through vmanage CLI Template - Sub int.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.05	TLOC Tunnel config using Group ID for internet.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.06	TLOC Tunnel config using Group ID for PRIVATE.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.07	INET TLOC to MPLS through Device CLI Template - Physical int.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.08	MPLS TLOC to INET through Device CLI Template - Physical int.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.09	DUAL Internet TLOC Extension on CLI Template.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.10	Enable ipv4 Tloc extn for the sub interface.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.11	Enable ipv4 Tloc extn for the loopback interface for extended wan circuits.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.12	To Config ipv4 Tloc Ext for the Loopback interface using vManage CLI template.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.13	INET TLOC to Private2 through Device CLI Template - Sub int.	Passed	

ENJ.TLOC.20.13.1_17.13.1_N.14	Private2 TLOC to INET through Device CLI Template - Sub int.	Passed	
ENJ.TLOC.20.13.1_17.13.1_N.15	INET TLOC to Private2 config through vmanage CLI Template - Sub Int.	Passed	

BFD

Logical ID	Title	Status	Defect ID
ENJ.BFD.20.13.1_17.13.1_N.01	To configure BFD for Biz or public interface-overlay.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.02	To configure BFD for MPLS or private 1 internet interface-overlay.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.03	To configure BFD for Transport-Side BGP using vmanage CLI add on template and attach the template to device template.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.04	To configure BFD for Service-Side BGP using vmanage CLI add on template and attach the template to device template.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.05	o configure BFD for Service-Side EIGRP using vmanage CLI add on template and attach the template to device template	Passed	
ENJ.BFD.20.13.1_17.13.1_N.06	To configure BFD for Service-Side OSPF using vmanage CLI add on template and attach the template to device template	Passed	
ENJ.BFD.20.13.1_17.13.1_N.07	To configure BFD for Transport-side BGP using device CLI.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.08	To configure BFD for Service-side BGP using device CLI.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.09	To configure BFD for Service-side EIGRP using device CLI	Passed	

ENJ.BFD.20.13.1_17.13.1_N.10	To configure BFD for Service-side OSPF using device CLI	Passed	
ENJ.BFD.20.13.1_17.13.1_N.11	To configure hello interval for BFD.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.12	To configure pmtu discovery for BFD.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.13	To configure Multiple BFD for Transport side.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.14	To configure app-route Multiplier for BFD.	Passed	
ENJ.BFD.20.13.1_17.13.1_N.15	To configure app-route poll-interval for BFD.	Passed	

ADHOC

Logical ID	Title	Description	Status	Defect ID
ENJ.Adhoc_20.13.1_17.13.1_N.01	Check The PMT Account is working or not	Check The PMT Account is working or not	Failed	CSCwh43416
ENJ.Adhoc_20.13.1_17.13.1_N.02	Check the Application priority & SLA for the Target interface drop-down list working fine or not	Check the Application priority & SLA for the Target interface drop-down list working fine or not	Failed	CSCwh47134
ENJ.Adhoc_20.13.1_17.13.1_N.03	Check The Smart Account is working or not in Administrator Settings	Check The Smart Account is working or not in Administrator Settings	Failed	CSCwh42373
ENJ.Adhoc_20.13.1_17.13.1_N.04	Verify By Invalid Hostname and Enabled Data Stream for transport	Verify By Invalid Hostname and Enabled Data Stream for transport	Failed	CSCwh48420
ENJ.Adhoc_20.13.1_17.13.1_N.05	Check by Wrong User Name & password accepted for UTD Snort Subscriber Signature for Download or not	Check by Wrong User Name & password accepted for UTD Snort Subscriber Signature for Download or not	Failed	CSCwh51728
ENJ.Adhoc_20.13.1_17.13.1_N.06	Check the Cancel Button is working fine or not & its Canceled all panel in Administrator settings or not	Check the Cancel Button is working fine or not & its Canceled all panel in Administrator settings or not	Failed	CSCwh48560
ENJ.Adhoc_20.13.1_17.13.1_N.07	Check the generated link or not for JSON and CSV File format when we Export	Check the generated link or not for JSON and CSV File format when we Export	Failed	CSCwh66772
ENJ.Adhoc_20.13.1_17.13.1_N.08	Generate Admin-tech file in vmanage	Generate Admin-tech file in vmanage	Failed	CSCwh75756

ENJ.Adhoc_20.13.1_17.13.1_N.09	Create Service VPN temp in Vmanage for Device Templates	Create Service VPN temp in Vmanage for Device Templates	Failed	CSCwh88830
ENJ.Adhoc_20.13.1_17.13.1_N.10	Having issue with UI dashboard - Not showing the report and explore name	Having issue with UI dashboard - Not showing the report and explore name	Failed	CSCwh89127
ENJ.Adhoc_20.13.1_17.13.1_N.11	Verify whether a user can navigate from Troubleshooting > Ping to Troubleshooting >Trace Route	Test whether the user can navigate from one page to other page within Troubleshooting.	Failed	CSCwh92610,CSCwh92905
ENJ.Adhoc_20.13.1_17.13.1_N.12	Verify whether a user can navigate to Troubleshooting Page.	Test whether the user can navigate to Troubleshooting Page.	Failed	CSCwh92804
ENJ.Adhoc_20.13.1_17.13.1_N.13	Verify whether a user can login to the vManage with a new user access.	Test whether a user can create a new user access and logging into vManage with new user access.	Failed	CSCwh89692
ENJ.Adhoc_20.13.1_17.13.1_N.14	Verify the dashboard and parameters needed to create/build a service instance in vManage	Verify the dashboard and parameters needed to create/build a service instance in vManage	Failed	CSCwh92524
ENJ.Adhoc_20.13.1_17.13.1_N.15	Single branch single edge having dual DIA link with a tracker and configure SLA policy.	Single branch single edge having dual DIA link with a tracker and configure SLA policy.	Failed	CSCwh89503, CSCwh90585

Related Documents

Related Documentation

Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.13 Release Notes

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/controllers-20-13/rel-notes-controllers-20-13.html

Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.13

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/m-configuring-cellular-gateway.html

Cisco SD-WAN Router Configuration Guide, Cisco IOS XE Release 17.13

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/transport-gw.html

Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.13

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/centralized-policy.html#concept_a2t_gjw_5xb

Cisco SD-WAN Monitor and Maintain Configuration Guide,Cisco IOS XE Release 17.13

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/m-dashboard-screen.html#explore

Cisco SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.13

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/cloudonramp/ios-xe-17/cloud-onramp-book-xe/cor-saas.html

Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release 17.13

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/intrusion-prevention.html