Test Results Summary for IOS XE SD-WAN for Japan (Release Version 20.9.1/17.9.1)

First Published: 2022-10-28

Last Modified: 2022-11-04

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 20.9.1 - IOS XE 17.9.1
- 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
- Cisco ISR C111X-8P
- Cisco ISR 4351
- Cisco ISR 4331
- Cisco ISR 1100
- Cisco Catalyst 8300
- Cisco Catalyst 8200
- Cisco Catalyst 8500
- Cisco ISR 4461
- Cisco ASR 1002-X
- Cisco Catalyst 9K PoE Switch

Acronyms

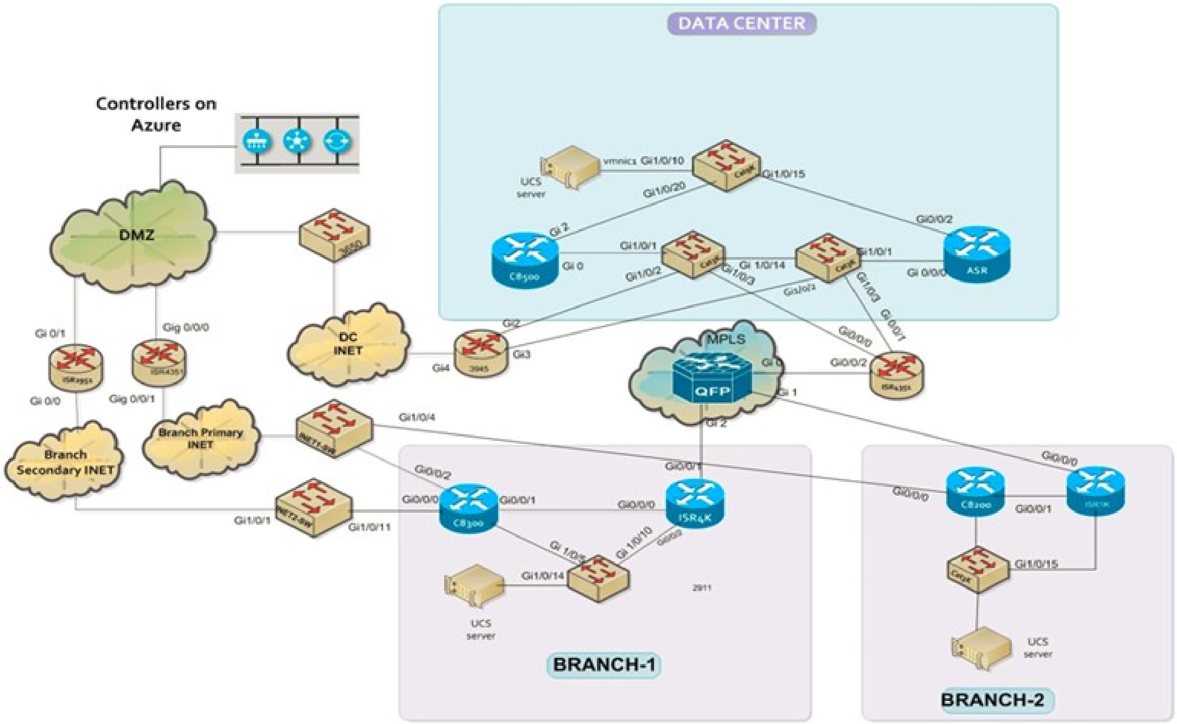
Acronym	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Address-family
API	Application Programming Interface
ASN	Autonomous System Number
ASR	Aggregation Services Routers

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	20.9.1
		vManage	20.9.1
		vSmart	20.9.1
	Switch	Cat 9K PoE	17.2
Communications Infrastructure	IOS XE SDWAN	ISR 4351, 4331	17.9.1
		ISR 1100, Cat 8300, C8200 & C8500	17.9.1
		ISR4461	17.9.1
		ASR 1002-X	17.9.1
		ISR C111X-8P	17.9.1
UCS	UCSC-C240-M5SX	ESXi Host	6.0, 6.5
Client	Operating System	End point	Windows 10
	Browsers	Mozilla	103.0.1
		Chrome	103.0.5060.66

What's New ?

SDWAN 20.9.1 - IOS XE 17.9.1 Solution testing

- Hierarchical SD-WAN - 3rd phase
- ALG Support for NAT and Firewall on IOS XE SDWAN
- SIG Tunnel Monitoring / Observability for Zscaler/Umbrella Services
- Cisco SD-WAN (on-prem security) - Identity Firewall (with AD integration) Services
- SDWAN UX 2.0 - Configuration 2.0,Feature Profiles & Configuration Groups
- PPP/Dialer interface support for DIA NAT use-cases
- Port forwarding on cedge/vedge with port change
- App aware routing for IPv6
- (Device Only-CLI-Template) Packet Tagging - Phase 2 - CLI Template
- [Phase 2] vManage support for dispatching CLI commands to cEdge and vEdge
- Co-management Ph2 - Ability to support granular RBAC and co-manage configuration 2.0
- vManage integration with On Prem SSM
- SDWAN UX 2.0 - Monitoring 2.0 - Customizable Dashboard, Site Topology and Troubleshooting
- Routing Table Scalability enhancements: Inter-Service VPN Route Leaking for PCI Compliance + vSmart only sends routes to an edge for which the next-hop TLOC is valid

Open Caveats

CSCwc93448	Cannot access Teleworker Profile Parcels unless Read permission granted for the whole Profile
CSCwc96142	Cannot access Feature Profiles/Parcels unless Read permission granted for the Feature Profile Section
CSCwc96156	Misalignment and difficulty granting permissions under User Groups unless scrolled slowly
CSCwd00454	Able to make superficial changes to parcels in Teleworker Profile Parcels with Read permission
CSCwc93470	Feature Profile Permissions not applied unless User logs in and out
CSCwd06835	Throwing error and unable to configure BGP route policy in service LAN profile
CSCwd06287	Unable to create SNMP user under configuration group
CSCwd02029	Unable to delete the profiles and features under Transport/Management and service lan profile
CSCwd23734	Route policy is not supported in 20.9.1 Document updating
CSCwd02002	Unable to apply the rules using tag for the devices
CSCwc97774	Unable to add new dashlet to the VManage dashboard
CSCwd19693	Timestamp is not displaying for the pxgrid sessions created in cli in vSmart
CSCwd11936	System profile cannot be deleted but able to delete the some features
CSCwd22733	Additionally added user/user group details are not reflecting in vSmart
CSCwd24595	Unable to see user sessions from ISE in vSmart
CSCwd19592	Unable to edit/add/delete user and user groups which are retrieved from ISE
CSCwd13690	Unbale to see routing information and multicast information option commands
CSCwd10798	Failed to integate ISE with vmanage - 20.9.1
CSCwd16975	Failed to integrate ISE with vmanage
CSCwd09809	Umbrella API registration in the device but its not showing by device-registration & dp statas
CSCwd10828	Without Showing Logs and Error Accepting the MTU Size

CSCwd13720	ALG application type is showing as NA in NAT translation output
CSCwd12426	Port forwarding has failed while assigning public address to the internal server
CSCwd28214	Test the AAR policy for ipv6 using vmanage - UI related issue
CSCwd10418	Clear omp routes" missing in the HSDWAN Affinity based Route Filtering documentation

New Features

Hierarchical SD-WAN - 3rd phase

Logical ID	Title	Description	Status	Defect ID
ENJ.HSDWAN.20.9.1_17.9.1_N.01	Configure and validate Secondary Region ID for an Edge Router Using CLI	Configure and validate Secondary Region ID for an Edge Router Using CLI	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.02	Configure the Secondary Region Mode to handle only Secondary Region traffic Using VManage	Configure the Secondary Region Mode to handle only Secondary Region traffic Using VManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.03	Configure the Secondary Region Mode to handle traffic in the primary and secondary regions using vManage	Configure the Secondary Region Mode to handle traffic in the primary and secondary regions using vManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.04	Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using VManage	Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using VManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.05	Configure Transport Gateway with ECMP Using vManage	Configure Transport Gateway with ECMP on the edge router between 2 networks Using vManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.06	Configure Transport Gateway with ECMP Using vManage and bring down a Transport Gateway	Configure Transport Gateway with ECMP on the edge router between 2 networks Using vManage. Shut down a Transport Gateway.	Passed	

ENJ.HSDWAN.20.9.1_17.9.1_N.07	Configure Transport Gateway with ECMP Using CLI	Configure Transport Gateway with ECMP on the edge router between 2 networks Using CLI	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.08	Without a direct path, configure Transport Gateway with preference Using vManage	Without a direct path, configure Transport Gateway with preference Using vManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.09	With a direct path, configure Transport Gateway with preference Using vManage	With a direct path, configure Transport Gateway with preference Using vManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.10	With a direct path, configure Transport Gateway with preference Using CLI	With a direct path, configure Transport Gateway with preference Using CLI	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.11	With a direct path, configure Transport Gateway with preference Using vManage and bring down the Transport Gateway	With a direct path, configure Transport Gateway with preference Using vManage and shut down the Transport Gateway interface	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.12	Configure Transport Gateway on multiple devices within the same region and verify that re-originated route is not advertised to another transport gateway	Configure Transport Gateway on multiple devices within the same region and verify that re-originated route is not advertised to another transport gateway	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.13	Configure an Affinity Group and Preference on a Device, Using vManage	Configure an Affinity Group and Preference on a Device, Using vManage	Passed	

ENJ.HSDWAN.20.9.1_17.9.1_N.14	Configure an Affinity Group and Preference to achieve Load Balancing for Access Region Traffic to Border Routers	Configure an Affinity Group and Preference to achieve Load Balancing for Access Region Traffic to Border Routers	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.15	Configure an Affinity Group and Preference with Only Paths in the Affinity Preference List	Configure an Affinity Group and Preference with Only Paths in the Affinity Preference List	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.16	Configure an Affinity Group and Preference to achieve Load Balancing for Access Region Traffic to Edge Routers	Configure an Affinity Group and Preference to achieve Load Balancing for Access Region Traffic to Edge Routers	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.17	Configure an Affinity Group and Preference to achieve Load Balancing for Core Region Traffic	Configure an Affinity Group and Preference to achieve Load Balancing for Core Region Traffic	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.18	Configure an Affinity Group, Preference, and affinity-preference outbound enable	Configure an Affinity Group, Preference, and affinity-preference outbound enable	Failed	CSCwd10418
ENJ.HSDWAN.20.9.1_17.9.1_N.19	Brownfield Migration to with new HSDWAN migration mode using vManage	Brownfield Migration to with new HSDWAN migration mode using vManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.20	Configure Migration mode from BGP Core using VManage	Configure Migration mode from BGP Core using VManage	Passed	

ENJ.HSDWAN.20.9.1_17.9.1_N.21	Configure a Application Route Policy for Edge router Matching Traffic-To, Region and Role	Configure a Application Route Policy for Edge router Matching Traffic-To, Region and Role	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.22	Configure a Application Route Policy for Border router Matching Traffic-To, Region and Role	Configure a Application Route Policy for Border router Matching Traffic-To, Region and Role	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.23	Configure a Application Route Policy for Border router Matching Traffic-To, Region and Role Using Cisco vManage	Configure a Application Route Policy for Border router Matching Traffic-To, Region and Role Using Cisco vManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.24	Create preferred color group list for region	Create preferred color group list for region	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.25	Configure Route Preference based on TLOC color and Path Type	Configure Route Preference based on TLOC color and Path Type	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.26	Configure Control Policy to Match Traffic-To Using vManage	Configure Control Policy to Match Traffic-To Using vManage	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.27	Match Traffic According to the Destination Region Using CLI	Match Traffic According to the Destination Region Using CLI	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.28	Configure the Path Preference for a Preferred Color Group List in a Data Policy	Configure the Path Preference for a Preferred Color Group List in a Data Policy	Passed	

ENJ.HSDWAN.20.9.1_17.9.1_N.29	With a direct path, configure Transport Gateway with preference Using vManage and test Re-Origination Dampening under 10 seconds	With a direct path, configure Transport Gateway with preference Using vManage and test Re-Origination Dampening under 10 seconds	Passed	
ENJ.HSDWAN.20.9.1_17.9.1_N.30	With a direct path, configure Transport Gateway with preference Using vManage and test Re-Origination Dampening over 10 seconds	With a direct path, configure Transport Gateway with preference Using vManage and test Re-Origination Dampening over 10 seconds	Passed	

ALG Support for NAT and Firewall on IOS XE SDWAN

Logical ID	Title	Description	Status	Defect ID
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.001	To configure NAT ALG for FTP server	To configure the NAT ALG for TFTP Server using the NATPOOL Address.	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.002	To configure NAT ALG for DNS server using UDP protocol	To configure NAT ALG for DNS server using UDP protoco	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.003	To configure NAT ALG for DNS server using TCP protocol.	To configure NAT ALG for DNS server using TCP protocol	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.004	To configure NAT ALG NAT translations exists if the device has reloaded	To configure NAT ALG NAT translations exists if the device has reloaded	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.005	To configure NAT ALG works on ISR platform and check the NAT performance.	To configure NAT ALG works on ISR platform and check the NAT performance	Failed	CSCwd13720
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.006	To configure NAT ALG works on at Cat 8k platform and check the NAT performance	To configure NAT ALG works on at Cat 8k platform and check the NAT performance	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.007	To performance NAT scaling along with ALG	To performance NAT scaling along with ALG.	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.008	To enable ALG Nat service for specific protocol	To enable ALG Nat service for specific protocol	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.009	To disable ALG Nat service for specific protocol.	To enable ALG Nat service for specific protocol	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.010	To create NAT ALG using DIA static route (Nat route vrf).	To create NAT ALG using DIA static route (Nat route vrf)	Passed	

ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.011	To create NAT ALG using DIA using Data Policy (Nat use - VPN 0)	To create NAT ALG using DIA using Data Policy (Nat use - VPN 0)	Passed	
ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.012	To create NAT ALG using dual Inet (Nat fall back) by shutting any one Inet connect interface.	To create NAT ALG using dual Inet (Nat fall back) by shutting any one Inet connect interface	Passed	
ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.013	To perform ALG along with ZFBW policy to inspect TCP application services.	To perform ALG along with ZFBW policy to inspect HTTP application services	Passed	
ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.014	To perform NAT ALG along with policy to drop TCP application services.	To perform NAT ALG along with policy to drop TCP application services.	Passed	
ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.015	To perform NAT ALG along with ZBFW policy match condition to inspect HTTP application services.	ALG Support for NAT and Firewall on IOS XE SDWAN	Passed	
ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.016	To perform NAT ALG along with DIA + ZBFW to pass specific protocol traffic	To perform NAT ALG along with DIA + ZBFW to pass specific protocol traffic	Passed	
ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.017	To Verify the NAT Timeouts and Protocol Listening by NAT ALG	To Verify the NAT Timeouts and Protocol Listening by NAT ALG.	Passed	
ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.018	To Check and Clear Nat translations and check for re-session creation.	To Verify the NAT Timeouts and Protocol Listening by NAT ALG.	Passed	
ENJ.ALGNAT. SDWAN.20.9.1_17.9.1. N.019	To check protocol timeout sessions and termination with NAT ALG.	To check protocol timeout sessions and termination with NAT ALG	Passed	

ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.020	To route the traffic between source and destination based on AD preference of the Inet links and perform ALG NAT translations.	To route the traffic between source and destination based on AD preference of the Inet links and perform ALG NAT translations.	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.021	To configure and enable NAT ALG service with NAT interface overload.	To configure and enable NAT ALG service with NAT interface overload	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.022	To configure and enable NAT ALG service with NAT interface overload.	To configure and enable NAT ALG service with NAT pool interface	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.023	To configure and verify NAT ALG statistics for TCP protocol.	To configure and verify NAT ALG statistics for TFTP protocol	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.024	To configure an ALG with NAT DIA using cli add on template.	To configure and verify NAT ALG statistics for TFTP protocol	Passed	
ENJ.ALGNAT.SDWAN.20.9.1_17.9.1.N.025	To perform NAT ALG for HTTP services using service side static NAT.	To configure and verify NAT ALG statistics for TFTP protocol	Passed	

SIG Tunnel Monitoring / Observability for Zscaler/Umbrella Services

Logical ID	Title	Description	Status	Defect ID
ENJ.SIGTM.20.9.1_17.9.1_N.01	Verify the enhanced visibility fields (HA pair, Provider, tracker, etc) with cEdge as compared to vEdge	Create and apply a SIG Feature Template and add a tracker and verify with Monitor in Vmanage	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.02	Change the Tunnel ID for Tunnel and verify the change is reflected under new visibility field	Create and apply a SIG Feature Template and change the tunnel id and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.03	Change the Site ID for Tunnel and verify the change is reflected under new visibility	Create and apply a SIG Feature Template and change The Site id and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.04	Enable Tracker for Tunnel and verify the change is reflected under new visibility field	Create and apply a SIG Feature Template and add a tracker with Enable and verify with Monitor in Vmanage	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.05	Disable Tracker for Tunnel and verify the change is reflected under new visibility field	Create and apply a SIG Feature Template and add a tracker and verify with Monitor then Disable theTracker in Vmanage	Passed	

ENJ.SIGTM.20.9.1_17.9.1_N.06	Configure Destination Data center for Tunnel and verify it is displayed under new visibility field	Create and apply a SIG Feature Template and Add the Destination Data center for tunnel and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.07	Change the Destination Data center for Tunnel and verify the change is reflected under new visibility field	Create and apply a SIG Feature Template and Add the Destination Data center for tunnel and then change the data center and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.08	Configure Active-Active SIG Tunnel and verify HA Pair shows as active	Create and apply a SIG Feature Template and Configure Active-Active SIG Tunnel with verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.09	Configure Active-Active SIG Tunnel, change it to Active-Backup and verify HA Pair shows as backup	Change it to Active-Backup and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.010	Configure Active-Backup SIG Tunnel and verify HA Pair shows as backup Pair shows as backup	Change it to Active-Backup and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.011	Configure Active-Backup SIG Tunnel, change it to Active-Active and verify	Change it to Active-Actisve and verify	Passed	

ENJ.SIGTM.20.9.1_17.9.1_N.12	Configure Source-Only Load sharing enabled SIG Tunnel and verify	Configure Source-Only Load sharing enabled SIG Tunnel and verify Tunnel Event details	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.13	Configure Weighted SIG Active-Active Source-Only Load Sharing and verify	Configure Weighted SIG Active-Active Source-Only Load Sharing and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.14	Configure Active-Backup SIG and verify Tunnel state is Up/Color is Green	Configure Active-Backup SIG and verify Tunnel state is Up/Color is Green	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.15	Without Tracker enabled, bring down Active Tunnel and verify Tunnel state is still Up/ Color is still Green	Without Tracker enabled, bring down Active Tunnel and verify Tunnel state is still Up/ Color is still Green	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.16	Without Tracker enabled, bring down Active and Backup Tunnels and verify Tunnel State is Down/Color is Red	Change it to Active-Backup and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.17	Bring down a Tracker, then verify Tunnel state is Down/Color is Orange, Tunnel Event details and counts	Bring down a Tracker, then verify Tunnel state is Down/Color is Orange, Tunnel Event details and counts	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.18	Bring up a downed Tracker and verify Tunnel state is Down/Color is Green and Tunnel Event details	Bring up a downed Tracker and verify Tunnel state is Down/Color is Green and Tunnel Event details	Passed	

ENJ.SIGTM.20.9.1_17.9.1_N.19	Under Top Application over SIG, verify the Top Applications are displayed as expected	Under Top Application over SIG, verify the Top Applications are displayed as expected	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.20	Change usage of Top Applications, verify the Top Applications are changed	Change usage of Top Applications, verify the Top Applications are changed	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.21	Shut the backup tunnel and check the tunnel traffic and status with verify the change is reflected under new visibility field	Shut the backup tunnel and check the tunnel traffic and status with verify the change is reflected under new visibility field	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.22	Shut the active tunnel and check the tunnel traffic and status with verify the change is reflected under new visibility field	Shut the active tunnel and check the tunnel traffic and status with verify the change is reflected under new visibility field	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.23	Create Gre Tunnel and Enable the tracker and check it should be reflected in Visibility field	Create Gre Tunnel and Enable the tracker and check it should be reflected in Visibility field	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.24	Bring down GRE Tunnel and tracker enabled, Monitor the Security and check Tracker is up & tunnel is Down	Bring down GRE Tunnel and tracker enabled, Monitor the Security and check Tracker is up & tunnel is Down	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.25	Configure latency due to tracker down and monitor Event or check through CLI	Configure latency due to tracker down and monitor Event or check through CLI	Passed	

ENJ.SIGTM.20.9.1_17.9.1_N.26	Create a tracker in vmanage to choose the user defined tracker created and Monitor the Event	Create a tracker in vmanage to choose the user defined tracker created and Monitor the Event	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.27	Delete Latency and check tracker should Up or not through Cli or Events	Delete Latency and check tracker should Up or not through Cli or Events	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.28	Create Umbrella root certificate and update in Administrator Setting and check its update or not	Change it to Active-Backup and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.29	Create manually Device Registration with umbrella by VPN and Verify	Create manually Device Registration with umbrella by VPN and Verify	Failed	CSCwd09809
ENJ.SIGTM.20.9.1_17.9.1_N.30	Check Device Vpn Through Traffic is Going or not	Check Device Vpn Through Traffic is Going or not	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.31	Create IPSec Tunnel By Zscaler and verify	Create IPSec Tunnel By Zscaler and verify	Passed	
ENJ.SIGTM.20.9.1_17.9.1_N.32	Configure GRE Tunnel By Zscaler and verify its working or not	Configure GRE Tunnel By Zscaler and verify	Passed	

Cisco SD-WAN (on-prem security) - Identity Firewall (with AD integration) Services

Logical ID	Title	Description	Status	Defect ID
ENJ.IDF.20.9.1_17.9.1_N01	To integrate ISE with SDWAN Vmanage and AD	Integration of ISE with vmanage	Failed	CSCwd16975, CSCwd10798
ENJ.IDF.20.9.1_17.9.1_N02	To Evaluate configured User in the ISE are being reflected in the Vmanage	To evaluate user details in Vmanage	Passed	
ENJ.IDF.20.9.1_17.9.1_N03	To Evaluate configured User groups in the ISE are being reflected in the Manage	To evaluate user group details in Vmanage	Passed	
ENJ.IDF.20.9.1_17.9.1_N04	To add/delete the user/user group in vmanage and to verify if the same has been updated in ISE and AD	Add/Delete of user/user group in Vmanage	Failed	CSCwd22733
ENJ.IDF.20.9.1_17.9.1_N05	To edit the user/user groups in vmanage and to verify if the same has been updated in ISE and AD	Edit the user/user group in vmanage	Failed	CSCwd19592
ENJ.IDF.20.9.1_17.9.1_N06	To check the re-sync performance after terminating the session from vmanage and ISE	To check the resync performance of ISE after session termination	Failed	CSCwd19693
ENJ.IDF.20.9.1_17.9.1_N07	To Check for the Logs and Reports in the Vmanage for the configured user and user group	To check logs and reports in vmanage	Passed	

ENJ.IDF.20.9.1_17.9.1_N08	To Create a set of 18 user in a Group A identity list Cisco ISE and observe the Results	To create set of users and map to the user group	Passed	
ENJ.IDF.20.9.1_17.9.1_N09	To Create a set of 4 user in a Group B identity list Cisco ISE and observe the Results	To create set of users and map to the user group	Passed	
ENJ.IDF.20.9.1_17.9.1_N10	To Restrict the access to YouTube applications for Group B users using ISE integrations	Integration of ISE with vmanage	Passed	
ENJ.IDF.20.9.1_17.9.1_N11	To Configure and verify the Identity Group " Employee", "Guest", "Partners", Allowing access to youtube.com only	Integration of ISE with vmanage	Passed	
ENJ.IDF.20.9.1_17.9.1_N12	Allowing a Specific user in the Guest to access the Youtube.com and verify the results	Integration of ISE with vmanage	Passed	
ENJ.IDF.20.9.1_17.9.1_N13	To configure and verify the URL's visited by Guest user in the Org using ISE integrations	Integration of ISE with vmanage	Passed	
ENJ.IDF.20.9.1_17.9.1_N14	To Configure and verify the URL filtering for Identity group "Partners" and allow the access Youtube.com with inspect	Integration of ISE with vmanage	Passed	
ENJ.IDF.20.9.1_17.9.1_N15	To Check the user logon session in the vsmart	To Check the user logon session in the vsmart	Passed	

ENJ.IDF.20.9.1_17.9.1_N16	To Check the user logon session in the cat8k platform via OMP	To Check the user logon session in the cat8k platform via OMP	Passed	
ENJ.IDF.20.9.1_17.9.1_N17	Configure Cisco vSmart Controller to Connect to Cisco ISE Using a CLI Template	Configure Cisco vSmart Controller to Connect to Cisco ISE Using a CLI Template	Passed	
ENJ.IDF.20.9.1_17.9.1_N18	To Configure Cisco SD-WAN Identity-Based Firewall Policy Using a CLI Template	To Configure Cisco SD-WAN Identity-Based Firewall Policy Using a CLI Template	Passed	
ENJ.IDF.20.9.1_17.9.1_N19	To Configure Cisco SD-WAN Identity-Based Firewall Policy Using a CLI Template	To Configure Cisco SD-WAN Identity-Based Firewall Policy Using a CLI Template	Passed	
ENJ.IDF.20.9.1_17.9.1_N20	To Create ZBFW policy for user from the created user group in AD/ISE "Employees" to access Google.com	To create ZBFW for the users create in ISE to access google.com	Passed	
ENJ.IDF.20.9.1_17.9.1_N21	To Create ZBFW policy for user from the created user group in AD/ISE "Employees" to access Yahoo.in Along with inspect	To Create ZBFW policy for user from the created user group in AD/ISE "Employees" to access Yahoo.in Along with inspect	Passed	
ENJ.IDF.20.9.1_17.9.1_N22	To Create ZBFW policy for user from the created user group in AD/ISE "Guest" to Drop the packets routed to Yahoo.in	To Create ZBFW policy for user from the created user group in AD/ISE "Guest" to Drop the packets routed to Yahoo.in	Passed	

ENJ.IDF.20.9.1_17.9.1_N23	To Create ZBFW policy for user from the created user group in AD/ISE "Guest" to Drop the packets routed to Yahoo.in	To create set of users and map to the user group	Passed	
ENJ.IDF.20.9.1_17.9.1_N24	To Create ZBFW policy for user from the created user group in AD/ISE "Employees" to access Yahoo.in Along with inspect in ASR platform	To create ZBFW to user group to access the URL in ASR platform	Passed	
ENJ.IDF.20.9.1_17.9.1_N25	To Restrict the access to User group "Employee “for the Internal Server hosted in DC identical list and verify the results with ACL	To restrict the access to the user group	Passed	
ENJ.IDF.20.9.1_17.9.1_N26	To Delete the ISE connections and check the user group and user details	To Delete the ISE connections	Passed	
ENJ.IDF.20.9.1_17.9.1_N27	Verify the behaviour when vSmart reboots	Verify the behaviour when smart reboots	Passed	
ENJ.IDF.20.9.1_17.9.1_N28	Verify the behaviour when "clear omp all" is triggered on vSmart	Verify the behaviour when "clear omp all" is triggered on vSmart	Passed	
ENJ.IDF.20.9.1_17.9.1_N29	Edit the IP address for existing ISE connection with vManage	To edit the IP address for existing ISE connection with vManage	Passed	
ENJ.IDF.20.9.1_17.9.1_N30	Edit the username/password for existing ISE connection with vManage	Edit the username/password for existing ISE connection with vManage	Passed	

ENJ.IDF.20.9.1_17.9.1_N31	To Check for ISE registeration and mapping redistribution when vSmarts are in cluster	To Check for ISE registeration and mapping redistribution when vSmarts are in cluster	Passed	
ENJ.IDF.20.9.1_17.9.1_N32	Edit the username/password for existing ISE connection with vManage	Edit the username/password for existing ISE connection with vManage	Passed	

SDWAN UX 2-0 - Configuration 2-0 Feature Profiles and Configuration Groups

Logical ID	Title	Description	Status	Defect ID
ENJ. CFPCG.20.9.1_17.9.1. N.001	To create a configuration group workflow for a single router	To create a configuration group workflow for a single router	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.002	To Use the new simplified workflow introduced in 20.9 to create configuration group	To Use the new simplified workflow introduced in 20.9 to create configuration group	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.003	To resume the Configuration Group Workflow	To resume the Configuration Group Workflow	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.004	To add Devices to a Configuration Group Using Rules and operations	To add Devices to a Configuration Group Using Rules and operations	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.005	To Create management VPN feature	To Create management VPN feature	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.006	To switch the profile to another profile	To switch the profile to another profile	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.007	To add feature and sub feature to perform LAN routing	To add feature and sub feature to perform LAN routing	Failed	CSCwd23734, CSCwd06835
ENJ. CFPCG.20.9.1_17.9.1. N.008	To create SVI profile using routing option with enabling the track OMP	To create SVI profile using routing option with enabling the track OMP	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.009	To edit SVI profile	To edit SVI profile	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.010	To create ThousandEyes profile with version v2/V	To create ThousandEyes profile with version v2/V	Passed	

ENJ.CFPCG.20.9.1_17.9.1.N.011	To Add/Remove/deploy associated devices from config groups	To Add/Remove/deploy associated devices from config groups	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.012	To Create Thousand Eye Parcel via API	To Create Thousand Eye Parcel via API	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.013	To Get SNMP details of an SNMP parcel via API	To Get SNMP details of an SNMP parcel via API	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.014	To Associate WAN BGP to Transport VPN via API	To Associate WAN BGP to Transport VPN via API	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.015	To Change System ID via Global Parcel API	To Change System ID via Global Parcel AP	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.016	To disassociate the profil	Disassociate the profil	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.017	To create Global parcel using global settings and other settings	To create Global parcel using global settings and other settings	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.018	To delete Global parcel	To delete Global parcel	Failed	CSCwd11936
ENJ.CFPCG.20.9.1_17.9.1.N.019	To create a cellular interface under configuration group feature with associated Tunnel and NAT	To create a cellular interface under configuration group feature with associated Tunnel and NAT	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.020	To create tracker to the WAN parcel	To create WAN VPN parcel using BGP routing	Passed	
ENJ.CFPCG.20.9.1_17.9.1.N.021	To Configure user and authentication with SNMP version 3	To Configure user and authentication with SNMP version 3	Failed	
ENJ.CFPCG.20.9.1_17.9.1.N.022	To trap the target server with SNMP V3	To trap the target server with SNMP V3	Failed	CSCwd06287

ENJ. CFPCG.20.9.1_17.9.1. N.023	To create SNMP V3 parcel with view and community	To create SNMP V3 parcel with view and community	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.024	To change the authentication of user using SNMP V3 parcel	To change the authentication of user using SNMP V3 parcel	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.025	To associate WAN VPN to WAN BGP parcel	To associate WAN VPN to WAN BGP parcel	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.026	To create BFD parcel	To create BFD parcel	Failed	CSCwd02002
ENJ. CFPCG.20.9.1_17.9.1. N.027	To edit LAN VPN Parcel	To edit LAN VPN Parcel	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.028	To create a Localized policy using cli profile	To create a Localized policy using cli profile	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.029	To Create system profile via API	To Create system profile via API	Passed	
ENJ. CFPCG.20.9.1_17.9.1. N.030	To Configure the Dialler interface with Ip address and Dialler pool over PP	By using Dialler interface, we have to configure the Ip Address and dialer pool over encapsulation PPP	Passed	

PPP/Dialer interface support for DIA NAT use-cases

Logical ID	Title	Description	Status	Defect ID
ENJ.PPP.20.9.1_17.9.1_N.01	Configure the Dialler interface with Ip address and Dialler pool over PPP	By using Dialler interface, we have to configure the Ip Address and dialer pool over encapsulation PPP	Passed	
ENJ.PPP.20.9.1_17.9.1_N.02	Configure to enable the PPPOE with Dialler pool by using physical interface	Configure to enable the PPPOE with Dialler pool by using physical interface	Passed	
ENJ.PPP.20.9.1_17.9.1_N.03	Configure the DIA for NAT fallback with Dialler interface by using Secondary interface	By using Dialler interface, need to Track the endpoint by enabling the NAT DIA fall back	Passed	
ENJ.PPP.20.9.1_17.9.1_N.04	Configure the Dialler interface support for DIA NAT by using loopback interface	By using Dialler interface, need to	Passed	
ENJ.PPP.20.9.1_17.9.1_N.05	Configure the static ip address negotiated support for Dailer with NAT DIA	By using Dialler interface, need to configure with Static ip address	Passed	
ENJ.PPP.20.9.1_17.9.1_N.06	Configure the Dailer interface for DIA in PPPOE by CHAP in PPP encapsulation	By using Dialler interface for DIA in PPPOE by CHAP	Passed	
ENJ.PPP.20.9.1_17.9.1_N.07	Configure the Dailer interface for DIA in PPPOE by CHAP in PPP encapsulation	By using Dialler interface for DIA in PPPOE by PPP	Passed	
ENJ.PPP.20.9.1_17.9.1_N.08	Configure the ip Nat inside through Vmanage by enabling the NAT type with interface	By using Vmanage configure the IP Nate inside with NAT type interface	Passed	

ENJ.PPP.20.9.1_17.9.1_N.09	Configure the PPPOE Dailer by using sub interface	By using sub interface, we have to configure the PPPOE dialler configuration	Passed	
ENJ.PPP.20.9.1_17.9.1_N.010	Configure the PPP Dailer interface to track the dual endpoint tracker by using WAN Interface	By using sub interface, we have to configure the PPPOE dialler configuration	Passed	
ENJ.PPP.20.9.1_17.9.1_N.011	Configure the PPP interface with enable the PPPOE over encapsulation PPP	By using Dialler interface, we need to enable the PPP CHAP over PPP	Passed	
ENJ.PPP.20.9.1_17.9.1_N.011	configure the PPPoE Dailer interface to track the endpoint IP addresS	By using PPPOE Dailer interface to track the endpoint IP address	Passed	
ENJ.PPP.20.9.1_17.9.1_N.013	Configure the PPPOE in Dailer interface with TCP MSS and NAT DIA	By using PPPOE Dailer interface with TCP MSS and NAT DIA	Passed	
ENJ.PPP.20.9.1_17.9.1_N.014	Configure the Dailer interface support for NAT DIA with endpoint tracker Along with PPPOE	By using Dailer interface with NAT DIA for Tracker along with PPPOE	Passed	
ENJ.PPP.20.9.1_17.9.1_N.015	Configure the PPP dialler interface to track the DNS server with type of interface	By using PPPOE Dailer interface to track the endpoint DNS server	Passed	
ENJ.PPP.20.9.1_17.9.1_N.016	To configure Dailer interface with ip nat outside with encapsulation ppp	To configure Dailer interface with ip nat outside with encapsulation ppp	Passed	
ENJ.PPP.20.9.1_17.9.1_N.017	Configure the PPPOE over (ATM) Sub interface PPP by using CLI	By using CLI PPPOE over Sub interface PPP	Passed	

ENJ.PPP.20.9.1_17.9.1_N.018	PPPoE Dialer with NAT interface overload by using Vmanage	By using PPPOE Dailer with NAT interface in Vmanage	Passed	
ENJ.PPP.20.9.1_17.9.1_N.019	Configure the PPPOE Dialer with Encapsulation PPP by Using Vmanage	By using PPPOE Dailer with encapsulation PPP in Vmanage	Failed	CSCwd10828
ENJ.PPP.20.9.1_17.9.1_N.019	Configure the PPPOE Dailer with NAT and endpoint tracker by using Vmanage	By using PPPOE Dailer with NAT and endpoint-tracker in Vmanage	Passed	
ENJ.PPP.20.9.1_17.9.1_N.021	Configure the Dialler with NAT DIA interface overload using Static inside	By using NAT DIA Interface overload using Static inside	Passed	
ENJ.PPP.20.9.1_17.9.1_N.022	Configure PPPOE Dialler interface with static port forwarding by using HTTP	Configure PPPOE Dialler interface with static port forwarding by using HTTP	Passed	
ENJ.PPP.20.9.1_17.9.1_N.023	Configure PPPOE Dailer egress interface with port forwarding by using Telnet	By using PPPOE Dialler egress interface with port forwarding	Passed	
ENJ.PPP.20.9.1_17.9.1_N.024	Configure the PPPOE with NAT DIA interface pool overload	Configure the PPPOE with NAT DIA interface pool overload	Passed	
ENJ.PPP.20.9.1_17.9.1_N.025	Configure and Check whether PPPOE NAT Translation exists if the device as reloaded	Configure and Check whether PPPOE NAT Translation exists if the device as reloaded	Passed	

Port forwarding on cedge/vedge with port change

Logical ID	Title	Description	Status	Defect ID
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.01	Configure Static NAT DIA port forwarding with vrf	Configuring Static NAT DIA port forwarding in the WAN for direct internet access.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.02	To check the NAT port translation after the device is reloaded.	Configuring DIA port forwarding with pool with port in the WAN for direct internet access.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.03	Configure Static NAT DIA port forwarding without VRF using port.	Configuring Static NAT DIA port forwarding without VRF in the WAN for direct internet access	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.04	Configure the DIA port forwarding with pool address with port	Configuring DIA port forwarding with pool with port in the WAN for direct internet access.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.05	Configure DIA port forwarding with interface address and port with port change with vrf	Configure DIA port forwarding with interface address and port with port change with vrf.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.06	Configure DIA port forwarding with WAN interface address and port with port change without vrf.	Configuring and checking NAT translations for Static NAT DIA with port change.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.07	To configure and verify whether loopback interface is supported for NAT DIA port forwarding	Configure the DIA port forwarding using loopback interface.	Passed	

ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.08	Configure the DIA port forwarding using Sub-interface	Configure the DIA port forwarding using loopback interface.	Passed	
ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.09	Configure DIA port forwarding with public address and port change using VRF.	Configure DIA port forwarding with public address and port change using vrf.	Failed	CSCwd12426
ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.10	Configuration through vmanage CLI add on template	Check NAT translations with port forwarding for DIA while configuring through vManage CLI template.	Passed	
ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.11	To check the timing session for NAT port translations.	Check the timing session for NAT port translations	Passed	
ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.12	Configuring port forwarding through vmanage feature template.	Configure port forwarding through vManage feature template.	Passed	
ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.13	Configuring port forwarding through vmanage feature template.	Comparison of NAT port forwarding on different platforms. (ISR and cat8k)	Passed	
ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.14	Configuring NAT DIA tracker to observe the connectivity	Configuring NAT DIA tracker to observe the connectivity	Passed	
ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.15	To check NAT translations for port forwarding through overlay tunnel	Check NAT translations for port forwarding through overlay tunnel when the DIA interface is down.	Passed	
ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.16	Configuring port forwarding on multiple interfaces	Check how NAT translations with port forwarding happens when it is configured on multiple interfaces	Passed	

ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.17	To check NAT translations when the device is accessed via TELNET.	Configure NAT DIA port forwarding with TCP traffic and observe NAT translations.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.18	To configure the static NAT Port forwarding in UDP port 5001 using cli template	To configure the static NAT Port forwarding in UDP port 5001 using cli template	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.19	To configure the static NAT Port forwarding in UDP port 5002 using cli template.	To configure the static NAT Port forwarding in UDP port 5002 using cli template	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.20	To check the NAT translations when the interface is flapping	Check NAT translations while the interface is flapping.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.21	To configure and check the Nat translations for SSNAT and DIA	Check NAT translations for DIA with port forwarding while the service side is behind NAT.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.22	To configure dynamic NAT inside and static port forwarding.	Check NAT translations for DIA with port forwarding while the service side is behind NAT.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.23	To configure the port forwarding using data policy with unmatched Nat pool.	Check NAT translations for DIA with port forwarding while the service side is behind NAT.	Passed	
ENJ.NDPF. SDWAN.20.9.1_17.9.1. N.24	To check NAT translations for different prefix lengths for port forwarding	Check NAT translations for DIA with port forwarding for various prefix lengths.	Passed	

ENJ.NDPF.SDWAN.20.9.1_17.9.1.N.25	To configure NAT DIA port forwarding on the Dialer interface in cEdge	Check NAT translations for DIA with port forwarding configured in the Dialer interface.	Passed	

App aware routing for IPv6

Logical ID	Title	Description	Status	Defect ID
ENJ.AARIPV6.20.9.1_17.9.1_N.01	To Configure the AAR policy for ipv6 using vmanage	To Configure the AAR policy for ipv6 using vmanage	Failed	CSCwd28214
ENJ.AARIPV6.20.9.1_17.9.1_N.02	To Configure the AAR policy with dual stack using vmanage	To Configure the AAR policy with dual stack using vmanage	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.03	To Configure the Best Tunnel path for IPV6 using backup-preferred colour	To Configure the Best Tunnel path for IPV6 using backup-preferred colour	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.04	To Configure the Best Tunnel path for IPV6 using Fallback-to-best-path	To Configure the Best Tunnel path for IPV6 using Fallback-to-best-path	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.05	To Configure the Best Tunnel path for Dual stack using backup-preferred colour	To Configure the Best Tunnel path for Dual stack using backup-preferred colour	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.06	Configure BFD parameters Hello Interval 1000ms and poll interval 30s & multiplier 2 and observe the performance for AAR for IPv6	Configure BFD parameters Hello Interval 1000ms and poll interval 30s & multiplier 2 and observe the performance for AAR for IPv6	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.07	Configure the Application Aware Routing for IPv6 using CLI	Configure the Application Aware Routing for IPv6 using CLI	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.08	To Configure and verify the AAR policy for ipv6 using vmanage in ISR platform	To Configure and verify the AAR policy for ipv6 using vmanage in ISR platform	Passed	

ENJ.AARIPV6.20.9.1_17.9.1_N.09	To Configure the Best Tunnel path for IPV6 using backup-preferred color in ISR platform	To Configure the Best Tunnel path for IPV6 using backup-preferred color in ISR platform	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.10	To Configure the Best Tunnel path for IPV6 using Fallback-to-best-path in ISR platform	To Configure the Best Tunnel path for IPV6 using Fallback-to-best-path in ISR platform	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.11	To Configure and verify the AAR policy using Default action for IPv6	To Configure and verify the AAR policy using Default action for IPv6	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.12	To Configure and Verify the AAR Policy based on Strict SLA Class for IPv6	To Configure and Verify the AAR Policy based on Strict SLA Class for IPv6	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.13	To Configure and Verify the AAR Policy based on Strict SLA Class for Dual Stack	To Configure and Verify the AAR Policy based on Strict SLA Class for Dual Stack	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.14	To Configure and verify the AAR apply policy to specific Site and VPN.00	To Configure and verify the AAR apply policy to specific Site and VPN.00	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.15	To Monitor the Data plane Tunnel Performance for AAR ipv6	To Monitor the Data plane Tunnel Performance for AAR ipv6	Passed	
ENJ.AARIPV6.20.9.1_17.9.1_N.16	To Configure and Verify the AAR Policy based on Strict SLA Class for IPv6 with ASR platform	To Configure and Verify the AAR Policy based on Strict SLA Class for IPv6 with ASR platform	Passed	

(Device Only-CLI-Template) Packet Tagging - Phase 2 - CLI Template

Logical ID	Title	Description	Status	Defect ID
ENJ.PT.20.9.1_17.9.1_N.01	To configure Tag ID & Tag Name using vmanage CLI Template	To Create Tag ID & Tag Name using vManage CLI Template	Passed	
ENJ.PT.20.9.1_17.9.1_N.02	To Delete Tag ID & Tag Name using vManage CLI Template	To Delete Tag ID & Tag Name using vManage CLI Template	Passed	
ENJ.PT.20.9.1_17.9.1_N.03	To Create Tag using data prefix-list name	Create Tag using data prefix-list name	Passed	
ENJ.PT.20.9.1_17.9.1_N.04	To Create Tag using data ipv6 prefix-list name	Create Tag using data ipv6 prefix-list name	Passed	
ENJ.PT.20.9.1_17.9.1_N.05	To Create Tag using app list name	Create Tag using app-list name	Passed	
ENJ.PT.20.9.1_17.9.1_N.06	To Create Tag match under policy using match attribute source- tag instance	Create Tag match under policy using match attribute source-tag instance	Passed	
ENJ.PT.20.9.1_17.9.1_N.07	To Create Tag match under policy using match attribute Destination- tag instance	Create Tag match under policy using match attribute Destination-tag instance	Passed	
ENJ.PT.20.9.1_17.9.1_N.08	To Create Tag match under policy using match attribute Source Destination- tag instance	Create Tag match under policy using match attribute source Destination-tag instance	Passed	
ENJ.PT.20.9.1_17.9.1_N.09	To Create Tag match under localized policy using ACL	Create Tag match under localized policy using ACL	Passed	

ENJ.PT.20.9.1_17.9.1_N.10	To Create Tag match under Centralized policy using match Data policy	Create Tag match under Centralized policy using data\u0002policy	Passed	
ENJ.PT.20.9.1_17.9.1_N.11	To Create Tag match under centralized policy using ARR-policy	Create Tag match under Centralized policy using AAR\u0002policy	Passed	
ENJ.PT.20.9.1_17.9.1_N.12	To create Direction tag to match parameter like data-prefix list when matched under policy, it can be matched as source or destination	Create Direction tag to match parameter like data-prefix	Passed	
ENJ.PT.20.9.1_17.9.1_N.13	To create Direction-less tag to match parameter like app-list	Create direction-less tag to match parameter like app-list	Passed	
ENJ.PT.20.9.1_17.9.1_N.14	To create Direction-less tag to match parameter like app-list using saas app	Create direction-less tag to match parameter like App-list using SaaS app	Passed	
ENJ.PT.20.9.1_17.9.1_N.15	To create Direction-less tag to match parameter like app-list using DIA	To Create direction-less tag to match parameter app-list using DIA	Passed	

[Phase 2] vManage support for dispatching CLI commands to cEdge and vEdge

Logical ID	Title	Description	Status	Defect ID
ENJ.VMSC.20.9.1_17.9.1_N.01	Check the CLI show command in vManage to check the clock - vEdge	To Check the CLI show command in vManage to check the clock - vEdge	Passed	
ENJ.VMSC.20.9.1_17.9.1_N.02	Check the CLI show command in vManage to check the hardware real time information - vEdge	Check the CLI show command in vManage to check the hardware real time information - vEdge	Passed	
ENJ.VMSC.20.9.1_17.9.1_N.03	Check the CLI show command in vManage to check the nslookup for dns - vEdge	Check the CLI show command in vManage to check the nslookup for dns - vEdge	Passed	
ENJ.VMSC.20.9.1_17.9.1_N.04	Check the CLI show command in vManage to check the control connection info - vEdge	Check the CLI show command in vManage to check the control connection info - vEdge	Passed	
ENJ.VMSC.20.9.1_17.9.1_N.05	Check the CLI show command in vManage to check the appqoe flow flow-id - cEdge	Check the CLI show command in vManage to check the appqoe flow flow-id - cEdge	Passed	
ENJ.VMSC.20.9.1_17.9.1_N.06	Check the CLI show command in vManage to check the appqoe flow flow-id - cEdge	Check the CLI show command in vManage to check the appqoe flow flow-id - cEdge	Passed	
ENJ.VMSC.20.9.1_17.9.1_N.07	Check the CLI show command in vManage to check the appqoe flow closed - cEdge	Check the CLI show command in vManage to check the appqoe flow closed - cEdge	Passed	

ENJ.VMSC.20.9.1_17.9.1_N.08	Check the CLI show command in vManage to check the data policy - cEdge	Check the CLI show command in vManage to check the data policy - cEdge	Passed	
ENJ.VMSC.20.9.1_17.9.1_N.09	Check the CLI show command in vManage to check the app-route policy - cEdge	Check the CLI show command in vManage to check the app-route policy - cEdge	Passed	
ENJ.VMSC.20.9.1_17.9.1_N.10	Check the CLI show command in vManage to check the committed configuration - cEdge	Check the CLI show command in vManage to check the committed configuration - cEdge	Passed	

Co-management Ph2 - Ability to support granular RBAC and co-manage configuration 2-0

Logical ID	Title	Description	Status	Defect ID
ENJ.RBAC.20.9.1_17.9.1_N.01	Configure RBAC NetworkProtocol Read access for user group	Configure granular permission granting a user group access to NetworkProtocol Template Read access.	Failed	CSCwc93448
ENJ.RBAC.20.9.1_17.9.1_N.02	Configure RBAC NetworkProtocol Write access for user group	Configure granular permission granting a user group access to NetworkProtocol Template Write access.	Failed	CSCwc96142
ENJ.RBAC.20.9.1_17.9.1_N.03	Moving a user out of group with SecurityPolicy read access to verify SecurityPolicy is not visible	Moving a user out of group with SecurityPolicy read access to verify SecurityPolicy is not visible	Failed	CSCwc96156
ENJ.RBAC.20.9.1_17.9.1_N.04	Moving a user out of group with SecurityPolicy write access to one with SecurityPolicy read access to verify NetworkProtocol feature Template is visible but not editable	Moving a user out of group with SecurityPolicy write access to one with SecurityPolicy read access to verify NetworkProtocol feature Template is visible but not editable	Failed	CSCwc96156
ENJ.RBAC.20.9.1_17.9.1_N.05	Removing SecurityPolicy read access to verify SecurityPolicy Template is not visible	Removing SecurityPolicy read access to verify SecurityPolicy Template is not visible	Failed	CSCwc96156

ENJ.RBAC.20.9.1_17.9.1_N.06	Removing SecurityPolicy write access to a group leaving SecurityPolicy read access to verify SecurityPolicy Template is visible but not editable	Removing SecurityPolicy write access to a group leaving SecurityPolicy read access to verify SecurityPolicy Template is visible but not editable	Failed	CSCwc93470
ENJ.RBAC.20.9.1_17.9.1_N.07	Configure RBAC NetworkProtocol Read access for user group	Configure granular permission granting a user group access to NetworkProtocol Template Read access.	Failed	CSCwc93470
ENJ.RBAC.20.9.1_17.9.1_N.08	Configure RBAC Snmp Write access for user group	Configure granular permission granting a user group access to Snmp Template Write access	Failed	CSCwc93470
ENJ.RBAC.20.9.1_17.9.1_N.09	GET API Call for RBAC Thousandeyes with permission	GET API Call for RBAC Thousandeyes with permission	Passed	
ENJ.RBAC.20.9.1_17.9.1_N.10	GET API Call for RBAC Service without permission	GET API Call for RBAC Service without permission	Passed	
ENJ.RBAC.20.9.1_17.9.1_N.11	POST API Call to create Permission for RBAC Service lan/vpn	POST API Call to create Permission for RBAC Service lan/vpn	Passed	
ENJ.RBAC.20.9.1_17.9.1_N.12	POST API Call to create Permission for RBAC Service lan/vpn	POST API Call to create Permission for RBAC Service lan/vpn	Passed	
ENJ.RBAC.20.9.1_17.9.1_N.13	DELETE API Call to delete Permission for RBAC Service lan/vpn	DELETE API Call to delete Permission for RBAC Service lan/vpn	Passed	
ENJ.RBAC.20.9.1_17.9.1_N.14	GET API Call for RBAC System Feature’s bfd details	GET API Call for RBAC System Feature’s bfd details	Passed	

ENJ.RBAC.20.9.1_17.9.1_N.15	GET API Call to display all the Configuration Groups	GET API Call to display all the Configuration Groups	Passed	
ENJ.RBAC.20.9.1_17.9.1_N.16	POST API to create a Role in a Service	POST API to create a Role in a Service	Passed	
ENJ.RBAC.20.9.1_17.9.1_N.17	PUT and GET API to modify and view a Role in a Service	PUT and GET API to modify and view a Role in a Service	Passed	

vManage integration with On Prem SSM

Logical ID	Title	Description	Status	Defect ID
ENJ.SSM.20.9.1_17.9.1_N.01	Configure SmartLicencing in Online mode in Vmanage and verify	Configure Smart Licensing in Online mode in Vmanage and verify	Passed	
ENJ.SSM.20.9.1_17.9.1_N.02	Configure Smart Licensing in Online mode in Vmanage and verify	Configure Smart Licensing in Online mode in Vmanage and verify	Passed	
ENJ.SSM.20.9.1_17.9.1_N.03	Configure Smart Licensing in Online mode in Vmanage and verify	Configure Smart Licensing in Online mode in Vmanage and verify	Passed	
ENJ.SSM.20.9.1_17.9.1_N.04	in offline mode Assign licenses to using a Template and License tags will be display Based on Selected VA	License tags will be displayed Based on Selected VA in Offline Mode and Verify	Passed	
ENJ.SSM.20.9.1_17.9.1_N.05	in Online mode Assign licenses to using a Template and License tags will be displayed Based on Selected VA	License tags will be displayed Based on Selected VA in Online Mode and Verify	Passed	
ENJ.SSM.20.9.1_17.9.1_N.06	After Assign Licenses check the license tags will display license type prepaid/postpaid/mixed	Verify license type prepaid/postpaid/mixed	Passed	
ENJ.SSM.20.9.1_17.9.1_N.07	OnPream mode, Cisco Smart Software Manager (SSM) is running on the Customer Premises or not	Verify license type prepaid/postpaid/mixed	Passed	
ENJ.SSM.20.9.1_17.9.1_N.08	Configure Smart Licensing In offline mode in Vmanage and verify	Configure Smart Licensing In offline mode in Vmanage and verify	Passed	

ENJ.SSM.20.9.1_17.9.1_N.09	Verify Vamange Send report to onpream SSM and Syncs Report Daily basis	Verify Vamange Send report to onpream SSM and Syncs Report Daily basis	Passed	
ENJ.SSM.20.9.1_17.9.1_N.10	Without Internet Customer communicate through SSM	Without Internet Customer communicate through SSM	Passed	
ENJ.SSM.20.9.1_17.9.1_N.11	Verify Report of assign license When Onpream SSM Connect with Vmanage	Verify Report of assign license When Onpream SSM Connect with Vmange	Passed	
ENJ.SSM.20.9.1_17.9.1_N.12	Verify OnPrem SSM syncs periodically with SSM	Verify OnPrem SSM syncs periodically with SSM	Passed	
ENJ.SSM.20.9.1_17.9.1_N.13	Verify Vamange Send report to onprem SSM and Syncs Report Weekly basis	Verify Vamange Send report to onprem SSM and Syncs Report Weekly basis	Passed	
ENJ.SSM.20.9.1_17.9.1_N.14	In Vmanage Assigned licenses are DNAC License with Installing HSEC License and verify	Vmanage Assigned licenses are DNAC License with Installing HSEC License and verify	Passed	
ENJ.SSM.20.9.1_17.9.1_N.15	Verify Vamange Send report to onpream SSM and Syncs Report Monthly basis	Verify Vamange Send report to onpream SSM and Syncs Report Monthly basis	Passed	
ENJ.SSM.20.9.1_17.9.1_N.16	After syncs report, verify Vmanage receives corresponding report ACK or not	After syncs report, verify Vmanage receives corresponding report ACK or not	Passed	
ENJ.SSM.20.9.1_17.9.1_N.17	Check When Vmanage clear the ACK Report then ACK is Available in DB or not	Check When Vmanage clear the ACK Report then ACK is Available in DB or not	Passed	

SDWAN UX 2-0 - Monitoring 2-0 - Customizable Dashboard, Site Topology and Troubleshooting

Logical ID	Title	Description	Status	Defect ID
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.001	To Add/edit dash lets using action dropdown option	To Add/edit dash lets using action dropdown option	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.002	To reset the dashboard to default view	Reset the dashboard to default view	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.003	To delete and rearrange the dashlet and restore to default view	To delete and rearrange the dashlet and restore to default view	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.004	To check the delete option available in edit mode to delete dashlet	To check the delete option available in edit mode to delete dashlet	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.005	Check device health using badge on device node	To check device health using badge on device node	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.006	Check device details using device 360 page	To check device details using device 360 page	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.007	Check the circuit link associated for the tunnels	Check the circuit link associated for the tunnels	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.008	Check tunnel interface status using VPN Interface side bar	To check tunnel interface status using VPN side ba	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.009	Rearrange the dashlet	To rearrange the dashle	Failed	CSCwc97774, CSCwd13690
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.010	Check the possible navigations allowed in site topology	check the possible navigations allowed in site topology using site health	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.011	To view a Configuration Commit List	To View a network path insight summary	Passed	

ENJ.UXM.SDWAN.20.9.1_17.9.1.N.012	Check top performing AAR applications in dashboard	To check top performing applications in dashboard	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.013	To View Top application and AppQoE Information	To View AppQoE Information	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.014	To view the device information from site topology	To View AppQoE Information	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.015	To monitor the AAR application in table and chart view	To monitor the AAR application in table and chart view	Passed	
ENJ.UXM.SDWAN.20.9.1_17.9.1.N.016	To view transport and service VPN information using site topology	To view transport and service VPN information using site topology.	Passed	

Routing Table Scalability enhancements: Inter-Service VPN Route Leaking for PCI Compliance + vSmart only sends routes to an edge for which the next-hop TLOC is valid

Logical ID	Title	Description	Status	Defect ID
ENJ.SVPNRL.20.9.1_17.9.1_N.01	To Route Leak Between VRF 100 and VRF 200 for the connected Interface, and verify the Results using CLI	To Leak the Routes between service side	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.02	To Redistribute Service VRF 100 and VRF 200 for the BGP and Connected in the Service side.	To Leak the Routes between service side, VRF 200 and VRF 100 for the connected Interface, and verify the Results using vmanage	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.03	To Route Leak Between VRF 100 and VRF 200 for the connected Interface, and verify the Results using CLI with ASR Platform	To Route Leak Between VRF 100 and VRF 200 for the connected Interface, and verify the Results using CLI with ASR Platform	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.04	To Route Leak Between VRF 100 and VRF 200 for the connected Interface, and verify the Results using CLI with ISR Platform	To Route Leak Between VRF 100 and VRF 200 for the connected Interface, and verify the Results using CLI with ISR Platform	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.05	To Redistribute Service VRF 100 and VRF 200 for the OSPF Process running in the service side	To Redistribute Service VRF 100 and VRF 200 for the OSPF Process running in the service side	Passed	

ENJ.SVPNRL.20.9.1_17.9.1_N.06	To Redistribute Service VRF 100 and VRF 200 for the OSPF Process running in the service side with ASR platform	To Redistribute Service VRF 100 and VRF 200 for the OSPF Process running in the service side with ASR platform	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.07	To Redistribute Service VRF 100 and VRF 200 for the ospf Process running in the service side with ISR platform	To Redistribute Service VRF 100 and VRF 200 for the ospf Process running in the service side with ISR platform	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.08	To Redistribute Service VRF 100 and VRF 200 for the BGP Process running in the service side and verify the leaked routes	To Redistribute Service VRF 100 and VRF 200 for the BGP Process running in the service side and verify the leaked routes	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.09	To Redistribute Service VRF 100 and VRF 200 for the BGP Process running in the service side with ASR Platform with ASR platform.	To Redistribute Service VRF 100 and VRF 200 for the BGP Process running in the service side with ASR Platform with ASR platform.	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.10	To Redistribute Service VRF 100 and VRF 200 for the BGP with Metric Process running in the service side and verify the leaked routes	To Redistribute Service VRF 100 and VRF 200 for the BGP with Metric Process running in the service side and verify the leaked routes	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.11	To Route Leak Between VRF 100 and VRF 200 for the connected Interface, and verify the Results using vmanage	To Route Leak Between VRF 100 and VRF 200 for the connected Interface, and verify the Results using vmanage	Passed	

ENJ.SVPNRL.20.9.1_17.9.1_N.12	To Redistribute Service VRF 200 and VRF 100 for the BGP Process running in the service side with ISR Platform Local attribute	To Redistribute Service VRF 200 and VRF 100 for the BGP Process running in the service side with ISR Platform.	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.13	To Redistribute Service VRF 200 and VRF 100 for the OSPF Process running in the service side	To Redistribute Service VRF 200 and VRF 100 for the OSPF Process running in the service side	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.14	To Redistribute Service VRF 100 and VRF 200 for the EIGRP Process running in the service side and verify the Distributed routes	To Redistribute Service VRF 100 and VRF 200 for the EIGRP Process running in the service side and verify the Distributed routes	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.15	To Redistribute Service VRF 200 and VRF 100 for the EIGRP Process running in the service side and verify the results	To Redistribute Service VRF 200 and VRF 100 for the EIGRP Process running in the service side and verify the results	Passed	
ENJ.SVPNRL.20.9.1_17.9.1_N.16	To Create the ZBFW policy for the user in VPN 100 to access Internet and restrict it to VPN 200, and to leak the routes from VPN 100 to VPN 200.	To Create the ZBFW policy for the user in VPN 100 to access Internet and restrict it to VPN 200, and to leak the routes from VPN 100 to VPN 200.	Passed	

ENJ.SVPNRL.20.9.1_17.9.1_N.17	To Create the ZBFW policy for the user in VPN 200 to access Internet and restrict it to VPN 100, and to leak the routes from VPN 200 to VPN 100	To Create the ZBFW policy for the user in VPN 200 to access Internet and restrict it to VPN 100, and to leak the routes from VPN 200 to VPN 100	Passed	

Regression Features

BFD

Logical ID	Title	Status	Defect ID
ENJ.BFD.20.9.1_17.9.1_N.01	To configure BFD for Biz or public interface-overlay	Passed	
ENJ.BFD.20.9.1_17.9.1_N.02	To configure BFD for MPLS or private 1 internet interface-overlay	Passed	
ENJ.BFD.20.9.1_17.9.1_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.20.9.1_17.9.1_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.20.9.1_17.9.1_N.05	To configure BFD for Service-Side EIGRP using vmanage CLI add on template and attach the template to device template	Passed	
ENJ.BFD.20.9.1_17.9.1_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.20.9.1_17.9.1_N.07	To configure BFD for Transport-side BGP using device CLI	Passed	
ENJ.BFD.20.9.1_17.9.1_N.08	To configure BFD for Service-side BGP using device CLI	Passed	
ENJ.BFD.20.9.1_17.9.1_N.09	To configure BFD for Service-side EIGRP using device CLI	Passed	

ENJ.BFD.20.9.1_17.9.1_N.10	To configure BFD for Service-side OSPF using device CLI	Passed	
ENJ.BFD.20.9.1_17.9.1_N.11	To configure hello interval for BFD	Passed	
ENJ.BFD.20.9.1_17.9.1_N.12	To configure pmtu discovery for BFD	Passed	
ENJ.BFD.20.9.1_17.9.1_N.13	To configure Multiple BFD for Transport side	Passed	
ENJ.BFD.20.9.1_17.9.1_N.14	To configure app-route Multiplier for BFD	Passed	
ENJ.BFD.20.9.1_17.9.1_N.15	To configure app-route poll-interval for BFD	Passed	

NBAR

Logical ID	Title	Status	Defect ID
ENJ.NBAR.20.9.1_17.9.1_N.01	Configure & Install NBAR using protocol pack & verify	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.02	Enable protocol discovery using NBAR in a tunnel Interface	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.03	Enable protocol discovery using NBAR in a service Interface	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.04	Enable protocol discovery using NBAR in a tloc tunnel Interface	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.05	Define custom application using ip address with subnet range b/w 24 to 32 for NBAR using centralized policy	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.06	Define custom application using ip address with subnet /29 for NBAR using centralized policy	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.07	Define custom application using port number for NBAR using centralized policy	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.08	Define custom application using port number range TCP/UDP for NBAR using centralized polic	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.09	Define custom application using protocol TCP for NBAR using centralized policy	Passed	
ENJ.NBAR.20.9.1_17.9.1_N.10	Define custom application using protocol UDP for NBAR using centralized policy	Passed	

ENJ.NBAR.20.9.1_17.9.1_ N.11	Define custom application using protocol TCP-UDP for NBAR uisng centralized policy	Passed	
ENJ.NBAR.20.9.1_17.9.1_ N.12	Define custom application using sig tunnel	Passed	
ENJ.NBAR.20.9.1_17.9.1_ N.13	Define custom application using DIA tunnel interface	Passed	
ENJ.NBAR.20.9.1_17.9.1_ N.14	Defining a Web-based Custom Protocol Match application amazon using CLI	Passed	
ENJ.NBAR.20.9.1_17.9.1_ N.15	Defining a Web-based Custom Protocol Match O365 using CLI	Passed	

Path MTU Size

Logical ID	Title	Status	Defect ID
ENJ.PMTU.20.9.1_17.9.1_N.01	To Branch 1 to DC with path mtu size 1496 and size 1496	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.02	To Branch 1 to DC with path mtu size 1256 and size 128	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.03	To Branch 1 to DC with path mtu size 1500 and size 1700 with DF=1	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.04	To Branch 1 to DC with path mtu size 1496 and size 1900 with DF=1	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.05	To Branch 1 to DC with path mtu size 128 and size 1250 with DF=1	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.06	To Branch 1 to DC with path mtu size 1500 and size 1024	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.07	To Branch 1 to DC with path mtu size 900 and size 4096	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.08	To Branch 1 to DC with path mtu size 1496 and size 1450	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.09	To Branch 1 to DC with path mtu size 1500 and size 1456 with DF=1	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.10	Enable PMTU discovery on BFD Tunnel Interface from Branch 1 to DC	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.11	Disable PMTU discovery on BFD Tunnel Interface from Branch 1 to DC	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.12	Enable PMTU discovery on Service side LAN interface in Branch 1 vrf 100	Passed	

ENJ.PMTU.20.9.1_17.9.1_N.13	Enable PMTU discovery on Service side LAN interface in DC vrf 200	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.14	Enable PMTU discovery on Service side LAN interface b/w service router in Branch1 vrf 100	Passed	
ENJ.PMTU.20.9.1_17.9.1_N.15	Enable PMTU discovery on Service side LAN interface b/w service switch in Branch1 vrf 100	Passed	

SD-AVC

Logical ID	Title	Status	Defect ID
ENJ.SD-AVC.20.9.1_17.9.1_N.01	Enable sd-AVC in vManage cluster to define custom application	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.02	Disable sd-AVC in vManage cluster to not define custom application	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.03	Enable app-visiblity & localized policy for SD-AVC to check the status in vManage	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.04	Enable sd-avc & monitor saas custom_application using ip address in vManage	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.05	Enable sd-avc & to monitor saas custom_application using protocol in vManage	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.06	Enable sd-avc & monitor saas custom_application using port no in vManage	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.07	Install the sd-avc package & configure network service in interface using CLI	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.08	Configure sd-avc agent & assign service-ip on edge router	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.09	Enable sd-avc to define nbar application	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.10	Enable sd-avc to check the AAR policy	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.11	Enable sd-avc to check the saas application using sig tunnel	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.12	Enable sd-avc to check the saas application-Family using sig tunnel	Passed	

ENJ.SD-AVC.20.9.1_17.9.1_N.13	Enable sd-avc to check the saas application using DIA site	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.14	Enable sd-avc to check the saas application_family using DIA site	Passed	
ENJ.SD-AVC.20.9.1_17.9.1_N.15	Enable sd-avc to check the saas application using Gateway tunnel	Passed	

Related Documents

Related Documentation

Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.9 Release Notes

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/xe-17-9/sd-wan-rel-notes-xe-17-9.html

Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.9

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/user-access-authentication.html#Cisco_Concept.dita_8717fb5f-8b8a-4ba3-ad42-e302d9b88c29

Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE Release 17.9

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/nat/nat-book-xe-sdwan/configure-nat.html

Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.9

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/redirect-dns.html

Cisco SD-WAN Monitor and Maintain Configuration Guide,Cisco IOS XE Release 17.9

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/centralized-policy.html#Cisco_Concept.dita_e07a2ae9-0df8-4a0d-ab7c-e66f5470159f

Cisco SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.9

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 17.9

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-firewall-17.html#Cisco_SD-WAN_Identity-based_Firewall_Policy