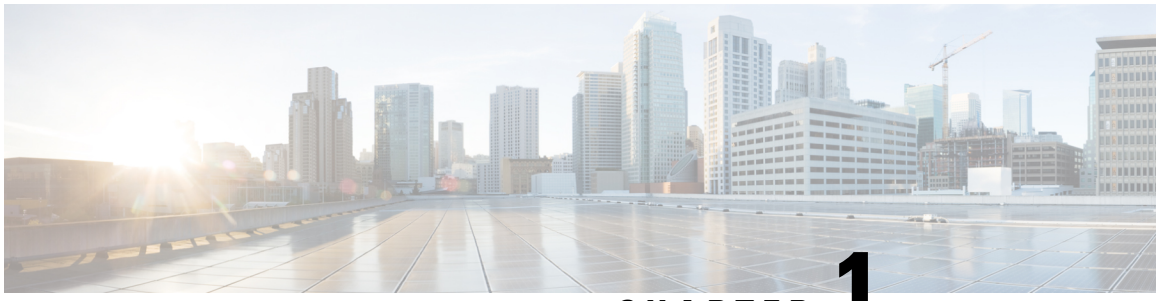
Test Results for SDWAN 20.3 Solution Testing for Japan

First Published: 2021-02-10

Last Modified: 2021-02-18

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



CHAPTER 1

Cisco SDWAN 20.3 Solution Test

Cisco SDWAN Solution Test

Cisco SDWAN Solution Test is an integral part of the Enterprise Networking Solution Management which includes key components such as Cisco IOSXE SDWAN platforms, Cisco SDWAN vManage/vBond/vSmart .

The requirements for Cisco SDWAN Solution Test is derived based on the following:

- Popular customer scenarios
- Customer demands for upgrade
- Inputs from various Business Units, fields and Cisco Services

The test bed architecture is built based on the Solution Reference Network Design (SRND), cross-section of product deployment models etc. The different types of testing carried out as a part of Cisco SDWAN Solution Test are:

- Interoperability/Compatibility
- Functionality
- Availability/Reliability/Stability
- Usability/Serviceability
- Special focus area - CAP (Customer Assurance Program)/Technical Assistance Center (TAC)

Cisco SDWAN Solution Test for Japan

Cisco SDWAN Solution test for Japan includes key components such as Cisco IOSXE SDWAN platforms, Cisco SDWAN vManage, Cisco SDWAN vBond, Cisco SDWAN vSmart which is in turn 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:

- Customer found defects in selected SDWAN products
- High priority cases
- Inputs from SE's and TAC team of Cisco Japan

The test execution is carried out on selected SDWAN products, which affects the Japanese segment and that are prioritized by SE's of the Cisco Japan team. Japanese specific equivalents such as Direct Internet Access(DIA) scenarios, Service Chaining and Route leaking scenarios are validated.

The objective of the Cisco SDWAN Solution Test for Japan is to validate the scope provided by Cisco Japan in SDWAN 20.3 Solution testing by deploying the controller network in Azure and data plane network in On-premises and validating all the features SDWAN 20.3 release with connectivity between controller network and data plane network

In this Cisco SDWAN Solution test for Japan, the following components are tested.

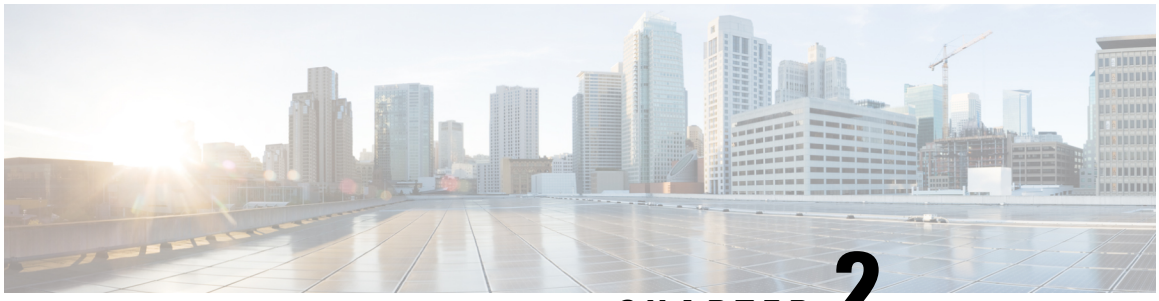
- Cisco SDWAN vManage
- Cisco SDWAN vSmart
- Cisco SDWAN vBond
- Cisco IOSXE SDWAN

Acronym

Acronym	Description
AAA	Authentication, Authorization and Accounting
AF	Address-family
ASN	Autonomous System Number
ASR	Aggregation Services Routers
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
CA	Certificate Authority
cEdge Router	Cisco Edge Router
Cisco DNA	Cisco Digital Network Architecture
Config	Configuration
Config-t	Configuration-transaction
COM Port	Communication Port
CLI	Command Line
CSP	Cisco Cloud Services Platform
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
DIA	Direct Internet Access
DNS	Domain Name System
DR	Disaster Recovery
DSCP	Differentiated Services Code Point

DTLS	Datagram Transport Layer Security
EF	Expedited Forwarding
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HA	High Availability
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
Int	interface
INET	Internet
IOS	Internetworking Operating System
ISR	Integrated Services Routers
LAN	Local Area Network
MAN	Metropolitan Area Network
MPLS	Multi-Protocol Label Switching
MSG	Message
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
PAT	Port Address Translation
PnP	Plug and Play
PnPA	Plug-and-Play Agent
QoS	Quality of Services
RD	Route Distinguisher
RIP	Routing Information Protocol
SCP	Secure copy protocol
SD-WAN	Software Defined Wide Area Network
SD-AVC	Software Defined Application Visibility & Control

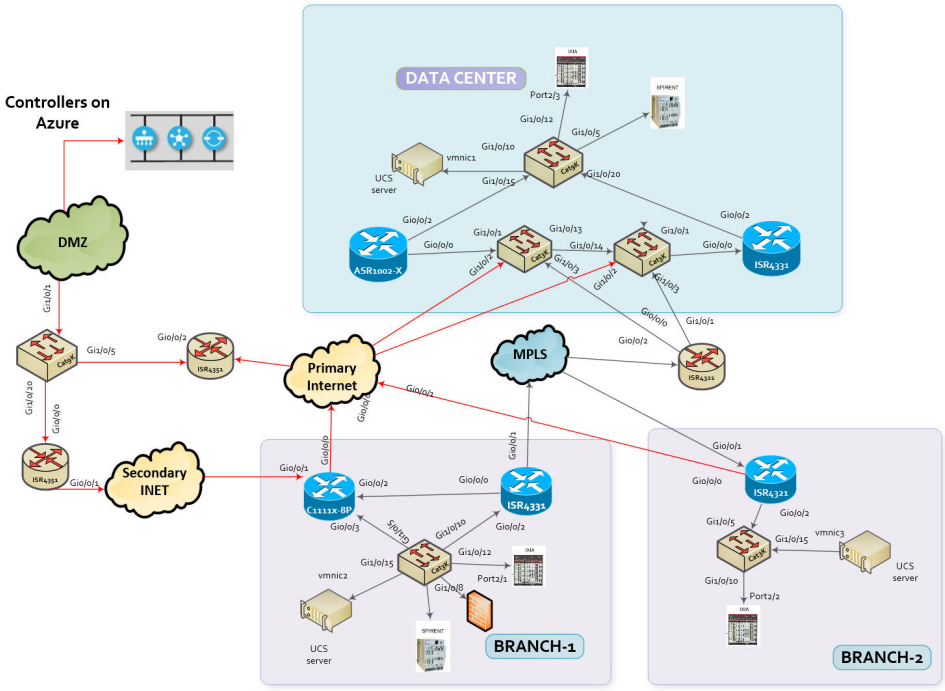
SDN	Software Defined Networking
Sec	Section
Sh	Show
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
S/N	Subnet Mask
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TLOC	Transport Location
UDP	User Datagram Protocol
Unified OS	unified Operating System
USB	Universal Serial Bus
UTC	Coordinated Universal Time or Universal Time Coordinated
UUID	Universal Unique Identifier
vEdge Router	Viptela Edge Router
VIP	Viptela
VPN	Virtual Private Network
VRF	Virtual Routing and forwarding
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
ZBF	Zone Based Firewall
ZTP	Zero Touch Provisioning



CHAPTER 2

Test Topology and Environment Matrix

Test Topology

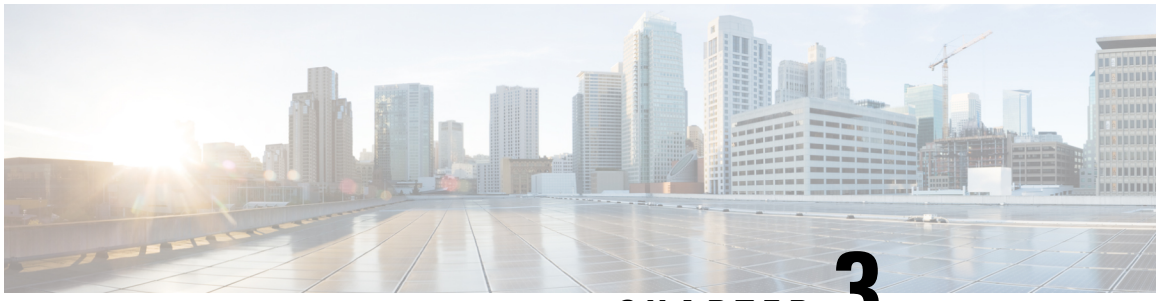


Environment Matrix

Table 1: Environment Matrix

Applications	Component		Version

Controller Network	vManage	Version	20.3
	vBond	Version	20.3
	vSmart	Version	20.3
Communications Infrastructure	ISR C111X-8P	IOS XE SDWAN	17.3
	ISR 4351, 4331	IOS XE	17.3
	ASR 1002-X	IOS XE SDWAN	17.3
	ISR 4321	IOS XE SDWAN	17.3
	Cat 9K PoE Switch	Version	17.2
UCS	ESXi Host	UCSC-C240-M5SX	ESXi 6.0, 6.5
Client	Operating system	Windows10	Windows10
	Browser	IE	11.836
		Microsoft Edge	83.0.478
		Mozilla Firefox	77.0.1(64-bit)
		Chrome	83.0.4103 (64-bit)



CHAPTER 3

Test Results Summary

vManage in Cloud

Logical ID	Title	Description	Status	Defects
ENJ.sdwan20.3.G.011	Container creation to upload vManage Images in Microsoft Azure cloud	Verify whether we able to create a container in for vManage in Microsoft cloud using blobs and services.	Passed	NA
ENJ.sdwan20.3.G.012	Uploading vManage Azure Image in Azure cloud container	Verify whether we able to upload vManage Azure image in Azure cloud container.	Passed	NA
ENJ.sdwan20.3.G.013	Creating Network Security groups in Microsoft Azure cloud	Verify whether we able to configure Network Security groups in Microsoft Azure Cloud.	Passed	NA

ENJ.sdwan20.3.G.014	Creating Virtual Network in Microsoft Azure cloud	Verify whether we able to configure Virtual Network in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.015	Creating Azure images for vManage in Microsoft Azure cloud	Verify whether we able to create Azure images for vManage in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.016	Creating Azure images for vManage in Microsoft Azure cloud	Verify whether we able to create Azure images for vManage in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.017	Creating Azure images for vBond & vSmart in Microsoft Azure cloud	Verify whether we able to create Azure images for vBond & vSmart in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.018	Adding network interface on vManage, vSmart & vBond in Microsoft Azure cloud	Verify whether we able to configure network interface on vManage and vSmart in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.019	Adding a Virtual disk in Microsoft Azure cloud	Verify whether we able to add virtual disk in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.020	Configuring vManage in Microsoft Azure cloud	Verify whether we able to configure vManage in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.021	Configuring vSmart in Microsoft Azure cloud	Verify whether we able to configure vSmart in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.022	Configuring vBond in Microsoft Azure cloud	Verify whether we able to configure vBond in Microsoft Azure Cloud.	Passed	NA

ENJ.sdwan20.3.G.023	Creating jump host and root certificate in Microsoft Azure cloud	Verify whether we able to create jump host and root certificate in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.024	Adding vSmart & vBond to vManage in Microsoft Azure Cloud	Verify whether vSmart & vBond is added to vManage in Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.025	Signing and installing CSR in Microsoft Azure Cloud	Verify whether vBond certificate is installed via Microsoft Azure Cloud.	Passed	NA
ENJ.sdwan20.3.G.026	Adding routers to vManage which is hosted in Microsoft Azure Cloud	Verify whether edge routers are added to vManage which is hosted in Microsoft Azure Cloud.	Passed	NA

One NAT Point

Logical ID	Title	Description	Status	Defects
ENJ.sdwan20.3.G.259	Service side traffic redirected to transport side VPN(VPN0) and reach internet with one NAT point	Verify when the user from the remote site can reach the internet locally when the service side traffic is redirected to transport side VPN via the one NAT link connected to the NAT router from cEdge.	Passed	NA
ENJ.sdwan20.3.G.269	branch 1 Nat enabled Primary internet link goes down divert the traffic via TLOC - Extension.	Verify branch 1 Nat enabled Primary internet link goes down divert the traffic towards DC via TLOC - Extension.	Passed	NA

ENJ.sdwan20.3.G.270	branch 1 Nat enabled Secondary internet link goes down divert the traffic via TLOC - Extension.	Verify branch 1 Nat enabled secondary internet link goes down divert the traffic towards DC via TLOC - Extension.	Passed	NA
ENJ.sdwan20.3.G.258	One NAT point exit to internet in Edge with data plane tunnel to DC. When fall back, traffic flow via DC backhaul	Verify when the traffic from the configured prefix list should go via NAT and remaining traffic will reach the destination via DC	Passed	NA
ENJ.sdwan20.3.G.262	Service side users (VPN 10) can access the DNS server located in DMZ via DC when primary goes down via DC.	Verify VPN 10 users can access the DNS server via DC when the primary link goes down.	Passed	NA
ENJ.sdwan20.3.G.263	Branch 2 service side users (VPN 110) can access the HTTPS and HTTP server located in DMZ, when primary goes down.	Verify VPN 110 users can access the HTTP & HTTPS server via DC when the primary link goes down.	Passed	NA
ENJ.sdwan20.3.G.264	Branch -2 Service side VPN 200 SSH traffic redirected to transport side VPN 0 and reach internet by DC backhaul.	Verify when primary goes down Branch -2 Service side VPN 200 SSH traffic redirected DC backhaul.	Passed	NA
ENJ.sdwan20.3.G.265	Branch -2 Service side VPN 151 Telnet traffic redirected to transport side VPN 0 and reach internet by DC backhaul.	Verify when primary goes down Branch -2 Service side VPN 151 Telnet traffic redirected DC backhaul.	Passed	NA
ENJ.sdwan20.3.G.266	Branch 2 service side users (VPN 110) can access the HTTPS and HTTP server located in cloud, when primary goes down.	Verify VPN 110 users can access the HTTP & HTTPS server via DC when the primary link goes down.	Passed	NA

ENJ.sdwan20.3.G.271	Branch 2 service side users (VPN 205) can access the server located in DMZ, when primary goes down.	Verify VPN 205 users can access the SFTP server via DC when the primary link goes down.	Passed	NA
ENJ.sdwan20.3.G.272	Branch 2 service side users (VPN 175) can access the server located in DMZ, when primary goes down.	Verify VPN 175 users can access the TFTP server via DC when the primary link goes down.	Passed	NA
ENJ.sdwan20.3.G.260	One NAT point exit to internet in Edge with data plane tunnel to DC. When fall back, traffic flow via DC backhaul.	Verify when the branch -2 NAT enabled internet goes down, the traffic should divert via DC.	Passed	NA
ENJ.sdwan20.3.G.261	One NAT point exit to internet in Edge with data plane tunnel to DC. When fall back, traffic flow via DC backhaul.	Verify when Branch 1 Nat enabled primary and secondary internet goes down the internet traffic divert via DC	Passed	NA
ENJ.sdwan20.3.G.267	One NAT point exit to internet in Edge with data plane tunnel to DC. When fall back, traffic flow via DC backhaul.	Verify when the branch 1 NAT enabled primary internet goes down, the traffic should divert via DC.	Passed	NA
ENJ.sdwan20.3.G.268	One NAT point exit to internet in Edge with data plane tunnel to DC. When fall back, traffic flow via DC backhaul.	Verify when the branch 1 NAT enabled secondary internet goes down, the traffic should divert via DC.	Passed	NA

Two NAT Point

Logical ID	Title	Description	Status	Defects

ENJ.sdwan20.3.G.027	Service side VPN(VPN2) traffic redirected to transport side VPN(VPN0) and reach internet with two NAT point link	Verify whether user in the remote site is able to reach the internet locally when the service side traffic is redirected to transport side VPN	Passed	NA
ENJ.sdwan20.3.G.028	Service side VPN(VPN2) traffic redirected to transport side VPN(VPN0) and reach internet with backup link enabled in two NAT point	Verify whether user in the remote site is able to reach the internet locally when the service side traffic is redirected to transport side VPN via the backup link connected to the NAT router from cEdge branch router	Passed	NA
ENJ.sdwan20.3.G.029	Service side VPN(VPN2) HTTPS data traffic redirected to transport side VPN(VPN0) and reach internet with two NAT point link	Verify whether user in the remote site is able to pass HTTPS data traffic locally when the service side traffic is redirected to transport side VPN	Passed	NA
ENJ.sdwan20.3.G.030	Service side VPN(VPN2) HTTP traffic redirected to transport side VPN(VPN0) and reach internet with backup link enabled in two NAT point	Verify whether user in the remote site is able to pass HTTPS data traffic locally when the service side traffic is redirected to transport side VPN via the backup link connected to the NAT router from cEdge branch router	Passed	NA
ENJ.sdwan20.3.G.031	Service side VPN(VPN2) SSH data traffic redirected to transport side VPN(VPN0) and reach internet with two NAT point link	Verify whether user in the remote site is able to pass SSH data traffic locally when the service side traffic is redirected to transport side VPN	Passed	NA

ENJ.sdwan20.3.G.032	Service side VPN(VPN2) SSH traffic redirected to transport side VPN(VPN0) and reach internet with backup link enabled in two NAT point	Verify whether user in the remote site is able to pass SSH data traffic locally when the service side traffic is redirected to transport side VPN via the backup link connected to the NAT router from cEdge branch router	Passed	NA
ENJ.sdwan20.3.G.033	Service side VPN(VPN2) Telnet data traffic redirected to transport side VPN(VPN0) and reach internet with two NAT point link	Verify whether user in the remote site is able to pass Telnet data traffic locally when the service side traffic is redirected to transport side VPN	Passed	NA
ENJ.sdwan20.3.G.034	Service side VPN(VPN2) Telnet traffic redirected to transport side VPN(VPN0) and reach internet with backup link enabled in two NAT point	Verify whether user in the remote site is able to pass Telnet data traffic locally when the service side traffic is redirected to transport side VPN via the backup link connected to the NAT router from cEdge branch router	Passed	NA
ENJ.sdwan20.3.G.040	DIA tracker enabled in secondary interface of cEdge router	Verify whether cEdge router is able to take up the backup link connected automatically and reach the internet directly when the DIA tracker is enabled	Passed	NA

ENJ.sdwan20.3.G.041	DIA tracker enabled in primary interface of cEdge router	Verify whether cEdge router is able to take up the backup link connected automatically and reach the internet directly when the DIA tracker is enabled	Passed	NA
ENJ.sdwan20.3.G.035	HTTPS Qos Monitoring data traffic redirected to primary INET using DSCP value	Verify whether we able to monitor HTTPS data traffic is redirected to Primary INET using DSCP value.	Passed	NA
ENJ.sdwan20.3.G.036	SSH Qos Monitoring data traffic redirected to primary INET using DSCP value	Verify whether we able to monitor SSH data traffic is redirected to Primary INET using DSCP value.	Passed	NA
ENJ.sdwan20.3.G.037	HTTPS Qos Monitoring data traffic redirected to Secondary INET using DSCP value	Verify whether we able to monitor HTTPS data traffic is redirected to Secondary INET using DSCP value.	Passed	NA
ENJ.sdwan20.3.G.038	SSH Qos Monitoring data traffic redirected to secondary INET using DSCP value	Verify whether we able to monitor SSH data traffic is redirected to Secondary INET using DSCP value.	Passed	NA
ENJ.sdwan20.3.G.039	HTTP Qos Monitoring data traffic redirected to primary INET using DSCP value	Verify whether we able to monitor SSH data traffic is redirected to primary INET using DSCP value.	Passed	NA

Direct Internet Access

Logical ID	Title	Description	Status	Defects

ENJ.sdwan20.3.G.073	Redirecting guest internet using NAT DIA Route.	Verify whether the guest internet traffic from service side is redirecting to transport side using NAT DIA route.	Passed	NA
ENJ.sdwan20.3.G.074	Redirecting guest internet via Primary INET using NAT DIA Route	Verify whether the guest internet traffic is redirected to primary INET using NAT DIA route.	Passed	NA
ENJ.sdwan20.3.G.075	Redirecting SSH data traffic via Primary INET using NAT DIA Route	Verify whether the remote user able to pass ssh data traffic from branch site via primary INET using NAT DIA route.	Passed	NA
ENJ.sdwan20.3.G.076	Redirecting telnet data traffic via Primary INET using NAT DIA Route	Verify whether the remote user able to pass ssh data traffic from branch site via primary INET using NAT DIA route.	Passed	NA
ENJ.sdwan20.3.G.080	Redirecting BIZ internet to DC via MPLS conection	Verify whether the remote user able to access BIZ internet via MPLS connection from remote branch site.	Passed	NA
ENJ.sdwan20.3.G.081	Reaching DNS Server from branch site to DC via MPLS	Verify whether the remote user able to access DNS server from branch site via MPLS connection.	Passed	NA
ENJ.sdwan20.3.G.082	Redirecting telnet data traffic from branch site to Secondary INET.	Verify whether the remote user able to access telnet traffic from branch site via secondary INET connection.	Passed	NA
ENJ.sdwan20.3.G.083	Redirecting ssh data traffic from branch site to Secondary INET.	Verify whether the remote user able to access ssh traffic from branch site via secondary INET connection.	Passed	NA

ENJ.sdwan20.3.G.084	Dynamic NAT enable for DIA to the branch users	Verify whether the branch user should be able to access the Direct internet user can access the inbound to branch servers.	Passed	NA
ENJ.sdwan20.3.G.085	Dynamic NAT enable for DIA to the branch users with NAT pool overload	Verify whether the user should be able to access internet and data center servers.	Passed	NA
ENJ.sdwan20.3.G.242	Create Centralized Data Policy to Redirect Employee Traffic	Verify after we Create Centralized Data Policy to Redirect Employee Traffic	Passed	NA
ENJ.sdwan20.3.G.243	Divert the Public traffic from VPN 10 users towards DIA by centralized policy	Verify after creating the centralized policy for the branch 2 VPN 10 users traffic goes to the DIA.	Passed	NA
ENJ.sdwan20.3.G.244	Redirect Public Traffic and Configure a centralized data policy to accomplish DIA.	Check whether the public traffic can access after configured DIA.	Passed	NA
ENJ.sdwan20.3.G.250	DIA using NAT DIA Route.	Verify branch -2 VPN 125 user’s internet traffic will go via VPN 0 without any filter.	Passed	NA
ENJ.sdwan20.3.G.251	Branch 2 VPN 199 user’s only access the HTTP & HTTPS sites via Nat enabled Primary internet link.	Verify when branch 2 VPN 199 users only can able to access the HTTP & HTTPS Site by using DIA Nat enabled primary internet link.	Passed	NA

ENJ.sdwan20.3.G.252	Branch 2 VPN 101 user's only access the SSH & Telnet services via Nat enabled Primary internet link.	Verify when branch 2 VPN 101 users only can able to access the SSH & Telnet by using DIA Nat enabled primary internet link.	Passed	NA
ENJ.sdwan20.3.G.253	Branch 1 VPN 115 user's only access the SSH & Telnet services via Nat enabled Primary internet link and VPN 185 users only can access the HTTP & HTTPS sites via Nat enabled secondary internet link.	Verify when Branch 1 VPN 115 user's only access the SSH & Telnet services via Nat enabled Primary internet link and VPN 185 users only can access the HTTP & HTTPS sites via Nat enabled secondary internet link by using the DIA.	Passed	NA
ENJ.sdwan20.3.G.246	How to Prefer Particular Uplink for Direct Internet Access.	Verify branch cEdge having two internets so that we are using DIA to prefer the Primary internet link.	Passed	NA
ENJ.sdwan20.3.G.247	How to Prefer Particular Uplink for Direct Internet Access.	Verify branch cEdge having two internets so that we are using DIA to prefer the Secondary internet link.	Passed	NA
ENJ.sdwan20.3.G.248	How to Prefer Particular Uplink for Direct Internet Access.	Verify branch cEdge having one public internet and one MPLS private so that we are using DIA and prefer the primary public internet link to reach the destination.	Passed	NA

ENJ.sdwan20.3.G.249	How to Prefer Particular Uplink for Direct Internet Access.	Verify branch cEdge having one public internet and one MPLS private so that we are using DIA and prefer the MPLS Private internet link to reach the destination.	Passed	NA
ENJ.sdwan20.3.G.078	Redirecting traffic based on destination prefix port number 448	Verify whether the remote user able to pass 448 data traffic from branch site via primary INET using NAT DIA route.	Passed	NA
ENJ.sdwan20.3.G.079	Redirecting traffic based on destination prefix port number 23	Verify whether the remote user able to pass 23 data traffic from branch site via primary INET using NAT DIA route.	Passed	NA
ENJ.sdwan20.3.G.077	Redirecting https data traffic via Primary INET using NAT DIA Route	Verify whether the remote user able to pass ssh data traffic from branch site via primary INET using NAT DIA route.	Passed	NA
ENJ.sdwan20.3.G.245	DIA Centralized data policy.	Verify Branch 1 and branch 2 particular source and destination port number and protocol matches should go outside (internet) other traffic like corporate to corporate will go without Nat and VPN 0 via Mpls network by using DIA centralized data policy.	Passed	NA

ENJ.sdwan20.3.G.254	DIA Centralized policy	Verify the source and destination prefix matches it should use the default action ECMP to access the destination via Both public internet link by using the DIA.	Passed	NA
ENJ.sdwan20.3.G.255	DIA Centralized policy	Verify when the primary DIA configured Nat enabled interface goes down the traffic will re-direct via MPLS.	Passed	NA
ENJ.sdwan20.3.G.256	DIA Centralized data policy.	Verify Branch 1 and branch 2 particular source and destination port number and protocol matches should go outside (internet) other traffic like corporate to corporate will go without Nat and VPN 0 via Mpls network by using DIA centralized data policy.	Passed	NA
ENJ.sdwan20.3.G.257	DIA Centralized data policy.	Verify Branch 1 and branch 2 between the service VPN traffic will go via MPLS and internet traffic (SFTP) will go via Nat enabled interface by using DIA.	Passed	NA

Service Chaining and Route Leak

Logical ID	Title	Description	Status	Defects

ENJ.sdwan20.3.G.042	Static route leaking between two vrf via vManage cli template	Verify whether the static route is leaking between two routers via vManage cli template.	Passed	NA
ENJ.sdwan20.3.G.043	Data Policy configuration from Transport side to service side.	Verify whether we able to configure data policy from transport side VPN0 to service side VPN110	Passed	NA
ENJ.sdwan20.3.G.044	IP route configuration from service side to transport side.	Verify whether we able to configure IP route from transport side to service side.	Passed	NA
ENJ.sdwan20.3.G.045	Reachability testing after configuring route leaking from VPN0 to VPN110	Verify whether we able to reach VPN0 from VPN110 using router leaking.	Passed	NA
ENJ.sdwan20.3.G.046	HTTPS reachability testing after configuring route leaking from VPN0 to VPN110	Verify whether we able to pass HTTPS traffic to VPN0 from VPN110 using router leaking.	Passed	NA
ENJ.sdwan20.3.G.047	Telnet reachability testing after configuring route leaking from VPN0 to VPN110.	Verify whether we able to pass Telnet traffic to VPN0 from VPN110 using router leaking.	Passed	NA
ENJ.sdwan20.3.G.048	Route leaking between VPN through MPLS connection.	Verify whether the user from branch site 1 VPN11 able to reach branch 2 VPN 12 via MPLS line using route leak.	Passed	NA
ENJ.sdwan20.3.G.049	Route leaking between VPN through INET connection.	Verify whether the user from branch site 1 VPN11 able to reach branch 2 VPN 12 via INET line using route leak.	Passed	NA

ENJ.sdwan20.3.G.050	Telnet data traffic between VPN through MPLS connection.	Verify whether the user from VPN11 able to pass telnet data traffic to VPN 12 via MPLS line using route leak.	Passed	NA
ENJ.sdwan20.3.G.051	SSH data traffic between VPN through MPLS connection.	Verify whether the user from VPN11 able to pass ssh data traffic to VPN 12 via MPLS line using route leak.	Passed	NA
ENJ.sdwan20.3.G.052	HTTPS data traffic between VPN through MPLS connection.	Verify whether the user from VPN11 able to pass https data traffic to VPN 12 via MPLS line using route leak.	Passed	NA
ENJ.sdwan20.3.G.053	HTTPS data traffic between VPN through INET connection.	Verify whether the user from VPN11 able to pass https data traffic to VPN 12 via INET line using route leak.	Passed	NA
ENJ.sdwan20.3.G.054	SSH data traffic between VPN through INET connection.	Verify whether the user from VPN11 able to pass ssh data traffic to VPN 12 via INET line using route leak.	Passed	NA
ENJ.sdwan20.3.G.055	Telnet data traffic between VPN through INET connection.	Verify whether the user from VPN11 able to pass Telnet data traffic to VPN 12 via INET line using route leak.	Passed	NA
ENJ.sdwan20.3.G.056	TFTP data traffic between VPN through INET connection.	Verify whether the user from VPN11 able to pass TFTP data traffic to VPN 12 via INET line using route leak.	Passed	NA

ENJ.sdwan20.3.G.057	Configure and track Line-protocol state of an interface.	Verify whether the state of the line protocol of an interface is tracked using system tracker.	Passed	NA
ENJ.sdwan20.3.G.058	Configure and track IP-Routing state of an interface.	Verify whether the state of the IP-Routing of an interface is tracked using system tracker.	Passed	NA
ENJ.sdwan20.3.G.070	Default track list configuration using system tracker	Verify whether we able to configure default track list using system tracker.	Passed	NA
ENJ.sdwan20.3.G.071	Tracking threshold of IP-Route metrics with priority.	Verify whether reachability of IP-Route with priority is tracking when a routing table entry exists for the route and the route is accessible.	Passed	NA
ENJ.sdwan20.3.G.072	Configure and track Line-protocol state of an interface with priority	Verify whether the state of the line protocol of an interface is tracked using priority value	Passed	NA
ENJ.sdwan20.3.G.101	Configure traffic flow from BR2 to DC ASR1002x router via firewall service using CLI	Check whether traffic flow from BR2 to DC ASR1002x router can be configured via Firewall service using CLI	Passed	NA
ENJ.sdwan20.3.G.102	Configure traffic flow from BR2 to DC ISR4331 router via firewall service using CLI	Check whether traffic flow from BR2 to DC ISR4331 router can be configured via Firewall service using CLI	Passed	NA

ENJ.sdwan20.3.G.103	Configure traffic flow from DC ASR1002x to BR2 router via firewall service using CLI	Check whether traffic flow from DC ASR1002x to BR2 router can be configured via Firewall service using CLI	Passed	NA
ENJ.sdwan20.3.G.104	Configure traffic flow from DC ISR4331 to BR2 router via firewall service using CLI	Check whether traffic flow from DC ISR4331 to BR2 router can be configured via Firewall service using CLI	Passed	NA
ENJ.sdwan20.3.G.105	Configure traffic flow from BR2 to DC ASR1002x router via firewall service using Feature Template and Centralized policy in vManage	Check whether traffic flow from BR2 to DC ASR1002x router can be configured via Firewall service using Feature template and Centralized policy in vManage	Passed	NA
ENJ.sdwan20.3.G.106	Configure traffic flow from BR2 to DC ISR4331 router via firewall service using Feature Template and Centralized policy in vManage	Check whether traffic flow from BR2 to DC ISR4331 router can be configured via Firewall service using Feature template and Centralized policy in vManage	Passed	NA
ENJ.sdwan20.3.G.107	Configure traffic flow from DC ASR1002x to BR2 router via firewall service using Feature Template and Centralized policy in vManage	Check whether traffic flow from DC ASR1002x to BR2 router can be configured via Firewall service using Feature template and Centralized policy in vManage	Passed	NA

ENJ.sdwan20.3.G.231	Access between the BR1 and BR2 using service FW by control policies	Verify after creating the Service chaining policy the traffic from branch -1 to branch -2 should go via FW service	Passed	NA
ENJ.sdwan20.3.G.230	Access branch 1 to branch 2 and vice versa using service Firewall by data policies	Configuring the data policy and applying from Vsmart to reach the BR-1 to BR-2 via FW	Passed	NA
ENJ.sdwan20.3.G.232	Branch 1 configured source IP able to access the BR2 using FW by Data policies	Service chaining, kept the FW behind the cEdge and the traffic from branch -1 to branch -2 should go via FW service for the configured source IP	Passed	NA
ENJ.sdwan20.3.G.236	Branch 1 configured data prefix list IP's only able to access the BR2 using FW by Data policies	When the traffic from branch 1 and match the source prefix list then it should reach branch 2 reach via service firewall.	Passed	NA
ENJ.sdwan20.3.G.238	Branch 1 configured source port only able to access the BR2 using FW by Data policies	Verify when the traffic from the source port can able to access the destination via service firewall.	Passed	NA
ENJ.sdwan20.3.G.237	Branch 1 able to access the BR-2 if the destination prefix match only by using service FW Data policies	When the traffic from particular prefix list in branch 1 can able to access branch 2 reach via service firewall.	Passed	NA
ENJ.sdwan20.3.G.234	Branch 1 can access BR-2 via configured protocol only using service FW by Data policies	Verify when the traffic from branch 1 and the it matching to the protocol then it should reach branch 2 via service firewall	Passed	NA

ENJ.sdwan20.3.G.059	Tracking google.com public IP address using system tracker	Verify whether reachability of IP-Route is tracking when a routing table entry exists for the route and the route is accessible.	Passed	NA
ENJ.sdwan20.3.G.060	Configuring system tracker in dual interface	Verify whether we able to configure system endpoint tracker in dual interface.	Passed	NA
ENJ.sdwan20.3.G.061	Tracking reachability of an IP using system tracker	Verify whether tracking state of an IP SLA IP Host operation is tracking using system tracker.	Passed	NA
ENJ.sdwan20.3.G.062	Configuring tracker list and threshold 200 using secondary interface.	Verify whether we able to configure track list and monitor threshold weight using system tracker.	Passed	NA
ENJ.sdwan20.3.G.063	Configuring tracker list and threshold 300 using secondary interface.	Verify whether we able to configure track list and monitor threshold weight using system tracker.	Passed	NA
ENJ.sdwan20.3.G.064	Configuring tracker list and threshold 400 using secondary interface.	Verify whether we able to configure track list and monitor threshold weight using system tracker.	Passed	NA
ENJ.sdwan20.3.G.065	Configuring tracker list and threshold 200 using system tracker.	Verify whether we able to configure track list and monitor threshold percentage using system tracker.	Passed	NA

ENJ.sdwan20.3.G.066	Configuring tracker list and threshold 300 using system tracker.	Verify whether we able to configure track list and monitor threshold percentage using system tracker.	Passed	NA
ENJ.sdwan20.3.G.067	Configuring tracker list and threshold 400 using system tracker.	Verify whether we able to configure track list and monitor threshold percentage using system tracker.	Passed	NA
ENJ.sdwan20.3.G.068	Configuring tracker list and threshold 500 using system tracker.	Verify whether we able to configure track list and monitor threshold percentage using system tracker.	Passed	NA
ENJ.sdwan20.3.G.069	Configuring tracker list and threshold 750 using system tracker.	Verify whether we able to configure track list and monitor threshold percentage using system tracker.	Passed	NA
ENJ.sdwan20.3.G.107	Configure traffic flow from DC ASR1002x to BR2 router via firewall service using Feature Template and Centralized policy in vManage	Check whether traffic flow from DC ASR1002x to BR2 router can be configured via Firewall service using Feature template and Centralized policy in vManage	Passed	NA
ENJ.sdwan20.3.G.202	Service chaining between DC VPN 110 user can able to access the BR2 VPN 120 user via service FW.	Verify after creating the Service chaining policy the traffic from DC VPN 110 user can able to access the BR2 VPN 120 user via service FW.	Passed	NA

ENJ.sdwan20.3.G.204	Service chaining between DC VPN 120 user can able to access the BR2 VPN 130 user via service FW.	Verify after creating the Service chaining policy the traffic from DC VPN 120 user can able to access the BR2 VPN 130 user via service FW.	Passed	NA
ENJ.sdwan20.3.G.209	Service chaining between DC VPN 130 user can able to access the BR2 VPN 110 & 120 user via service FW.	Verify after creating the Service chaining policy the traffic from DC VPN 130 user can able to access the BR2 VPN 110 & 120 user via service FW.	Passed	NA
ENJ.sdwan20.3.G.210	Service chaining between BR2 VPN 110 user can able to access the DC VPN 130 user via service FW.	Verify after creating the Service chaining policy the traffic from BR2 VPN 110 user can able to access the DC VPN 130 user via service FW.	Passed	NA
ENJ.sdwan20.3.G.206	Service chaining between BR2 VPN 130 user can able to access the DC VPN 110 & 120 user via service FW.	Verify after creating the Service chaining policy the traffic from BR2 VPN 130 user can able to access the DC VPN 110 & 120 user via service FW.	Passed	NA
ENJ.sdwan20.3.G.207	Service chaining between BR2 VPN 120 user can able to access the DC VPN 110 user via service FW.	Verify after creating the Service chaining policy the traffic from BR2 VPN 120 user can able to access the DC VPN 110 user via service FW.	Passed	NA
ENJ.sdwan20.3.G.228	Service chaining – Local service	Verify whether the VPN 130 users can access the SFTP server behind the cEdge-1 with respective port number.	Passed	NA

ENJ.sdwan20.3.G.229	Service chaining local service	Verify when the traffic from branch 1 to branch 2 reach via service firewall, behind the branch 1	Passed	NA
ENJ.sdwan20.3.G.233	Service chaining local service	Verify when the traffic from configured app-list then it passes from branch 1 to branch 2 reach via service firewall.	Passed	NA
ENJ.sdwan20.3.G.235	Service chaining local service	Verify when the TCP or UDP traffic is matching the data policy then pass the traffic form branch 1 to branch 2 via service firewall.	Passed	NA
ENJ.sdwan20.3.G.239	Service Chaining - Local service	Verify whether we can save the logging information to the Remote server, which is hosted in the branch 1.	Passed	NA
ENJ.sdwan20.3.G.240	Service chaining local service	Verify when the TCP or UDP traffic is matching the data policy then pass the traffic form branch 2 to branch 1 via service firewall.	Passed	NA
ENJ.sdwan20.3.G.241	Service chaining local service	Verify when the traffic from the particular source port is matching the data policy then pass the traffic form branch 2 to branch 1 via service firewall.	Passed	NA

Service Side NAT

Logical ID	Title	Description	Status	Defects

ENJ.sdwan20.3.G.111	Configure Static NAT from BR2 Customer3 to windows server server via CLI template in vManage	Check whether Static NAT can be configured in Customer3 BR2 to reach windows server using CLI Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.112	Configure Static NAT from BR2 Customer2 to DNS server via CLI template in vManage	Check whether Static NAT can be configured in Customer 2 BR2 to reach DNS server using CLI Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.115	Configure Static NAT from BR1 Customer1 to NTP server via CLI template in vManage	Check whether Static NAT can be configured in Customer1 BR1 to reach NTP server using CLI Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.116	Configure Static NAT from BR2 Customer2 to Windows server via CLI template in vManage	Check whether Static NAT can be configured in Customer2 BR2 to reach Windows Server using CLI Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.117	Configure Static NAT from BR1 Customer2 to Windows server via Feature template in vManage	Check whether Static NAT can be configured in Customer2 BR1 to reach Windows server using CLI Template via vManage successfully	Passed	NA

ENJ.sdwan20.3.G.118	Configure Static NAT from DC Customer3 to windows server via Feature template in vManage	Check whether Static NAT can be configured in Customer3 DC to reach WIndows server using Feature Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.120	Configure Static NAT from BR2 Customer1 to Google server via Feature template in vManage	Check whether Static NAT can be configured in Customer1 BR2 to reach Google server using Feature Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.121	Configure Static NAT from DC Customer1 to Window server via Feature template in vManage	Check whether Static NAT can be configured in Customer1 DC to reach Window server using Feature Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.122	Configure Static NAT from DC Customer2 to Windows server via Feature template in vManage	Check whether Static NAT can be configured in Customer2 DC to reach Windows server using Feature Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.123	Configure Static NAT from BR2 Customer1 to Windows server via Feature template in vManage	Check whether Static NAT can be configured in Customer1 BR2 to reach Windows server using Feature Template via vManage successfully	Passed	NA

ENJ.sdwan20.3.G.274	Traffic from service VPN NATed and pass via Transport VPN for the configured ip prefix list only.	Verify the Service VPN traffic to Exit to the Internet Based Only on IP Prefix directly for the branch 2.	Passed	NA
ENJ.sdwan20.3.G.276	Branch 1 service VPN traffic NATed with given natpool range by CLI.	Verify when we apply the dynamic NAT and configured the data policy the traffic is NATed with the dynamic NAT pool.	Passed	NA
ENJ.sdwan20.3.G.277	Traffic from service VPN NATed and pass via Transport VPN	Verify the Service VPN traffic to Exit to the Internet Based Only on IP Prefix directly for the branch 2.	Passed	NA
ENJ.sdwan20.3.G.278	Traffic from Branch 1 service VPN NATed, if the configured prefix and port number matches.	Verify when we apply the dynamic NAT and configured the data policy for the prefix and port number traffic is NATed with the dynamic NAT pool.	Passed	NA
ENJ.sdwan20.3.G.279	Traffic from service VPN NATed with the Natpool range by vManage	Verify if the outgoing traffic is NATed with the given public ip range.	Passed	NA
ENJ.sdwan20.3.G.282	Branch 1 service VPN 10 users need to access the DNS server using Dynamic NAT.	Verify whether the VPN 10 users able to access the DNS server with respective port number.	Passed	NA
ENJ.sdwan20.3.G.283	Branch -1 Service side VPN 251 SSH data traffic redirected to transport side VPN 0 and reach internet via Nat enabled interface.	Verify when branch 1 service side VPN 251 user’s SSH data traffic Nated via secondary internet link.	Passed	NA

ENJ.sdwan20.3.G.284	Branch -1 Service side VPN 251 Telnet data traffic redirected to transport side VPN 0 and reach internet via Nat enabled interface.	Verify when branch 1 service side VPN 225 user's telnet data traffic Nated via secondary internet link.	Passed	NA
ENJ.sdwan20.3.G.285	Branch -1 Service side VPN 333 Telnet data traffic redirected to transport side VPN 0 and reach internet via Nat enabled interface.	Verify when branch 1 service side VPN 333 user's telnet data traffic Nated via primary internet link.	Passed	NA
ENJ.sdwan20.3.G.273	Traffic from Branch 2 service VPN NATed and reach to DC via Transport VPN	Verify when the Traffic from Branch 2 service VPN NATed and reach FTP server hosted in DC via Transport VPN.	Passed	NA
ENJ.sdwan20.3.G.275	Traffic from service VPN NATed and pass via Transport VPN, Only for the destination IP Prefix from the branch 2.	Verify the Service VPN traffic Exit to the Internet Only for the destination IP Prefix from the branch 2.	Passed	NA
ENJ.sdwan20.3.G.280	Configure dynamic NAT for BR2 to DNS server	Check whether dynamic NAT can be configured from BR2 hosts to DNS server successfully	Passed	NA
ENJ.sdwan20.3.G.281	Branch 2 VPN 5 users accessing the DMZ web server via PAT enabled NAT interface.	Verify branch 2 service VPN 5 users accessing the DMZ web server via configured port numbers (PAT) in the NAT enabled interface.	Passed	NA

ENJ.sdwan20.3.G.109	Configure Static NAT from BR1 Customer1 to Windows server via CLI template in vManage	Check whether Static NAT can be configured in Customer1 BR1 to reach Windows server using CLI Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.110	Configure Static NAT from BR1 Customer3 to Windows server via CLI template in vManage	Check whether Static NAT can be configured in Customer3 BR1 to reach Windows server in using CLI Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.111	Configure Static NAT from BR2 Customer1 to DNS server via CLI template in vManage	Check whether Static NAT can be configured in Customer1 BR2 to reach DNS server using CLI Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.113	Configure Static NAT from DC Customer1 to NTP server via CLI template in vManage	Check whether Static NAT can be configured in Customer1 DC to reach NTP server using CLI Template via vManage successfully	Passed	NA
ENJ.sdwan20.3.G.114	Configure Static NAT from DC Customer2 to DNS server via CLI template in vManage	Check whether Static NAT can be configured in Customer2 DC to reach DNS server in DC using CLI Template via vManage successfully	Passed	NA

VRRP LAN With Layer2

Logical ID	Title	Description	Status	Defects

ENJ.sdwan20.3.G.201	Branch 1 cEdge 1 & 2 form VRRP and track the OMP connection by using OMP Track feature.	Verify when Master router OMP goes down Backup take Master role and if the old Master came back it take the Master role.	Passed	NA
ENJ.sdwan20.3.G.203	Branch 1 cEdge 1 & 2 form VRRP and achieve redundancy by Master and Backup	Verify when Master router OMP goes down Backup take Active role and the traffic should pass via current Master (cEdge-B)	Passed	NA
ENJ.sdwan20.3.G.205	Branch 1 cEdge 1 & 2 form VRRP and stop the frequent state changes by disable_preempt	Verify when Master router OMP goes down Backup take Master role and if the old Master came back it should be Backup due to preempt disabled	Passed	NA
ENJ.sdwan20.3.G.212	Branch 1 cEdge 1 & 2 form VRRP to achieve the redundancy and also will support both ipv4 and ipv6.	Verify when VRRP forming the Master and Backup role and achieve redundancy for both ipv4 and ipv6 by enabling the version 3.	Passed	NA
ENJ.sdwan20.3.G.213	Branch 1 cEdge 1 & 2 form VRRP to achieve the LAN redundancy by using the advertise timers' value.	Verify when VRRP achieve the redundancy response time in Master and Backup role, when changing the advertise timer's values.	Passed	NA
ENJ.sdwan20.3.G.214	Branch 1 cEdge 1 & 2 form VRRP to achieve the LAN redundancy and enabled delay timer value to avoid the state changes due to loss of hello packets.	Verify when VRRP achieve the redundancy response time in Master and Backup role, we enabled delay timer value to avoid the state changes due to loss of hello packets.	Passed	NA

Customer Found Defect

Logical ID	Title	Description	Status	Defects
ENJ.sdwan20.3.G.001	Bandwidth & Buffer allocation based on data traffic in Queue 1	Verify whether the queue is added to class map policy, bandwidth & buffer rates are mapped & forwarded to Queue 1 via cli template from vManage	Passed	NA
ENJ.sdwan20.3.G.002	Bandwidth & Buffer allocation based on data traffic in Queue 2	Verify whether the queue is added to class map policy, bandwidth & buffer rates are mapped & forwarded to Queue 2 via cli template from vManage	Passed	NA
ENJ.sdwan20.3.G.003	Bandwidth & Buffer allocation based on data traffic in Queue 3	Verify whether the queue is added to class map policy, bandwidth & buffer rates are mapped & forwarded to Queue 2 via cli template from vManage	Passed	NA
ENJ.sdwan20.3.G.007	Monitor ICMP packets based on Color through vManage CLI template	Verify whether the data traffic is routing between cEdge routers via vManage cli template by configuring single rate two color class policy and monitor whether the data packets are moving as per the schedule bit rate	Passed	NA

ENJ.sdwan20.3.G.009	Monitor Tracert packets based on Color through vManage CLI template	Verify whether the data traffic is routing between cEdge routers via vManage cli template by configuring single rate two color class policy and monitor whether the data packets are moving as per the schedule bit rate	Passed	NA
ENJ.sdwan20.3.G.010	Zone Based Firewall via CLI Template by configuring via class-map and policy-map	Verify whether the zone-pairs to inspect, block and permit via vManage cli template and monitor the traffics by applying to edge devices	Passed	NA
ENJ.sdwan20.3.G.124	Configure IP address for INET transport interface in BR1 C1111x-8p router and map the interface to a tunnel in order to configure TLOC	Check whether IP address for INET transport interface in BR1 C1111 x-8prouter and map the interface to a tunnel in order to configure TLOC	Passed	NA
ENJ.sdwan20.3.G.125	Configure IP address for MPLS transport interface in BR1 ISR4331 router and map the interface to a tunnel in order to configure TLOC	Check whether IP address for MPLS transport interface in BR1 ISR4331 router and map the interface to a tunnel in order to configure TLOC	Passed	NA
ENJ.sdwan20.3.G.126	Configure IP address for INET transport interface in BR2 ISR4321 router and map the interface to a tunnel in order to configure TLOC	Check whether IP address for INET transport interface in BR2 ISR4321 router and map the interface to a tunnel in order to configure TLOC	Passed	NA

ENJ.sdwan20.3.G.127	Configure IP address for MPLS transport interface in BR2 ISR4321 router and map the interface to a tunnel in order to configure TLOC	Check whether IP address for MPLS transport interface in BR2 ISR4321 router and map the interface to a tunnel in order to configure TLOC	Passed	NA
ENJ.sdwan20.3.G.128	Create 2 sub interface on transport interface in DC ASR1002x router and map the sub interfaces to a tunnel in order to configure TLOC	Check whether 2 sub interfaces are created on transport interface in DC ASR1002x router and the created sub interfaces are mapped to a tunnel in order to configure TLOC	Passed	NA
ENJ.sdwan20.3.G.129	Create 2 sub interface on transport interface in DC ISR4331 router and map the sub interfaces to a tunnel in order to configure TLOC	Check whether 2 sub interfaces are created on transport interface in DC ISR4331 router and the created sub interfaces are mapped to a tunnel in order to configure TLOC	Passed	NA
ENJ.sdwan20.3.G.130	Configure TLOC for INET transport interface in DC ASR1002X router for created sub interface	Check whether TLOC can be configured for INET transport interfaces in DC ASR1002X router for the created sub interfaces successfully	Passed	NA
ENJ.sdwan20.3.G.131	Configure TLOC for MPLS transport interface in DC ASR1002X router for created sub interface	Check whether TLOC can be configured for MPLS transport interfaces in DC ASR1002X router for the created sub interfaces successfully	Passed	NA

ENJ.sdwan20.3.G.132	Configure TLOC for INET transport interface in DC ISR4331 router for created sub interface	Check whether TLOC can be configured for INET transport interfaces in DC ISR4331 router for the created sub interfaces successfully	Passed	NA
ENJ.sdwan20.3.G.133	Configure TLOC for MPLS transport interface in DC ISR4331 router for created sub interface	Check whether TLOC can be configured for MPLS transport interfaces in DC ISR4331 router for the created sub interfaces successfully	Passed	NA
ENJ.sdwan20.3.G.134	Configure TLOC for INET transport interface in BR2 ISR4321 router for the assigned IP address	Check whether TLOC can be configured for INET transport interfaces in BR2 ISR4321 router for the assigned IP address successfully	Passed	NA
ENJ.sdwan20.3.G.135	Configure TLOC for MPLS transport interface in BR2 ISR4321 router for the assigned IP address	Check whether TLOC can be configured for MPLS transport interfaces in BR2 ISR4321 router for the assigned IP address successfully	Passed	NA
ENJ.sdwan20.3.G.136	Configure TLOC for MPLS transport interface in BR1 ISR4331 router for the assigned IP address	Check whether TLOC can be configured for MPLS transport interfaces in BR1 ISR4331 router for the assigned IP address successfully	Passed	NA

ENJ.sdwan20.3.G.137	Configure TLOC for INET transport interface in BR1 C1111x-8p router for the assigned IP address	Check whether TLOC can be configured for INET transport interfaces in BR1 C1111x-8p router for the assigned IP address successfully	Passed	NA
ENJ.sdwan20.3.G.138	Configure TLOC extension for INET interface in BR1 C1111x-8p router	Check whether TLOC extension can be configured for INET transport interface in BR1 C1111x-8p router	Passed	NA
ENJ.sdwan20.3.G.139	Configure TLOC extension for MPLS interface in BR1 ISR4331 router	Check whether TLOC extension can be configured for MPLS transport interface in BR1 ISR4331 router	Passed	NA
ENJ.sdwan20.3.G.140	Configure TLOC extension for INET interface in BR1 C1111x-8p router via CLI template in vManage	Check whether TLOC extension can be configured for INET transport interface in BR1 C1111x-8p router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.141	Configure TLOC extension for MPLS interface in BR1 ISR4331 router via CLI template in vManage	Check whether TLOC extension can be configured for MPLS transport interface in BR1 ISR4331 router in vManage	Passed	NA
ENJ.sdwan20.3.G.142	Configure TLOC for MPLS transport interface in BR2 ISR4321 router via CLI template in vManage	Check whether TLOC can be configured for MPLS transport interface in BR2 ISR4321 router via CLI template in vManage	Passed	NA

ENJ.sdwan20.3.G.143	Configure TLOC for INET transport interface in BR2 ISR4321 router via CLI template in vManage	Check whether TLOC can be configured for INET transport interface in BR2 ISR4321 router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.144	Configure TLOC for INET transport interface in BR1 C1111x-8p router via CLI template in vManage	Check whether TLOC can be configured for INET transport interface in BR1 ISR4331 router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.145	Configure TLOC for MPLS transport interface in BR1 ISR4331 router via CLI template in vManage	Check whether TLOC can be configured for MPLS transport interface in BR1 ISR4331 router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.146	Configure TLOC for MPLS transport interface in DC ASR1002x router via CLI template in vManage	Check whether TLOC can be configured for MPLS transport interface in DC ASR1002x router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.147	Configure TLOC for INET transport interface in DC ASR1002x router via CLI template in vManage	Check whether TLOC can be configured for INET transport interface in DC ASR1002x router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.148	Configure TLOC for MPLS transport interface in DC ISR4331router via CLI template in vManage	Check whether TLOC can be configured for MPLS transport interface in DC ISR4331 router via CLI template in vManage	Passed	NA

ENJ.sdwan20.3.G.149	Configure TLOC for INET transport interface in DC ISR4331 router via CLI template in vManage	Check whether TLOC can be configured for INET transport interface in DC ASR1002x router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.150	Upgrade vManage to 20.3 via vManage UI	Check whether vManage 20.3 upgrade file is downloaded, uploaded in the repository and upgraded successfully via vManage UI.	Passed	NA
ENJ.sdwan20.3.G.151	Upgrade vSmart/vBond to 20.3 via vManage UI	Check whether vSmart 20.3 upgrade file is downloaded, uploaded in the repository and upgraded successfully via vManage UI.	Passed	NA
ENJ.sdwan20.3.G.152	Upgrade ISR/ASR registered as cEdge to 17.3 via vManage UI	Check whether ISR/ASR 17.3 upgrade file is downloaded, uploaded in the repository and upgraded successfully via vManage UI.	Passed	NA
ENJ.sdwan20.3.G.154	Standard ACL via CLI Template in vManage to allow ICMP packets in DC side and monitor the traffic flow	Create Standard Access List via CLI Template to allow SSH access for the source IP address of DC in vManage and apply it to edge devices	Passed	NA

ENJ.sdwan20.3.G.155	Standard ACL via CLI Template in vManage to deny ICMP packets in Branch 1 and monitor the traffic flow	Create Standard Access List via CLI Template to deny TELNET access for the source IP address of Branch 1 side in vManage and apply it to cEdge devices	Passed	NA
ENJ.sdwan20.3.G.156	Standard ACL via CLI Template in vManage to deny ICMP packets in Branch 2 and monitor the traffic flow	Create Standard Access List via CLI Template to deny ICMP packets for the source IP address of Branch 2 network in vManage and apply it to cEdge devices	Passed	NA
ENJ.sdwan20.3.G.171	Redistribute OMP routes into OSPF for vrf100 in BR1 C1111x-8p router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf100 in BR1 C1111x-8p router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.172	Redistribute OMP routes into OSPF for vrf200 in BR1 C1111x-8p router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf200 in BR1 C1111x-8p router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.173	Redistribute OMP routes into OSPF for vrf100 in BR1 ISR4331 router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf100 in BR1 ISR4331 router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.174	Redistribute OMP routes into OSPF for vrf200 in BR1 ISR4331 router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf200 in BR1 ISR4331 router via CLI template in vManage	Passed	NA

ENJ.sdwan20.3.G.175	Redistribute OMP routes into OSPF for vrf100 in BR2 ISR4321 router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf100 in BR2 ISR4321 router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.176	Redistribute OMP routes into OSPF for vrf200 in BR2 ISR4321 router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf200 in BR2 ISR4321 router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.177	Redistribute OMP routes into OSPF for vrf100 in DC ISR4331 router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf100 in DC ISR4331 router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.178	Redistribute OMP routes into OSPF for vrf200 in DC ISR4331 router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf200 in DC ISR4331 router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.179	Redistribute OMP routes into OSPF for vrf100 in DC ASR1002x router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf100 in DC ASR1002x router via CLI template in vManage	Passed	NA
ENJ.sdwan20.3.G.180	Redistribute OMP routes into OSPF for vrf200 in DC ASR1002x router via CLI template in vManage	Check whether OMP routes can be redistributed into OSPF for vrf200 in DC ISR ASR1002x router via CLI template in vManage	Passed	NA

ENJ.sdwan20.3.G.218	VRRP OMP Track	Verify when OMP went down Master router goes down Backup take Master role and if the old Master take back its role when it comes up again	Passed	NA
ENJ.sdwan20.3.G.219	VRRP OMP Track scenario - 1	Verify OMP goes down Master router goes backup and backup take Master role and traffic pass via current Master.	Passed	NA
ENJ.sdwan20.3.G.220	VRRP OMP Track – scenario -2	Verify when Master router OMP goes down Backup take Master role and if the old Master came back it should not take Master role.	Passed	NA
ENJ.sdwan20.3.G.215	cEdge configuration scenarios	Verify when login to the device it shows warning message in banner.	Passed	NA
ENJ.sdwan20.3.G.216	cEdge configuration scenarios	Verify the time-zones after configuring the default date and time across all the devices in the topology.	Passed	NA
ENJ.sdwan20.3.G.217	cEdge configuration scenarios	Verify after configuring the system logging, what is the disk size in the device.	Passed	NA
ENJ.sdwan20.3.G.221	Advertise OSPF External routes in to the OMP	Verify OSPF External routes able to configure and redistributed successfully in to the OMP.	Passed	NA
ENJ.sdwan20.3.G.225	Configure DNS name server on the Router	Configure DNS name server on the Router to check the commit command	Passed	NA

ENJ.sdwan20.3.G.222	BGP routes advertised via omp	Verify when we configure the BGP routes advertised successfully without any error on the OMP.	Passed	NA
ENJ.sdwan20.3.G.226	cEdge configuration scenarios to check the BFD session flapping from branch 2	Verify when the control plane has deleted from branch – 2 at the same time the BFD goes down or its working.	Passed	NA
ENJ.sdwan20.3.G.223	feature-template: Editing VPN number	Verify after editing the VPN number in the feature template and push the configuration to cEdge.	Passed	NA
ENJ.sdwan20.3.G.004	QoS classification with telnet data traffic via vManage CLI template	Verify whether the data traffic is routing between cEgde routers using classify class map policy based on port numbers	Passed	NA
ENJ.sdwan20.3.G.005	QoS classification with SSH data traffic via vManage CLI template	Verify whether the data traffic is routing between cEgde routers using classify class map policy based on port numbers	Passed	NA
ENJ.sdwan20.3.G.006	QoS classification with HTTP data traffic via vManage CLI template	Verify whether the data traffic is routing between cEgde routers using classify class map policy based on port numbers	Passed	NA

ENJ.sdwan20.3.G.008	Monitor HTTP packets based on Color through vManage CLI template	Verify whether the data traffic is routing between cEdge routers via vManage cli template by configuring single rate two color class policy and monitor whether the data packets are moving as per the schedule bit rate	Passed	NA
ENJ.sdwan20.3.G.163	Policies to drop TCP packets and monitor the traffic flow with cflowd	Monitor traffic flow with cflowd to drop TCP packets in vManage, apply it to edge devices	Passed	NA
ENJ.sdwan20.3.G.164	Policies to Pass TCP packets and monitor the traffic flow with cflowd	Monitor traffic flow with cflowd to Pass TCP packets in vManage, apply it to edge devices	Passed	NA
ENJ.sdwan20.3.G.165	Policies to drop UDP packets and monitor the traffic flow with cflowd	Monitor traffic flow with cflowd to drop UDP packets in vManage, apply it to edge devices	Passed	NA
ENJ.sdwan20.3.G.166	Policies to Pass UDP packets and monitor the traffic flow with cflowd	Monitor traffic flow with cflowd to Pass UDP packets in vManage, apply it to edge devices	Passed	NA
ENJ.sdwan20.3.G.167	Create Policies to drop TCP from packets and monitor the traffic flow with cflowd for Site 200 branch	Monitor traffic flow with cflowd to drop TCP packets in vManage, apply it to edge devices for Site 200 branch	Passed	NA
ENJ.sdwan20.3.G.168	Create Policies to pass TCP from packets and monitor the traffic flow with cflowd for Site200 branch	Monitor traffic flow with cflowd to Pass TCP packets in vManage, apply it to edge devices for Site 200 branch	Passed	NA

ENJ.sdwan20.3.G.169	Create Policies to drop UDP from packets and monitor the traffic flow with cflowd for Site200 branch	Monitor traffic flow with cflowd to drop UDP packets in vManage, apply it to edge devices for Site 200 branch	Passed	NA
ENJ.sdwan20.3.G.170	Create Policies to pass UDP from packets and monitor the traffic flow with cflowd for Site200 branch	Monitor traffic flow with cflowd to Pass UDP packets in vManage, apply it to edge devices for Site 200 branch	Passed	NA
ENJ.sdwan20.3.G.157	Zone Based Firewall via CLI Template by configuring via class-map and policy-map in WAN side to drop ICMP packets to LAN side and monitor the traffic flow	Create zones, class-map, policy-map, zone-pair in WAN side to drop the ICMP to LAN side in vManage and apply it to edge devices and monitor the traffic	Passed	NA
ENJ.sdwan20.3.G.158	Zone Based Firewall via CLI Template by configuring via class-map and policy-map in LAN side to drop ICMP packets to WAN side and monitor the traffic flow	Create zones, class-map, policy-map, zone-pair in LAN side to drop ICMP packets to WAN side in vManage and apply it to edge devices and monitor the traffic	Passed	NA
ENJ.sdwan20.3.G.159	Zone Based Firewall via CLI Template by configuring via class-map and policy-map in LAN side to drop SSH access to DMZ side and monitor the traffic flow	Create zones, class-map, policy-map, zone-pair in LAN side to drop SCP access to DMZ side in vManage and apply it to edge devices and monitor the traffic	Passed	NA

ENJ.sdwan20.3.G.160	Zone Based Firewall via CLI Template by configuring via class-map and policy-map in DMZ side to drop HTTP/HTTPS packets to LAN side and monitor the traffic flow	Create zones, class-map, policy-map, zone-pair in DMZ side to drop HTTP/HTTPS packets to LAN side in vManage and apply it to edge devices and monitor the traffic	Passed	NA
ENJ.sdwan20.3.G.161	Create a Firewall policy in vManage for dropping ICMP packets and monitor the traffic flow	Create zones, zone pairs, rules for zone-based firewall in vManage to dropping ICMP packets and apply it to edge devices and monitor the traffic	Passed	NA
ENJ.sdwan20.3.G.162	Create a Firewall policy in vManage for dropping SSH access and monitor the traffic flow	Create zones, zone pairs, rules for zone-based firewall in vManage to dropping SSH Access and apply it to edge devices and monitor the traffic	Passed	NA
ENJ.sdwan20.3.G.156	Standard ACL via CLI Template in vManage to deny ping from BR1 ISR4331 and monitor the traffic flow	Create Standard Access List via CLI Template to deny ICMP packets for the source IP address of LAN network in vManage and apply it to cEdge devices	Passed	NA
ENJ.sdwan20.3.G.208	CFD -- CSCvs51630	Verify after configuring the security IPsec replay-window 2048 on cedges it should be same on both the end.	Passed	NA

ENJ.sdwan20.3.G.211	CFD -- CSCvs51630	Verify after configuring the security IPsec replay-window 8192 on cedges it should be same on both the end.	Passed	NA
ENJ.sdwan20.3.G.227	CFD -- CSCvo81091	Verify when we configure the rewrite rule, edge should not restart continuously after committing QoS rewrite-rule	Passed	NA
ENJ.sdwan20.3.G.224	CFD -- CSCvs51630	Verify after configuring the security IPsec replay-window 4096' on cedges it should be same on both the end.	Passed	NA

Related Documentation

Cisco SDWAN 20.3

Release Notes

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/xe-17-3/sd-wan-rel-notes-xe-17-3.html

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/vedge-20-3/sd-wan-rel-notes-20-3.html

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

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