Test Results Summary for IOS XE SD-WAN for Japan (Release Version 20.8.1/17.8.1)

First Published: 2022-07-28

Last Modified: 2022-08-02

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 20.8.1 - IOS XE 17.8.1
- 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
- Cisco 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

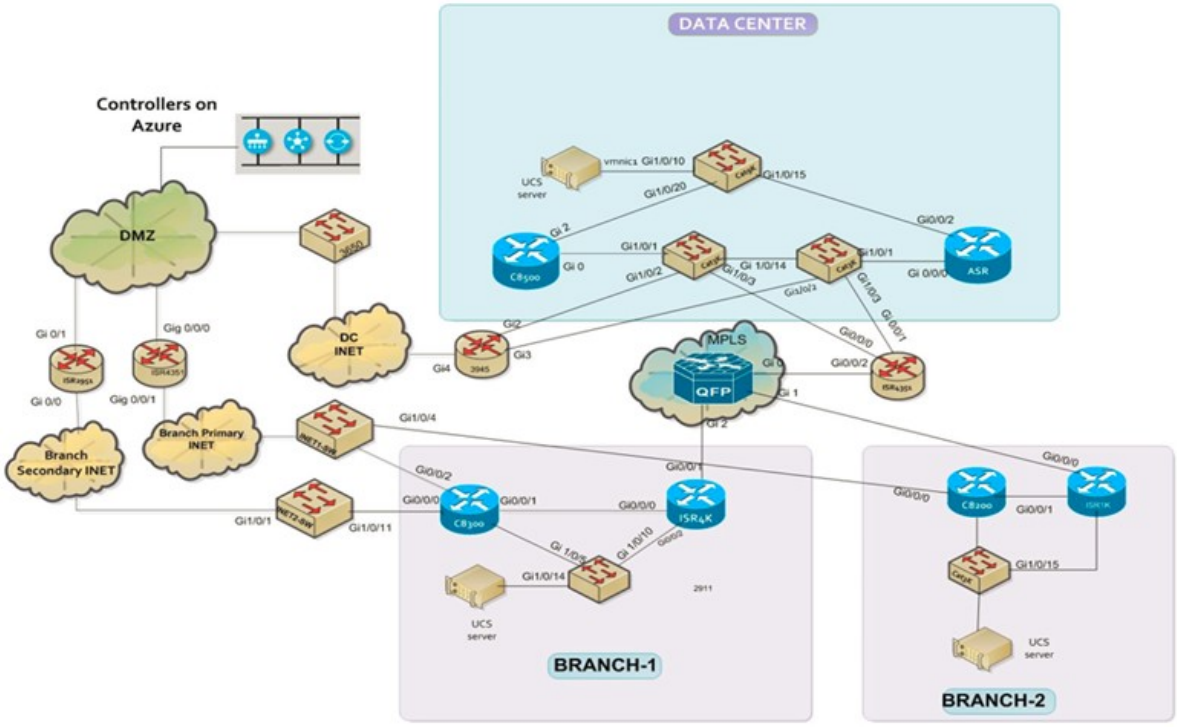
Acronym	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Address-family
API	Application Programming Interface
ASN	Autonomous System Number
ASR	Aggregation Services Routers

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
Geo	Graphical
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	20.8.1
		vManage	20.8.1
		vSmart	20.8.1
	Switch	Cat 9K PoE	17.2
Communications Infrastructure	IOS XE SDWAN	ISR 4351, 4331	17.8.1
		ISR 1100, Cat 8300, C8200 & C8500	17.8.1
		ISR4461	17.8.1
		ASR 1002-X	17.8.1
		ISR C111X-8P	17.8.1
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 20.8.1 - IOS XE 17.8.1 Solution testing

- Configuration Groups and Feature Profiles
- Bidirectional support for packet tracer
- Service-Side NAT Object Tracker
- Service-Side Static Network NAT
- Service-Side Conditional Static NAT
- Redirect DNS in service side VPN
- Support for NAT DIA IPv4 over IPv6 Tunnel
- Cisco Thousand Eyes Support for Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers
- User-defined Device Tagging
- User-defined SAAS Application
- Layer 7 Health Check for Manual Tunnels
- Software upgrade workflow for Cisco SD-WAN edge devices
- Sig Integration improvement(source only load sharing)
- Fallback to Routing
- Sig Integration improvement (IPSec Tunnel Creation Improvements in a Active-Active Setup)

Open Caveats

Defect ID	Title
CSCwc20012	Unable to allocate resources for Thousand eye in cli in cat 8500 device
CSCwc20779	Default values are not taken if parameters values are not specified for the layer 7 health tracker
CSCwc31540	Tunnel parameters values are not matching with the values mentioned in 17.8.1 release notes
CSCwc30674	To configure the object id values are getting mis-matched
CSCwc30650	Unable to create a static NAT in vamange without Nat pool for service side static network
CSCwc10849	No Back/Home button in the Configuration Group Edit page
CSCwc32046	Configuration - Secure Internet Gateway Tunnels API with misleading input field

New Features

Configuration Groups and Feature Profiles

Logical ID	Title	Description	Status	Defect ID
ENJ.CGFP.20.8.1_17.8.1_N.01	Create a Configuration Group from Workflow dialog	Navigate to Workflow Library section. Create a configuration group by entering details by following the workflow.	Passed	
ENJ.CGFP.20.8.1_17.8.1_N.02	Create a Configuration Group from Templates page	Navigate to Templates page. Create a configuration group by entering details.	Passed	
ENJ.CGFP.20.8.1_17.8.1_N.03	Create a feature profile parcel from Templates page	Navigate to Workflow Library section. Create a configuration group by entering details by following the workflow. Edit and create a corresponding feature profile from Templates page.	Failed	CSCwc10849
ENJ.CGFP.20.8.1_17.8.1_N.04	Remove a Configuration Group from Templates page	Navigate to Templates page. Remove the Configuration Group from Templates page	Passed	
ENJ.CGFP.20.8.1_17.8.1_N.05	Add Devices to a Configuration Group Manually	Navigate to Configuration groups. Add Device to a Configuration Group by following the workflow.	Passed	
ENJ.CGFP.20.8.1_17.8.1_N.06	Add Devices to a Configuration Group Using Rules	Tag devices. Navigate to Configuration groups. Create and apply a rule referencing the created tags.	Passed	

ENJ.CGFP.20.8.1_17.8.1_N.07	Verify it's not possible to attach a Configuration Group to a device already attached to a template	Attach a device to a template. Navigate to Configuration Groups page and try to add the device to a Configuration Group with the workflow. Verify the device is unavailable	Passed	
ENJ.CGFP.20.8.1_17.8.1_N.08	Verify it's not possible to attach a template group to a device already attached to a configuration group	Navigate to Configuration Groups page and add a device with the workflow. Try to attach the device to a template. Verify the device is unavailable for association with a Configuration Group.	Passed	
ENJ.CGFP.20.8.1_17.8.1_N.09	Verify it's not possible to attach an additional Configuration Group to a device	Navigate to Configuration Groups page and add a device to a configuration group with the workflow. Repeat the process for another configuration group. Verify failure	Passed	
ENJ.CGFP.20.8.1_17.8.1_N.10	Verify it's not possible to add an additional tag rule to a configuration group	Navigate to a configuration with a Tag rule. Verify there is no option to create an additional tag rule for the Configuration Group.	Passed	
ENJ.CGFP.20.8.1_17.8.1_N.11	Remove Devices from a Configuration Group	Navigate to Configuration Groups. Remove Devices from a Configuration Group.	Passed	

ENJ.CGFP. 20.8.1_17.8.1_N.12	Get a Configuration Group by ID via API	Get a Configuration Group by ID via API	Passed	
ENJ.CGFP. 20.8.1_17.8.1_N.13	Create Config Group Association with devices via API	Associate a Configuration Group to a device via an API call	Passed	
ENJ.CGFP. 20.8.1_17.8.1_N.14	Delete Config Group Association from devices via API	Delete Config Group Association from devices via API	Passed	
ENJ.CGFP. 20.8.1_17.8.1_N.15	Delete Configuration Group via API	Delete Configuration Group via API	Failed	CSCwc32046
ENJ.CGFP. 20.8.1_17.8.1_N.16	Get a SDWAN Feature Profile with CLI profile type via API	Get a SDWAN Feature Profile with CLI profile type via API	Passed	
ENJ.CGFP. 20.8.1_17.8.1_N.17	Edit a SDWAN Feature Profile with CLI profile type via API	Edit a SDWAN Feature Profile with CLI profile type via API	Passed	
ENJ.CGFP. 20.8.1_17.8.1_N.18	Delete a SDWAN Feature Profile with CLI profile type via API	Delete a SDWAN Feature Profile with CLI profile type via API	Passed	
ENJ.CGFP. 20.8.1_17.8.1_N.19	Create a profile with LAN configuration	Navigate to Workflow Library section. Configure LAN details and create Configuration Group.	Passed	
ENJ.CGFP. 20.8.1_17.8.1_N.20	Create a profile with WAN configuration	Navigate to Workflow Library section. Configure WAN details and create Configuration Group.	Passed	
ENJ.CGFP. 20.8.1_17.8.1_N.21	Configure Local Policy with CLI profile	Navigate to Workflow Library section. Create a configuration group with CLI profile for Local Policy	Passed	

Cisco Thousand Eyes Support for Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers

Logical ID	Title	Description	Status	Defect ID
ENJ.TES .20.8.1_17.8.1_N.01	Upload Cisco Thousand Eyes Enterprise Agent Software to Cisco vManage	By using vManage we upload the Thousand Eyes Enterprise Agent Software to Cisco vManage	Passed	
ENJ.TES .20.8.1_17.8.1_N.02	Upload Cisco Thousand Eyes Enterprise Agent Software on CISCO ASR 1000 and cat 8500 devices using Cli& vManage and check the feature compatibility	To upload the 1000 eye agent in cli and vManage on cat 8500 and ASR 1000 to check the features	Passed	
ENJ.TES .20.8.1_17.8.1_N.03	Provision Cisco Thousand Eyes Enterprise Agent in Transport VPN (VPN 0) in ASR 1000 device	By using vManage we configure and upload the Thousand Eyes Enterprise Agent VPN	Passed	
ENJ.TES .20.8.1_17.8.1_N.04	Provision Cisco Thousand Eyes Enterprise Agent in Transport VPN (VPN 0) in C8500 device	By using VManage we configure and upload the Thousand Eyes Enterprise Agent VPN	Passed	
ENJ.TES .20.8.1_17.8.1_N.05	Provision Cisco Thousand Eyes Enterprise Agent in a Service VPN in ASR 1000 device	By using vManage we configure and upload the Thousand Eyes Enterprise Agent VPN	Passed	
ENJ.TES .20.8.1_17.8.1_N.06	Provision Cisco Thousand Eyes Enterprise Agent in a Service VPN in cat 8500 device using feature/cli template	By using vManage we configure and upload the Thousand Eyes Enterprise Agent VPN	Passed	

ENJ.TES .20.8.1_17.8.1_N.07	Provision Cisco Thousand Eyes Enterprise Agent in a Service VPN Using CLI in ASR 1000 device	By using CLI we configure the Thousand Eyes Enterprise Agent Software	Passed	
ENJ.TES .20.8.1_17.8.1_N.08	Provision Cisco Thousand Eyes Enterprise Agent in a Service VPN Using CLI in cat 8500 device	By using CLI we configure the Thousand Eyes Enterprise Agent Software	Passed	
ENJ.TES .20.8.1_17.8.1_N.09	Upgrade Cisco Thousand Eyes Enterprise Agent Software to Cisco vManage	By using VManage we upgrade the Thousand Eyes whole package Software	Passed	
ENJ.TES .20.8.1_17.8.1_N.10	Upgrade Cisco Thousand Eyes Enterprise Agent Software in Cli	By using cli we upgrade the 1000 eye agent	Passed	
ENJ.TES .20.8.1_17.8.1_N.11	Uninstall Cisco Thousand Eyes Enterprise Agent Software in VManage and CLI	By using CLI and vManage we uninstall the 1000 eye agent.	Passed	
ENJ.TES .20.8.1_17.8.1_N.12	Configure HTTP server test on thousand eye portal and check the network performance	By using agent portal we can configure HTTP server test.	Passed	
ENJ.TES .20.8.1_17.8.1_N.13	Configure test to check the network performance of the server hosted on the DC from the TE agent	By using 1000 eye agent we can check the server performance hosted on DC	Passed	
ENJ.TES .20.8.1_17.8.1_N.14	Allocate the resource for the TE application and check the status.	By using CLI we configure the resources	Failed	CSCwc32046

ENJ.TES .20.8.1_17.8.1_N.15	Configure a test to reach a destination server from source node and check the path visualization and its parameters	By using 1000 agent we can check the reachability of destination server	Passed	
ENJ.TES .20.8.1_17.8.1_N.16	Configure the protocol settings (TCP/ICMP) in path visualization and check the information displayed on the path.	By using 1000 agent set the protocol setting for the server	Passed	
ENJ.TES .20.8.1_17.8.1_N.17	Modify the hostname of TE using cli and vManage	By using vManage and cli we configure the Thousand Eyes default hostname & modify	Passed	
ENJ.TES .20.8.1_17.8.1_N.18	Configure TE through management interface instead of virtual port group.	By using Cli to create management interface of 1000 eye agent	Passed	
ENJ.TES .20.8.1_17.8.1_N.19	Create DNS server test and check the availability of DNS server	By using 1000 eye agent to Create DNS server test	Passed	
ENJ.TES .20.8.1_17.8.1_N.20	Check the network availability and performance between two agents	By using vManage we configure the Thousand Eyes default hostname & modify	Passed	

Fallback to Routing

Logical ID	Title	Description	Status	Defect ID
ENJ.SIGFOR .20.8.1_17.8.1_N.01	Check when sig up Traffic Re-directed of SIG	Fallback to Routing	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.02	Check When sig Down Traffic follows routing table instead of drops	Check When sig Down Traffic follows routing table instead of drops	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.03	Verify Packet trace drop count of fallback routing	verify Packet trace drop count of fallback routing	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.04	Configure manually Sig-action fallback routing and verify	Configure manually Sig-action fallback routing and verify	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.05	Configure App Probe Class	Configure App Probe Class	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.06	Configure policer	Configure Policer	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.07	Configure Site	Configure Site	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.08	Configure Colour and Community	Configure color and Community	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.09	Configure Data prefix	Redirect the block page to the external block page and display with blocked by which category.	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.10	Configure TLOC	Configure TLOC	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.11	Configure Traffic rules	Configure Traffic Rules	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.12	Check the Fallback to Routing check box to route internet-bound traffic through the Cisco SD-WAN overlay when all SIG tunnels are down	Check the Fallback to Routing check box to route internet-bound traffic through the Cisco SD-WAN overlay when all SIG tunnels are down	Passed	

ENJ.SIGFOR .20.8.1_17.8.1_N.13	Match Parameters-Control policy	Match Parameters - Control Policy	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.14	Configure Topology and VPN Membership	Configure Topology and VPN Membership	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.15	Configure SLA Class	Configure SLA Class	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.16	Check When sig come-back up new flows redirect to sig,old flows stick to routing	Check When sig come-back up new flows redirect to sig,old flows stick to routing	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.17	Data Center to internet traffic transfer via OMP that time route-falling or not	Check When OMP to transport traffic to a remote DATA center, and from DATA center to internet that time route-falling or not	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.18	Configure DIA fallback with NAT route	Check traffic go or not via DIA fallback with NAT route	Passed	
ENJ.SIGFOR .20.8.1_17.8.1_N.19	Check the Traffic is routed to a NAT-enabled WAN transport VPN from the service-side VPN based on the destination prefix in the NAT DIA route or not	Check traffic go or not via DIA fallback with NAT route	Passed	

Support for NAT DIA IPv4 over IPv6 Tunnel

Logical ID	Title	Description	Status	Defect ID
ENJ.NDV4V6T .20.8.1_17.8.1_N.01	Configuring NAT DIA IPv4 over an IPv6 Tunnel using Cli template	. The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface	Passed	
ENJ.NDV4V6T .20.8.1_17.8.1_N.02	Configuring NAT DIA IPv4 over an IPv6 Tunnel using CLI	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	

ENJ.NDV4V6T .20.8.1_17.8.1_N.03	To Verify NAT DIA IPv4 over an IPv6 Tunnel Configuration	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	
ENJ.NDV4V6T .20.8.1_17.8.1_N.04	To configure the IP-SLA to track the ipv6 Tunnel	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	
ENJ.NDV4V6T .20.8.1_17.8.1_N.05	Enable NAT Route Advertisement Through OMP using CLI	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	

ENJ.NDV4V6T .20.8.1_17.8.1_N.06	Verify NAT Route Advertisements Through OMP Using the CLI	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	
ENJ.NDV4V6T .20.8.1_17.8.1_N.07	Configure and verify NAT DIA Routes using CLI	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	
ENJ.NDV4V6T .20.8.1_17.8.1_N.08	To configure and verify OSPFv3 from service side(overlay) to transit through NAT DIA ipv4 over Ipv6 Tunnel	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface	Passed	

ENJ.NDV4V6T .20.8.1_17.8.1_N.09	To configure and verify BGP from service side to transit through NAT DIA ipv4 over Ipv6 Tunnel	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	
ENJ.NDV4V6T .20.8.1_17.8.1_N.10	To configure and verify BGP with metrics from service side to transit through NAT DIA ipv4 over Ipv6 Tunnel	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	
ENJ.NDV4V6T .20.8.1_17.8.1_N.11	To configure and verify BGP with BFD enabled from service side & transit through NAT DIA ipv4 over Ipv6 Tunnel	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	

ENJ.NDV4V6T .20.8.1_17.8.1_N.12	To configure and verify OSPFv3 with BFD enabled from service side to transit through NAT DIA ipv4 over Ipv6 Tunnel	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	
ENJ.NDV4V6T .20.8.1_17.8.1_N.13	Loopback Interface WAN over IPv4 over IPv6 tunnel sdwan connection case using CLI	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface.	Passed	

Bidirectional support for packet tracer

Logical ID	Title	Description	Status	Defect ID
ENJ.BPC. 20.8.1_17.8.1_ N.01	Configure the Bidirectional packet capture with source and destination IP filter	By using src/dst ip filter we capture the packets with bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.02	Configure the Bidirectional packet capture with source and destination IP prefix filter	By using src/dst ip filter we capture the packets with bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.03	Configure the Bidirectional packet capture with ipv4 address and tcp protocol with port filter	By using ipv4 filter we capture the packets tcp protocol with port filter bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.04	Configure the Bidirectional packet capture with mac filter	By using Mac address filter we capture the packets with bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.05	Configure the Bidirectional packet capture with mac range filter	By using mac range filter we capture the packets with bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.06	Configure the Bidirectional packet capture on lan interface with src/dst IP filter	By using src/dst ip filter we capture the packets with bidirectional in lan interface	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.07	Configure the Bidirectional packet capture on LAN interface with MAC filter	By using conditional debug command we capture the packets with bidirectional of src/ds tip filter	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.08	Configure the packet capture without bidirectional to capture the packets by using IN bound direction	By using packet capture without bidirectional to capture the traffic by using IN direction	Passed	

ENJ.BPC. 20.8.1_17.8.1_ N.09	Configure the Bidirectional packet capture punt packets with src/dst IP filter	By using src/dst ip filter we capture the punt packets with bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.10	Configure the Bidirectional packet capture inject packets with src/dst IP filter	By using src/dst ip filter we capture the inject packets with bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.11	Configure the packet capture without bidirectional to capture the packets by using OUT bound direction	By using packet capture without bidirectional to capture the traffic by using OUT direction	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.12	Configure the packet capture without bidirectional to capture the packets by using IN bound direction	By using buffer packet capture with bidirectional to capture the traffic by using IN direction	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.13	Configure the Bidirectional packet capture on wan interface with src/dst IP filter	By using src/dst ip filter we capture the packets with bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.14	Configure and enable the packet trace for the traffic and specify the max number of packets	By using src/dst ip filter we capture the packets with max number of packets bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.15	Configure the Bidirectional packet capture with ipv4 address and udp protocol with port filter	By using ipv4 filter we capture the packets udp protocol with port filter bidirectional	Passed	
ENJ.BPC. 20.8.1_17.8.1_ N.16	Configure the debug platform packet caputre from ingress direction with ip interface	By using debug platform we capture the packets with ingress direction	Passed	

Layer 7 Health Check for Manual Tunnels

Logical ID	Title	Description	Status	Defect ID
ENJ.L7HC .20.8.1_17.8.1_N.01	Create a Layer7 health tracker in vManage for manual tunnel	Configure layer 7 health tracker	Failed	CSCwc20779
ENJ.L7HC .20.8.1_17.8.1_N.02	Redirect traffic to SIG using Service route	Redirect traffic to SIG	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.03	Configure Layer 7 health check with interface	Configure Layer 7 health check with interface	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.04	Take down active tunnels and ensure L7 health checks also works for new active (previously standby) tunnels	Layer 7 health check for active tunnel	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.05	Configure tunnel with SLA and check the Tunnel interface status	latency with SLA and check the Tunnel interface status	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.06	Check Active backup tunnel fail-over	Active backup tunnel fail-over	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.07	Create tunnel with custom and user defined tracker for automatic /manual tunnels	Create a tunnel with custom and user defined tracker	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.08	Check Active backup tunnel failover with interface flap both on different interface	Active backup tunnel failover with interface flap both on different interface	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.09	High Availability and Load Balancing	High Availability and Load Balancing	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.10	Check Threshold range (100-1000 ms) for New Tracker	Threshold range (100-1000 ms) for New Tracker	Failed	CSCwc31540

ENJ.L7HC .20.8.1_17.8.1_N.11	Check Interval range (10-600 sec) for New Tracker	Interval range (10-600 sec) for New Tracker	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.12	Check Multiplier range (1-10) for New Tracker	Multiplier range(1-10) for New Tracker	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.13	Configure same weight on the active and backup tunnel and check ECMP has achieved or not	Configure same weight on the active and backup tunnel and to achieve ECMP	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.14	Shut the active tunnel and check the tunnel traffic and status	Shut the active tunnel and check the tunnel traffic and status	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.15	Shut the backup tunnel and check the tunnel traffic and status	To shut the backup tunnel and check the tunnel traffic and status	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.16	Revert back the active and backup tunnel and verify the status	Revert back the active and backup tunnel and verify the status	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.17	Configure a generic SIG tunnel and route the traffic via firewall to reach the end host	To route the traffic via firewall	Passed	
ENJ.L7HC .20.8.1_17.8.1_N.18	Configure a Umbrella SIG tunnel in cisco ASA firewall to reach the end host destination	Using umbrella SIG tunnel in ASA firewall	Passed	

Redirect DNS in service side VPN

Logical ID	Title	Description	Status	Defect ID
ENJ.RDSSV .20.8.1_17.8.1_N.01	To configure Service side conditional Redirect DNS using CLI	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.02	To configure Service side conditional Redirect DNS using VManage	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.03	To configure Service side un-conditional Redirect DNS using CLI	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs	Passed	

ENJ.RDSSV .20.8.1_17.8.1_N.04	To configure Service side un-conditional Redirect DNS using VManage	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.05	To allow only the particular Service VPN (VPN100) traffic to conditional redirect DNS	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.06	To configure Service side conditional Redirect DNS using CLI App-List (YouTube)	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	

ENJ.RDSSV .20.8.1_17.8.1_N.07	To verify the centralised Data policy from vSmart	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.08	To configure Service side conditional Redirect DNS using CLI with NAT overload	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.09	To configure Service side un-conditional Redirect DNS using CLI with NAT	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	

ENJ.RDSSV .20.8.1_17.8.1_N.10	To configure the Service side Conditional Redirect DNS Passing through CEDGE	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.11	To configure the Service side un–Conditional Redirect DNS Passing through CEDGE	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.12	To test the conditional DNS redirect working well with TLOC extension	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	

ENJ.RDSSV .20.8.1_17.8.1_N.13	To test the unconditional DNS redirect working well with TLOC extension	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.14	To configure conditional DNS redirect with dynamic IP NAT pool using CLI	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs	Passed	
ENJ.RDSSV .20.8.1_17.8.1_N.15	To configure conditional DNS redirect with static NAT using CLI	This feature allows you to configure Cisco IOS XE SD-WAN device to respond to DNS queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirect inside the service VPNs.	Passed	

ENJ.RDSSV .20.8.1_17.8.1_N.16	Service side unconditional Redirect DNS for App-List with NAT using CLI	The NAT DIA IPv4 over an IPv6 tunnel enables IPv6-only devices to access IPv4 websites and services. The traffic flow is from the service side (LAN) to the transport side (WAN) in the overlay network. Service-side source IPv4 addresses are translated to public IPv4 addresses on the tunnel interface	Passed	

Service-Side Conditional Static NAT

Logical ID	Title	Descrption	Status	Defect id
ENJ.SSCSN .20.8.1_17.8.1_N.01	To configure a conditional static Nat with single source at dual destination through cli template using data policy	To assign the dual public Ip address from the single host based on the destination.	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.02	To configure a dual destination with a dual source in conditional static NAT using data policy	To assign the many public Ip address for a single host based on the destination	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.03	To configure a conditional static Nat with single source at dual destination without data policy	To assign the many public Ip address for a single host based on the destination	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.04	To configure a conditional static Nat with single source at dual destination without overload	To assign the many public Ip address for a single host based on the destination	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.05	To configure a conditional static Nat with single source at dual destination and delete the Nat pool and check	To check the Dual public Ip address from the single host based on the destination and check	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.06	To configure a conditional static Nat with inside Nat pool in a multiple destination	To assign the many public Ip address for a single host based on the destination	Passed	

ENJ.SSCSN .20.8.1_17.8.1_N.07	To configure the inside Nat pool with different prefix length on conditional static Nat using cli Template	To assign the many public Ip address for a single host based on the destination	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.08	To configure the and check the Conditional static Nat with single source at dual destination without Nat pool	To assign the many public Ip address for a single host based on the destination	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.09	To configure the multiple Nat pool for a single host in conditional static	To assign the many public Ip address for a single host based on the destination	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.10	To configure the single source with single destination in conditional NAT through vManage	To assign the many public Ip address for a single host based on the destination	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.11	To configure the conditional service side NAT with a multiple Nat pool with different prefix length using data policy	To configure the conditional service side NAT with a multiple Nat pool with different prefix length using data policy	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.12	To configure the conditional static NAT with overload and without matching sequence in data policy through cli.	To assign the many public Ip address for a single host based on the destination	Passed	
ENJ.SSCSN .20.8.1_17.8.1_N.13	To configure the conditional static NAT by using vManage feature template with centralized data policy	To assign the many public Ip address for a single host based on the destination	Passed	

Service-Side NAT Object Tracker

Logical ID	Title	Description	Status	Defect ID
ENJ.SSNOT. 20.8.1_17.8.1_N.01	To configure the service side static Nat single object tracker for Lan interface (inside) cli with DP	To tracker the one of the Lan interface line protocols after we applied the NAT	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.02	To configure the service side static Nat single object tracker for Lan prefix (inside)cli with DP	We are going to tracker the LAN prefix after the we applied the NAT	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.03	To configure the service side dynamic Nat single object tracker for Lan interface (inside) cli	We are going to apply the Dynamic NAT to the LAN interface and tracker that interface.	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.04	To configure the service side dynamic Nat single object tracker for Lan prefix (inside) cli	We are going to apply the Dynamic NAT to the LAN prefix and tracker the prefix	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.05	To configure the service side static Nat single object tracker for Lan Ip route reachability (inside) cli.	To tracker the Ip route reachability for the Lan interface for a single host.	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.06	To configure the service side static Nat single object tracker for Lan interface (inside) vManage template	To configure the NAT object tracker for single LAN through vManage.	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.07	To configure the service side static Nat dual object tracker for Lan interface (inside) cli	To track the dual LAN Interface after we applied the NAT.	Passed	

ENJ.SSNOT. 20.8.1_17.8.1_N.08	To configure the service side static Nat single object tracker for Lan Ip route reachability (inside) cli add-on-template	To configure the service side static Nat single object tracker for Lan Ip route reachability (inside) cli add-on-template	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.09	To configure the service side static Nat single object tracker for Lan interface (inside) cli template without data policy	Configure the service side static Nat single object tracker for Lan interface (inside) cli template without data policy..	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.10	To configure the service side static Nat single object tracker for Lan interface (inside) cli template without Nat pool	Configure the service side static Nat single object tracker for Lan interface (inside) cli template without Nat pool	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.11	To configure the dynamic Nat and static NAT are not mapped to pool with same tracker	Configure the dynamic Nat and static NAT are not mapped to pool with same tracker	Failed	CSCwc30674
ENJ.SSNOT. 20.8.1_17.8.1_N.12	To configure the dynamic Nat and static NAT are not mapped to pool with two tracker	Configure the dynamic Nat and static NAT that are not mapped to pool with two tracker.	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.13	To configure the service side static Nat single object tracker for Lan interface (inside) cli template without overload	Configure the service side static Nat single object tracker for Lan interface (inside) cli template without overload..	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.14	To configure the service side static Nat single object tracker for Lan interface (inside) with delay up 15s and down 20s in cli template	Configure the service side static Nat single object tracker for Lan interface (inside) with delay up 15s and down 20s in cli template.	Passed	

ENJ.SSNOT. 20.8.1_17.8.1_N.15	To monitor the single object tracker for Lan interface with delay down 25s in cli template	Going to monitor the single object tracker for Lan interface with delay down 25s in cli template	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.16	Configure the service side VRRP Object tracker to add on interface with Boolean AND parameter	Configure the service side VRRP object tracker with Boolean parameter, bring down the one of the trackers and check the traffic flow.	Passed	
ENJ.SSNOT. 20.8.1_17.8.1_N.17	Configure the VRRP Object tracker to service side with Boolean OR parameter with line protocol	Configure the service side VRRP object tracker with Boolean parameter	Passed	

Service-Side Static Network NAT

Logical ID	Title	Description	status	Defect ID
ENJ.SSSN .20.8.1_17.8.1_N.01	To configure the service side Single static N/W NAT using vManage without DP	To configure the overall public network address can be mapped to the over all private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.02	To configure the service side single static N/W NAT using vManage with DP	To configure the overall public network address can be mapped to the overall private network address	Failed	CSCwc30650
ENJ.SSSN .20.8.1_17.8.1_N.03	To configure the service side single static N/W NAT using cli with Data policy	To configure the overall public network address can be mapped to the overall private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.04	To configure the service side dual static n/w Nat for dual destination using DP	To configure the overall public network address can be mapped to the overall private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.05	To configure the service side static single network with multiple destination using DP	To configure the overall public network address can be mapped to the overall private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.06	To configure a service side network Nat with and without match the sequence using CLI Template	To configure the overall public network address can be mapped to the overall private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.07	To configure the service side single static N/W NAT for single destination using cli with DP.	To configure the overall public network address can be mapped to the overall private network address	Passed	

ENJ.SSSN .20.8.1_17.8.1_N.08	To configure the service side single static N/W NAT for dual destination with a tracker using DP	To configure the overall public network address can be mapped to the overall private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.09	To configure the service side single static N/W NAT for destination with a tracker using DP IN vManage.	To configure the overall public network address can be mapped to the overall private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.10	To configure the service side static N/W NAT port forwarding using DP in CLI Template	To configure the overall public network address can be mapped to the overall private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.11	To configure the service side single static N/W NAT using cli with DP and overlapping in Nat pool using cli.	To configure the service side NAT with overlapping the public Ip address.	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.12	To configure the inside service side NAT network using cli with DP	To configure the overall public network address can be mapped to the overall private network address	Passed	
ENJ.SSSN .20.8.1_17.8.1_N.13	To configure the inside service side NAT network with data policy direction service using cli	To configure the overall public network address can be mapped to the overall private network address	Passed	

Sig Integration improvement(source only load sharing)

Logical ID	Title	Description	Status	Defect ID
ENJ.SIGSOLS .20.8.1_17.8.1_N.01	Manual SIG Tunnel with Source-Only Load Sharing via Templates	Create and apply a SIG Feature Template and a Source-Only Load Sharing CLI Add-on Template. Check the traffic from an IP address is using a specific Tunnel.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.02	Failover Manual SIG Tunnel with Source-Only Load Sharing via Templates	Create and apply a SIG Feature Template and a Source-Only Load Sharing CLI Add-on Template. Check the traffic from an IP address is using a specific Tunnel.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.03	Failover and Bring-up Manual SIG Tunnel with Source-Only Load Sharing via Templates	Create and apply a SIG Feature Template and a Source-Only Load Sharing CLI Add-on Template. Check the traffic from an IP address is using a specific Tunnel.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.04	Manual SIG Tunnel with Source-Only Load Sharing and Policy for Custom application	Create and apply a SIG Feature Template and a Source-Only Load Sharing CLI Add-on Template. Create Policy for Custom Application List/Family with a particular Source IP. Check the traffic from an IP address is using a specific Tunnel for different Applications.	Passed	

ENJ.SIGSOLS .20.8.1_17.8.1_N.05	Manual SIG Tunnel with Source-Only Load Sharing and Policy for Allowing and blocking the sites based on the Destination lists	Create Manual SIG Tunnels. Check Allow for Website prefix(es), ports with a particular Source IP. Check the traffic from an IP address is using a specific Tunnel for different Websites.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.06	Check whether performance improvement due to Source-only load sharing	Configure SIG tunnels without Source-only configure. Then, configure Source-only and check the traffic Performance improves. Check the traffic from an IP address is using a specific Tunnel.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.07	Source-Only Load Sharing with Automatic SIG Tunnels	Create SIG Feature Template for Automatic SIG Tunnels. Create CLI Add-On Template for Source-Only Load Sharing. Apply the Templates.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.08	SIG Active-Active Source-Only Load Sharing via CLI	Configure 2 Active SIG tunnels and enable Source-Only Load Sharing	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.09	Failover and Bring-up SIG Active-Active Source-Only Load Sharing via CLI	Sig Integration improvement(source only load sharing)	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.10	Weighted SIG Active-Active Source-Only Load Sharing via CLI	Configure 2 Weighted Active SIG tunnels and enable Source-Only Load Sharing. Check the traffic from an IP address is using a specific Tunnel.	Passed	

ENJ.SIGSOLS .20.8.1_17.8.1_N.11	Failover and Bring-up with Weighted SIG Active-Active Source-Only Load Sharing via CLI	Configure 3 Weighted Active SIG tunnels and enable Source-Only Load Sharing. Fail an Active Tunnel and bring it back up to verify the Source-Only mapping is not sticky.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.12	SIG Active-Backup Source-Only Load Sharing via CLI	Configure 4 SIG tunnels for 2 Active-Backup HA pairs and enable Source-Only Load Sharing. Check the traffic from an IP address is using a specific Tunnel.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.13	Failover and Bring-up with SIG Active-Backup Source-Only Load Sharing via CLI	Configure 4 SIG tunnels for 2 Active-Backup HA pairs and enable Source-Only Load Sharing. Fail an Active Tunnel and bring it back up to verify the Source-Only mapping is not sticky.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.14	Manual SIG Tunnel without and with Redirect Traffic to SIG and Source-Only Load Sharing via Templates	Create and apply a SIG Feature Template and a Source-Only Load Sharing CLI Add-on Template. Modify Service VPN Template for SIG redirection. Check the Internet traffic from an IP address is using a specific Tunnel.	Passed	

ENJ.SIGSOLS .20.8.1_17.8.1_N.15	GET Manual SIG Tunnel with Source-Only Load Sharing via API	Create and apply a SIG Feature Template and a Source-Only Load Sharing CLI Add-on Template. Check the traffic from an IP address is using a specific Tunnel. Check the Tunnels are contained in the API response.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.16	Failover and Bring-up Manual SIG Tunnel with Source-Only Load Sharing via Templates	Create and apply a SIG Feature Template and a Source-Only Load Sharing CLI Add-on Template. Check the traffic from an IP address is using a specific Tunnel.	Passed	
ENJ.SIGSOLS .20.8.1_17.8.1_N.17	Create and user-defined tracker in cli to monitor the endpoint	Create and apply a SIG Feature Template and a Source-Only Load Sharing CLI Add-on Template. Modify Service VPN Template for SIG redirection. Check the Internet traffic from an IP address is using a specific Tunnel.	Passed	

Sig Integration improvement (IPSec Tunnel Creation Improvements in a Active-Active Setup)

Logical ID	Title	Description	Status	Defect ID
ENJ.SIGAA .20.8.1_17.8.1_N.01	Manual Network Tunnel configuration with cEdge and Umbrella	Manual Network Tunnel configuration with cEdge and Umbrella.	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.02	Automatic Network Tunnel configuration with cEdge and Umbrella	Automatic Network Tunnel configuration with cEdge and Umbrella.	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.03	Cisco Umbrella SIG integration with CEdge via VManage	Cisco Umbrella SIG integration with cEdge via vManage	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.04	Create SIG tunnel with active-active and verify	Create Sig tunnel with active-active and verify	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.05	Cisco Umbrella SIF with Manual IPsec tunnel	Cisco Umbrella SIG with Manual IPsec Tunnel	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.06	Configuring cloud-delivered firewall and filter traffic at layer 3 and layer 4 and layer 7	Configuring cloud-delivered firewall and filter traffic at layer 3 and layer 4 and layer 7.	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.07	Enable File Inspection for DNS Policies	Enable File Inspection for DNS Policies.	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.08	Enable File Inspection for WEB Policies	Enable File Inspection for WEB Policies.	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.09	Verify user can be able to access Umbrella Single-Org API Key	Verify user can be able to access Umbrella Single-Org API Key	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.10	Define Domain lists	Define Domain Lists	Passed	

ENJ.SIGAA .20.8.1_17.8.1_N.11	Configure Umbrella DNS policy Using vManage	Redirect the block page to default umbrella blocked page.	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.12	To configure the device as a pass -through server	To configure the Device as a Pass-through Server	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.13	Verify Umbrella show commands at Fp layer	Verify Umbrella show commands at FP Layer	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.14	Verify Umbrella show commands at CPP	Verify Umbrella show commands at CPP Layer	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.15	LayerTroubleshooting the Umbrella Integration	Troubleshooting the Umbrella Integration	Passed	
ENJ.SIGAA .20.8.1_17.8.1_N.16	Verify Umbrella Data-Plane show Commands	Verify Umbrella Data-Plane show commands	Passed	

User-defined Device Tagging

Logical ID	Title	Description	Status	Defect ID
ENJ.UDDT .20.8.1_17.8.1_N.01	Create & delete tag in cisco vManage 17.8	To check whether we can deleted & create tag in vManage via device page	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.02	Create & delete tag in cisco vManage 17.8.1	To check whether we can deleted & create tag in vManage via workflow	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.03	Create device tag for grouping the device by adding same tag	To Add same tag for two or more device for grouping	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.04	Create device tag for describing the function to configure	To check whether we can deleted & create tag in vManage via device page	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.05	Create device tag to find or manage device in network using vManage	To find or manage the single or multiple device using tag	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.06	Create device tag based using configuration group for system profile	To configure system profile by adding tag using configuration group	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.07	Create device tag based on configuration group using Transport profile	To configure Transport profile by adding tag using configuration group	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.08	Create device tag based on configuration group using service profile	To configure service profile by adding tag using configuration group	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.09	Create device tag based and add device to a configuration group Manually	To configure profile by adding tag using configuration group Manually	Passed	

ENJ.UDDT .20.8.1_17.8.1_N.10	Create device tag based and add device to a configuration group using rules with operator Equal	To configure service profile by adding tag using configuration group with rule	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.11	Create device tag based and add device to a configuration group using rules with operator Not Equal	To configure profile by adding tag using configuration group with rule	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.12	Create device tag based and add device to a configuration group using rules with operator Contain	To configure profile by adding tag using configuration group with rule	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.13	Create device tag based and add device to a configuration group using rules with operator Not Contain	To configure profile by adding tag using configuration group with rule	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.14	Create a maximum of 25 tag per device & ensure tag name should be 25 characters	To check whether we can create maximum 25 tag & tag should be maximum 25 characters in vManage via device page	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.15	Verify a new rule cannot be created if it conflicts with an existing rule	To configure service profile by adding tag using configuration group with rule	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.16	Verify a device cannot be tagged if it is already attached to a template	To configure profile by adding tag using configuration group with template	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.17	Configure attached a template to a device, and the task is in progress, you can add a tag to the device	To configure profile by adding tag using configuration group with template	Passed	

ENJ.UDDT .20.8.1_17.8.1_N.18	If a device is automatically added to a configuration group based on a tag rule, you cannot remove the device from the group	To configure profile by adding tag using configuration group with tag rule	Passed	
ENJ.UDDT .20.8.1_17.8.1_N.19	Tag 2 Device A with group A & Tag 2 Device B with group B with conflicting rules.	To configure profile by adding tag using configuration group with tag rule to checking confilict	Passed	

User-defined SAAS Application

Logical ID	Title	Description	Status	Defect ID
ENJ.SaaSA .20.8.1_17.8.1_N.01	Configure SD-AVC server to create custom application for User-defined SAAS Application	To Create Custom Application for User-defined SAAS Application	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.02	Configure or enable NBAR by using protocol pack to identify the network traffic according to the network application that produced the traffic	To identify the network traffic according to the network application that produced the traffic	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.03	Configure monitoring/vpn/policy/cloud SLA to initiate the Quality of Experience probing to find the best path for User-defined SAAS Application	To initiate the Quality of Experience probing to find the best path	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.04	Disable monitoring stops the Quality of Experience probing for the User-defined SAAS Application	To check the Quality of Experience probing while disabling the Monitoring	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.05	Configure Cloud OnRamp for SaaS both on the client sites and on the gateway sites for User-defined SAAS Application	To check User-defined SAAS Application via Gateway sites	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.06	Enable load balancing for cloud application traffic across multiple interfaces on the WAN edge device for User-defined SAAS Application	To check User-defined SAAS Application via Multiple interface using Load balacacing	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.07	Configure Cloud OnRamp for SaaS on DIA sites for User-defined SAAS Application	To check User-defined SAAS Application via DIA sites	Passed	

ENJ.SaaSA .20.8.1_17.8.1_N.08	Create a User-Defined SaaS Application List Using Cisco vManage app Gmail traffic	To check User-defined SAAS Application for audio/video traffic	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.09	Configure Cloud OnRamp for SaaS on DIA sites for User-defined SAAS Application using SIG tunnels using vManage	To check User-defined SAAS Application using SIG Tunnels	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.10	Configure Cloud OnRamp for SaaS on DIA sites for User-defined SAAS Application using sig tunnels using cli	To check User-defined SAAS Application using SIG Tunnels via CLI	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.11	Create a User-Defined SaaS Application List Using Cisco vManage using O365 application standard application	To check User-defined SAAS Application using Standard Application	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.12	Create a User-Defined SaaS Application List Using DIA & MPLS using load balancing for vpn0 interface	To check User-defined SAAS Application for DIA & MPLS using load balancing for vpn0 interface	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.13	Create a User-Defined SaaS Application List Using service VPN	To check User-defined SAAS Application using service VPN	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.14	Using NBAR, Switchover from network from biz-internet to MPLS to modify loss & latency	To check the loss & latency using nbar	Passed	
ENJ.SaaSA .20.8.1_17.8.1_N.15	Using Custom Application, Switchover from network from biz-internet to MPLS to modify loss & latency	To check the loss & latency using wan emulator MPLS using custom application	Passed	

Software upgrade workflow for Cisco SD-WAN edge devices

Logical ID	Title	Description	Status	Defect ID
ENJ.SUW .20.8.1_17.8.1_N.01	Copy the IOS XE image to the bootflash using cli	Copy the image to Bootflash	Passed	
ENJ.SUW .20.8.1_17.8.1_N.02	Copy the iosxe image to the bootflash using vManage	Copy the image to Bootflash via vManage	Passed	
ENJ.SUW .20.8.1_17.8.1_N.03	Delete the ios xe image in the bootflash using cli	Delete the image to Bootflash via cli	Passed	
ENJ.SUW .20.8.1_17.8.1_N.04	Delete the ios xe image in the bootflash using vManage	Delete the image to software rep via vManage	Passed	
ENJ.SUW .20.8.1_17.8.1_N.05	Upgrade software using workflow Single attempt	Upgrade image using single attempt	Passed	
ENJ.SUW .20.8.1_17.8.1_N.06	Upgrade software using workflow download and install method	Upgrade image using download and install method	Passed	
ENJ.SUW .20.8.1_17.8.1_N.07	Upgrade software using workflow download	Upgrade image using download	Passed	
ENJ.SUW .20.8.1_17.8.1_N.08	Upgrade software using workflow install	Upgrade image using install	Passed	
ENJ.SUW .20.8.1_17.8.1_N.09	Upgrade software using workflow install and activate/reboot	Upgrade image using install and activate/reboot	Passed	
ENJ.SUW .20.8.1_17.8.1_N.10	Upgrade software using workflow activate/reboot	Upgrade image using activate/reboot	Passed	
ENJ.SUW .20.8.1_17.8.1_N.11	Upgrade software using workflow remote-server	Upgrade image using remote-server	Passed	
ENJ.SUW .20.8.1_17.8.1_N.12	Upgrade software using workflow vManage	Upgrade image using vManage	Passed	

ENJ.SUW .20.8.1_17.8.1_N.13	Upgrade software using workflow remote-server and vManage	Upgrade image using remote-server and vManage	Passed	

Regression Features

HSRP Authentication on Cisco IOS XE SD-WAN Devices

Logical ID	Title	Status	Defect ID
ENJ.HSRP. 20.8.1_17.8.1_N.01	Enable & activate HSRP & Change the version of HSRP to HSRPv2	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.02	Configure HSRP priority and check higher priority is preferred	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.03	Configure HSRP priority. In case of same priority, higher IP device isn't elected when the interface is brought up after shutting down	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.04	Configure & validate HSRP preemption on standby	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.05	Configure HSRP Authentication using MD5 and verify it's supported	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.06	Configure HSRP hello & hold timers. Check when hello sent matches timer	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.07	Configure HSRP using Vmanage CLI template	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.08	Configure the HSRP with Active/Standby	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.09	Configure HSRP with multiple standby - Requirement 3 routers	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.10	Configure HSRP Authentication using text and verify it's supported	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.11	Static NAT with HSRP configuration	Passed	
ENJ.HSRP. 20.8.1_17.8.1_N.12	Configure HSRP object tracking and verify it's supported	Passed	

ENJ.HSRP. 20.8.1_17.8.1_N.13	Configure HSRP interface tracking and verify it's supported	Passed	

SNMPv3 AES 256 support

Logical ID	Title	Status	Defect ID
ENJ.SNMPv3 .20.8.1_17.8.1_N.01	Configure SNMPv3 on Cisco cEdge Devices Using Cisco vManage	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.02	Configure the sha256 authentication Support for SMNPv3 on Cisco IOSXE Cat8k platforms using Cisco vManage	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.03	Configure SNMPv3 with Encrypted Strings Using CLI Templates	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.04	Upgrade existing user encryption details from "aes-cfb-128" to "aes-256-cfb-128" encryption level with AUTH level SHA256	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.05	Configure SNMP on Cisco IOS XE SD-WAN Devices Using CLI	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.06	Configure and enable SNMPv3 notifications on Cisco IOS XE SD-WAN Devices Using CLI	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.07	Configure SNMPv2 backward compatibility on Cisco Cede Devices Using the CLI	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.08	Configure SNMPv3 Traps on Cisco cEdge Devices	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.09	Create user with aes-256-cfb-128 privacy level encryption and auth level SHA256 on Cisco SDWAN device	Passed	
ENJ.SNMPv3 .20.8.1_17.8.1_N.10	Validate the AES256 bit support along with AES 128bit support in SNMPv3 in vManage	Passed	

RIPv2 support on Cisco IOS XE SD-WAN Devices

Logical ID	Title	Status	Defect ID
ENJ.RIPv2 .20.8.1_17.8.1_N.01	Configure the RIPV2 neighborship between WAN edge routers	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.02	Configure timers in RIPV2 in both routers	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.03	Configure the RIPV2 by using authentication in routing protocol	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.04	To enable Routing Information Protocol (RIP) under a Virtual Routing and Forwarding (VRF)	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.05	To disable the sending of routing updates on interface	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.06	Configure RIPv2 routes summarization between two sd-wan routers	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.07	Configure the BFD for RIPV2 neighbour	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.08	Configure interpacket delay for outbound RIP updates, in milliseconds	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.09	Configure and verify the redistribute OSPF routes into RIP	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.10	To advertise and redistribute RIPv2 routes to OMP	Passed	
ENJ.RIPv2 .20.8.1_17.8.1_N.11	Configure and verify the redistribute BGP routes into RIP	Passed	

TCP-UDP port tracker for static route

Logical ID	Title	Status	Defect ID
ENJ.TCP/UDP. 20.8.1_17.8.1_N.01	Configure the Single Static Route to Track the Endpoint	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.02	Configure the TCP port Tracker for Static Route endpoint	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.03	Configure TCP/UDP port tracker with tracker group for static route	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.04	Configure the tracking group with TCP/UDP port tracking by using Boolean operation (AND)	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.05	Configure the combination of TCP port tracker and static route by using tracking group with default Boolean operation.	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.06	Configure the modification of multiple/threshold /interval parameters Instead of default values	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.07	Configure the combination of TCP port tracker with combination of DNS by using tracking group	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.08	TCP/UDP port tracker for static route with tracking group by using VManage	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.09	Configure the TCP/UDP tracker with tracking group by using Vmanage--AND operation	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.10	Configure the TCP port tracker with IP Address by using VManage	Passed	

ENJ.TCP/UDP. 20.8.1_17.8.1_N.11	Configure the single TCP Port tracker with combination of IPaddress by using tracking group --AND operation	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.12	configure the combination of TCP port and DNS address by using tracker group	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.13	Configure the single UDP port tracker and static route with tracking group by using Boolean operation	Passed	
ENJ.TCP/UDP. 20.8.1_17.8.1_N.14	Configure the UDP port Tracker for Static Route endpoint	Passed	

INTRA VPN Service Side NAT

Logical ID	Title	Status	Defect ID
ENJ.SSN .20.8.1_17.8.1_N.01	To configure the static Ip Nat inside mapping Nat pool with vpn 900 in same site(sub-interface)	Passed	
ENJ.SSN .20.8.1_17.8.1_N.02	To configure the dynamic Ip Nat inside mapping Nat pool with vpn 900 in same site (sub interface)	Passed	
ENJ.SSN .20.8.1_17.8.1_N.03	To configure the Inside Dynamic & Dynamic Overload Service Side NAT in same site(sub-interface)	Passed	
ENJ.SSN .20.8.1_17.8.1_N.04	To configure an inside dynamic with outside static in the same site(sub-interface)	Passed	
ENJ.SSN .20.8.1_17.8.1_N.05	To configure the static Ip Nat outside mapping with Nat pool with VPN 900	Passed	
ENJ.SSN .20.8.1_17.8.1_N.06	To Verify the Outside Dynamic with Inside static in the same site VPN 900	Passed	
ENJ.SSN .20.8.1_17.8.1_N.07	To configure static Ip Nat outside mapping with Nat pool and port forwarding	Passed	
ENJ.SSN .20.8.1_17.8.1_N.08	To configure the outside Dynamic & Dynamic Overload intra vpn Service Side NAT	Passed	
ENJ.SSN .20.8.1_17.8.1_N.09	To configure the Ip Nat outside by using sub interface in same site	Passed	
ENJ.SSN .20.8.1_17.8.1_N.10	To configure the dynamic Ip Nat outside mapping Nat pool with same site	Passed	
ENJ.SSN .20.8.1_17.8.1_N.11	To Verify the outside Static & port forwarding Service Side NAT	Passed	

ENJ.SSN .20.8.1_17.8.1_N.12	To configure the static Nat of service side source Ip address vpn 900	Passed	
ENJ.SSN .20.8.1_17.8.1_N.13	To configure the static Ip Nat with port forwarding in same site with interface	Passed	
ENJ.SSN .20.8.1_17.8.1_N.14	To configure the intra VPN inside service side NAT with interface	Passed	
ENJ.SSN .20.8.1_17.8.1_N.15	To configure static ip nat outside mapping with natpool and port forwarding	Passed	

Related Documents

Related Documentation

Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.8 Release Notes

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/xe-17-8/sd-wan-rel-notes-xe-17-8.html

Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.8

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

Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE Release 17.8

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

Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.8

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 17.8

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/packet-trace.html

Cisco SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.8

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

Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release 17.8

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-secure-internet-gateway.html