Cisco SD-WAN WAAS Deployment and Migration Guide

Deploying Cisco WAAS with Cisco SD-WAN

May 2020

Version 1

TABLE OF CONTENTS

1 Introduction

This document includes the following:

- The procedure to deploy Cisco WAAS with Cisco SD-WAN using AppNav-XE
- The procedure to migrate legacy WAAS deployments to Cisco SD-WAN

For detailed configuration steps, please refer AppNav-XE for SD-WAN Configuration Guide.

Cisco SD-WAN WAAS brings WAAS capabilities to Cisco IOS XE SD-WAN by enabling AppNav-XE feature on Cisco IOS XE SD-WAN devices, for traffic interception and redirection to WAAS nodes for optimization.

Note: AppNav-XE is relevant only to Cisco IOS XE SD-WAN devices and is not supported on Cisco vEdge devices. Therefore, the term Cisco SD-WAN device in this document refers to Cisco IOS XE SD-WAN device.

Following are some of the key functionalities of AppNav-XE on Cisco SD-WAN devices.

- A Cisco SD-WAN device enabled with AppNav-XE feature plays the role of an AppNav-XE controller. The AppNav-XE controllers form a cluster with WAAS nodes (referred to as AppNav-XE cluster) as depicted in the figure 1. Note that a cluster is local to a site and each site can have one or more clusters centrally managed by WAAS Central Manager (WCM).

- AppNav-XE cluster supports load balancing flows across WAAS nodes, handles asymmetric flows and the AppNav-XE controller failover.

- Cisco SD-WAN devices are configured with AppNav-XE redirection policy and WAAS nodes are configured with optimization policy from WCM

- The AppNav-XE feature on Cisco SD-WAN devices performs the following functions.

    - Tracks liveness and load of each WAAS node in the cluster

    - Peers with and synchronizes flows with other Cisco SD-WAN devices enabled with AppNav-XE in the cluster, for asymmetric flow and AppNav-XE controller failover handling

    - Intercepts inbound and outbound cleartext SD-WAN traffic (post-decryption and pre-encryption) as well as Direct Internet Access (DIA) traffic and redirects the traffic matching AppNav-XE redirection policy to WAAS nodes for optimization over the automatically created AppNav GRE tunnels.

Note: Cisco SD-WAN devices do not require route leaking or any other policies for traffic redirection to WAAS nodes for optimization and return traffic from the WAAS nodes.

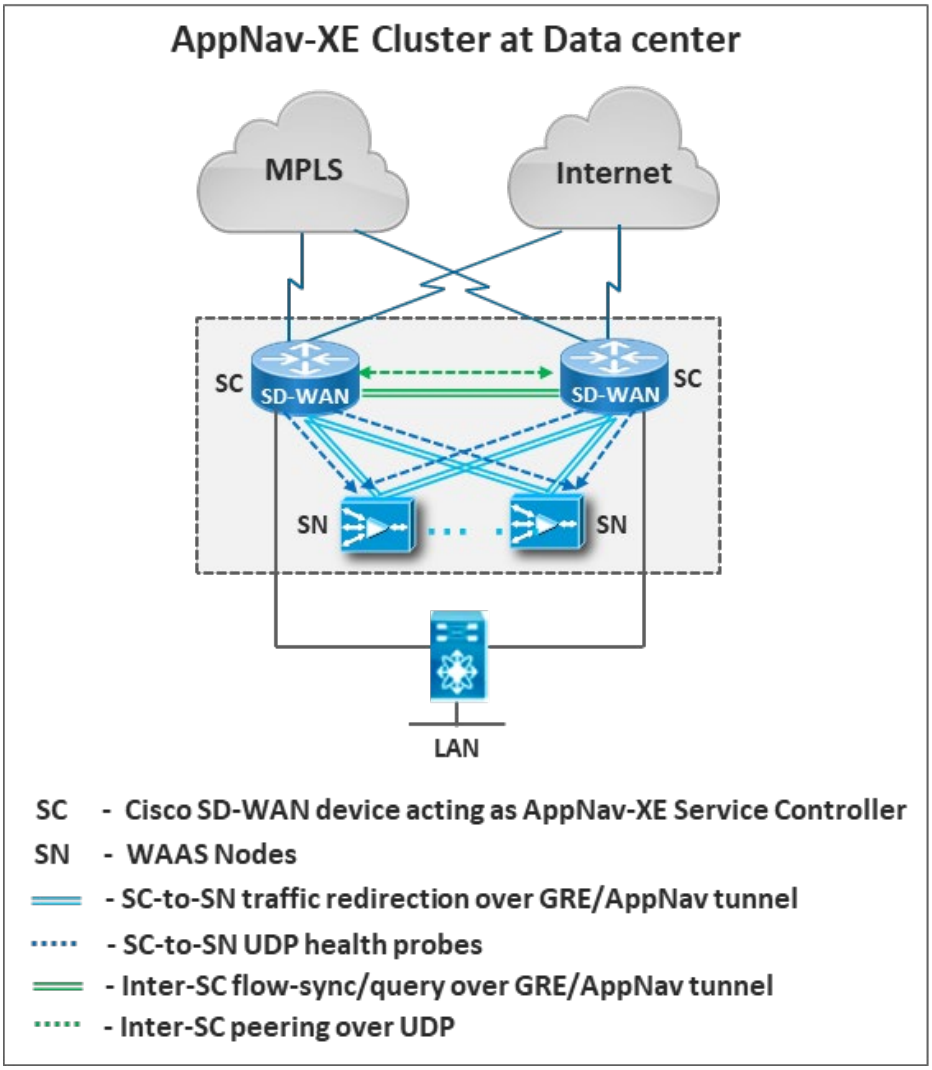

Figure 1

Supported Releases

- Cisco IOS XE SD-WAN device - Cisco IOS XE Release 17.2.1r
- Cisco vManage - Version 20.1.1
- WAAS Central Manager (WCM) - Version 6.4.5
- WAAS nodes - Version- 6.4.5

Restrictions

- Only the AppNav-XE redirection method is supported on Cisco SD-WAN devices. Other redirection methods such as WCCP, PBR and the inline mode are not supported
- For WAAS nodes, only the WAE/WAVE, vWaaS and vWaaS on UCSE are supported. ISR-WAAS is not supported

Prerequisites

- Before migrating to SD-WAN WAAS, legacy WAAS deployments must first be migrated to AppNav-XE and to the supported WAAS nodes - WAE/WAVE, vWAAS and vWAAS on UCS-E
- WCM must be registered as third party controller with Cisco vManage. For cloud-hosted Cisco vManage, to allow HTTPS connection from WCM, WCM public IP address must be whitelisted as per the cloud-provider security requirements.

Performance Considerations

In order to achieve the required performance after legacy WAAS to SD-WAN WAAS migration, appropriate Cisco IOS XE SD-WAN device platforms must be selected, taking the below considerations into account

- Performance difference between the currently deployed redirection methods or inline-mode and AppNav-XE
- AppNav-XE performance difference between Cisco IOS XE and Cisco IOS XE SD-WAN devices

2 Deployment Considerations

2.1 WAAS Management Traffic in Cisco SD-WAN

Like legacy WAAS, SD-WAN WAAS uses WCM for centralized management of WAAS nodes and AppNav-XE on Cisco SD-WAN devices across all the sites. WCM is commonly deployed on-prem at the data center, as cloud hosting of WCM is not supported.

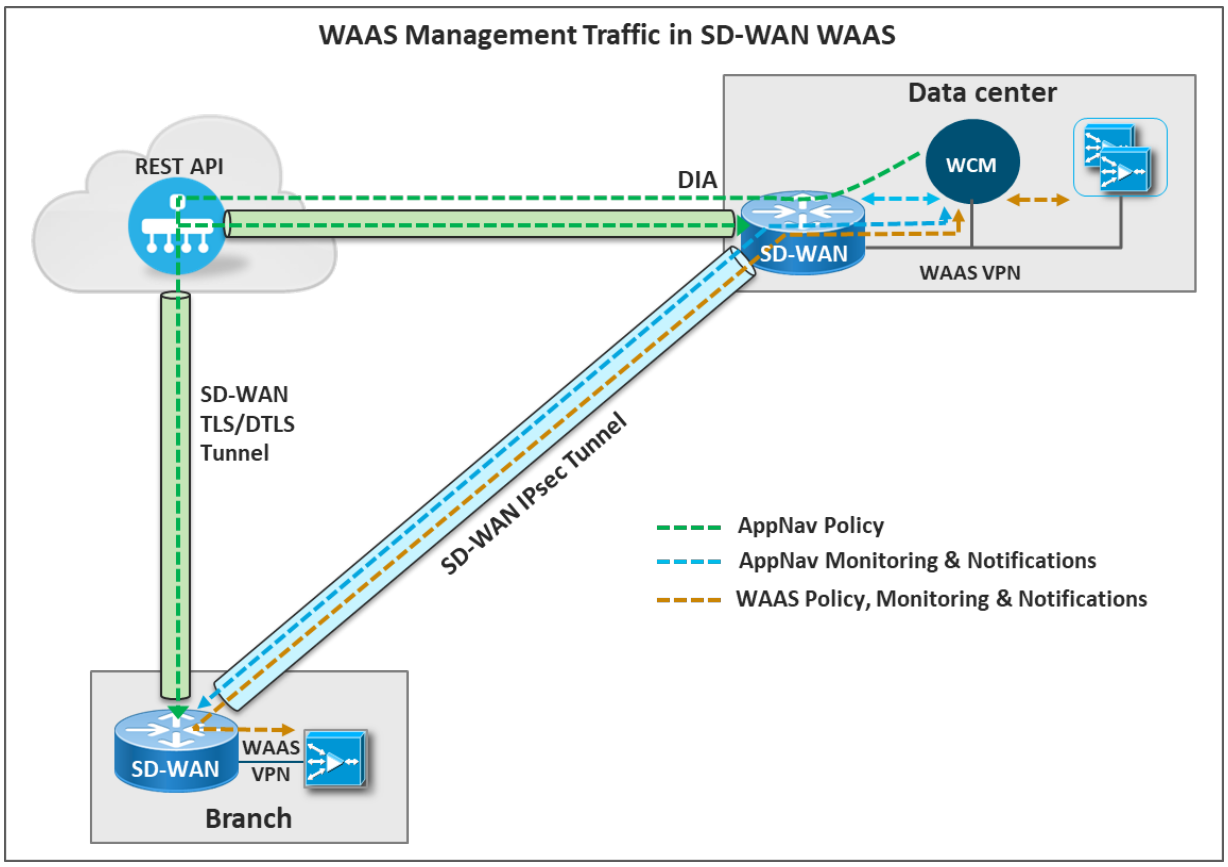

Figure 2

The figure 2 depicts the various communication requirements between WCM and Cisco vManage, Cisco SD-WAN devices and WAAS nodes, as explained below.

- **AppNav-XE Redirection Policy through Cisco vManage**

  WCM configures AppNav-XE redirection policy on Cisco SD-WAN devices through Cisco vManage using the northbound REST-API interface, as Cisco SD-WAN devices can only be configured by Cisco vManage. Therefore, WCM must be able to reach and initiate connection to Cisco vManage (on-prem or cloud-hosted). WCM deployed at the data center in a service VPN must use a DIA policy to communicate with Cisco vManage. WCM must register with Cisco vManage as a third-party controller and the Cisco SD-WAN devices that need to be managed by WCM must be attached to WCM from Cisco vManage UI.

- **AppNav-XE Monitoring and Notifications**

  For AppNav-XE specific monitoring and notifications, WCM is configured with IP addresses of Cisco SD-WAN devices at the data center and branches. WCM initiates HTTPS connection to and pulls monitoring data from Cisco SD-WAN devices. Also, the Cisco SD-WAN devices push event notifications to WCM. Therefore, WCM at data

center must be able to reach Cisco SD-WAN devices at the branch sites that can be behind NAT.

- **WAAS Optimization Policy, Monitoring and Notifications**

  For WAAS configuration, monitoring and notifications, the WAAS nodes at the data center and branches are configured with the IP address of and register with WCM. WCM pushes the configuration to WAAS nodes and then pulls the monitoring data from the same WAAS nodes. WAAS nodes also push event notifications to WCM. Therefore, WAAS nodes at the data center and branches must be able to reach WCM at the data center.

2.2 WCM and WAAS nodes in Service VPN

From the WCM communication requirements described in the earlier section, WCM must be able to initiate communication to the branch WAAS nodes and Cisco SD-WAN devices that can be behind NAT.

For NAT and firewall traversal, WCM and WAAS nodes must be deployed on the SD-WAN service side that is, must be reachable through the SD-WAN overlay. Note that WCM and WAAS must be in an end-end service VPN that is, must be deployed in same service VPN at all the WAAS-enabled sites.

While WAAS and WCM can be deployed in any service VPN, the recommendation is to use a dedicated service VPN (referred to as WAAS VPN in this document) for WCM and WAAS nodes. The WAAS VPN would be used for the following.

- WAAS management traffic between WCM at the data center, and the WAAS nodes and Cisco SD-WAN devices at the data center and branches
- Optimization traffic between Cisco SD-WAN devices and the WAAS nodes at WAAS-enabled sites

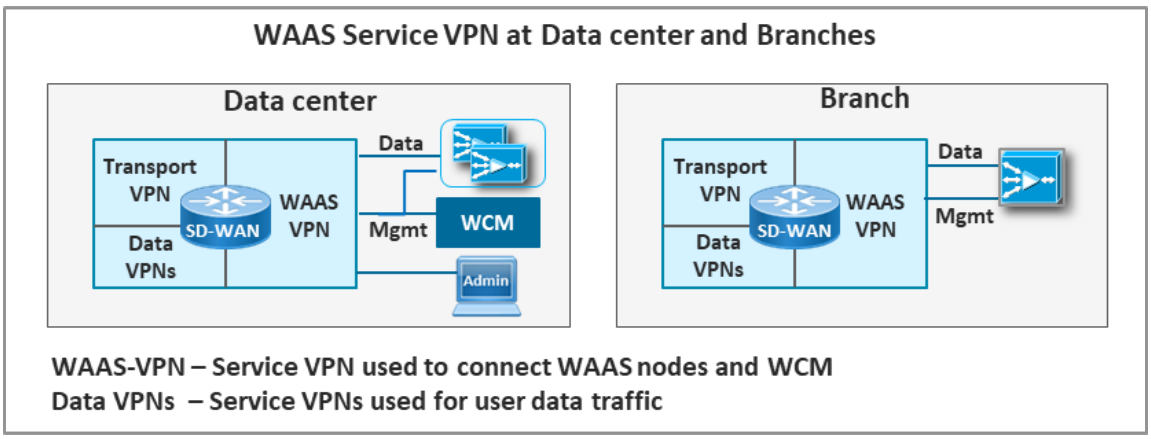

Figure 3

2.3 Accessing WCM GUI and WAAS node CLI

Administrators at the data center and branch sites connected to WAAS service VPN can access WCM GUI and WAAS node CLI for monitoring and troubleshooting. However, if the administrators are connected to a non-WAAS service VPN, route leaking to/from WAAS VPN would be required to provide access to WCM GUI and WAAS node CLI.

2.4 WCM to Cisco vManage Communication

WCM is deployed at the data center and is connected to Cisco SD-WAN device in a service VPN. A DIA policy must be configured on the Cisco SD-WAN device to enable WCM communication with Cisco vManage.

WCM must register with Cisco vManage as third party controller. After successful registration, Cisco SD-WAN devices to be managed by WCM must be attached to WCM, from Cisco vManage GUI.

To allow HTTPS connection from WCM to Cisco vManage, perform the following steps.

- On WCM, specify the Cisco vManage FQDN or IP address and login credentials
- Upload the Cisco vManage web server's trusted issuer certificate bundle into WCM

Please refer AppNav-XE for SD-WAN Configuration Guide for detailed configuration steps.

2.5 WCM to Cisco SD-WAN Device Communication

For AppNav-XE specific monitoring and notifications, WCM initiates HTTPS connection to and pulls monitoring data from Cisco SD-WAN devices.

To allow HTTPS connections from WCM to Cisco SD-WAN device, perform the following steps.

- Enable HTTPS server on the Cisco SD-WAN device using Cisco vManage
- On WCM, specify the Cisco SD-WAN device IP address (WAAS service VPN IP address) and login credentials

Please refer AppNav-XE for SD-WAN Configuration Guide for detailed configuration steps.

2.6 SD-WAN WAAS Greenfield Deployment

For greenfield Cisco SD-WAN WAAS deployments, the recommended deployment sequence is same as the Cisco SD-WAN along with a few additional steps and considerations described below.

2.6.1 Set up Cisco SD-WAN Controllers

a) Upgrade Cisco vManage to version 20.1.1

2.6.2 Set up Cisco SD-WAN WAAS at Data center

1) **Bring up Cisco SD-WAN Devices at Data center**
   a) Upgrade Cisco SD-WAN devices to IOS XE version 17.2.1r

2) **Bring up WCM at Data center**
   a) Upgrade WCM to version 6.4.5
   b) Connect WCM to Cisco SD-WAN devices in a service VPN (WAAS VPN)
   c) Advertise WCM IP address into SD-WAN fabric through OMP
   d) Establish reachability between WCM and Cisco vManage
   e) Register WCM as third-party controller with Cisco vManage
   f) Attach Cisco SD-WAN devices to be managed by WCM from Cisco vManage GUI

3) **Bring up WAAS nodes at Data center**
   a) Connect WAAS nodes to Cisco SD-WAN devices in a service VPN (WAAS VPN)
   b) Advertise WAAS node IP addresses into SD-WAN fabric through OMP
   c) Establish communication between WCM and WAAS nodes
   d) Upgrade WAAS nodes to version 6.4.5

4) **Enable AppNav-XE on the Data center Cisco SD-WAN Devices**
   a) Establish communication between WCM and the data center Cisco SD-WAN devices
      - Specify Cisco SD-WAN device WAAS VPN IP address on WCM
      - Specify Cisco SD-WAN device credentials on WCM
   b) Provision AppNav-XE policy on Cisco SD-WAN devices from WCM GUI
      - Ensure that the AppNav-XE feature is enabled on the SD-WAN tunnel interfaces for enterprise traffic and the WAN interfaces for DIA traffic

2.6.3 Set up Cisco SD-WAN WAAS at Branches

1) **Bring up Cisco SD-WAN Devices at Branches**
   a) Upgrade Cisco SD-WAN devices to IOS XE version 17.2.1r

b) Advertise Cisco SD-WAN device WAAS VPN IP address into SD-WAN fabric through OMP

2) **Bring up WAAS nodes at Branches**
   a) Connect WAAS nodes to Cisco SD-WAN device in a service VPN (WAAS VPN)
   b) Advertise WAAS node IP addresses into SD-WAN fabric through OMP
   c) Establish communication between WAAS nodes and WCM through Cisco SD-WAN overlay
   d) Upgrade WAAS nodes to version 6.4.5

3) **Enable AppNav-XE on branch Cisco SD-WAN devices**
   a) Establish communication between Cisco SD-WAN devices and WCM
      - Specify Cisco SD-WAN device WAAS VPN IP address on WCM
      - Specify Cisco SD-WAN device credentials on WCM
   b) Provision AppNav-XE policy on Cisco SD-WAN devices from WCM GUI
      - Ensure that the AppNav-XE feature is enabled on SD-WAN tunnel interfaces for enterprise traffic and the WAN interfaces for DIA traffic

2.6.4 Validation

a) Validate traffic with WAAS optimization between the data center and branches
b) Validate traffic with WAAS optimization between branches
c) Validate monitoring of the data center and branch Cisco SD-WAN devices and WAAS nodes from WCM
d) Validate notifications from the data center and branch Cisco SD-WAN devices and WAAS nodes on WCM

3 Migration Considerations

Migration from legacy WAAS to SD-WAN WAAS involves the same steps and recommendations as described in the Cisco SD-WAN Migration Guide along with a few additional considerations that are described in this section.

The recommended Cisco SD-WAN migration sequence is

1) Set up Cisco SD-WAN controllers
2) Migrate data center sites
3) Migrate branch sites that host services
4) Migrate other branches in a phased manner

The figure 4 depicts the example topology used to describe Cisco SD-WAN WAAS migration steps in this document.

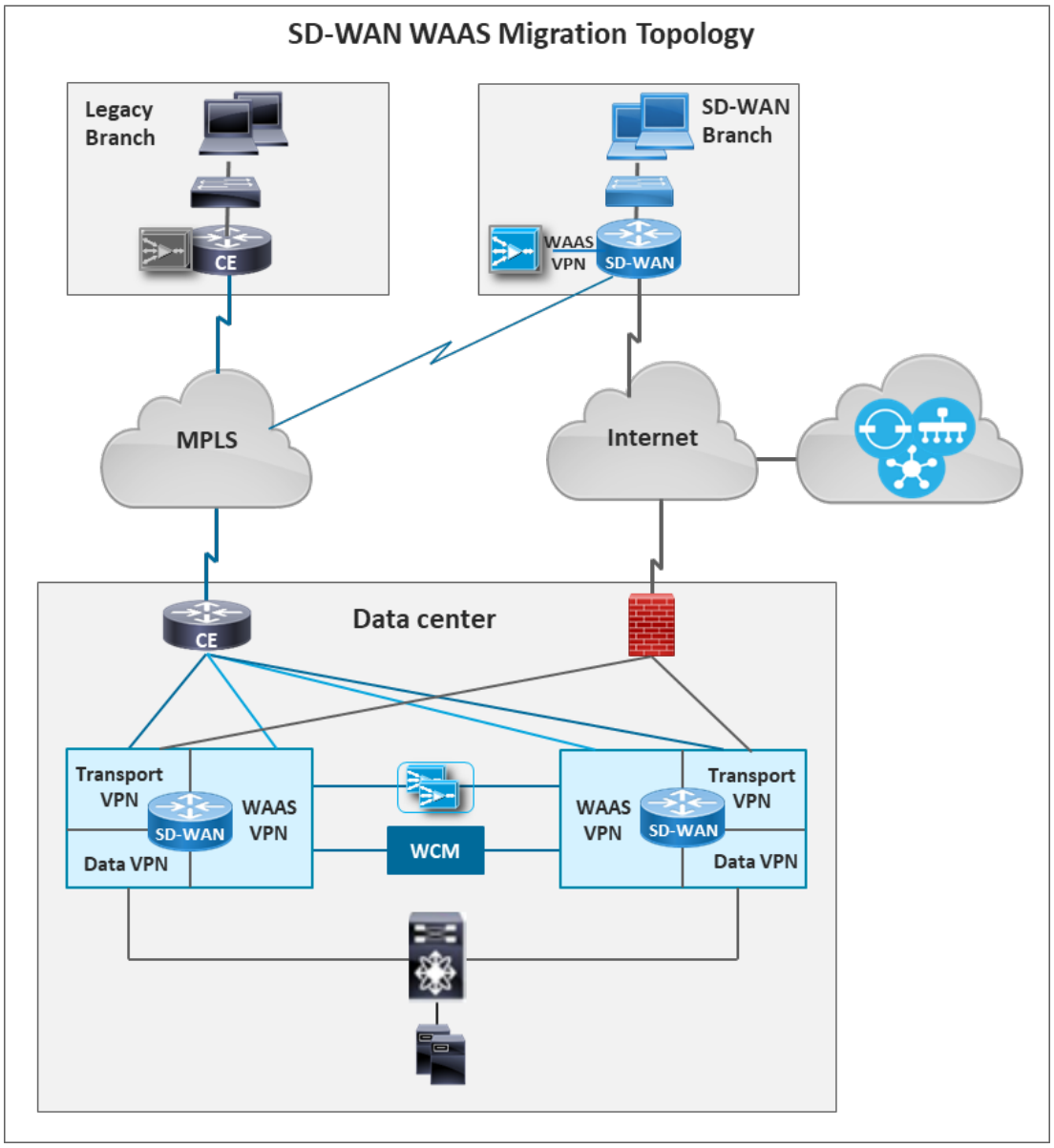

Figure 4

3.1 Need for Two-box Solution for Cisco SD-WAN Migration

During Cisco SD-WAN migration, for sites such as data centers, that need to handle both SD-WAN and non-SD-WAN (legacy WAN) traffic, Cisco SD-WAN devices must be placed behind the existing WAN-edge/CE routers. The two-box solution is required for the following reasons.

- Only limited traffic types and protocols are allowed inbound on the TLOC interfaces in transport VPN, for security reasons. Though this restriction can be overridden, and

additional or all traffic types allowed, it is not recommended. Therefore, legacy WAN link such as MPLS configured as TLOC interface would not allow non-SD-WAN traffic.

- Traffic/route leaking between transport and service VPNs is currently not supported. Therefore, even if non-SD-WAN traffic lands in transport VPN through a non-TLOC interface (for example, TLOC on loopback interface), the traffic cannot be forwarded to a service VPN, which is required for management traffic from branches to WCM.

Therefore, legacy WAN link, such as MPLS, is terminated on a separate CE router. Two links are then extended from the CE router - one link to the Cisco SD-WAN device as a TLOC interface for SD-WAN traffic; and another link directly to the LAN-side router or switch for non-SD-WAN traffic. The second link bypasses the Cisco SD-WAN device as shown in the figure 5.

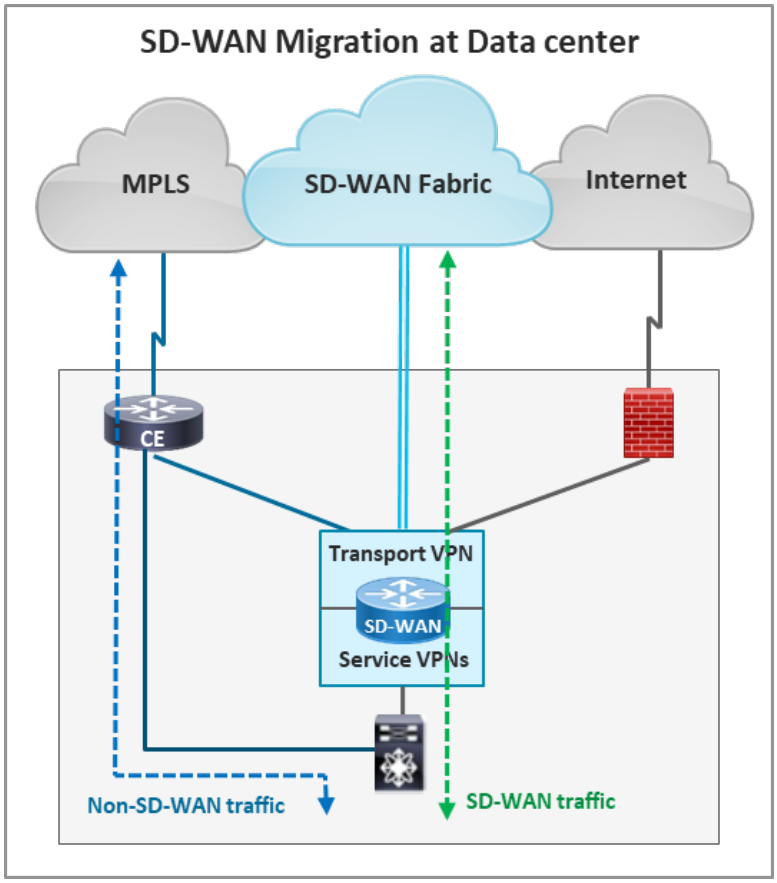

Figure 5

Note: After all the sites are successfully migrated to Cisco SD-WAN, the two-box solution is no longer needed. A single-box solution can be used with legacy WAN link directly terminating on the Cisco SD-WAN device, thus eliminating the need for an additional CE router.

3.2 Non-SD-WAN Traffic through Cisco SD-WAN Device

Cisco SD-WAN WAAS migration has an additional requirement that even the non-SD-WAN traffic from legacy branches must traverse Cisco SD-WAN devices at the data center for the following reasons

- As WAAS nodes are connected to the Cisco SD-WAN devices (in a service VPN), non-SD-WAN traffic to/from legacy branches must traverse Cisco SD-WAN device in order to be redirected for WAN optimization

- As WCM is connected to the Cisco SD-WAN devices (in a service VPN), WAAS management traffic from legacy branches must traverse Cisco SD-WAN devices to reach WCM

One approach to accomplish this is to extend a link from the CE-router to the Cisco SD-WAN device WAAS service VPN for non-SD-WAN traffic as depicted in the figure 6. AppNav-XE would be enabled on the WAAS service VPN interface connecting to the CE router, that would intercept inbound and outbound non-SD-WAN traffic and redirect it to the WAAS nodes for optimization.

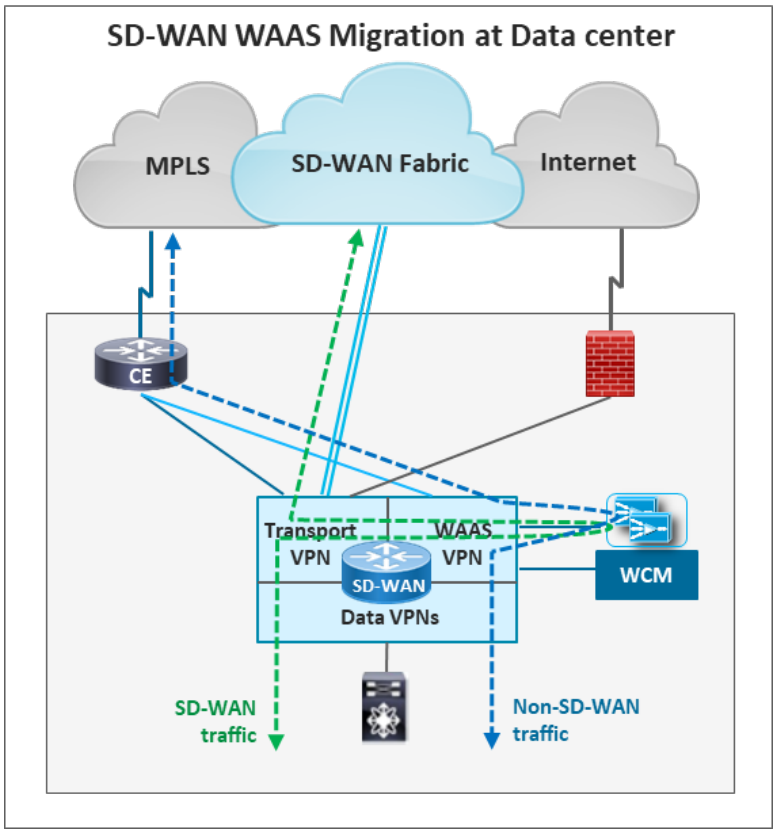

Figure 6

3.3 Routing of SD-WAN and Non-SD-WAN Prefixes

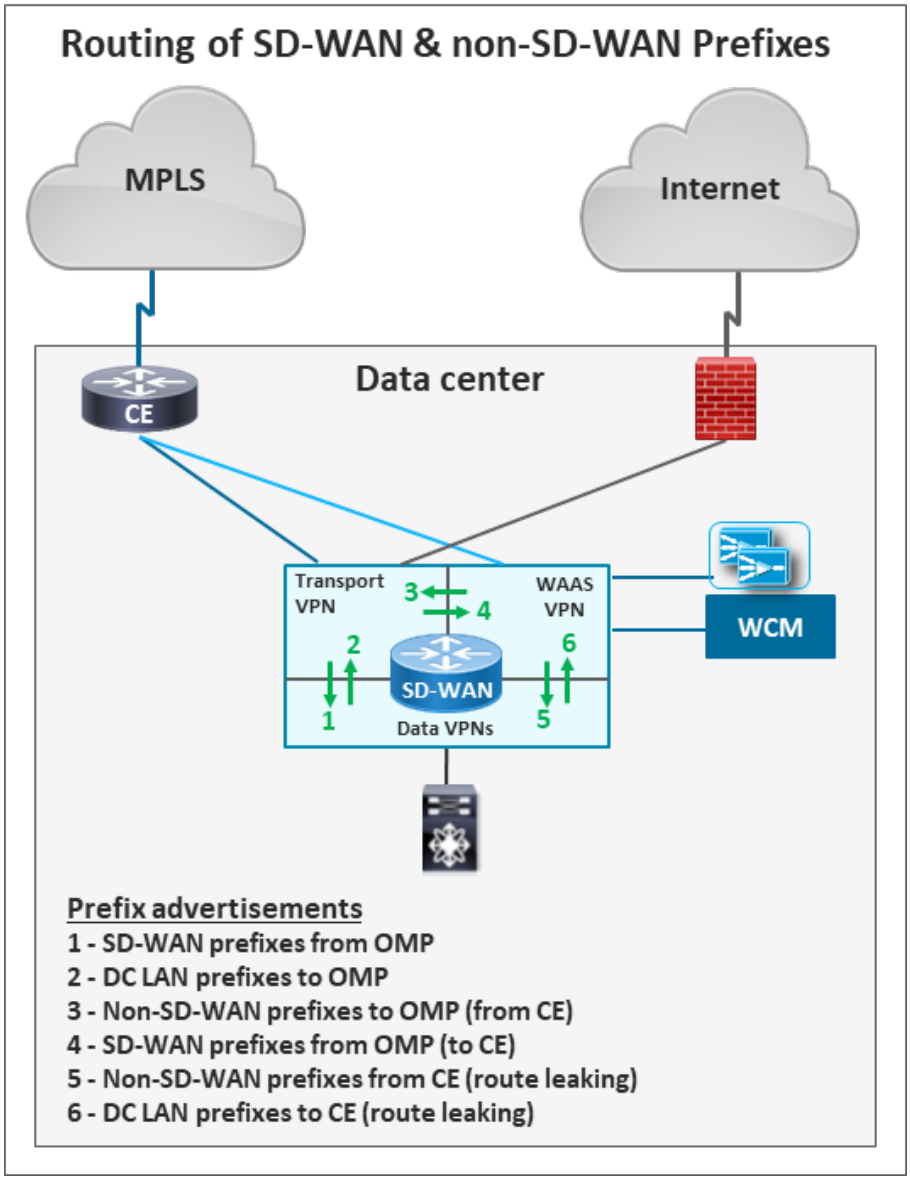

Figure 7

The figure 7 depicts the routing of SD-WAN and non-SD-WAN prefixes at the data center, for SD-WAN WAAS migration.

Route filtering and selective route advertisement and redistribution as described in the table 1 must be used in order to avoid routing loops and unintended traffic paths.

Prefix Exchange	Prefixes Advertised / Re-distributed	Use Case

OMP to Data VPNs **Note:** Data-VPNs here refer to service VPNs that are used for end user data traffic	SD-WAN remote site LAN prefixes from corresponding data VPNs	End-end service VPN traffic between SD-WAN sites
Data VPNs to OMP	Only SD-WAN local site (data center) LAN prefixes from corresponding data VPNs	End-end service VPN traffic between SD-WAN sites
OMP to WAAS VPN **Note:** WAAS-VPN here refers to Service VPN used to connect WAAS nodes and WCM	SD-WAN remote site WAAS VPN prefixes (WAAS nodes)	WAAS management traffic between WCM at data center and WAAS nodes as well as Cisco SD-WAN devices at remote sites
WAAS VPN to OMP	a) SD-WAN local site (data center) WAAS VPN prefixes b) Non-SD-WAN remote site prefixes learnt from the CE router	a) WAAS management traffic between WCM at data center and WAAS nodes as well as Cisco SD-WAN devices at remote sites b) Branch-to-branch traffic between legacy and SD-WAN branches through the data center Cisco SD-WAN devices
Data VPNs to WAAS VPN Inter service VPN route leaking	Only SD-WAN local site (data center) LAN prefixes from corresponding data VPNs	Data traffic from non-SD-WAN remote sites to data center LAN
WAAS VPN to Data VPNs Inter service VPN route leaking	Only non-SD-WAN remote site prefixes learnt from the CE router	Data traffic from data center LAN to non-SD-WAN remote sites

Table 1

3.4 Data center and Branch Migration Steps

This section describes the steps for migration to SD-WAN WAAS at the data center and branches.

3.4.1 Legacy WAAS deployment

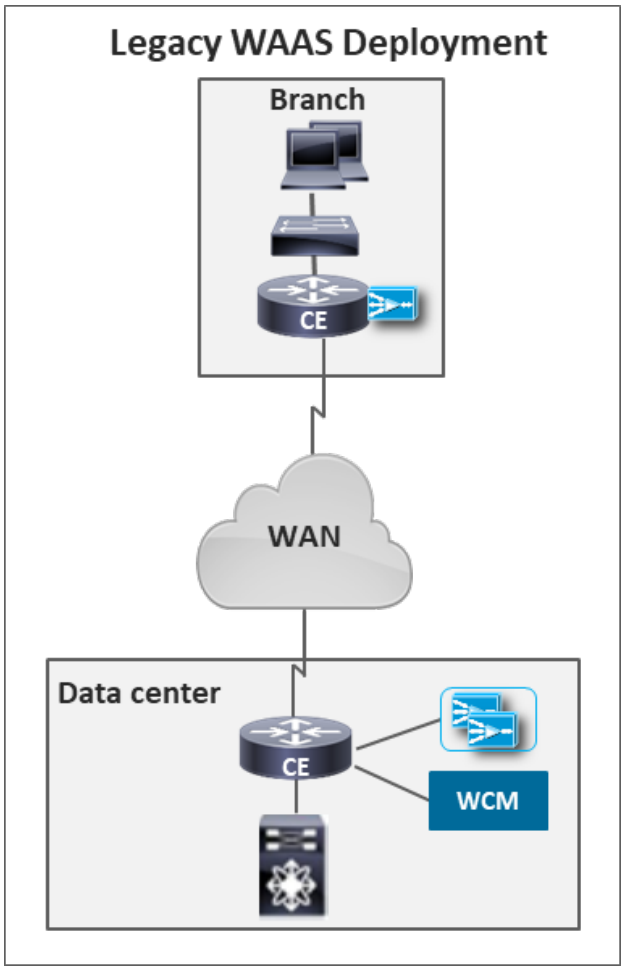

Figure 8

The figure 8 depicts an example legacy WAAS deployment, that consists of the following:

- Data center connected to branch over legacy WAN such as MPLS, DMVPN or IWAN
- AppNav-XE feature enabled on the Cisco IOS-XE WAN-edge/CE routers at data center and branch, for traffic redirection to WAAS nodes
- WCM deployed at data center centrally manages WAAS nodes and the Cisco IOS XE devices at all sites

3.4.2 Setup Cisco SD-WAN Controllers

Please refer SD-WAN documentation for setting up SD-WAN controllers. Ensure that Cisco vManage version is 20.1.1 or above.

3.4.3 Enable SD-WAN WAAS at Data center

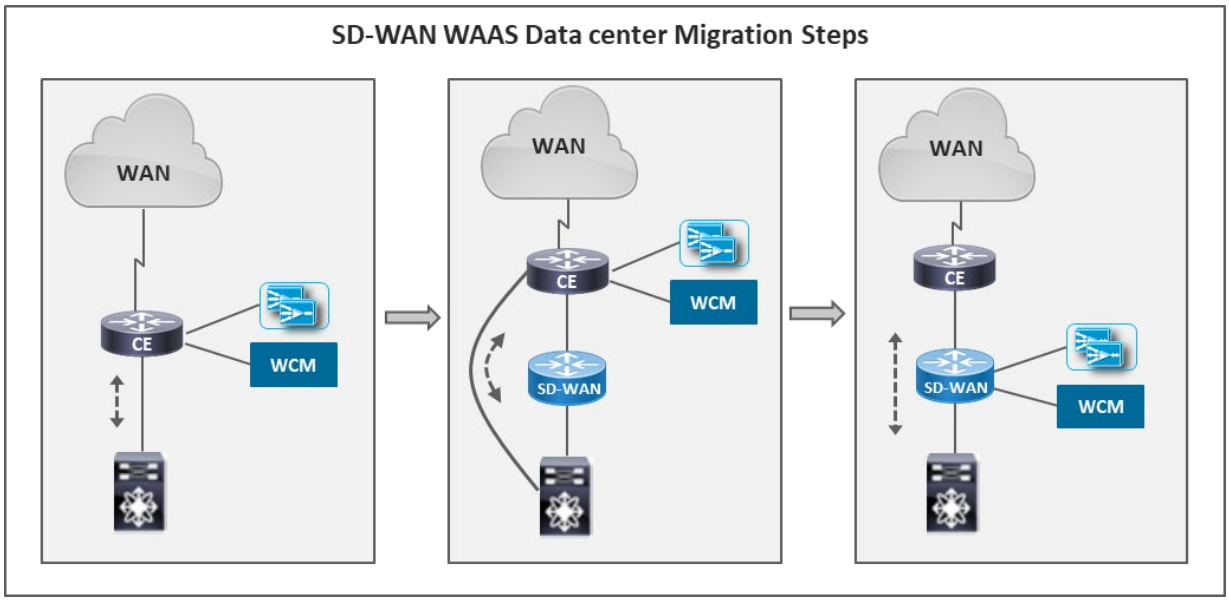

Figure 9

The figure 9 depicts the SD-WAN WAAS migration steps at the data center, as listed below.

1) Initial state - WAAS nodes and WCM connected to the WAN-edge/CE router

2) Insert Cisco SD-WAN device (version 17.2.1r) between the CE router and the LAN-side router/switch without disrupting traffic

3) Disable AppNav-XE feature on the CE router. Disconnect WCM and WAAS nodes from the CE router

   This will disable optimization and reset TCP connections that were getting redirected and optimized. After the reset, traffic to/from data center would continue without optimization.

4) Connect WCM and WAAS nodes to the Cisco SD-WAN device in WAAS service VPN
   a) Upgrade WCM to version 6.4.5
   b) Upgrade WAAS nodes to version 6.4.5

c) Advertise WCM IP address and the Cisco SD-WAN device IP address (WAAS service VPN IP) into SD-WAN fabric through OMP
d) Ensure reachability and communication between the following entities
    - WCM and the data center Cisco SD-WAN devices and WAAS nodes
    - WCM and the branch Cisco IOS-XE WAN-edge devices enabled with AppNav-XE and WAAS nodes
e) Enable AppNav-XE feature on the Cisco SD-WAN devices at the data center, on the following interfaces
    - The interface in WAAS service VPN that is connected to the CE router. This is to enable optimization of non-SD-WAN traffic from/to legacy branches
    - The SD-WAN tunnel and TLOC interfaces to enable optimization of SD-WAN enterprise and DIA traffic

5) Switch traffic between the CE router and LAN-side router/switch through Cisco SD-WAN device that would redirect interesting traffic to WAAS nodes for optimization.

   Note: SD-WAN WAAS migration at the data center causes disruption of WAN optimization due to movement of WCM and WAAS nodes from CE router to the Cisco SD-WAN device.
    - During this process, traffic would continue to flow unoptimized
    - After this process, any existing connections would continue without optimization. Any new connections matching the redirection and optimization policy will get optimized.

   .
   At the end of SD-WAN WAAS migration, the data center is ready to handle WAAS traffic from legacy as well as SD-WAN branches.

6) Validate that WAAS data and management traffic from non-SD-WAN branches to the data center is working fine

3.4.4 Enable SD-WAN WAAS at Branches

1) Branches that need to handle both non-SD-WAN and SD-WAN traffic such as branches hosting services, must use the two-box solution and use the same migration steps as the data center

2) Branches that only need to handle SD-WAN traffic post migration, can use the single-box solution and upgrade existing Cisco IOS XE CE routers to Cisco SD-WAN image (version 17.2.1r). This would cause traffic disruption due to image upgrade and configuration of AppNav-XE policy on the Cisco SD-WAN device

3) Advertise WAAS node IP addresses and the Cisco SD-WAN device IP address (WAAS service VPN IP) into the Cisco SD-WAN fabric through OMP

4) Ensure reachability and communication between WCM at the data center and the branch Cisco SD-WAN devices and WAAS nodes in the WAAS service VPN

5) Upgrade branch WAAS nodes to the recommended version 6.4.5

6) Enable AppNav-XE feature on the branch Cisco SD-WAN devices, on the SD-WAN tunnel and TLOC interfaces to enable optimization of SD-WAN enterprise and DIA traffic

7) Validate the following traffic flows
   a) WAAS data and management traffic between non-SD-WAN branches and the data center
   b) WAAS data and management traffic between SD-WAN branches and the data center
   c) WAAS data traffic between non-SD-WAN and SD-WAN branches

3.5 SD-WAN and Non-SD-WAN Traffic Flows

This section depicts various SD-WAN and non-SD-WAN traffic flows between branches and the data center for SD-WAN WAAS migration.

3.5.1 WCM to Cisco vManage Reachability

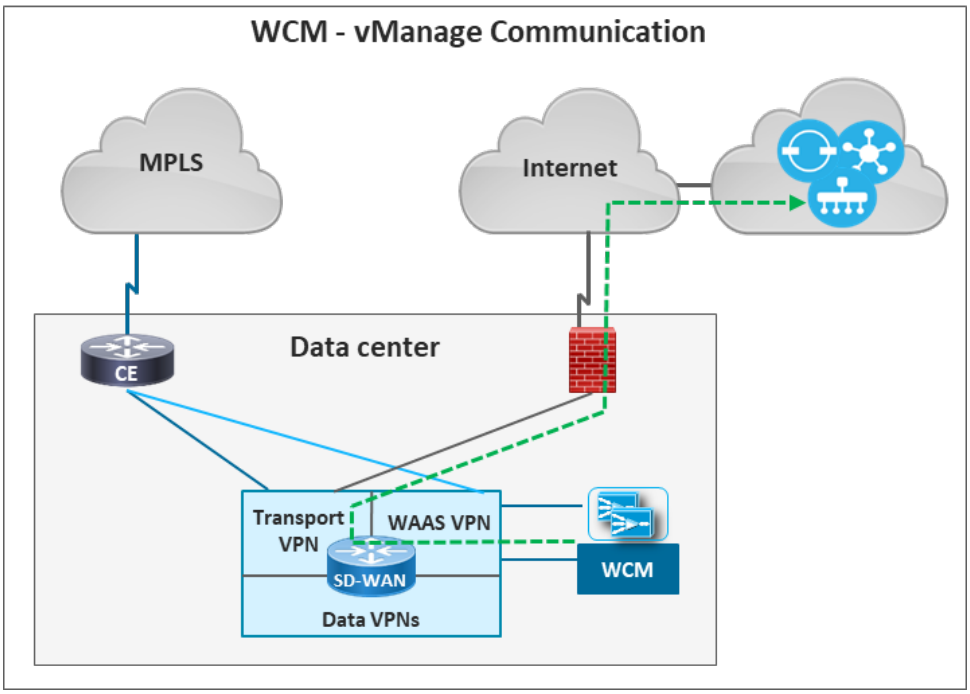

Figure 10

The figure 10 depicts forwarding of traffic between WCM and Cisco vManage.

WCM is deployed at the data center and is connected to the Cisco SD-WAN devices in a service VPN. A DIA policy must be configured on the Cisco SD-WAN devices for WCM to communicate with Cisco vManage deployed in the cloud.

3.5.2 WAAS Traffic from Legacy Branches

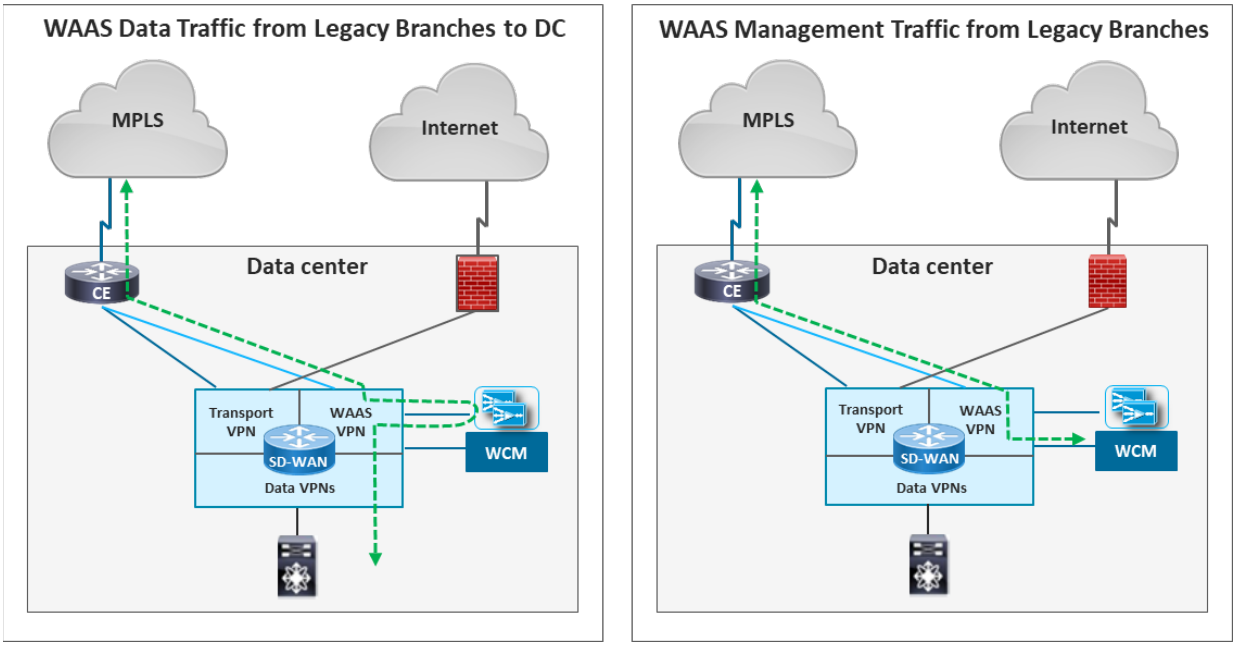

Figure 11

The figure 11 depicts traffic from legacy branches and it's forwarding at the data center.

At the data center, the incoming WAAS data and management traffic from legacy branches would be forwarded by the CE router to the Cisco SD-WAN device interface in WAAS service VPN, that has AppNav-XE feature enabled on it.

- The AppNav-XE feature would redirect interesting traffic to the WAAS nodes for optimization over an auto-created GRE tunnel. When the traffic returns from WAAS node, it is forwarded from WAAS service VPN to the data service VPNs using route leaking.

  The return data traffic from the data center LAN to legacy branches would take the same path.

- The WAAS management traffic that is destined to WCM, would be forwarded to WCM that is connected in the WAAS service VPN.

3.5.3 WAAS Traffic from SD-WAN Branches

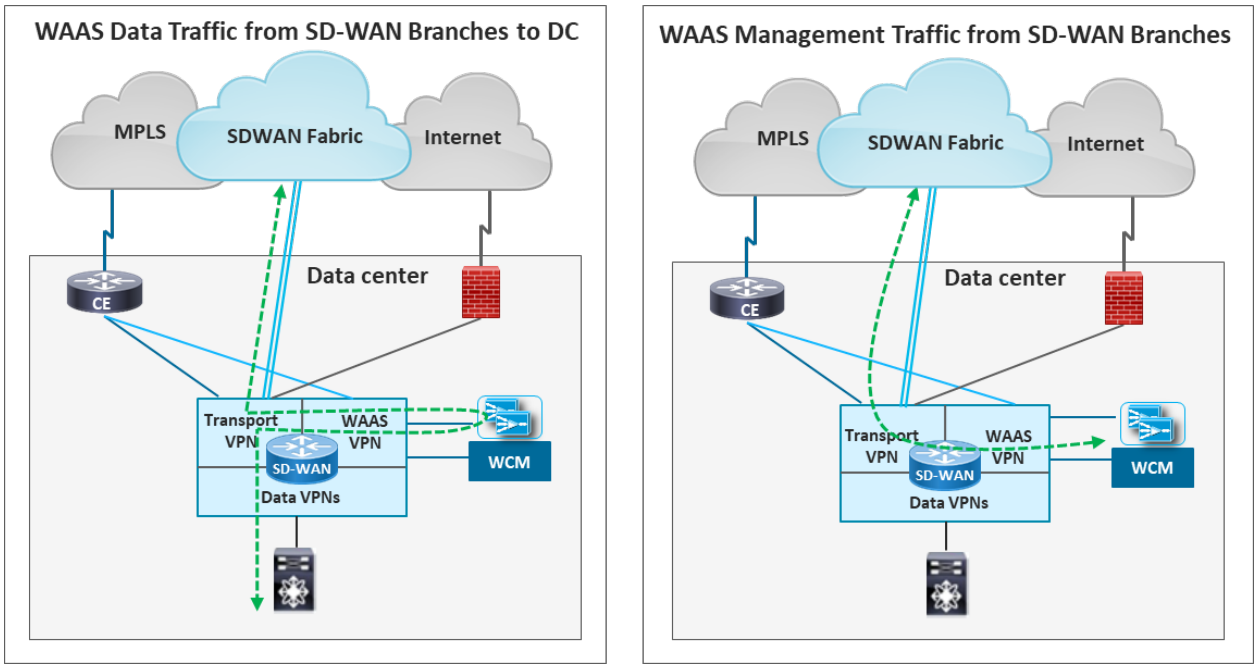

Figure 12

The figure 12 depicts traffic from SD-WAN branches and it's forwarding at the data center.

At the data center, the incoming WAAS data and management traffic from the Cisco SD-WAN branches would be either IPsec encrypted or GRE encapsulated, and destined to the Cisco SD-WAN device TLOC interface. The CE router would forward this traffic to the Cisco SD-WAN devices.

- After decryption and/or decapsulation, the AppNav-XE feature enabled on the SD-WAN tunnel interfaces would redirect interesting traffic to WAAS nodes for optimization over an auto-created GRE tunnel. When the traffic returns from WAAS node, it is forwarded to its destination through the data service VPNs using the regular SD-WAN forwarding

  The return data traffic from the data center LAN to SD-WAN branches would take the same path.

- After decryption and/or decapsulation, the WAAS management traffic that is destined to WCM, would be forwarded to WCM in the WAAS service VPN using the regular SD-WAN forwarding

- The Internet bound traffic from the data center service VPNs would need a DIA policy on the SD-WAN devices and the traffic would exit and enter the SD-WAN TLOC interfaces.

The AppNav-XE feature enabled on the SD-WAN TLOC interfaces will redirect the inbound and outbound interesting traffic to the WAAS nodes for optimization before forwarding the traffic to its destination.

3.5.4 WAAS Data Traffic between Legacy and SD-WAN Branches

The figure 13 depicts forwarding of traffic between legacy and SD-WAN branches, at the data center.

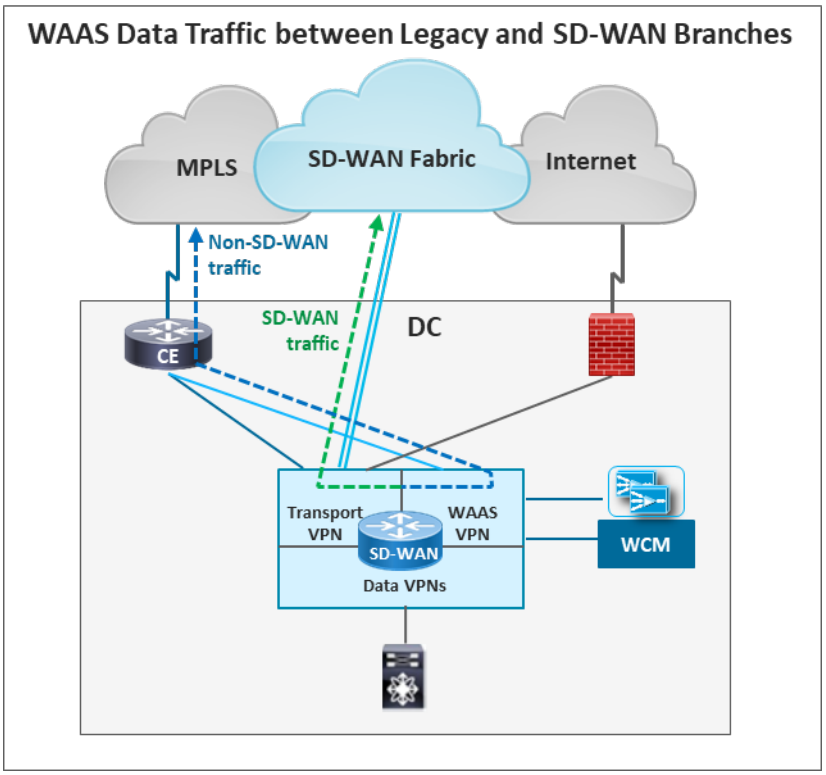

Figure 13

WAAS data traffic between the legacy and SD-WAN branches would transit through the data center Cisco SD-WAN device transport VPN and WAAS service VPN. WAN optimization would be performed at the branches and bypassed at the data center.

4 Known Issues and Alternatives

There is an interoperability issue between the AppNav-XE feature and the inter service VPN route leaking feature, when both are enabled in the same service VPN.

An alternative that helps work around the issue involves connecting WAAS VPN to the LAN-side router for non-SD-WAN traffic. Ensure that the LAN-side router does not re-advertise SD-

WAN and non-SD-WAN prefixes learnt from the Data service VPNs and the WAAS service VPNs.

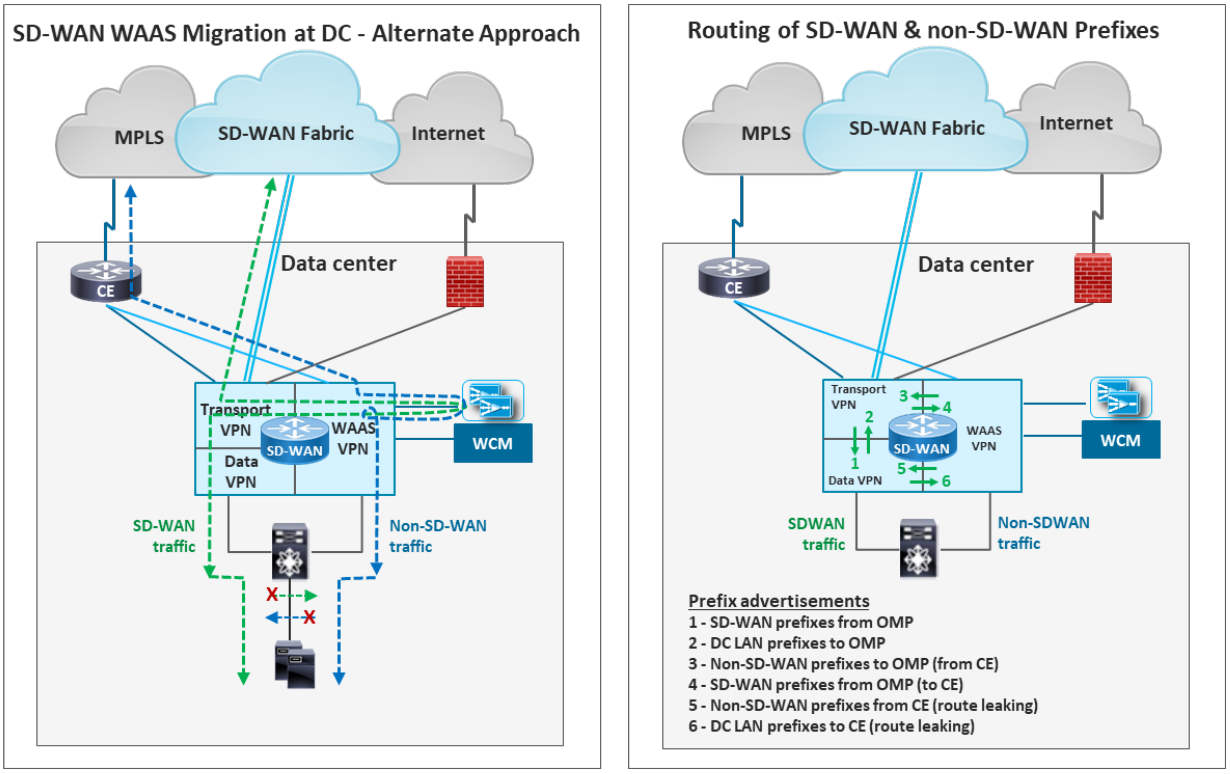

Figure 14

5 References

- AppNav-XE for SD-WAN Configuration Guide
- Cisco SD-WAN Migration Guide

End of Document