CVP
Enterprise SD-WAN
Financial Profile
(Hybrid WAN, Segmentation, Quality of Service, Centralized Policies)

Contents

Profile Introduction

The Cisco® Software-Defined WAN (SD-WAN) is a cloud-hosted and cloud-delivered overlay WAN solution, Cisco SDWAN offers the option for those customers who desire it to host their controllers on-premise. Though hosted on premises, Cisco SD-WAN would not limit the functionalities provided through cloud-managed services, such as the time needed to deploy services, build application resiliency, and provide a robust security architecture for hybrid networks.

Cisco SD-WAN solves many critical enterprise problems, including:

- Establishing a transport-independent WAN for lower cost and higher diversity
- Meeting Service-Level Agreements (SLAs) for business-critical and real-time applications
- Providing end-to-end segmentation for protecting critical enterprise compute resources
- Extending seamlessly into the private and public cloud
- Providing secured control and data plane connectivity

Cisco SD-WAN provides data plane and control plane separation by having controllers in the private network (hosted in the data center). The diagram below shows the high-level architecture of the solution.

(The firewall ports listed below need to be opened in order for edge devices to communicate with controllers hosted within the data center network.)

Core number	Ports for DTLS (UDP)	Ports for TLS (TCP)
Core0	12346	23456
Core1	12446	23556
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

This document covers the enterprise solution built with the features described below.

Security

The Cisco SD-WAN solution offers secure control-and-management communications between the routers and the control components. Data plane communication between the WAN edge routers is encrypted and secured based on IPsec encapsulation.

Hybrid transport

There are two data centers in this profile (DC1 and DC2), with each data center having two SD-WAN routers. All of the data centers' SD-WAN routers are connected to the Internet and to Multiprotocol Label-Switching, Customer-Premises Equipment (MPLS CPE) routers.

The branches have a range-of-connectivity model. Some are hybrid and connected to the Internet and MPLS. Some are connected to only one transport: either to the Internet or to MPLS.

The same profile was configured and tested with dual Internet transports. Lab environment consists of Ethernet interfaces with DHCP IP address provided by service provider.

Segmentation

In the branches, there can be multiple segments; with Cisco SD-WAN, the user can keep the segments separate. In this profile, two VPN segments have been defined. One segment is used for Corporate Network (vpn10) and PCI (vpn40) for credit-card transactions, which requires flow through a firewall.

Policy-based hub-and-spoke topology

A Centralized policy is deployed to establish a hub-and-spoke topology between the data centers and the branches.

One set of branches prefers the default route from DC1, and another set of branches prefers the default from DC2.

Quality of Service (QoS)

Quality of service is configured on all devices. The WAN bandwidth is appropriately distributed between different types of applications. Voice is given dedicated bandwidth on WAN interfaces and placed in the Low Latency Queue. Other traffic classes share the remaining bandwidth among them, based on weight assignment.

App-route policies

A Centralized app-route policy is configured for hybrid sites. Voice SLAs are defined, and the MPLS is defined as the preferred path for voice traffic.

Dynamic Host Configuration Protocol (DHCP) servers for the branches

WAN edge routers in the branches are configured as DHCP servers for some of the segments, for allocating IP addresses to the clients.

High availability

In the data center, the Open Shortest Path First (OSPF) is deployed for dynamic routing.

One set of branches utilize the Virtual Router Redundancy Protocol (VRRP) on the SD-WAN edge routers connected to L2 switches within the branch. Another set of branches run Open Shortest Path First (OSPF) between the SD-WAN edge router and L3 switches within the branch.

Table 1. Profile feature summary

Deployment area	Features
Security	TLS/DTLS-certificate-based control plane, IPsec-based data plane, segmentation, Zone-Based Firewall
Services	QoS, DIA, NAT, ACL, DHCP server
Routing	BGP, OSPF, VRRP
App-aware policies	SLA-based path selection, policy-based hub-and-spoke topology
Centralized management	Configuration, monitoring, and policy management through vManage

Network profile

Based on research and customer feedback and configuration samples, the Cisco SD-WAN profile is designed with a generic deployment topology that can be easily modified to fit specific deployment scenarios. This profile caters to enterprise network deployments with a large number of remote or branch offices and few data centers.

Topology diagram

Figure 1. Topology overview

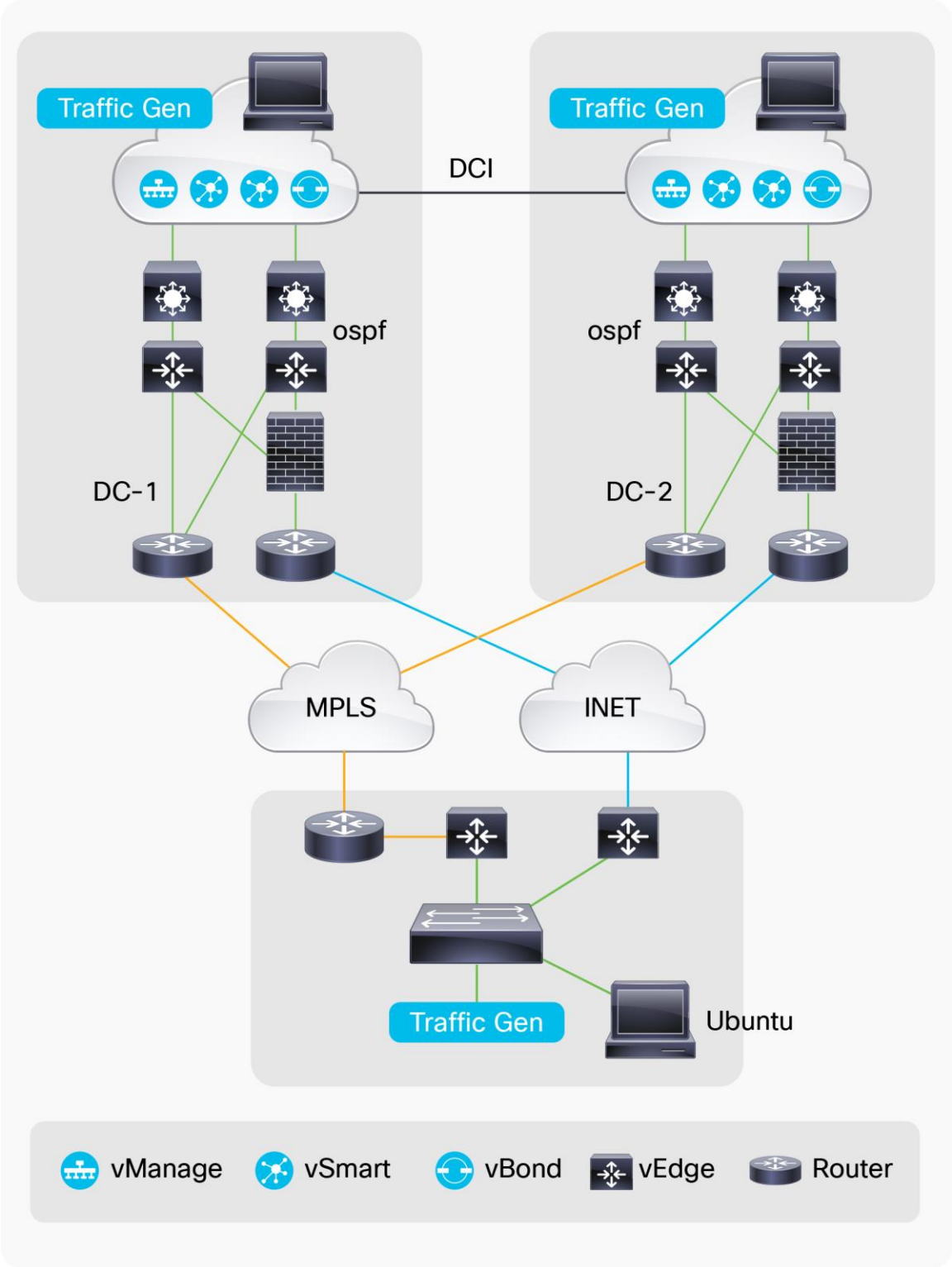
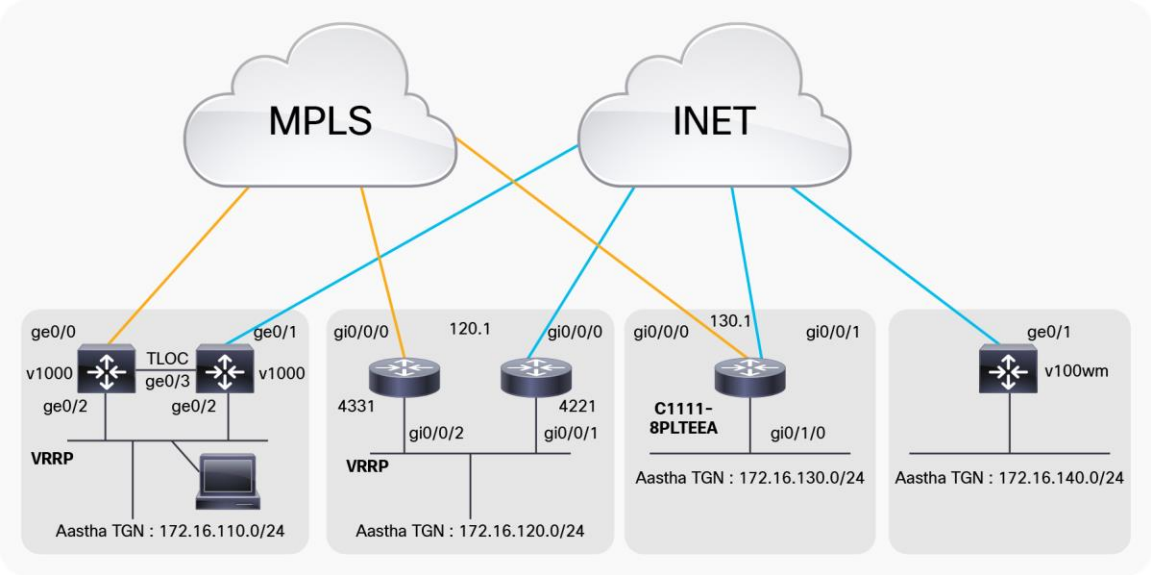


Figure 2. Branch topology

Detailed topology for remote Type A and Type B sites.



Hardware and feature specifications

This section describes the 3-D feature matrix, where the hardware platforms are listed along with their Place-In-Network (PIN), and the relevant vertical deployment.

Key vertical features

Table 2 defines the hardware, PIN, and SD-WAN feature deployed.

Table 2. 3-D feature summary with hardware

Deployment layer (PIN)	Platforms	Critical vertical features
Management plane	3x vManage	To scale the solution, clustering is utilized within the data-center (DC) site among the instances of vManage operating together as a single system interface from the active DC site. Within the DC site, synchronous replication among the vManage instances in the cluster is utilized to maintain states among the instances.
Control plane	4x vBond, 8x vSmart	Consisting of vBond and vSmart entities, this is used to control traffic flow and policies.
Data plane	vEdge 1K, vEdge 2K	Terminates the tunnels from the branches and receives and sends data packets between the branches and the data center.
Customer Edge (CE) (MPLS circuit termination at customer edge)	2x Cisco ASR 1006	Cisco ASR 1006 routers terminate AT&T and VZN 2-Gig MPLS. AT&T MPLS terminates on a Cisco ASR 1006 in both DC1 and DC2. VZN MPLS terminates on a Cisco ASR 1006 in both DC1 and DC2. Internet connectivity terminates on a Cisco Nexus® device in both GF0 and GF1.
DC distribution layer	4x Catalyst® 4500-x	Catalyst 4500-x layered in pairs that work as an aggregation point for traffic between data center and headends.

Hardware profile

Table 3 defines the set of relevant servers, test equipment, and endpoints that are used to complete the end-to-end deployment.

This list of hardware, along with the relevant software versions and the role of these devices, complements the actual physical topology shown in Figure 1.

Table 3. Hardware profile of servers and endpoints

VM and HW	Software version	Description
Spirent	Spirent TestCenter	Generates L7 traffic
Ubuntu	16.04	End host

Use case scenarios

Test methodology

To validate a new release, the network topology is upgraded, including the new software image, with the existing configuration composed of the use cases and the relevant traffic profile. New use cases acquired from the field or from customer deployments are added on top of the existing configuration.

With respect to the longevity for this profile, the setup, the CPU, and memory use/leaks are monitored during the validation phase. Furthermore, to test the robustness of the software release and platform, negative events are triggered while executing the use cases.

Use cases

Table 4 describes the use cases that were executed as a part of this profile test. These use cases are divided into buckets of technology areas to see the complete coverage of the deployment scenarios.

These technology buckets comprise System Upgrade, Security, Network Service, Monitoring & Troubleshooting, simplified management, system health monitoring, and system and network resiliency.

Table 4. List of use case scenarios

No.	Focus area	Use cases
System upgrade		
1	Upgrades/downgrades	The network administrator should be able to perform controller and vEdge upgrades (and downgrades) seamlessly between releases. All of the applied configurations should migrate seamlessly during upgrades and downgrades.
Security		
2	ACL/IPsec/NAT	Only authenticated devices are allowed to send traffic to one another. Provides secure communication between pairs of devices. Prevents unwanted data traffic from passing through the Viptela® vEdge routers and to the LAN networks in the service-side networks connected to the routers.

No.	Focus area	Use cases
Network services		
3	Control policy	The network administrator is able to define the routing policies such that: **For AT&T-Single MPLS locations:** The routers must install a default route from GF0 data headends with higher preference 100 over a default route received from GF1 data headends with preference 50. **For VZN-Single MPLS locations:** The routers must install a default route from GF0 data headends with higher preference 100 over a default route received from GF1 data headends with preference 50. AT&T hubs will accept routes only from sites that are AT&T MPLS as Primary, whether single or dual. VZN headends follow the same criteria, but for VZN hubs and VZN MPLS sites. The hub should not accept a default route from any remote router at any time.
4	Traffic steering policy	The network administrator is able to steer critical vs. noncritical traffic based on the circuit to which the traffic is connected. Critical (DSCP 46, 34, 28, 26, 24, and 18) and noncritical (all other traffic): critical traffic is sent over the more reliable WAN connection while other traffic is sent over other WAN connections, for a resulting active/active path on the remote routers. **For single MPLS locations:** All critical traffic must traverse the MPLS while noncritical traffic takes broadband, with a possibility of failover between both connections if the SLA is violated (latency and loss). **For dual MPLS where AT&T is primary:** All critical traffic must traverse the AT&T MPLS while noncritical traffic takes the VZN MPLS, with a possibility of failover between both connections if the SLA is violated (latency and loss). **For dual MPLS where VZN is primary:** All critical traffic must traverse the VZN MPLS while noncritical traffic takes the AT&T MPLS, with a possibility of failover between both connections if the SLA is violated (latency and loss).
5	Quality of Service (QoS)	The network administrator needs to enhance the user experience by ensuring traffic and application delivery using QoS policies by classifying data packets into appropriate forwarding classes and rewriting the differentiated Services Code Point (DSCP) values.
6	Application visibility	The network administrator is able to define the application-visibility parameters so that the IPFIX information can be viewed from the collector.
Monitoring and troubleshooting		
7	Wireshark	The network administrator is able to troubleshoot the network by capturing and analyzing traffic.
Simplified management		
8	Manageability	Simplified network troubleshooting and debugging for IT administration: ● Monitors network for alarms, syslog issues, and traps.
System health monitoring		
9	System health	Monitors system health for CPU use, memory consumption, and memory leaks during testing.
System and network resiliency and robustness		
10	System resiliency	Verifies system-level resiliency during the following events: ● Power failure ● WAN/LAN interface flapping ● Network impairments, as per SLA requirements.
11	Network resiliency	Verifies that the system holds up well at the level of network-level resiliency.
12	Negative events and triggers	Verifies that the system holds up well and recovers to working condition after the following negative events are triggered: ● Configuration changes: addition or removal of configuration snippets, configuration replacements routes ● Clearing of counters, clearing of routes ● Routing protocol interface flapping

Appendix A: System configuration

The system configuration is the same across all controllers and WAN edge routers.

```
system
 host-name               Spoke3
 system-ip               1.1.130.1
 site-id                 130
 admin-tech-on-failure
 no route-consistency-check
 sp-organization-name    " esc-sdwan-dmz"
 organization-name       " esc-sdwan-dmz"
 vbond vbonddmz.com
```

Appendix B: Hybrid transports VPN 0 configuration

vEdge with Hybrid Transport

```
vpn 0
 dns 8.8.8.8 primary
 host vbonddmz.com ip 35.164.223.65
 interface ge0/0
  ip address 10.151.110.1/16
  nat
  tunnel-interface
   encapsulation ipsec
   color gold restrict
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
```

```
 ip route 0.0.0.0/0 10.151.1.1
 !
 interface ge0/1
  ip address 10.161.110.2/16
  tunnel-interface
   encapsulation ipsec
   color mpls restrict
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
  shaping-rate 10000
  qos-map      WANQoS
 !
 ip route 0.0.0.0/0 10.161.1.1
!
```

cEdge with Hybrid Transport

```
ip host vbonddmz.com ip 35.164.223.65
ip name-server 8.8.4.4 8.8.8.8
ip route 0.0.0.0 0.0.0.0 10.151.1.1 1
ip route 0.0.0.0 0.0.0.0 10.161.1.1 1

interface GigabitEthernet0/0/0
 no shutdown
 arp timeout 1200
 mtu 1500
 negotiation auto
 service-policy output shape_GigabitEthernet0/0/1
 ip mtu 1500
```

```
 ip address 10.151.130.1 255.255.0.0
exit

interface GigabitEthernet0/0/1
 no shutdown
 arp timeout 1200
 mtu 1500
 negotiation auto
 service-policy output shape_GigabitEthernet0/0/0
 ip mtu 1500
 ip nat outside
 ip address 10.161.130.1 255.255.0.0
exit

interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet0/0/1
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/1
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/1
 tunnel mode sdwan
exit
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec weight 1
   color mpls restrict
   no last-resort-circuit
```

```
  vmanage-connection-preference 5
  allow-service all
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
 exit
exit
interface GigabitEthernet0/0/1
 tunnel-interface
  encapsulation ipsec weight 1
  color gold restrict
  no last-resort-circuit
  vmanage-connection-preference 5
  allow-service all
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
 exit
exit
```

Appendix C: Data center LAN–side configuration

vEdge Configuration

```
vpn 10
 router
  ospf
   router-id 1.1.20.1
   timers spf 200 1000 10000
   redistribute omp
   area 0
    interface ge0/2
    exit
   exit
  !
 !
 interface ge0/2
  ip address 172.16.20.2/24
  no shutdown
 !
!
vpn 40
 router
  ospf
   router-id 1.1.20.2
   timers spf 200 1000 10000
   redistribute omp
   area 0
    interface ge0/3
    exit
   exit
  !
 !
 interface ge0/3
  ip address 172.16.24.2/24
  no shutdown
 !
!
```

cEdge Configuration

```
vrf definition 10
 rd 1:10
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition 10
 rd 1:40
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!

interface GigabitEthernet1/0/0
 no shutdown
 arp timeout 1200
 vrf forwarding 10
 ip address 172.16.10.1 255.255.255.0
 ip mtu 1500
 ip ospf 1 area 0
 ip ospf network broadcast
 mtu 1500
 negotiation auto
!
interface GigabitEthernet1/0/1
 no shutdown
 arp timeout 1200
 vrf forwarding 40
 ip address 172.16.14.1 255.255.255.0
 ip mtu 1500
```

```
 ip ospf 2 area 0
 ip ospf network broadcast
 mtu 1500
 negotiation auto
!
router ospf 1 vrf 10
 auto-cost reference-bandwidth 100
 max-metric router-lsa
 timers throttle spf 200 1000 10000
 router-id 1.1.10.1
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
!
router ospf 2 vrf 40
 auto-cost reference-bandwidth 100
 max-metric router-lsa
 timers throttle spf 200 1000 10000
 router-id 1.1.10.2
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
!
```

Appendix D: Quality-of-Service (QoS) configuration

vEdge Configuration

```
vpn 0
interface ge0/0
  shaping-rate 10000
  qos-map      WANQoS
 !
interface ge0/1
  shaping-rate 10000
  qos-map      WANQoS
```

```
 !

vpn 10
 interface ge0/7.10

  access-list LAN-Classification in


policy

 class-map
  class Queue0 queue 0
  class Voice_EF queue 0
  class Queue1 queue 1
  class Queue2 queue 2
  class NetProtocol_CS3 queue 3
  class Queue3 queue 3
  class NetMgmt_CS2 queue 4
  class Queue4 queue 4
  class CriticalData_AF21 queue 5
  class Queue5 queue 5
  class Queue6 queue 6
  class Scavanger_AF11 queue 6
  class BestEffort_CS1 queue 7
  class Queue7 queue 7
 !
 access-list LAN-Classification
  sequence 1
   match
    destination-port 1719-1721
   !
   action accept
    class Voice_EF
    set
     dscp 46
    !
   !
  !
```

```
sequence 11
 match
  destination-port 2326-2485
 !
 action accept
  class Voice_EF
  set
   dscp 46
  !
 !
!
sequence 21
 match
  protocol 8 88 89
 !
 action accept
  class NetProtocol_CS3
  set
   dscp 24
  !
 !
!
sequence 31
 match
  destination-port 22
 !
 action accept
  class NetProtocol_CS3
  set
   dscp 24
  !
 !
!
sequence 41
 match
  destination-ip 10.200.200.0/24
 !
 action accept
```

```
  class NetMgmt_CS2
  set
   dscp 16
  !
 !
!
sequence 51
 match
  destination-ip   10.200.201.0/24
  destination-port 161 162 514
 !
 action accept
  class CriticalData_AF21
  set
   dscp 20
  !
 !
!
sequence 61
 match
  destination-port 20 21
 !
 action accept
  class BestEffort_CS1
  set
   dscp 8
  !
 !
!
sequence 71
 match
  destination-ip 10.200.202.0/24
 !
 action accept
  class Scavanger_AF11
  set
   dscp 10
  !
```

```
   !
  !
  sequence 81
   action accept
    class BestEffort_CS1
    set
     dscp 10
    !
   !
  !
  default-action accept
 !
qos-scheduler WANQoS_0
  class             Queue0
  bandwidth-percent 11
  buffer-percent    11
  scheduling        llq
 !
 qos-scheduler WANQoS_1
  class             Queue1
  bandwidth-percent 10
  buffer-percent    10
  drops             red-drop
 !
 qos-scheduler WANQoS_2
  class             Queue2
  bandwidth-percent 10
  buffer-percent    10
  drops             red-drop
 !
 qos-scheduler WANQoS_3
  class             Queue3
  bandwidth-percent 5
  buffer-percent    5
  drops             red-drop
 !
 qos-scheduler WANQoS_4
  class             Queue4
```

```
 bandwidth-percent 2
 buffer-percent    2
 drops             red-drop
!
qos-scheduler WANQoS_5
 class             Queue5
 bandwidth-percent 48
 buffer-percent    48
 drops             red-drop
!
qos-scheduler WANQoS_6
 class             Queue6
 bandwidth-percent 5
 buffer-percent    5
 drops             red-drop
!
qos-scheduler WANQoS_7
 class             Queue7
 bandwidth-percent 9
 buffer-percent    9
 drops             red-drop
!
qos-map WANQoS
 qos-scheduler WANQoS_0
 qos-scheduler WANQoS_1
 qos-scheduler WANQoS_2
 qos-scheduler WANQoS_3
 qos-scheduler WANQoS_4
 qos-scheduler WANQoS_5
 qos-scheduler WANQoS_6
 qos-scheduler WANQoS_7
!
!
```

Appendix E: DHCP and VRRP configuration

cEdge Configuration

```
interface GigabitEthernet0/0/2
 vrf forwarding 1
```

```
 ip address 172.16.120.1 255.255.255.0
 ip helper-address 172.16.10.5
 negotiation auto
 vrrp 1 address-family ipv4
  priority 110
  vrrpv2
  address 172.16.120.3 primary
  exit-vrrp
 arp timeout 1200
```

vEdge Configuration

```
vpn 1
 interface ge0/2
  ip address 172.16.110.2/24
  dhcp-helper 172.16.10.4
  no shutdown
  vrrp 1
   priority 110
   ipv4 172.16.110.3
  !
 !
!
```

Appendix F: Centralized policies

Control policy applied toward branches in Group1

```
policy
 control-policy PreferDC2
    sequence 1
     match route
      site-list DC2
     !
     action accept
      set
       preference 100
      !
     !
    !
    sequence 11
     match route
```

```
     site-list AllBranches
     vpn-list pciVPN
    !
    action accept
     set
      tloc-list DC-TLOCS
     !
    !
   !
 default-action accept
!
control-policy PreferDC1
   sequence 1
    match route
     site-list DC1
    !
    action accept
     set
      preference 100
     !
    !
   !
   sequence 11
    match route
     site-list AllBranches
     vpn-list pciVPN
    !
    action accept
     set
      tloc-list DC-TLOCS
     !
    !
   !
 default-action accept
!
vpn-membership vpnMembership_-258379630
   sequence 10
    match
```

```
     vpn-list corpVPN
    !
    action accept
    !
   !
   sequence 20
    match
     vpn-list pciVPN
    !
    action accept
    !
   !
 default-action reject
!
data-policy _guestVPN_Drop1918
 vpn-list guestVPN
   sequence 1
    match
     destination-data-prefix-list RFC1918Plus
    !
    action accept
    !
   !
 default-action accept
!
lists
 data-prefix-list RFC1918Plus
  ip-prefix 10.0.0.0/8
  ip-prefix  172.16.0.0/16
  ip-prefix  192.168.0.0/16
  ip-prefix  198.18.128.0/18
 !
 site-list AllBranches
  site-id 300-499
 !
 site-list BranchG1
  site-id 300-399
 !
```

```
  site-list BranchG2
   site-id 400-499
  !
  site-list DC1
   site-id 100
  !
  site-list DC2
   site-id 200
  !
  tloc-list DC-TLOCS
   tloc 10.1.0.1 color mpls encap ipsec
   tloc 10.1.0.1 color biz-internet encap ipsec
   tloc 10.1.0.2 color mpls encap ipsec
   tloc 10.1.0.2 color biz-internet encap ipsec
   tloc 10.2.0.1 color mpls encap ipsec
   tloc 10.2.0.1 color biz-internet encap ipsec
   tloc 10.2.0.2 color mpls encap ipsec
   tloc 10.2.0.2 color biz-internet encap ipsec
  !
  vpn-list corpVPN
   vpn 10
  !
  vpn-list guestVPN
   vpn 40
  !
  vpn-list pciVPN
   vpn 20
  !
 !
!
apply-policy
 site-list BranchG1
  control-policy PreferDC1 out
 !
 site-list AllBranches
  data-policy _guestVPN_Drop1918 from-service
  vpn-membership vpnMembership_-258379630
 !
```

```
 site-list BranchG2
  control-policy PreferDC2 out
 !
!
```

Application-aware routing policy for the branches

```
 policy
 sla-class BestEffort
  latency 250
  loss 10
  jitter 30
 !
 sla-class CriticalData
  latency 200
  loss 3
  jitter 20
 !
 sla-class Voice
  latency 150
  loss 1
  jitter 5
 !
app-route-policy _storeVPN_CVP-APP-Route1
 vpn-list storeVPN
   sequence 1
    match
     dscp 46
    !
    action
     sla-class Voice  preferred-color mpls
    !
   !
   sequence 11
    match
     dscp 20
    !
    action
     sla-class CriticalData  preferred-color mpls
```

```
     !
    !
    sequence 21
     match
      dscp 0-10
     !
     action
      sla-class BestEffort  preferred-color gold
     !
    !
 !
lists
  prefix-list DefaultPrefix
   ip-prefix 0.0.0.0/0
  !
  site-list BranchGroup1
   site-id 1000-1999
  !
  site-list BranchGroup2
   site-id 2000-2999
  !
  site-list DC1
   site-id 100
  !
  site-list DC2
   site-id 200
  !
  vpn-list storeVPN
   vpn 10
  !
 !
!
apply-policy
 site-list BranchGroup1
  control-policy Group1BranchControl-Out out
!
!
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C17-741379-00 10/18