CVP – Enterprise Cisco SD-WAN Retail Profile (Hybrid WAN, Segmentation, Zone-Based Firewall, Quality of Service, and Centralized Policies)
Contents

Profile introduction................................................................................................................................. 3

Network profile........................................................................................................................................ 5
  Topology diagram ................................................................................................................................. 5
  Hardware and feature specifications ...................................................................................................... 6
    Key vertical features ............................................................................................................................ 6
  Hardware profile .................................................................................................................................... 7

Use case scenarios................................................................................................................................. 7
  Test methodology .................................................................................................................................. 7
  Use cases ............................................................................................................................................. 7

Appendix A: System configuration ........................................................................................................ 9

Appendix B: Hybrid transports VPN 0 configuration ............................................................................... 9
  vEdge with Hybrid Transport ................................................................................................................ 9
  cEdge with Hybrid Transport ............................................................................................................. 11

Appendix C: Data center LAN-side configuration .................................................................................. 13
  vEdge Configuration ............................................................................................................................ 13
  cEdge Configuration ............................................................................................................................ 14

Appendix D: DHCP and VRRP branch configuration ............................................................................. 15
  vEdge Configuration ............................................................................................................................ 15
  cEdge Configuration ............................................................................................................................ 16

Appendix E: Quality-of-Service (QoS) configuration ............................................................................. 16
  vEdge Configuration ............................................................................................................................ 16
  cEdge Configuration ............................................................................................................................ 22

Appendix F: Guest Wi-Fi with DIA and ZBFW ..................................................................................... 28
  vEdge Configuration ............................................................................................................................ 28
  cEdge Configuration ............................................................................................................................ 30

Appendix G: Centralized policies ........................................................................................................... 33
  Control policy applied toward branches in Group1 .............................................................................. 33
  Application-aware routing policy for the branch .................................................................................. 35
Profile introduction

The Cisco Software Defined WAN (SD-WAN) is a cloud-hosted and cloud-delivered overlay WAN architecture that facilitates digital and cloud transformation for enterprises. It significantly drops WAN costs, reduces the time to deploy services, build application resiliency and provides a robust security architecture for hybrid networks.

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

- Establishing 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/public cloud
- Providing direct Internet access from the branches with Zone-Based Firewall
- Providing secured control and data plane connectivity

Cisco SD-WAN provides data plane and control plane separation by having controllers in the cloud (public or private).

This document covers the enterprise solution profile 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 with each data center having two SD-WAN routers. All of the data-center SD-WAN routers are connected to Internet and Multiprotocol Label Switching (MPLS) transports.

The branches have a range of connectivity models. 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.

Segmentation and Zone-Based Firewall (ZBFW)

There can be multiple segments in the branches, and, with Cisco SD-WAN, a user is able to keep the segments separate within the branch and on the overlay. In this profile, two VPN segments have been defined. One segment is used for Guest Wi-Fi (VPN 40) and requires Direct Internet Access (DIA) only. A guest segment is not allowed to talk to any other segment within the branch or on the overlay. The store segment (VPN 10) has three VLANs, for VoIP, for Point-Of-Sale (POS) systems, and for employees.

Zone-Based Firewall is deployed for the traffic from Guest Wi-Fi VPN to DIA.
Policy-based hub-and-spoke topology
Centralized policies are deployed to establish a hub-and-spoke topology between the data centers and the branches.

One set of branches prefers the default route from Data Center 1 (DC1), and another set of branches prefers the default from Data Center 2 (DC2).

Quality of Service
Quality of Service (QoS) 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 a Low Latency Queue. Other traffic classes share the remaining bandwidth among them based on weight assignment.

SLA based application-aware routing policies
Centralized application-aware routing policies are configured for hybrid sites. Voice SLAs are defined and MPLS is defined as the preferred path for Voice traffic. Internet is defined as the preferred path for Best-Effort traffic.

Dynamic Host Configuration Protocol (DHCP) servers for the branches
The 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, Border Gateway Protocol (BGP) is deployed for dynamic routing.

One set of branches utilizes Virtual Router Redundancy Protocol (VRRP) on the SD-WAN edge routers connected to the Layer2 (L2) switch within the branch. Another set of branches run Open Shortest Path First (OSPF) Protocol between the SD-WAN edge router and the Layer 3 (L3) switch within the branch.

Table 1. Profile feature summary

<table>
<thead>
<tr>
<th>Deployment area</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>TLS/DTLS certificate-based control plane, IPsec-based data plane, Segmentation, Zone-Based Firewall</td>
</tr>
<tr>
<td>Services</td>
<td>QoS, DIA, NAT, ACL, DHCP Server</td>
</tr>
<tr>
<td>Routing</td>
<td>BGP, OSPF, VRRP</td>
</tr>
<tr>
<td>Centralized Policies</td>
<td>SLA-based path selection, policy-based hub-and-spoke topology</td>
</tr>
<tr>
<td>Centralized Management</td>
<td>Configuration, Monitoring and Policy management through vManage</td>
</tr>
</tbody>
</table>
Network profile

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

Topology diagram

Figure 1. Topology overview
Figure 2. Branch topology (Branch Type A and Type B)

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 features deployed.

Table 2. 3-D feature summary with hardware and PIN

<table>
<thead>
<tr>
<th>PIN</th>
<th>Platforms</th>
<th>Critical features</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN routers in the data centers</td>
<td>Viptela vEdge 2000, Viptela vEdge 5000, Cisco® ASR 1001-HX, ASR 1002-HX</td>
<td>Dynamic routing (BGP), Quality of Service (QoS), Hybrid WAN, ACL</td>
</tr>
<tr>
<td>SD-WAN routers in the branches</td>
<td>vEdge100, vEdge1000, ISR 4331</td>
<td>Segmentation, Zone-Based Firewall, VRRP/OSPF, DHCP Server, Quality of Service (QoS), Hybrid WAN, NAT/DIA, TLOC-Extension, ACL</td>
</tr>
<tr>
<td>Controller deployment</td>
<td>EXi6.0, vBond, vSmart, vManage</td>
<td>Centralized Management, Control, Provisioning, Monitoring, Policy</td>
</tr>
</tbody>
</table>
**PIN**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Critical features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet transport</td>
<td>ISR/ASR Routers</td>
</tr>
<tr>
<td>MPLS transport</td>
<td>ISR/ASR Routers</td>
</tr>
<tr>
<td>L2/L3 access switches</td>
<td>CAT3K</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Virtual machine and hardware</th>
<th>Software version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spirent</td>
<td>Spirent Test Center</td>
<td>Generates L4/L7 traffic</td>
</tr>
</tbody>
</table>

**Use case scenarios**

**Test methodology**

To validate a new release, the network topology is upgraded with the new software image with an 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 to the existing configuration.

With respect to the longevity of this profile, the setup, CPU, and memory use/leaks are monitored during the validation phase. Furthermore, to test the robustness of the software release and platform being tested, negative events are triggered during the use-case execution process.

**Use cases**

Table 4 describes the use cases executed as part of this profile test. The use cases are divided into buckets of technology areas to view complete coverage of the deployment scenarios.

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

**Table 4. List of use case scenarios**

<table>
<thead>
<tr>
<th>No</th>
<th>Focus area</th>
<th>Use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System health monitoring</td>
<td>● Monitor site health</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Monitor device health</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Monitor Bidirectional Forwarding Detection (BFD) session state from the devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Monitor control session state</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Monitor BFD / transport performance statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● View alarms and events</td>
</tr>
<tr>
<td>2</td>
<td>Configuration templates</td>
<td>● Utilize the configuration template from vManage to update the device configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Configure/update ACLs and route policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Define/update ZBFW policies</td>
</tr>
<tr>
<td>3</td>
<td>Centralized policy management</td>
<td>● Utilize vManage GUI interface to provision and update centralized policies</td>
</tr>
<tr>
<td>4</td>
<td>Software upgrade</td>
<td>● Upgrade the controllers and SD-WAN routers through vManage</td>
</tr>
<tr>
<td>5</td>
<td>Admin-tech</td>
<td>● Collect admin-tech from the controllers and SD-WAN edges</td>
</tr>
<tr>
<td>No</td>
<td>Focus area</td>
<td>Use cases</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 6  | Troubleshooting             | • SSH into devices from vManage portal  
• Issue real-time commands from device dashboard                                                                                       |
| 7  | Security                    |                                                                                                                                              |
| 8  | Zone-Based Firewall         | • Define and apply ZBFW to traffic that is allowed to use DIA from Guest Wi-Fi VPN/VRF                                                  |
| 9  | Network services            |                                                                                                                                              |
| 10 | Segmentation                | • Configure VLAN segments in the branch  
• Guest Wi-Fi VPN segmented from corporate VPN  
• VPN membership policy for the centralized vSmart policies                                                                |
| 11 | Quality of Service (QoS)    | • Provide classification of traffic for QoS using Access Control List (ACL) and map it to forwarding classes  
• BW allocation forwarding class mapping to queues  
• Voice traffic is mapped to Low Latency Queuing (LLQ)  
• Shaping on the WAN interfaces                                                                                               |
| 12 | Centralized control policies| • Hub-and-spoke topology between data centers and remote branches  
• Different branch groups prefer one data center over another for a default route                                                  |
| 13 | Centralized SLA-based routing policy | • Define SLA threshold for voice  
• Prefer MPLS for voice  
• Prefer Internet for best-effort data                                                                                           |
| 14 | VPN membership policy       | • Utilize VPN membership policy to restrict Guest Wi-Fi routing from overlay                                                              |
| 15 | Routing                     |                                                                                                                                              |
| 16 | Quality of Service (QoS)    | • In the data center, run BGP between the SD-WAN edge routers and the data-center aggregation routers  
• Redistribute routes between BGP and Overlay Management Protocol (OMP)                                                             |
| 17 | Application visibility      |                                                                                                                                              |
| 18 | BGP                         | • Run OSPF in the branches access switch/router  
• Redistribute OSPF into OMP                                                                                                            |
| 19 | System resiliency           | • Run VRRP on the vLANs in the branches                                                                                                     |
| 20 | DPI/NBAR                    | • Enable application visibility                                                                                                             |
| 21 | Application visibility      |                                                                                                                                              |
| 22 | System resiliency           | • Enable cFLOWD/netflow export to collector                                                                                                 |
| 23 | System resiliency           | • Verify system-level resiliency during the following events:  
• Power failure  
• WAN/LAN interface flaps  
• Network impairments as per SLA requirements                                                                                     |
| 24 | Negative testing            | • Verify that the system holds well and recovers to working condition after the following negative events are triggered:  
• Configuration changes: add/remove configuration snippets, replace configuration  
• Clear counters, clear routes  
• Routing protocol interface flap                                                                                                   |
Appendix A: System configuration

The system configuration is the same across all controllers and WAN Edge routers, including Cisco XE SDWAN (cEdge) and Viptela SDWAN (vEdge).

    system
    host-name vEdge3
    system-ip 11.2.1.3
    site-id 1200
    admin-tech-on-failure
    no route-consistency-check
    sp-organization-name "Cisco Sy1 - 19968"
    organization-name "Cisco Sy1 - 19968"
    vbond vbondesc.com

Appendix B: Hybrid transports VPN 0 configuration

vEdge with Hybrid Transport

    vpn 0
    name "Transport VPN"
    dns 8.8.4.4 secondary
    dns 8.8.8.8 primary
    host vbondesc.com ip 21.1.1.11 21.1.2.11
    interface ge0/0
    ip address 20.1.3.101/24
    nat
    !
    tunnel-interface
    encapsulation ipsec
    color gold
    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
!
interface ge0/1
ip address 20.2.3.101/24
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
!
interface ge0/7
mtu 1504
no shutdown
!
!
ip route 0.0.0.0/0 20.1.3.1
ip route 0.0.0.0/0 20.2.3.1
!
cEdge with Hybrid Transport

```plaintext
ip host vbondesc.com 21.1.1.11 21.1.2.11
ip name-server 8.8.4.4 8.8.8.8
ip route 0.0.0.0 0.0.0.0 20.1.15.1 1
ip route 0.0.0.0 0.0.0.0 20.2.15.1 1

interface GigabitEthernet0/0/0
   no shutdown
   arp timeout 1200
   mtu 1500
   negotiation auto
   service-policy output shape_GigabitEthernet0/0/0
   ip mtu 1500
   ip nat outside
   ip address 20.1.15.101 255.255.255.0
exit

interface GigabitEthernet0/0/1
   no shutdown
   arp timeout 1200
   mtu 1500
   negotiation auto
   service-policy output shape_GigabitEthernet0/0/1
   ip mtu 1500
   ip address 20.2.15.101 255.255.255.0
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
```

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
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
  color gold restrict
  no last-resort-circuit
  vmanage-connection-preference 5
  no 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
  encapsulation ipsec weight 1
exit
exit

interface GigabitEthernet0/0/1
  tunnel-interface
  color mpls restrict
  no last-resort-circuit
  vmanage-connection-preference 5
  no 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
encapsulation ipsec weight 1
exit
exit

Appendix C: Data center LAN-side configuration

vEdge Configuration

vpn 10
router
bgp 65220
  address-family ipv4-unicast
    maximum-paths paths 2
    redistribute ospf
  !
neighbor 10.201.1.2
  no shutdown
  remote-as 65221
  !
neighbor 10.201.2.2
  no shutdown
  remote-as 65221
  !
  !
interface 10ge2/2
  ip address 10.201.1.1/24
  no shutdown
  access-list LAN-Classification in
interface 10ge2/3
ip address 10.201.2.1/24
no shutdown
access-list LAN-Classification in
!
!
cEdge Configuration

vrf definition 10
rd 1:10
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
!
interface GigabitEthernet1/0/0
no shutdown
vrf forwarding 10
ip address 10.201.3.1 255.255.255.0
!
interface GigabitEthernet1/0/1
no shutdown
vrf forwarding 10
ip address 10.201.4.1 255.255.255.0
!

router bgp 65220
timers bgp 60 180
bgp log-neighbor-changes
distance bgp 20 200 20
address-family ipv4 unicast vrf 10
maximum-paths 2
neighbor 10.201.3.2 remote-as 65221
neighbor 10.201.3.2 activate
neighbor 10.201.3.2 ebgp-multihop 1
neighbor 10.201.4.2 remote-as 65221
neighbor 10.201.4.2 activate
neighbor 10.201.4.2 ebgp-multihop 1
redistribute omp
exit-address-family
!
!

Appendix D: DHCP and VRRP branch configuration

vEdge Configuration

vpn 10
interface ge0/7.10
ip address 10.10.1.1/24
no shutdown
access-list LAN-Classification in
vrrp 10
track-omp
ipv4 10.10.1.3
!
dhcp-server
address-pool 10.10.1.0/25
exclude 10.10.1.1-10.10.1.100
offer-time 600
lease-time 86400
admin-state up
options
default-gateway 10.10.1.3
dns-servers 8.8.8.8 8.8.4.4
!
!
!
cEdge Configuration

ip dhcp excluded-address vrf 10 10.40.1.0 10.40.1.100
ip dhcp pool vrf-10-GigabitEthernet1/0/0.10
vrf 10
default-router 10.40.1.3
dns-server 8.8.4.4 8.8.8.8
network 10.40.1.0 255.255.255.0
lease 1 0 0
exit

interface GigabitEthernet1/0/0.10
no shutdown
encapsulation dot1Q 10
vrf forwarding 10
ip mtu 1500
ip address 10.40.1.1 255.255.255.0
vrrp 10 address-family ipv4
  vrrpv2
  priority 40
  address 10.40.1.3
  track omp shutdown
exit
exit

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

vEdge Configuration

vpn 0
interface ge0/0
  shaping-rate 10000
  qos-map WANQoS
!
in 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
!
!
cEdge Configuration

sdwan

interface GigabitEthernet1/0/0.10
access-list LAN-Classification in exit

class-map match-any BestEffort_CS1
  match qos-group 7
!
class-map match-any CriticalData_AF21
  match qos-group 5
!
class-map match-any NetMgmt_CS2
  match qos-group 4
!
class-map match-any NetProtocol_CS3
  match qos-group 3
!
class-map match-any Queue0
  match qos-group 0
!
class-map match-any Queue1
  match qos-group 1
!
class-map match-any Queue2
  match qos-group 2
!
class-map match-any Queue3
  match qos-group 3
!
class-map match-any Queue4
  match qos-group 4
!
class-map match-any Queue5
  match qos-group 5
!
class-map match-any Queue6
  match qos-group 6
!
class-map match-any Queue7
  match qos-group 7
!
class-map match-any Scavanger_AF11
  match qos-group 6
!
class-map match-any Voice_EF
  match qos-group 0
!
policy-map WANQoS
  class Queue0
    priority percent 11
  
  class Queue1
    random-detect
    bandwidth percent 10
  
  class class-default
    random-detect
    bandwidth percent 10
  
  class Queue3
    random-detect
    bandwidth percent 5
  
  class Queue4
    random-detect
    bandwidth percent 2
  
  class Queue5
    random-detect
    bandwidth percent 48
  
  class Queue6
    random-detect
bandwidth percent 5
!
class Queue7
  random-detect
  bandwidth percent 9
!
!
policy-map shape_GigabitEthernet0/0/0
  class class-default
    service-policy WANQoS
    shape average 10000000
!
!
policy-map shape_GigabitEthernet0/0/1
  class class-default
    shape average 100000000
!
!
interface GigabitEthernet0/0/0
  no shutdown
  arp timeout 1200
  ip address 20.1.16.101 255.255.255.0
  ip mtu 1500
  ip nat outside
  mtu 1500
  negotiation auto
  service-policy output shape_GigabitEthernet0/0/0
exit
interface GigabitEthernet0/0/1
  no shutdown
  arp timeout 1200
  ip address 20.2.16.101 255.255.255.0
  ip mtu 1500
  mtu 1500
  negotiation auto
  service-policy output shape_GigabitEthernet0/0/1
exit
policy
class-map
  class BestEffort_CS1 queue 7
  class CriticalData_AF21 queue 5
  class NetMgmt_CS2 queue 4
  class NetProtocol_CS3 queue 3
  class Queue0 queue 0
  class Queue1 queue 1
  class Queue2 queue 2
  class Queue3 queue 3
  class Queue4 queue 4
  class Queue5 queue 5
  class Queue6 queue 6
  class Queue7 queue 7
  class Scavanger_AF11 queue 6
  class Voice_EF queue 0
!
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
  
  !
Appendix F: Guest Wi-Fi with DIA and ZBFW

vEdge Configuration

```plaintext
! default-action accept
!

vpn 40
 name "Guest Wifi"
 interface ge0/7.40
 ip address 10.10.4.1/24
 no shutdown
 access-list WIFI-Classification in
 policer LimitWIFI out
 vrrp 40
  track-omp
  ipv4 10.10.4.3
!

dhcp-server
  address-pool 10.10.4.0/25
  exclude 10.10.4.1-10.10.4.100
  offer-time 600
  lease-time 86400
  admin-state up
  options
   default-gateway 10.10.4.3
   dns-servers 8.8.8.8 8.8.4.4
!
!
ip route 0.0.0.0/0 vpn 0
!
policy
 policer LimitWIFI
  rate 2000000
  burst 30000
  exceed drop
!
```
zone GuestWifi
    vpn 40
!
zone InternetZone
    vpn 0
!
zone-pair ZP_GuestWifi_Internet_-_630006705
    source-zone GuestWifi
    destination-zone InternetZone
    zone-policy GuestWifiZBFW
!
zone-based-policy GuestWifiZBFW
    sequence 1
        match
            protocol 6
            destination-port 443 80 8080 8443
        !
        action inspect
        !
    !
    sequence 11
        match
            protocol 6 17
            destination-port 53
        !
        action inspect
        !
    !
    default-action drop
!
zone-to-nozone-internet allow
!
cEdge Configuration

interface GigabitEthernet0/0/0
  no shutdown
  arp timeout 1200
  ip address 20.1.16.101 255.255.255.0
  ip mtu 1500
  ip nat outside
  mtu 1500
  negotiation auto
  service-policy output shape_GigabitEthernet0/0/0
exit

sdwan
  interface GigabitEthernet1/0/0.10
    access-list LAN-Classification in
exit
vrf definition 40
  rd 1:40
  address-family ipv4
    exit-address-family
  !
  address-family ipv6
    exit-address-family
  !
  !
  ip dhcp excluded-address vrf 40 10.40.1.0 10.40.1.100
  ip dhcp pool vrf-40-GigabitEthernet1/0/0.40
    vrf 40
    lease 1 0 0
    default-router 10.40.1.3
    dns-server 8.8.4.4 8.8.8.8
    network 10.40.1.0 255.255.255.0
exit
  ip dhcp use hardware-address client-id

  ip access-list extended GuestWifiZFW-seq-1-acl_
11 permit object-group GuestWifiZBFW-seq-1-service-og_ any any
!

ip access-list extended GuestWifiZBFW-seq-11-acl_
11 permit object-group GuestWifiZBFW-seq-11-service-og_ any any
!

ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload
ip nat translation tcp-timeout 60
ip nat translation udp-timeout 1
ip nat route vrf 40 0.0.0.0 0.0.0.0 global
!

! policy-map type inspect GuestWifiZBFW
class GuestWifiZBFW-seq-1-cm_
    inspect
!
class GuestWifiZBFW-seq-11-cm_
    inspect
!
class class-default
drop
!
!
interface GigabitEthernet1/0/0.40
no shutdown
encapsulation dot1Q 10
vrf forwarding 40
ip address 10.40.1.1 255.255.255.0
vrrp 10 address-family ipv4
vrrpv2
    address 10.40.1.3
    priority 40
    track omp shutdown
exit
exit
!
object-group service GuestWifiZBFW-seq-1-service-og_
tcp-udp 53
!
object-group service GuestWifiZBFW-seq-11-service-og_
tcp 80
tcp 443
tcp 8080
tcp 8443
!
parameter-map type inspect-global
  alert on
  log dropped-packets
  multi-tenancy
  vpn zone security
!
zone security GuestWifi
  vpn 40
!
zone security InternetZone
  vpn 0
!
zone-pair security ZP_GuestWifi_Internet_630006705 source GuestWifi destination InternetZone
  service-policy type inspect GuestWifiZBFW
!
policy
  policer LimitWIFI
    rate 2000000
    burst 30000
    exceed drop
!
access-list WIFI-Classification
  sequence 1
    action accept
      policer LimitWIFI
      class Scavanger_AF11
      set
dscp 10
!

Appendix G: Centralized policies

Control policy applied toward branches in Group1

policy
  control-policy Group1BranchControl-Out
    sequence 1
      match route
        site-list DC1
      prefix-list DefaultPrefix
    !
    action accept
    set
      preference 100
    !
    !
    sequence 11
      match route
        site-list DC1
      !
      action accept
      !
      !
    sequence 21
      match route
        site-list DC2
      prefix-list DefaultPrefix
    !
    action accept
set
  preference 50
!
!
!
sequence 31
  match route
    site-list DC2
    !
    action accept
    !
    
!
sequence 41
  match tloc
    site-list DC1
    !
    action accept
    !
    
!
sequence 51
  match tloc
    site-list DC2
    !
    action accept
    !
    
  default-action reject
    !

vpn-membership vpnMembership_303141673
  sequence 10
    match
      vpn-list storeVPN
      !
      action accept
      !
      
  default-action reject
    !
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-1 out
  vpn-membership vpnMembership_303141673
  !
  !

**Application-aware routing policy for the branch**

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-Routelu
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
!
!