Possibilities

#CiscoLive

Building and Using Policies with Cisco SD-WAN

Become Sufficiently Dangerous

Stefan Olofsson, Technical Solutions Architect

DGTL-BRKRST-2791

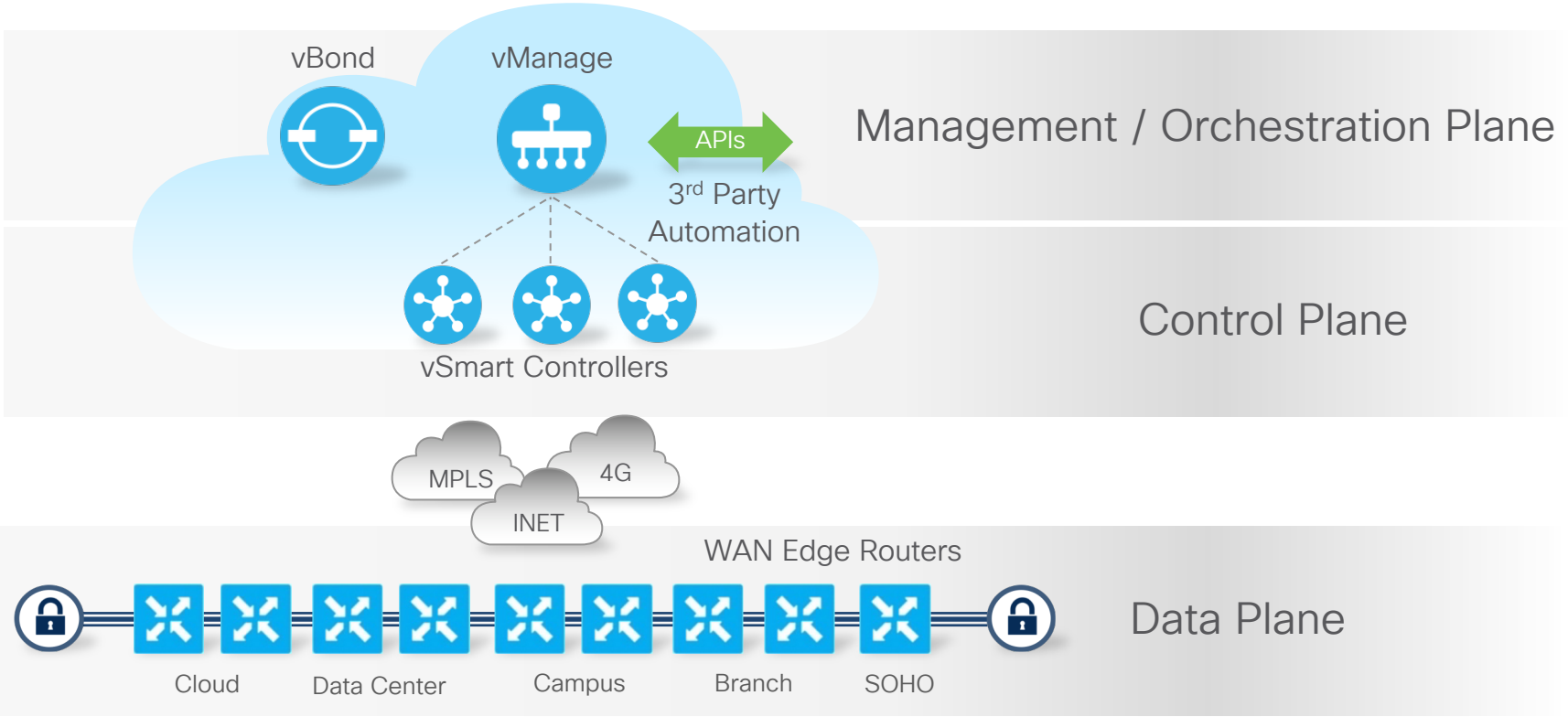
Agenda

- Cisco SD-WAN Crash Course
- Introduction to the Cisco SD-WAN Policy Framework
- Control Policies and Applications
- Data Policies and Applications
- Application Aware Routing Policies and Applications
- More Policies and Applications
- Tips, Tricks, Scalability and Best Practices
- Conclusion

Cisco SD-WAN Crash Course

Cisco SD-WAN Architecture Overview

Applying SDN Principles Onto The Wide Area Network



Cisco SD-WAN Terminology

- Transport Side – Controller or WAN Edge Interface connected to the underlay/WAN network
  - Always VPN 0
  - Traffic typically tunneled/encrypted, unless split-tunneling is used
- Service Side – WAN Edge interface attaching to the LAN
  - VPN 1-511 (512 Reserved for OOB Mgmt)
  - Traffic forwarded as is from original source
- TLOC – Collection of entities making up a transport side connection
  - System-IP: IPv4 Address (non-routed identifier)
  - Color: Interface identifier on local WAN Edge
  - Private TLOC: IP Address on interface sitting on inside of NAT
  - Public TLOC: IP Address on interface sitting on outside of NAT
  - Private/Public can be the same if connection is not subject to NAT
- vRoute – Routes learnt/connected on Service Side
  - vRoute tagged with attributes as it is picked up by OMP

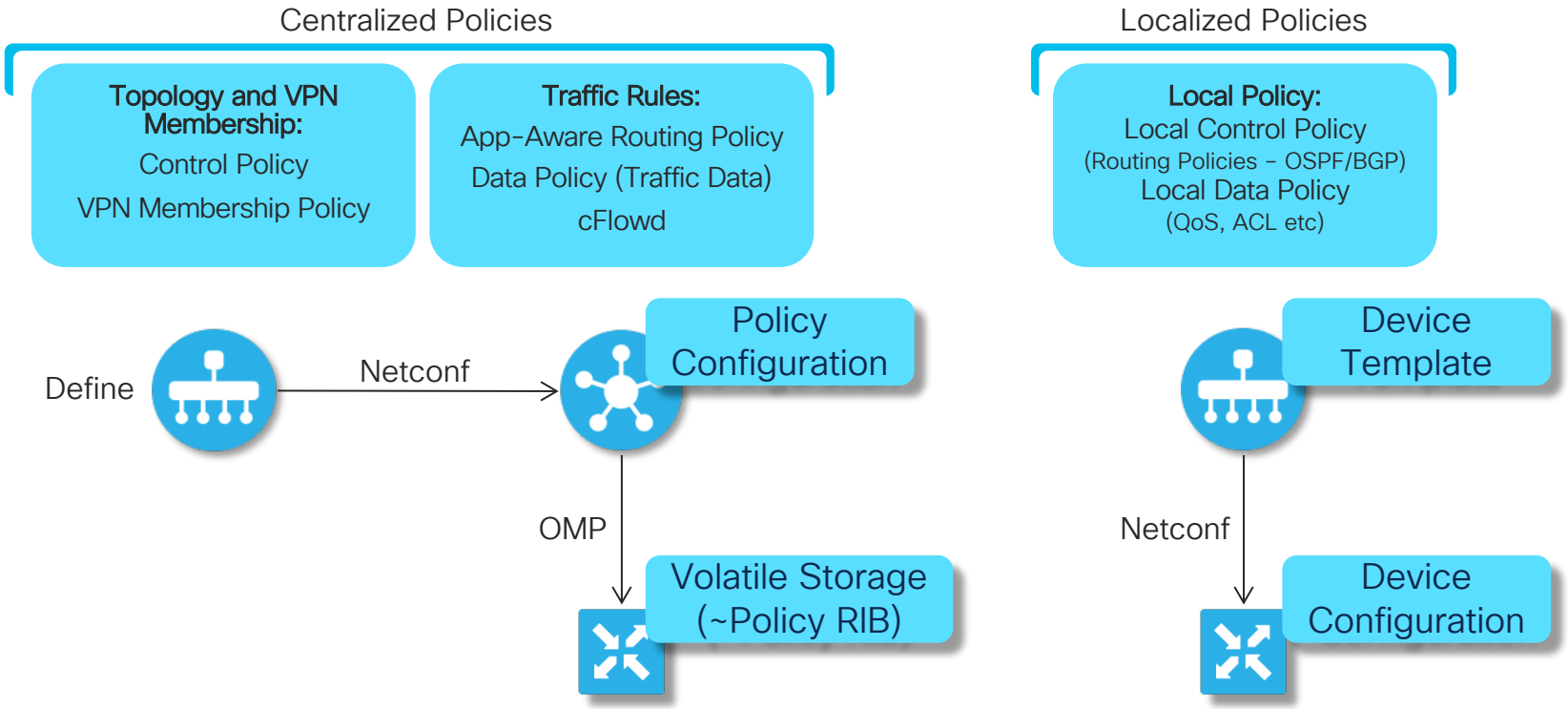
Cisco SD-WAN Terminology

- OMP – Overlay Management Protocol
  - Dynamic Routing Protocol managing the Overlay domain
  - Integrated mechanism for distribution Routing, Encryption and Policies
- Site-ID – Identifies the Source Location of an advertised prefix
  - Configured on every WAN Edge, vSmart and vManage
  - Does not have to be unique, but then assumes same location
  - Required configuration for OMP and TLOC to be brought up
- System-IP – Unique identifier of an OMP Endpoint
  - 32 Bit dot decimal notation (an IPv4 Address)
  - Logically a VPN 0 Loopback Interface, referred to as “system”
  - The system interface is the termination point for OMP

Introduction to the Cisco SD-WAN Policy Framework

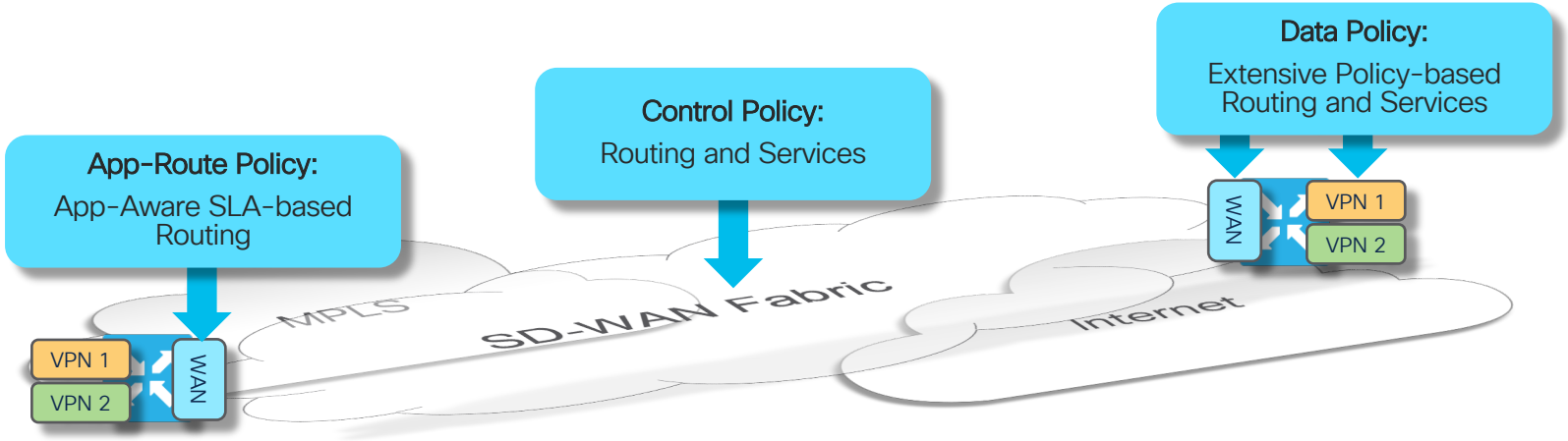
Cisco SD-WAN Policy Architecture

Policy Categories



Cisco SD-WAN Policy Architecture

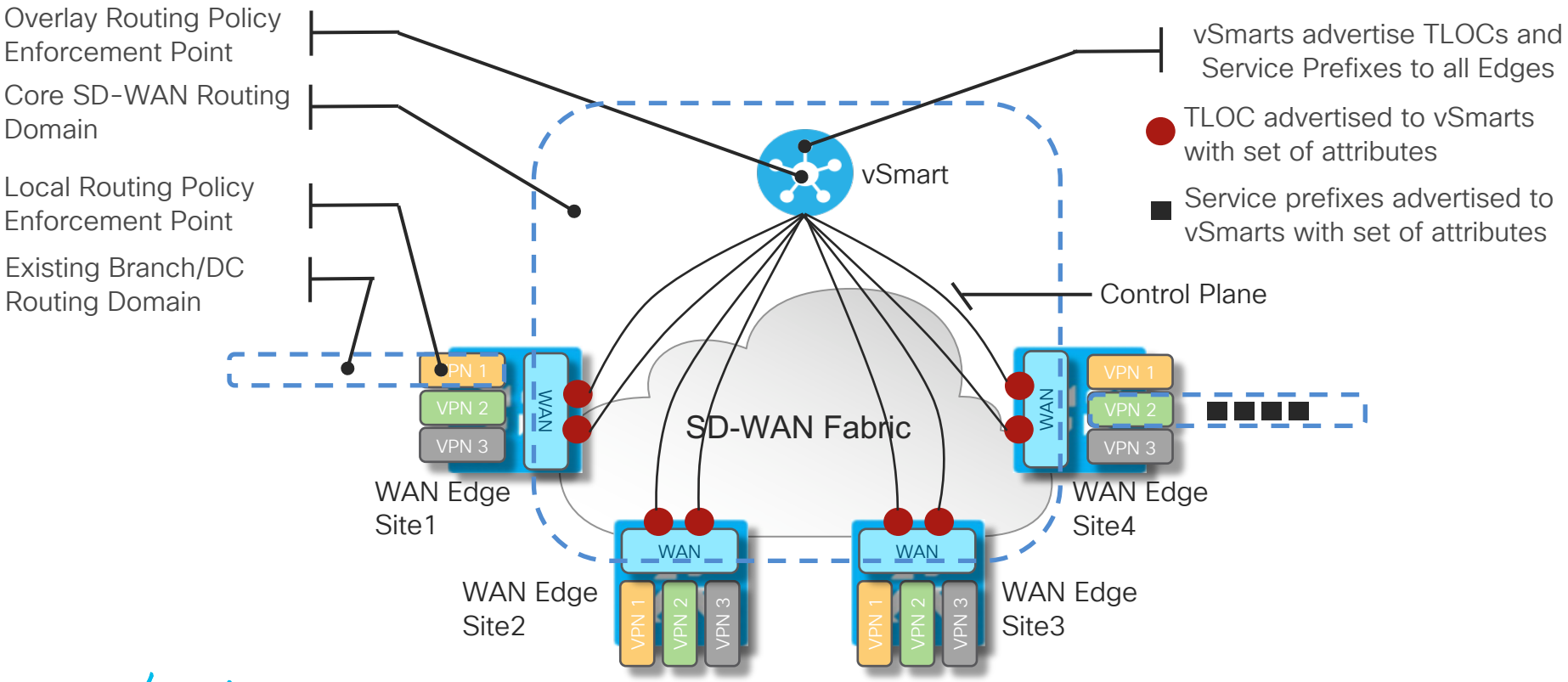
Suite of Policies to address different functional domains



- Control Policies are applied at vSmart: Tailors routing information advertised to WAN endpoints
- App-Route Policies are applied at WAN Edge: SLA-driven path selection for applications
- Data Policies are applied at WAN Edge: Extensive Policy driven routing

Cisco SD-WAN Overlay Routing

Multi-domain Routing Fabric



Overlay Management Protocol

High Level Description

- Path Vector Routing Protocol specifically designed for overlay networks
- Natively Multiprotocol, Multipath and VPN/Segment Aware
- Peer Auto-discovery w/ Zero line config for basic operation
- Inherent Route Target Constraint Capability
- Automatic Distribution of targeted local routing
- Overlay and Legacy Domain Loop Avoidance capabilities
- Reliable and Secure Transport (SSL)
- Broad Attribute Support
  - Preference
  - Identification
  - Legacy Source Protocol Information
- Consistent Routing and Encryption Synchronization
- Multi-domain capable

Overlay Management Protocol

Distribution of Routing Information for Topology-driven Routing

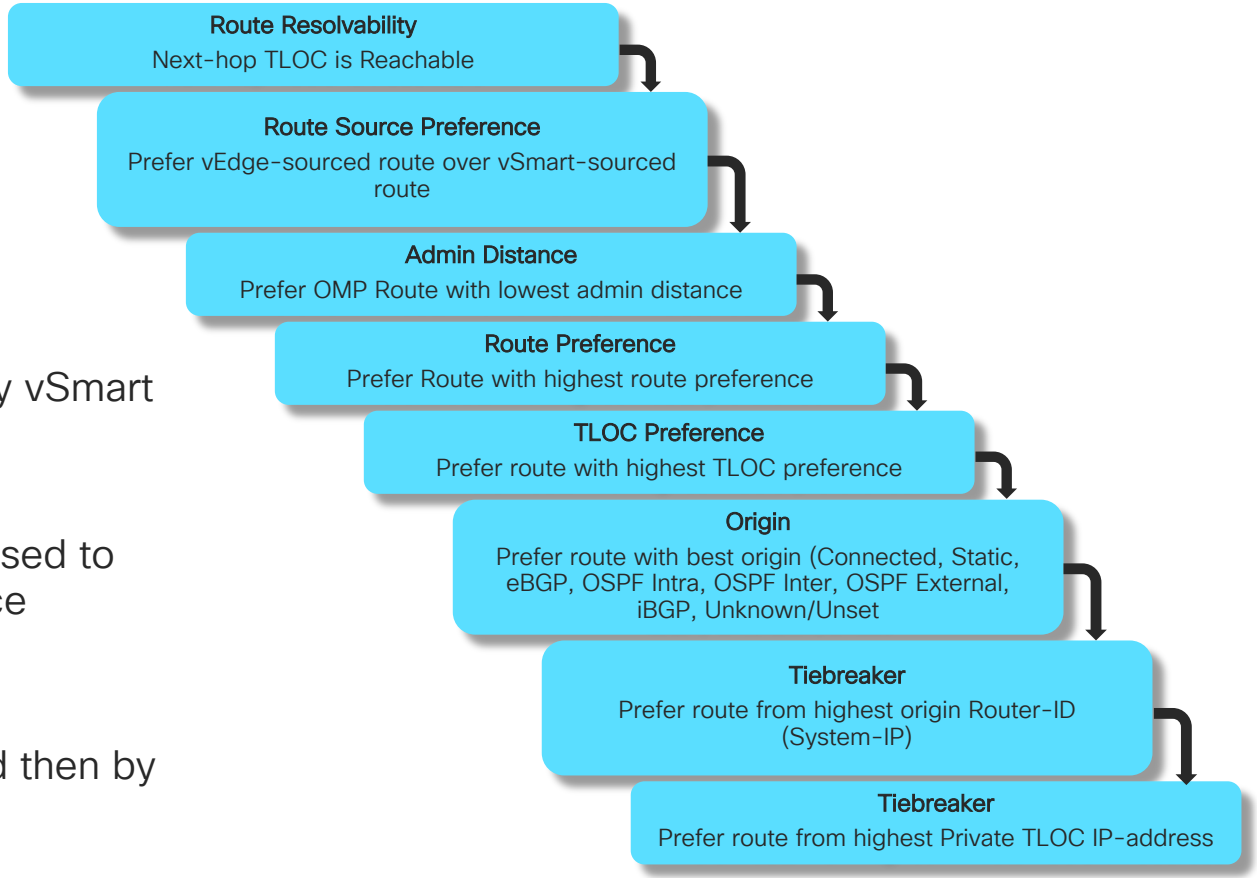
vRoutes	TLOCs	Services	Policies
Branch Routing into Overlay Routing + Attributes	WAN Attachment: Private IP/Public IP Color / Encap Encryption Keys + Attributes	Services: Type of Service Location (TLOC) Forwarding Information	Data Policy App-Route Policy VPN Membership cFlowd Template

Distribution of Routing Information and Policies subject to endpoint push

Updates sent only on changes – Routing engine operates as with existing protocols (BGP)

Overlay Management Protocol

Path Selection



- Default: 4 paths advertised by vSmart

```
omp
  Send-path-limit [1-16]
```

- Backup routes can be advertised to vEdges for faster convergence

```
omp
  Send-backup-paths
```

- Origin by Admin Distance and then by Protocol Cost / Metric

Building, Applying and Processing SD-WAN Policies

Construction of SD-WAN Policies

Policy Building Blocks

Lists

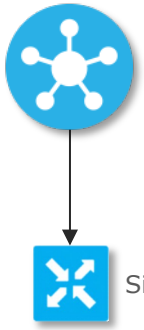
- Application
- Color
- Data Prefix
- Policer
- Prefix
- Site
- SLA Class
- TLOC
- VPN

Policy

```
Policy Type

Policy Sequence 1
Match <route | tloc | Application>
Action <Accept | Reject | set >

Policy Sequence 2
Match <route | tloc | Application>
Action <Accept | Reject | set >

Default Action
<Accept | Reject>
```

Apply Policy

```
Site-List

Policy <type> <name>
Direction (if applicable)
```



Cisco SD-WAN Policy Orchestration Process

1 vManage GUI – Policy Orchestration

Control Policy: Routing and Services

App-Route Policy: App-Aware SLA-based Routing

Data Policy: Extensive Policy-based Routing and Services

Combine and Apply per Site

2 vSmart controller – Policy Enforcement/Advertisement

Execute Control Policy

Advertise AAR/Data Policies to Sites

3 WAN Edge router – Policy Enforcement

Execute AAR and Data Policy as received

Dynamic Routing and Policies Combine to dictate behavior

Service Side

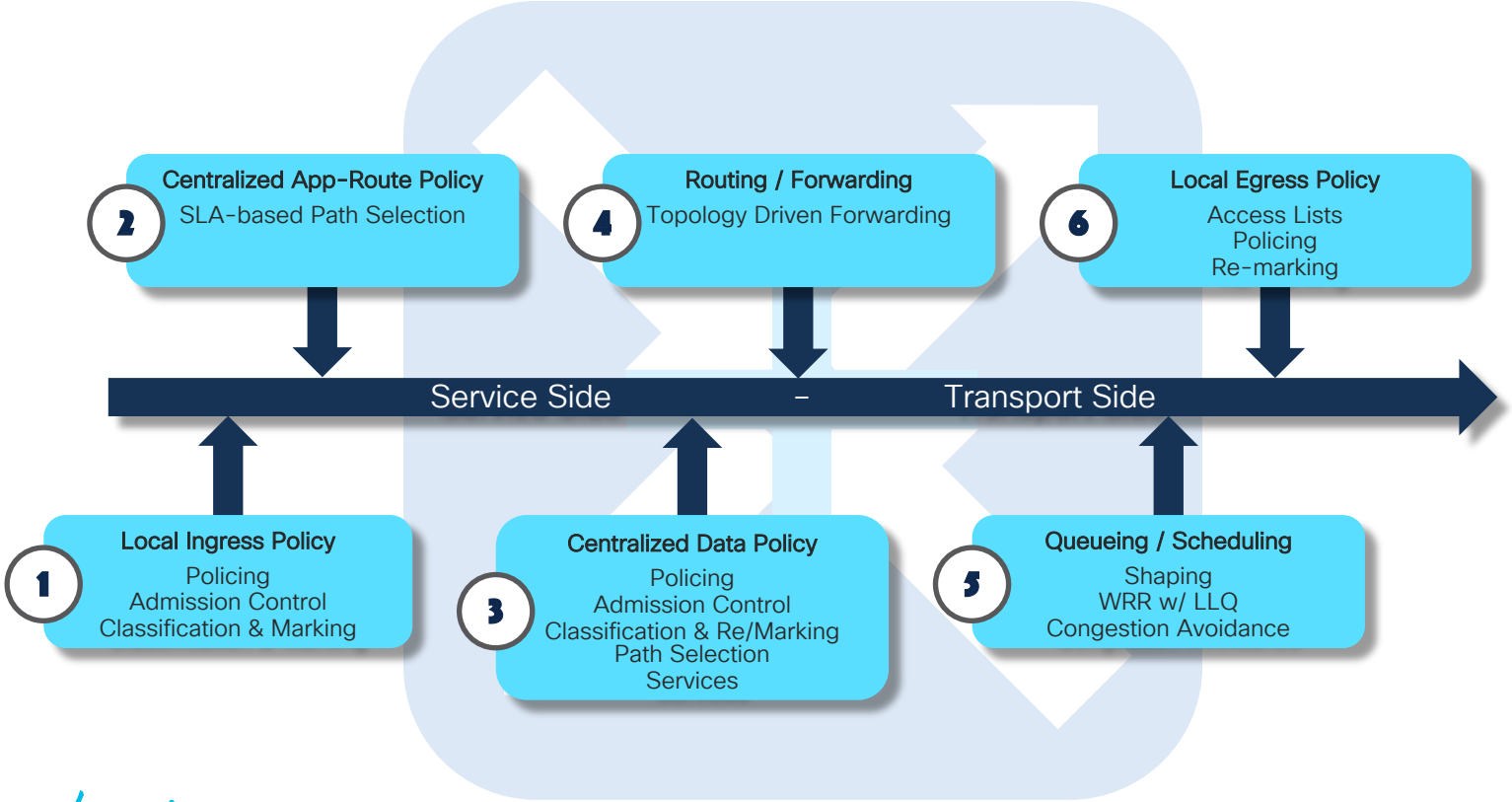
Processing Policies

Policy Processing Logic

- Policies are processed sequentially. Order is important!
- When a match occurs, the matched entity is subject to the configured action of the sequence and is then no longer subject to continued processing.
- Entity not matched in a sequence is subject to default action for the policy.
- Any node will make use of any and all available routing information
- In a multi-vSmart deployment, every vSmart acts independently to disseminate information to other vSmarts and vEdges
- vManage acts to ensure all vSmarts are synchronized

Cisco SD-WAN Policy Execution

Topology-driven routing and Policy execution chain

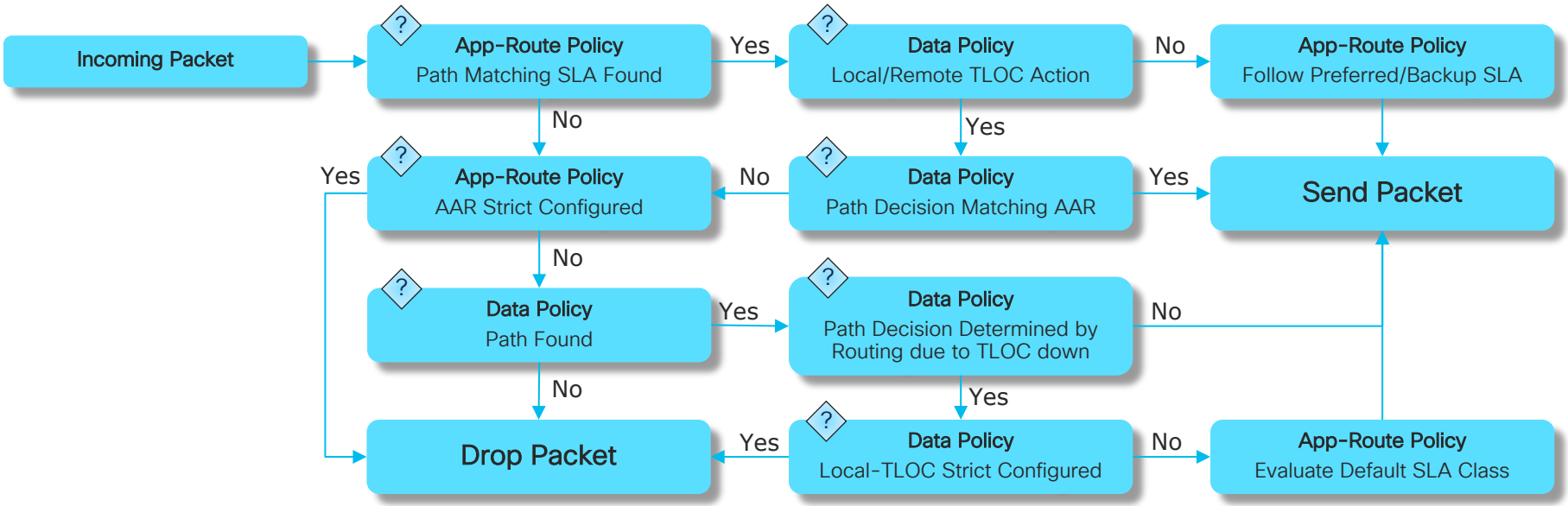


App-Aware Routing and Data Policy Overlap

Policy Processing when packet is subject to match in both policies

Guiding Principle:

Data Policy Makes Final Decision with Consideration for AAR SLA Match



Policy Management
Ensuring Intended End-to-End Policy Application

- vManage
- vSmart
  - Policy Configuration section

    `show running-config policy`
  - Apply-policy configuration section

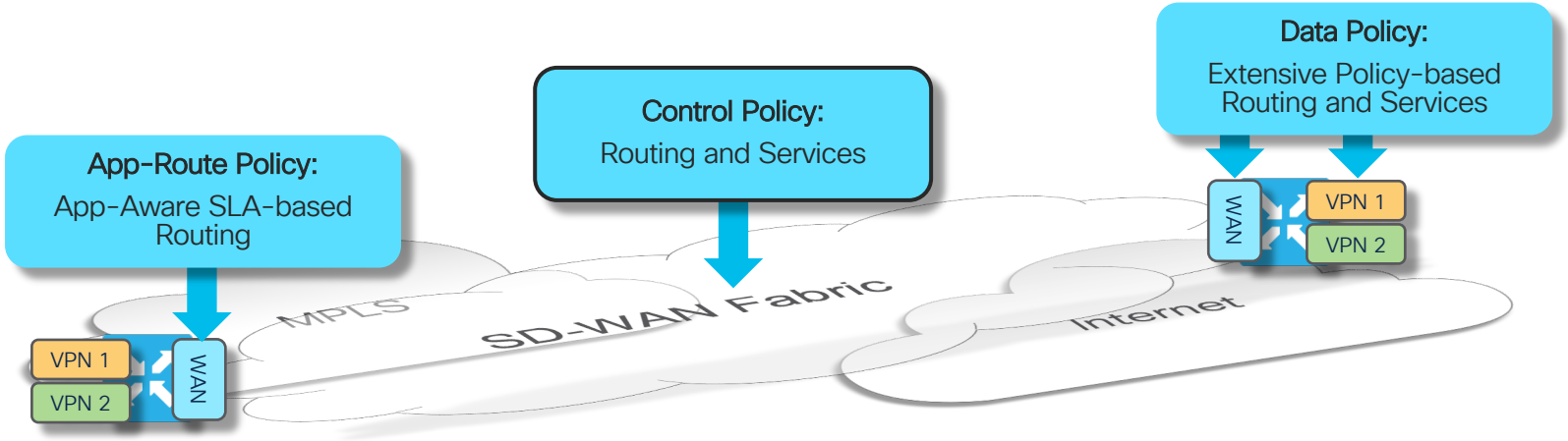
    `show running-config apply-policy`
- WAN Edge
  - View policy as received from vSmart via OMP

    `Show policy from vsmart`

Policy Framework: Control Policies

Cisco SD-WAN Policy Architecture

Suite of Policies to address different functional domains



- Control Policies are applied at vSmart: Tailors routing information advertised to WAN endpoints
- App-Route Policies are applied at WAN Edge: SLA-driven path selection for applications
- Data Policies are applied at WAN Edge: Extensive Policy driven routing

Control Policies

Overlay Management Protocol Routing Policies

- Control policies are applied and executed on vSmart to influence routing in the Overlay domain
- Control policies filter or manipulate OMP Routing information to:
  - Enable services
  - Influence path selection
- Control Policies controls the following services:
  - Service Chaining
  - Traffic Engineering
  - Extranet VPNs
  - Service and Path affinity
  - Arbitrary VPN Topologies
  - and more …
- The Control Policy is one of the most powerful tools in the Cisco SD-WAN toolbox

Control Policies

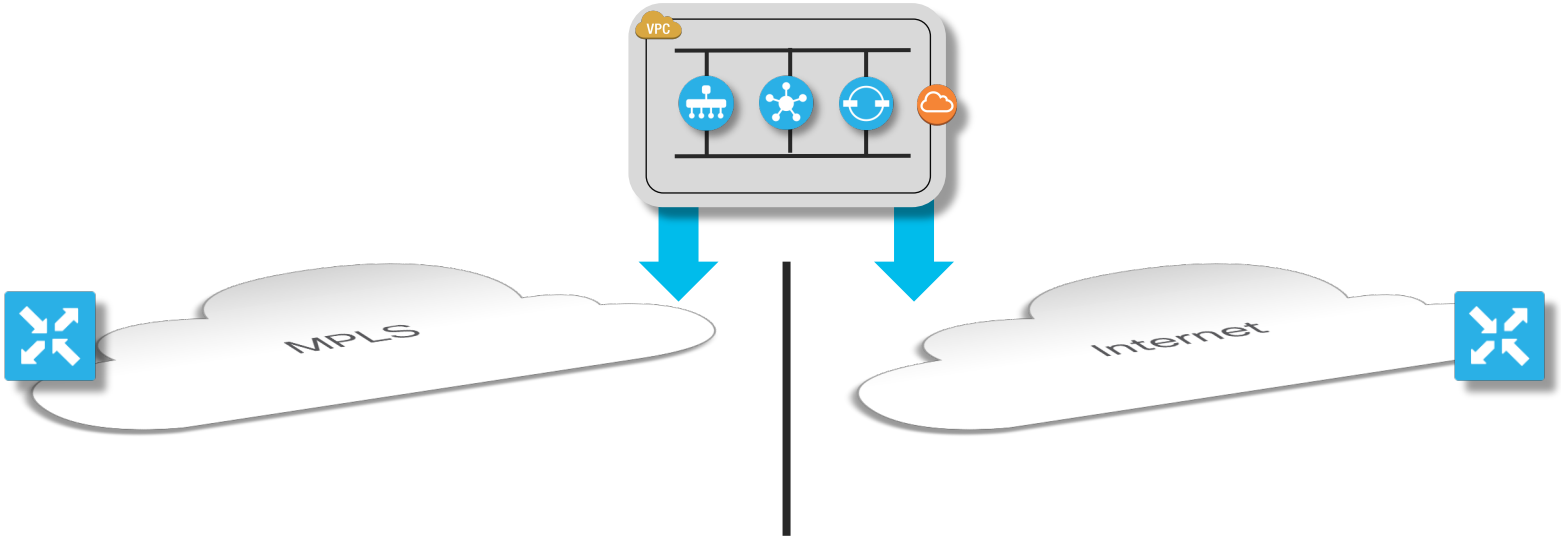
Policy Structure

```
control-policy <name>
  sequence <n>
   match tloc
    carrier <carrier>
    color <color>
    color-list <name>
    domain-id <domain-id> - Not Supported
    group-id <group-id>
    omp-tag <tag>
    originator <system-ip>
    preference <preference>
    site-id <site-id>
    site-list <name>
    tloc <tloc>
    tloc-list <name>
   !
   action accept
    set
     omp-tag <tag>
     preference <preference>
    !
   !
  !
  default-action accept
 !
```

```
control-policy <name>
  sequence <n>
   match route
    color <color>
    color-list <name>
    ipv6-prefix-list <name>
    omp-tag <tag>
    origin <protocol>
    originator <system-ip>
    preference <preference>
    prefix-list <name>
    site-id <site-id>
    site-list <name>
    tloc <tloc>
    tloc-list <name>
    vpn <vpn-id>
    vpn-list <name>
   !
   action accept
    export-to <vpn> | vpn-list
    set
     omp-tag <tag>
     preference <preference>
     service <service-type>
     tloc <tloc>
     tloc-action <action>
     tloc-list <name>
    !
   !
  !
  default-action accept
 !
```

Control Policy Case #1

Interconnecting Dis-contiguous Data Planes

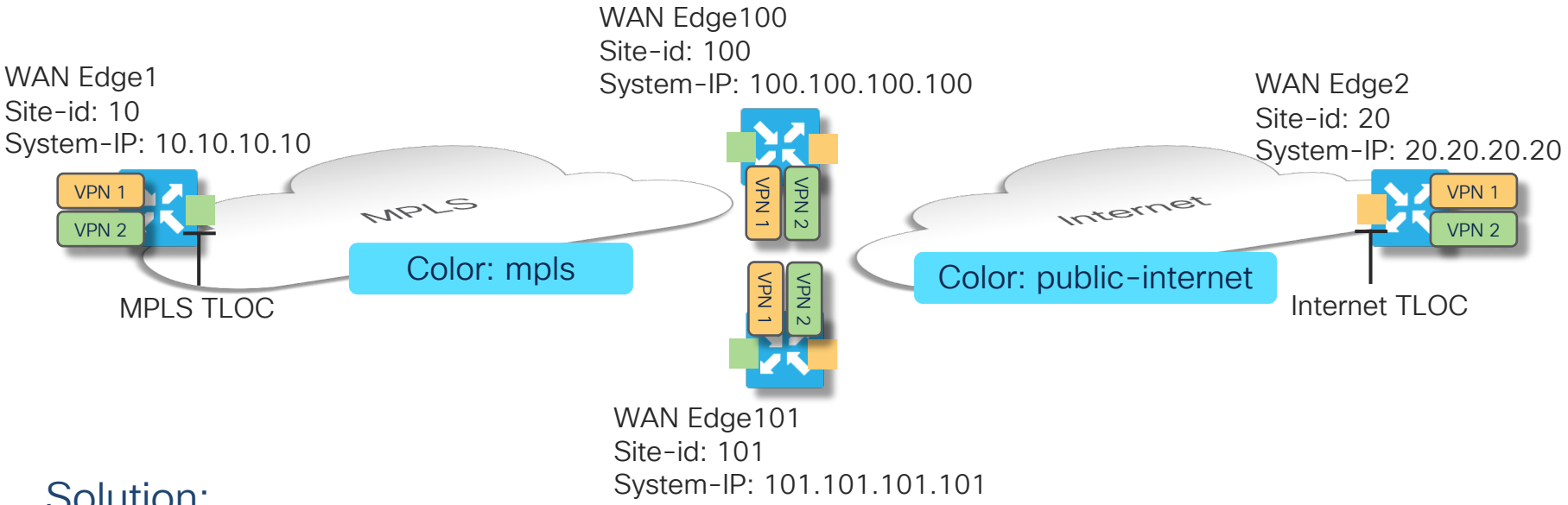


Problem:

Overlay with a dis-contiguous data plane and endpoints need to communicate end-to-end

Control Policy Case #1

Interconnecting Dis-contiguous Data Planes



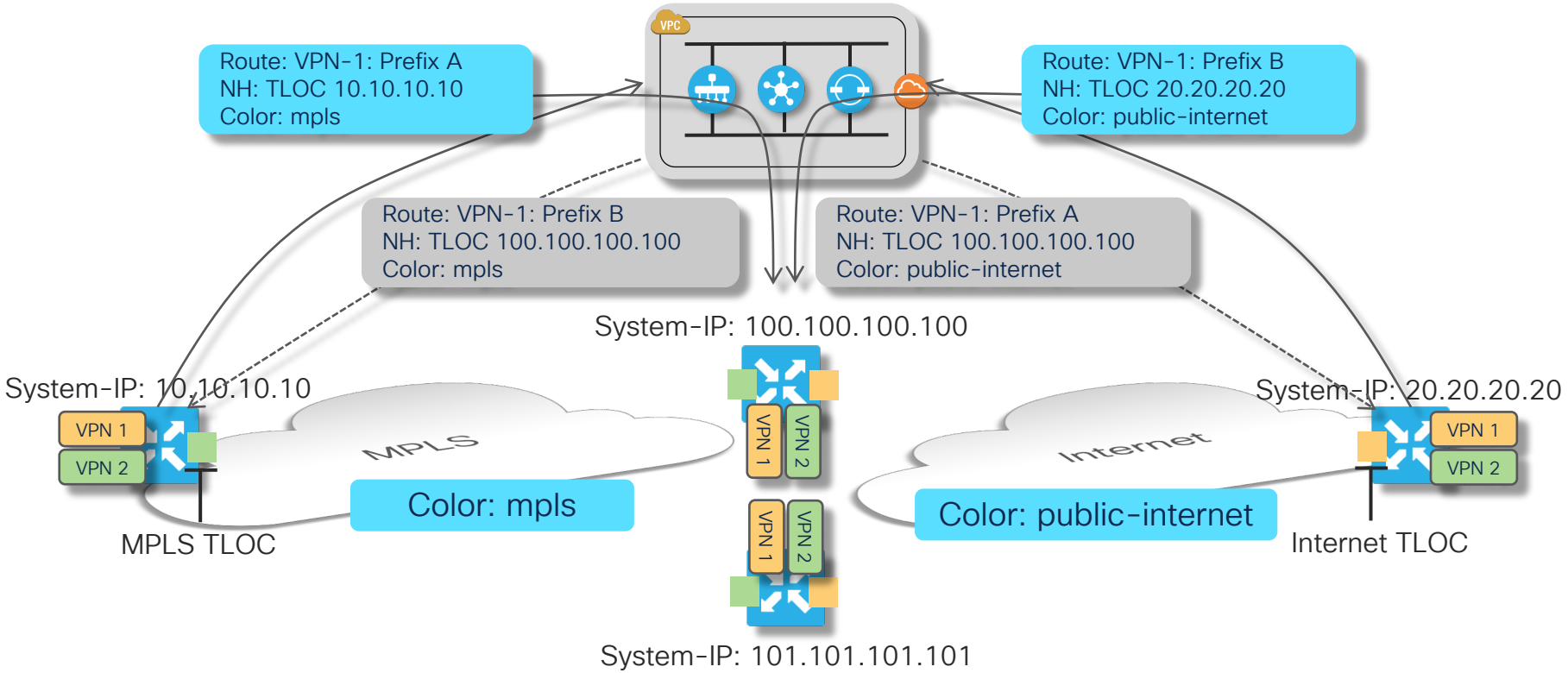
Solution:

Identify one or more multi-homed sites to bridge the data plane gap and act as gateways

Use a control policy to enable distribution of routing information between domains enabling gateway-supported paths

Control Policy Case #1

Interconnecting Dis-contiguous Data Planes



Control Policy Case #1

Interconnecting Dis-contiguous Data Planes

For Your Reference

1 Define Gateway TLOC-lists

```
policy
 lists
  tloc-list internet-gateways
   tloc 100.100.100.100 color mpls encap ipsec
   tloc 101.101.101.101 color mpls encap ipsec
  !
  tloc-list mpls-gateways
   tloc 100.100.100.100 color public-internet encap ipsec
   tloc 101.101.101.101 color public-internet encap ipsec
  !
  site-list internet-sites
   site-id 20
  !
  site-list mpls-sites
   site-id 10
```

2 Declare Target Sites

3 Define the Control Policies

```
control-policy announce-internet-sites
  sequence 10
   match route
    site-list internet-sites
   !
   action accept
    set
     tloc-list internet-gateways
    !
   !
  !
  default-action accept
 !
 control-policy announce-mpls-sites
  sequence 10
   match route
    site-list mpls-sites
   !
   action accept
    set
     tloc-list mpls-gateways
    !
   !
  !
  default-action accept
 !
!
```

```
apply-policy
 site-list internet-sites
  control-policy announce-mpls-sites out
 !
 site-list mpls-sites
  control-policy announce-internet-sites out
 !
!
```

4 Apply Policies to the target site-lists

Wait...
We're doing what?

Dis-contiguous Data Planes

TLOC Distribution and State – No Policy Applied

Color: public-internet

Color: mpls

OMP State: C=Chosen, I=Installed, R=Resolved, Red=Redistributed, Inv=Invalid, U=Unreachable

```
vSmart# show omp tlocs
ADDRESS                                                    BFD
FAMILY   TLOC IP          COLOR            STATUS        STATUS
-----------------------------------------------------------------
ipv4     10.10.10.10      mpls             C,I,R         -
         20.20.20.20      public-internet  C,I,R         -
         100.100.100.100  mpls             C,I,R         -
         100.100.100.100  public-internet  C,I,R         -
         101.101.101.101  mpls             C,I,R         -
         101.101.101.101  public-internet  C,I,R         -
```

WAN Edge1
Site-id: 10
System-IP: 10.10.10.10

VPN 1

```
WAN Edge1# show omp tlocs
ADDRESS                                                    BFD
FAMILY   TLOC IP          COLOR            STATUS        STATUS
-----------------------------------------------------------------
ipv4     10.10.10.10      mpls             C,Red,R       up
         20.20.20.20.     public-internet  C,I,R         down
         100.100.100.100  mpls             C,I,R         up
         100.100.100.100  public-internet  C,I,R         down
         101.101.101.101  mpls             C,I,R         up
         101.101.101.101  public-internet  C,I,R         down
```

WAN Edge2
Site-id: 20
System-IP: 20.20.20.20

VPN 1

```
WAN Edge2# show omp tlocs
ADDRESS                                                    BFD
FAMILY   TLOC IP          COLOR            STATUS        STATUS
-----------------------------------------------------------------
ipv4     10.10.10.10      mpls             C,I,R         down
         20.20.20.20.     public-internet  C,Red,R       up
         100.100.100.100  mpls             C,I,R         down
         100.100.100.100  public-internet  C,I,R         up
         101.101.101.101  mpls             C,I,R         down
         101.101.101.101  public-internet  C,I,R         up
```

```
WAN Edge100# show omp tlocs
ADDRESS                                                    BFD
FAMILY   TLOC IP          COLOR            STATUS        STATUS
-----------------------------------------------------------------
ipv4     10.10.10.10      mpls             C,I,R         up
         20.20.20.20.     public-internet  C,I,R         up
         100.100.100.100  mpls             C,Red,R       up
         100.100.100.100  public-internet  C,Red,R       up
         101.101.101.101  mpls             C,I,R         up
         101.101.101.101  public-internet  C,I,R         up
```

VPN 1 VPN 2

Site-id: 100
System-IP: 100.100.100.100

```
WAN Edge101# show omp tlocs
ADDRESS                                                    BFD
FAMILY   TLOC IP          COLOR            STATUS        STATUS
-----------------------------------------------------------------
ipv4     10.10.10.10      mpls             C,I,R         up
         20.20.20.20.     public-internet  C,I,R         up
         100.100.100.100  mpls             C,I,R         up
         100.100.100.100  public-internet  C,I,R.        up
         101.101.101.101  mpls             C,Red,R       up
         101.101.101.101  public-internet  C,Red,R       up
```

VPN 1 VPN 2

Site-id: 101
System-IP: 101.101.101.101

Dis-contiguous Data Planes

vRoute Distribution and State – No Policy Applied

Color: public-internet

Color: mpls

OMP State: C=Chosen, I=Installed, R=Resolved, Red=Redistributed, Inv=Invalid, U=Unreachable

```
vSmart# show omp routes
VPN PREFIX        STATUS  TLOC IP         COLOR
-------------------------------------------------------
1   10.1.1.0/24   C,R     10.10.10.10     mpls
    20.1.1.0/24   C,R     20.20.20.20     public-internet
    100.1.1.0/24  C,R     100.100.100.100 mpls
                  C,R     100.100.100.100 public-internet
    101.1.1.0/24  C,R     101.101.101.101 mpls
                  C,R     101.101.101.101 public-internet
```

WAN Edge1
Site-id: 10
System-IP: 10.10.10.10

VPN 1

```
WAN Edge1# show omp routes
VPN PREFIX        STATUS    TLOC IP         COLOR
-----------------------------------------------------------
1   10.1.1.0/24   C,Red,R   10.10.10.10     mpls
    20.1.1.0/24   Inv,U     20.20.20.20     public-internet
    100.1.1.0/24  C,I,R     100.100.100.100 mpls
                  Inv,U     100.100.100.100 public-internet
    101.1.1.0/24  C,I,R     101.101.101.101 mpls
                  Inv,U     101.101.101.101 public-internet
```

WAN Edge2
Site-id: 20
System-IP: 20.20.20.20

VPN 1

```
WAN Edge2# show omp routes
VPN PREFIX        STATUS    TLOC IP         COLOR
-----------------------------------------------------------
1   10.1.1.0/24   Inv,U     10.10.10.10     mpls
    20.1.1.0/24   C,Red,R   20.20.20.20     public-internet
    100.1.1.0/24  Inv,U     100.100.100.100 mpls
                  C,I,R     100.100.100.100 public-internet
    101.1.1.0/24  Inv,U     101.101.101.101 mpls
                  C,I,R     101.101.101.101 public-internet
```

```
WAN Edge100# show omp routes
VPN PREFIX        STATUS    TLOC IP         COLOR
-----------------------------------------------------------
1   10.1.1.0/24   C,I,R     10.10.10.10     mpls
    20.1.1.0/24   C,I,R     20.20.20.20     public-internet
    100.1.1.0/24  C,Red,R   100.100.100.100 mpls
                  C,Red,R   100.100.100.100 public-internet
    101.1.1.0/24  C,I,R     101.101.101.101 mpls
                  C,I,R     101.101.101.101 public-internet
```

VPN 1 VPN 2

WAN Edge100
Site-id: 100
System-IP: 100.100.100.100
VPN 1 Pfx: 100.1.1.0/24

```
WAN Edge101# show omp routes
VPN PREFIX        STATUS    TLOC IP         COLOR
-----------------------------------------------------------
1   10.1.1.0/24   C,I,R     10.10.10.10     mpls
    20.1.1.0/24   C,I,R     20.20.20.20     public-internet
    100.1.1.0/24  C,I,R     100.100.100.100 mpls
                  C,I,R     100.100.100.100 public-internet
    101.1.1.0/24  C,Red,R   101.101.101.101 mpls
                  C,Red,R   101.101.101.101 public-internet
```

VPN 1 VPN 2

WAN Edge101
Site-id: 101
System-IP: 101.101.101.101
VPN 1 Pfx: 101.1.1.0/24

Dis-contiguous Data Planes

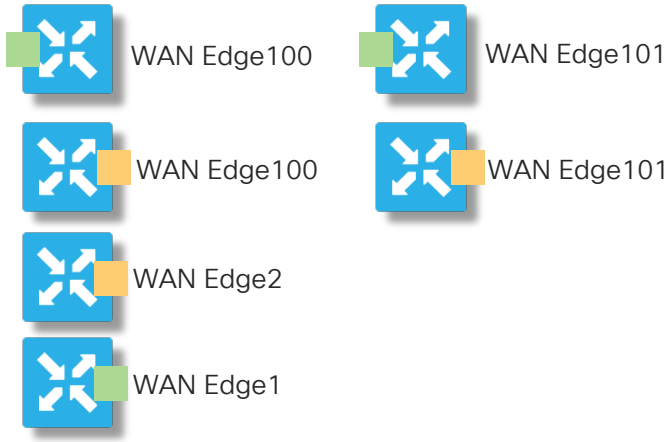
Policy Components and Application Direction

Color: public-internet

Color: mpls

OMP State: C=Chosen, I=Installed, R=Resolved, Red=Redistributed, Inv=Invalid, U=Unreachable

```
policy
 lists
  tloc-list internet-gateways
   tloc 100.100.100.100 color mpls encap ipsec
   tloc 101.101.101.101 color mpls encap ipsec
  !
  tloc-list mpls-gateways
   tloc 100.100.100.100 color public-internet encap ipsec
   tloc 101.101.101.101 color public-internet encap ipsec
  !
  site-list internet-sites
   site-id 20
  !
  site-list mpls-sites
   site-id 10
```




```
apply-policy
 site-list internet-sites
  control-policy announce-mpls-sites out
 !
 site-list mpls-sites
  control-policy announce-internet-sites out
 !
!
```

Dis-contiguous Data Planes

Policy Application and Outgoing Advertisement – Site 20

Color: public-internet

Color: mpls

OMP State: C=Chosen, I=Installed, R=Resolved, Red=Redistributed, Inv=Invalid, U=Unreachable

```
control-policy announce-mpls-sites
 sequence 10
  match route
   site-list mpls-sites
  !
  action accept
   set
    tloc-list mpls-gateways
   !
  !
 !
 default-action accept
!
!
```

WAN Edge2
Site-id: 20
System-IP: 20.20.20.20


```
vSmart# show omp tlocs
ADDRESS                                  BFD
FAMILY   TLOC IP          STATUS         STATUS
-----------------------------------------------
ipv4     10.10.10.10      C,I,R          -
         20.20.20.20.     C,I,R          -
         100.100.100.100  C,I,R          -
         101.101.101.101  C,I,R          -
```

```
WAN Edge2# show omp tlocs
ADDRESS                                  BFD
FAMILY   TLOC IP          STATUS         STATUS
-----------------------------------------------
ipv4     10.10.10.10      C,I,R          down
         20.20.20.20.     C,Red,R        up
         100.100.100.100  C,I,R          up
         101.101.101.101  C,I,R          up
```

```
vSmart# show omp routes
VPN PREFIX          STATUS   TLOC IP          COLOR
-----------------------------------------------------------
1   10.1.1.0/24     C,R      10.10.10.10      mpls
    20.1.1.0/24     C,R      20.20.20.20      public-internet
    100.1.1.0/24    C,R      100.100.100.100  mpls
                    C,R      100.100.100.100  public-internet
    101.1.1.0/24    C,R      101.101.101.101  mpls
                    C,R      101.101.101.101  public-internet
```

```
WAN Edge2# show omp routes
VPN PREFIX          STATUS   TLOC IP          COLOR
-----------------------------------------------------------
1   10.1.1.0/24     C,I,R    100.100.100.100  public-internet
                    C,I,R    101.101.101.101  public-internet
    20.1.1.0/24     C,Red,R  20.20.20.20      public-internet
    100.1.1.0/24    Inv,U    100.100.100.100  mpls
                    C,I,R    100.100.100.100  public-internet
    101.1.1.0/24    Inv,U    101.101.101.101  mpls
                    C,I,R    101.101.101.101  public-internet
```

Dis-contiguous Data Planes

Policy Application and Outgoing Advertisement – Site 10

Color: public-internet

Color: mpls

OMP State: C=Chosen, I=Installed, R=Resolved, Red=Redistributed, Inv=Invalid, U=Unreachable

```
control-policy announce-internet-sites
  sequence 10
   match route
    site-list internet-sites
   !
   action accept
    set
     tloc-list internet-gateways
    !
   !
  !
  default-action accept
 !
!
```

WAN Edge1
Site-id: 10
System-IP: 10.10.10.10


```
vSmart# show omp tlocs
ADDRESS                                    BFD
FAMILY   TLOC IP          STATUS           STATUS
-----------------------------------------------
ipv4     10.10.10.10      C,I,R            -
         20.20.20.20.     C,I,R            -
         100.100.100.100  C,I,R            -
         101.101.101.101  C,I,R            -
```

```
WAN Edge1# show omp tlocs
ADDRESS                                    BFD
FAMILY   TLOC IP          STATUS           STATUS
-----------------------------------------------
ipv4     10.10.10.10      C,Red,R          up
         20.20.20.20.     C,I,R            down
         100.100.100.100  C,I,R            up
         101.101.101.101  C,I,R            up
```

```
vSmart# show omp routes
VPN PREFIX          STATUS   TLOC IP          COLOR
-----------------------------------------------------------
1   10.1.1.0/24     C,R      10.10.10.10      mpls
    20.1.1.0/24     C,R      20.20.20.20      public-internet
    100.1.1.0/24    C,R      100.100.100.100  mpls
                    C,R      100.100.100.100  public-internet
    101.1.1.0/24    C,R      101.101.101.101  mpls
                    C,R      101.101.101.101  public-internet
```

```
WAN Edge1# show omp routes
VPN PREFIX          STATUS   TLOC IP          COLOR
-----------------------------------------------------------
1   10.1.1.0/24     C,Red,R  10.10.10.10      mpls
    20.1.1.0/24     C,I,R    100.100.100.100 mpls
                    C,I,R    101.101.101.101 mpls
    100.1.1.0/24    C,I,R    100.100.100.100 mpls
                    Inv,U    100.100.100.100 public-internet
    101.1.1.0/24    C,I,R    101.101.101.101 mpls
                    Inv,U    101.101.101.101 public-internet
```

Back on track

Control Policy Case #2

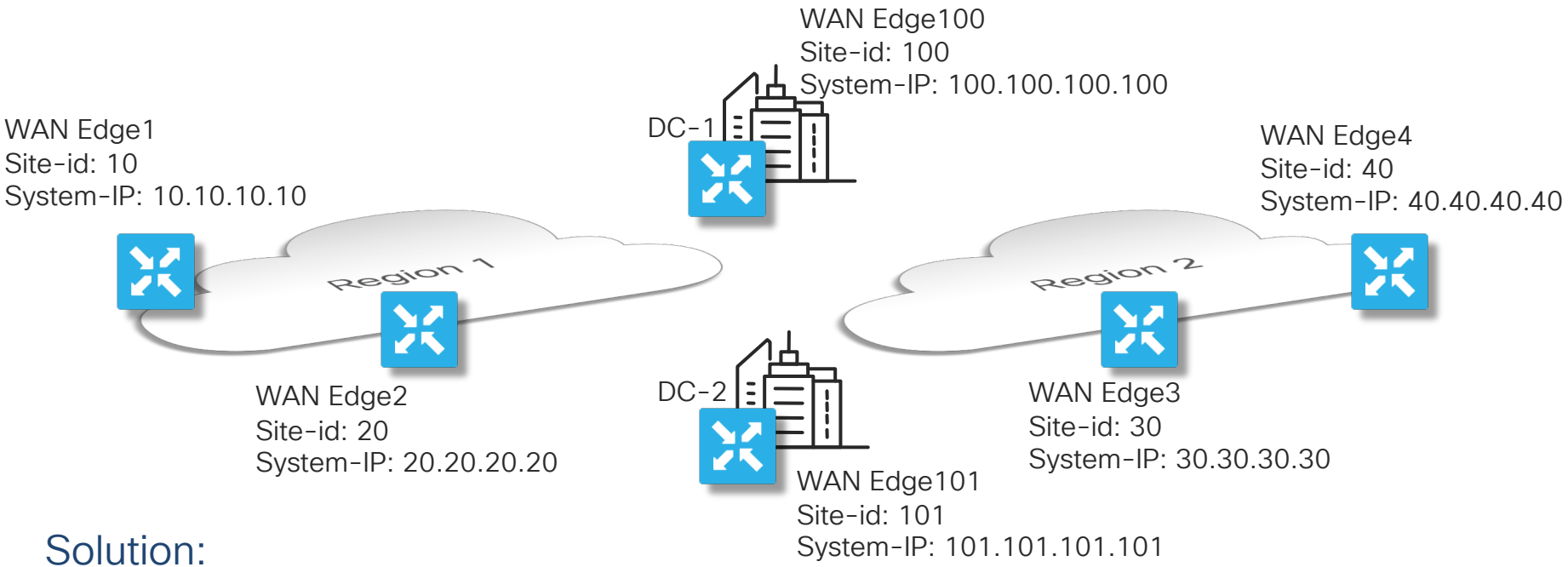
Network Resource (e.g. Data Center) Preference or Active/Backup

Problem:

Data Center access must be regionalized with neighboring DCs backing each other up

Control Policy Case #2

Network Resource (e.g. Data Center) Preference or Active/Backup



Solution:

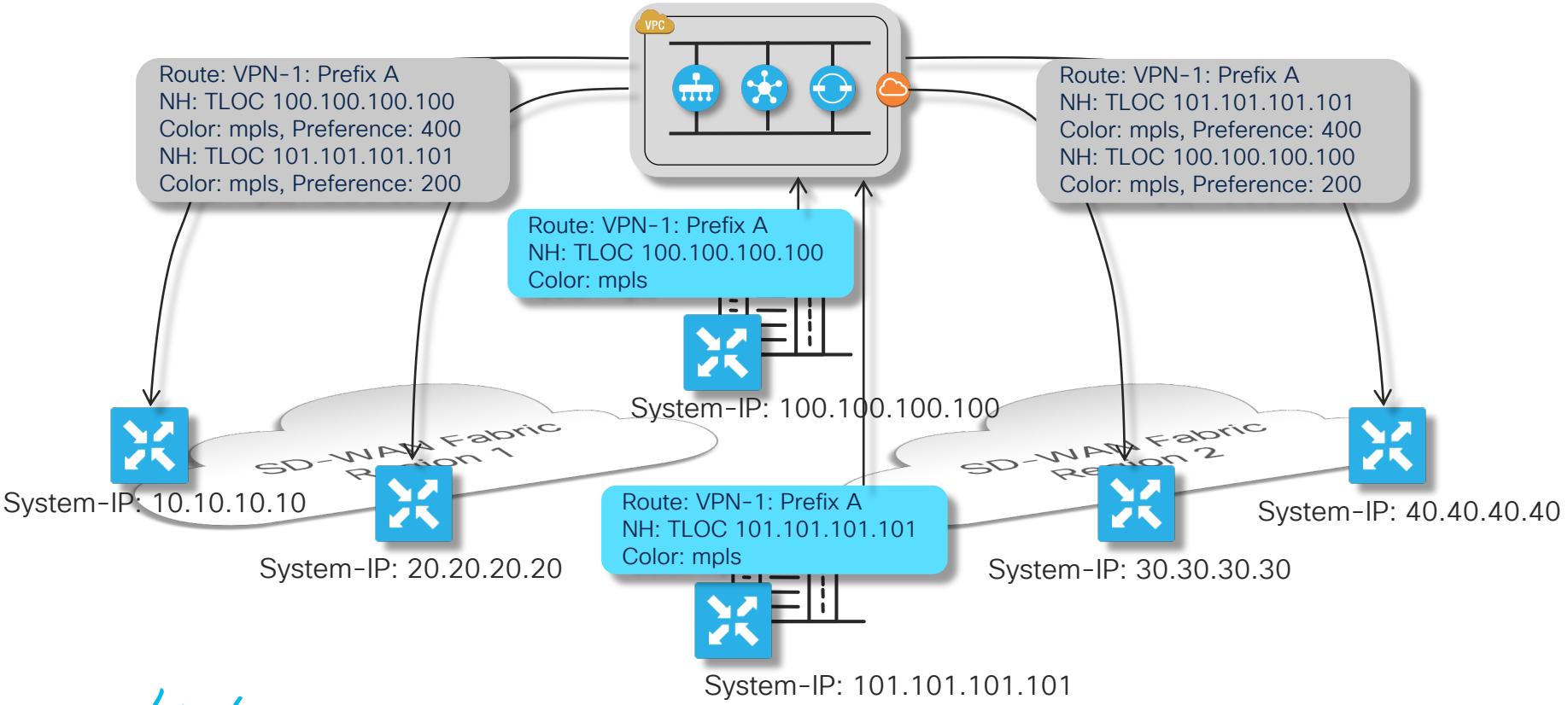
Identify regions by Site-Id and associate Primary and Backup DC locations with the regions

A control policy is used to make the associations and defining DC preference

Control Policy Case #2

Network Resource (e.g. Data Center) Preference or Active/Backup

Legend:
- Original Advertisement from Endpoint
- Un/Modified Advertisement from Controller



Control Policy Case #2

Network Resource (e.g. Data Center) Preference or Active/Backup

For Your Reference

1 Define Data Center TLOC-lists

```
policy
 lists
  tloc-list dc-preference-west
   tloc 100.100.100.100 color mpls encap ipsec preference 400
   tloc 101.101.101.101 color mpls encap ipsec preference 200
  !
  tloc-list dc-preference-east
   tloc 100.100.100.100 color mpls encap ipsec preference 200
   tloc 101.101.101.101 color mpls encap ipsec preference 400
  !
  site-list sites-region-west
   site-id 1-20
  !
  site-list sites-region-east
   site-id 21-40
  !
  site-list dc-sites
   site-id 100-101
```

2 Declare Regions

3 Declare Data Centers

```
apply-policy
 site-list sites-region-west
  control-policy adv-dc-preference-west out
 !
 site-list sites-region-east
  control-policy adv-dc-preference-east out
 !
!
```

5 Apply Policies to the target site-lists

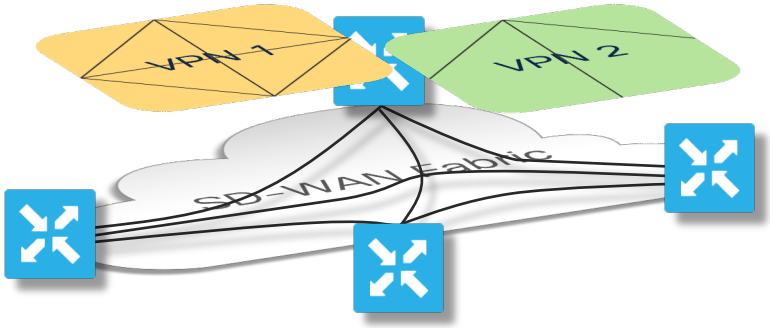
```
control-policy adv-dc-preference-west
  sequence 10
   match route
    site-list dc-sites
   !
   action accept
    set
     tloc-list dc-preference-west
    !
   !
  !
  default-action accept
 !
 control-policy adv-dc-preference-east
  sequence 10
   match route
    site-list dc-sites
   !
   action accept
    set
     tloc-list dc-preference-east
    !
   !
  !
  default-action accept
 !
!
```

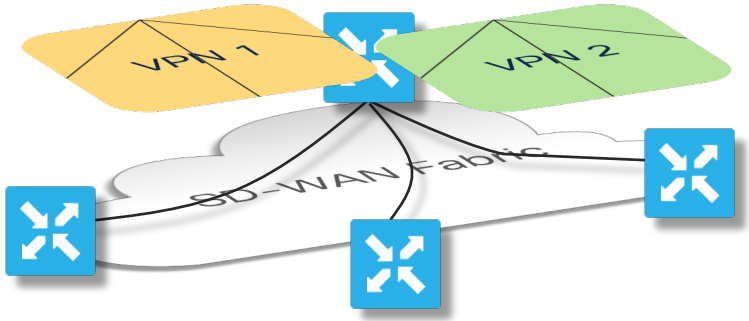
4 Define the Control Policies

Control Policy Case #3

Fabric Data Plane or VPN Plane Topologies

- Fabric Plane or Individual VPNs subject to specific topologies / connectivity models





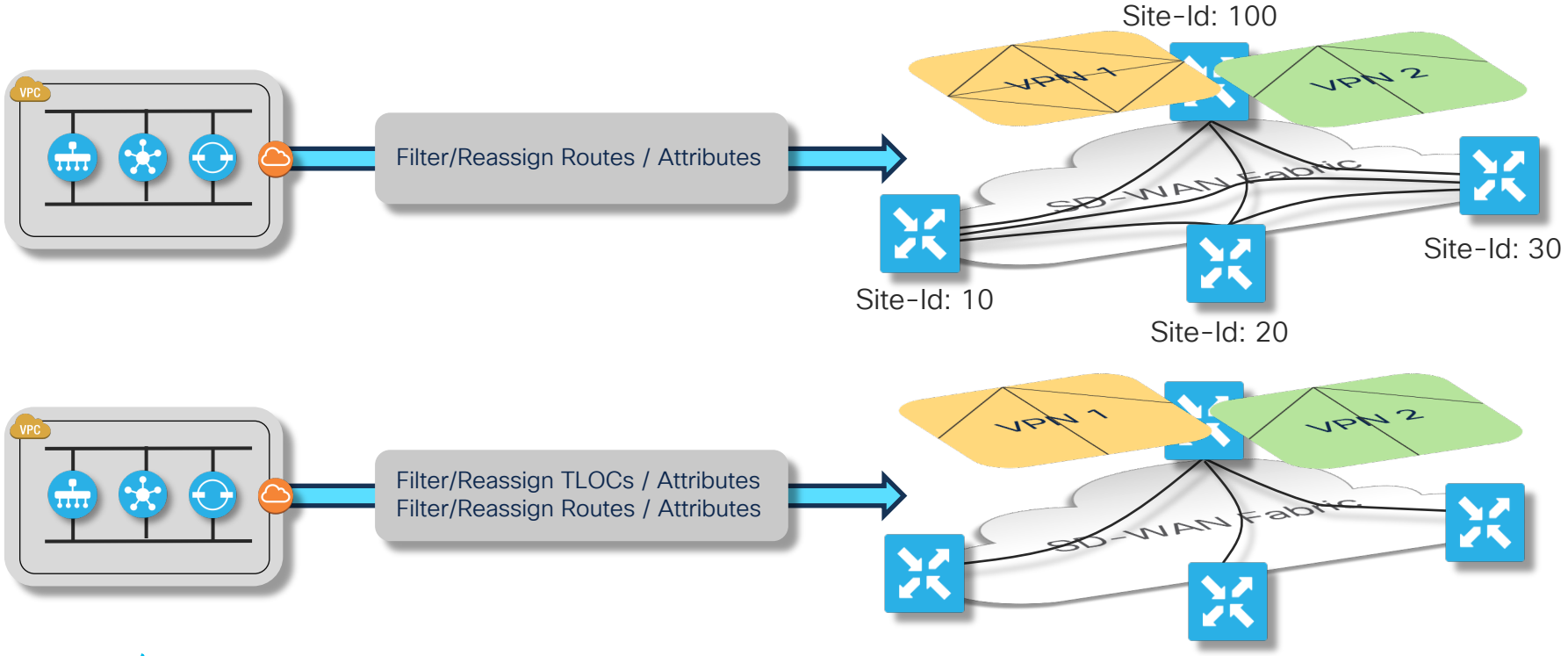
- Fully meshed fabric data plane
- Individual VPNs can use any topology

- Restricted fabric data plane
- Individual VPNs restricted to connectivity model used by underlying fabric

Control Policy Case #3

Fabric Data Plane or VPN Plane Topologies

- Fabric Plane or Individual VPNs subject to specific topologies / connectivity models



Control Policy Case #3

Fabric Data Plane and VPN Hub-and-Spoke Topologies

For Your Reference

1 Define Hub Site TLOC-list

```
policy
 lists
  tloc-list hub-site_tlocs
   tloc 1.1.1.1 color red encap ipsec preference 100
   tloc 2.2.2.2 color red encap ipsec preference 100
   tloc 3.3.3.3 color red encap ipsec
  !
  site-list branch_sites
   site-id 1000-2000
  !
  site-list hub_sites
   site-id 1-100
  !
 !
```

2 Declare Branches

3 Declare Hubs

4 Define the Control Policy

```
policy
 control-policy restricted_data_plane
  sequence 10
   match tloc
    site-list hub_sites
   !
   action accept
   !
  !
  sequence 20
   match route
    site-list branch_sites
   !
   action accept
    set
     tloc-list hub_site_tlocs
    !
   !
  !
  sequence 30
   match tloc
   !
   action reject
   !
  !
  default-action accept
```

Advertise Hub TLOCs

Branch Prefixes

Drop Branch TLOCs

```
apply-policy
 site-list branch_sites
  control-policy restricted_data_plane out
 !
!
```

5 Apply Policy to the target site-list

Control Policy Case #3

VPN 1 Full Mesh and VPN 2 Hub-and-Spoke Topologies

For Your Reference

Loose Hub-and-Spoke
Spokes communicate via hub(s)

```
policy
 lists
  vpn-list VPN2
   vpn 2
  !
site-list branch_sites
  site-id 100-200
  !
 !
 control-policy vpn_multi-topology
  sequence 10
   match route
    site-list branch_sites
    vpn-list  VPN2
   !
   action accept
    set
     tloc 1.1.1.1 color red
    !
   !
  !
  default-action accept
```

Branch Prefixes

Hub site TLOC

Strict Hub-and-Spoke
No spoke to spoke communication

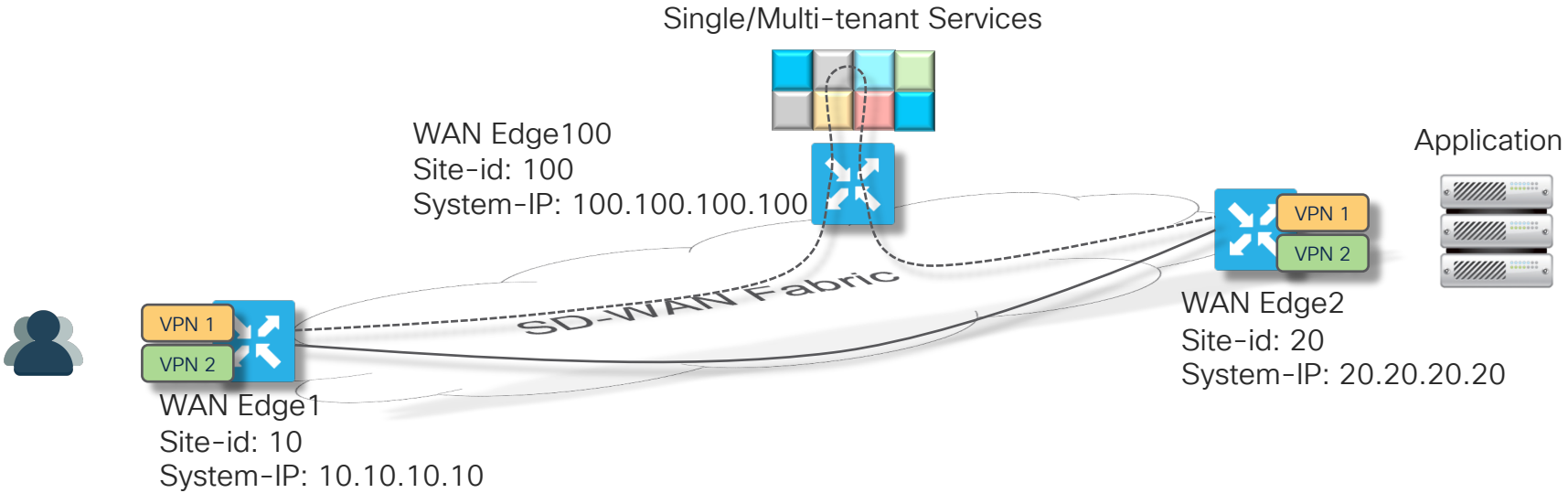
```
policy
 lists
  vpn-list VPN2
   vpn 2
  !
site-list hub_sites
  site-id 1-2
  !
 !
 control-policy vpn_multi-topology
  sequence 10
   match route
    site-list hub_sites
    vpn-list  VPN2
   !
   action accept
  !
  sequence 20
   match route
   !
   action reject
  !
  default-action accept
```

Advertise Hub Prefixes

Drop Branch Prefixes

Control Policy Case #4

Service Chaining of Centralized Services

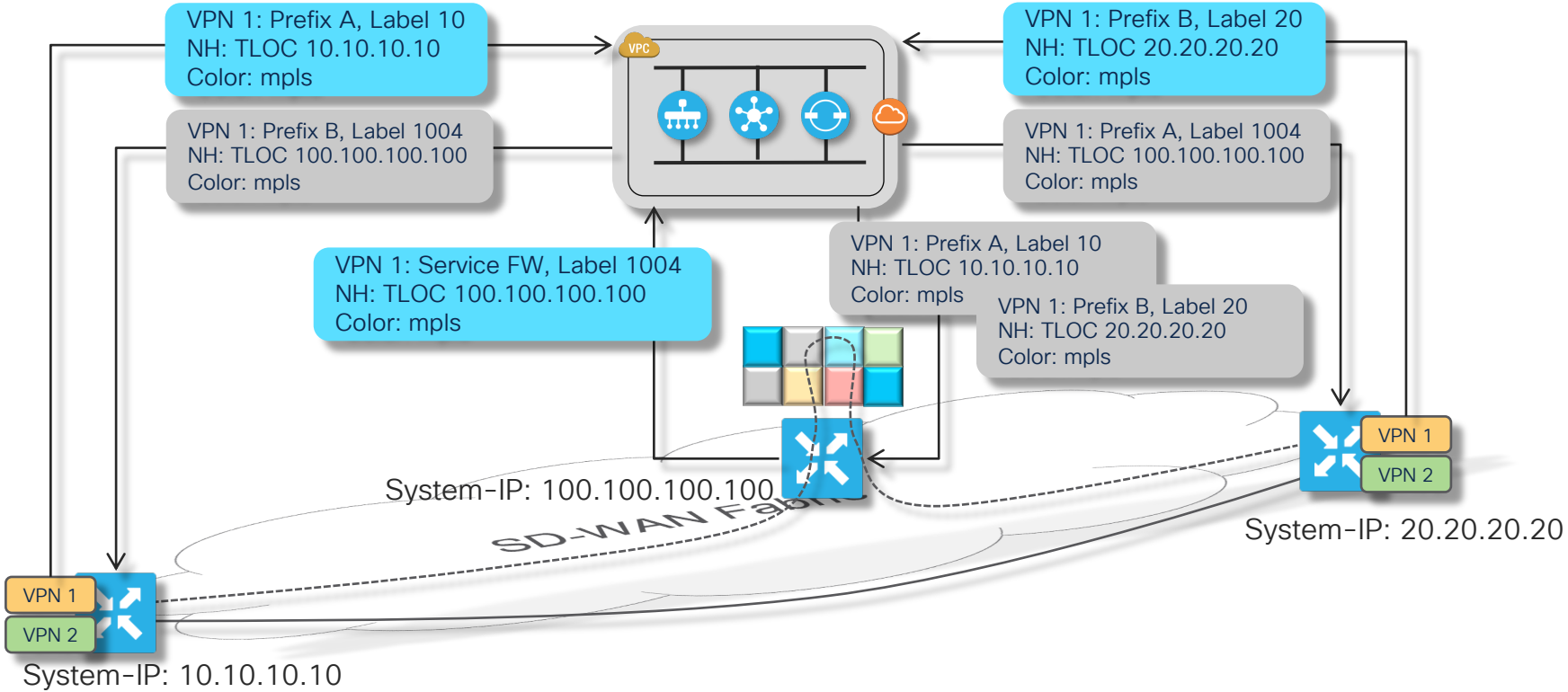


- Problem: Services to be consumed in-path for selected traffic
- Solution: Enable Service-Chaining Across the WAN

Control Policy Case #4

Service Chaining of Centralized Services

Legend:
- Original Advertisement from Endpoint
- Un/Modified Advertisement from Controller



Control Policy Case #4

Service Chaining

For Your Reference

```
WAN-Edge-100
vpn 1
 service FW address 10.0.13.150
```

1 Define Central FW Service

```
policy lists
  site-list upstream-exit
   site-id 20
  !
  site-list service-chain-branches
   site-id 10
!
```

2 Declare Exit Point

3 Declare Attached Branches

```
apply-policy
 site-list upstream-exit
  control-policy service-chain-downstream out
 !
 site-list service-chain-branches
  control-policy service-chain-upstream out
 !
!
```

6 Apply Policies to the target site-lists

```
policy
 control-policy service-chain-upstream
  sequence 10
   match route
    tloc 20.20.20.20 color red
    vpn 1
   !
   action accept
    set
     service FW
    !
   !
  !
  default-action accept
 !
 control-policy service-chain-downstream
  sequence 10
   match route
    site-list service-chain-branches
   !
   action accept
    set
     service FW
    !
   !
  !
  default-action accept
 !
```

4 Define Upstream Service Chain

5 Define Downstream Service Chain

Wait...
How does Service Chaining Actually work?

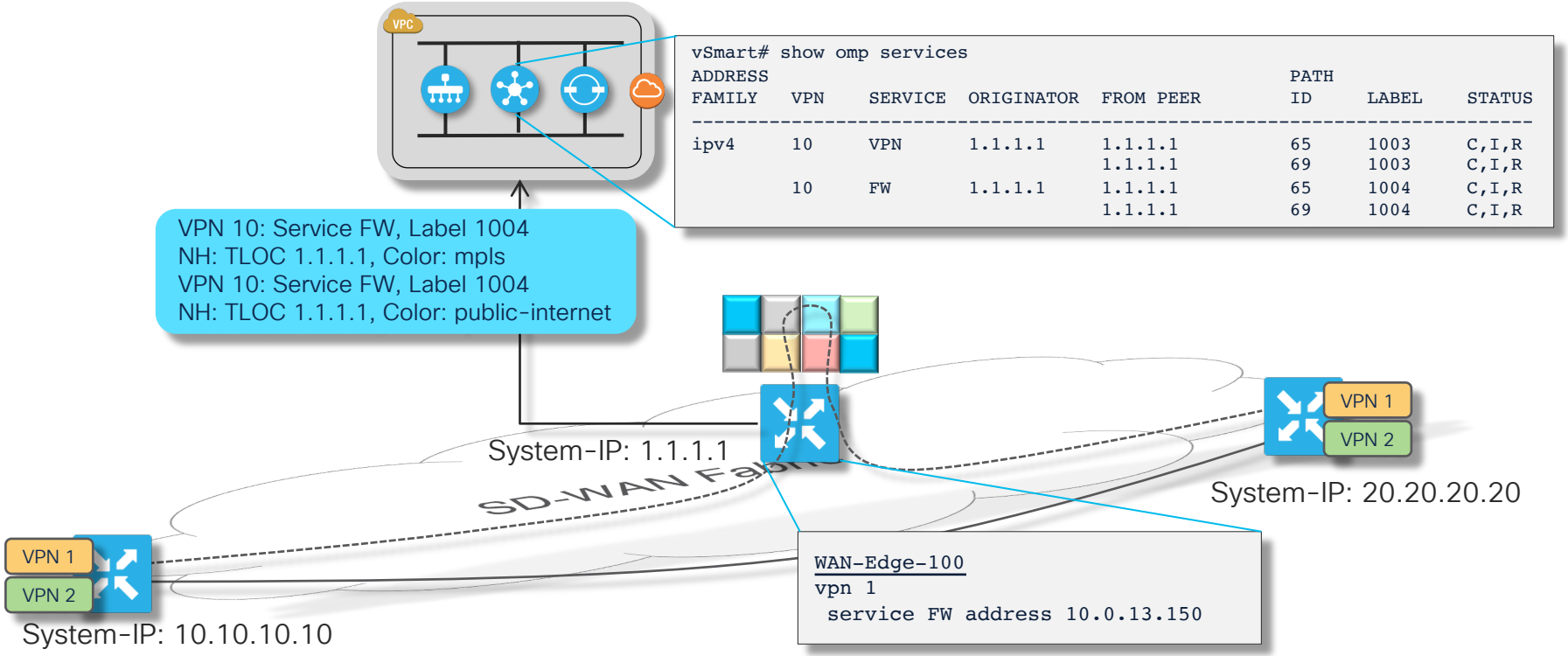
Service Chaining

Centralized Services – Setting Up a Service

Legend:

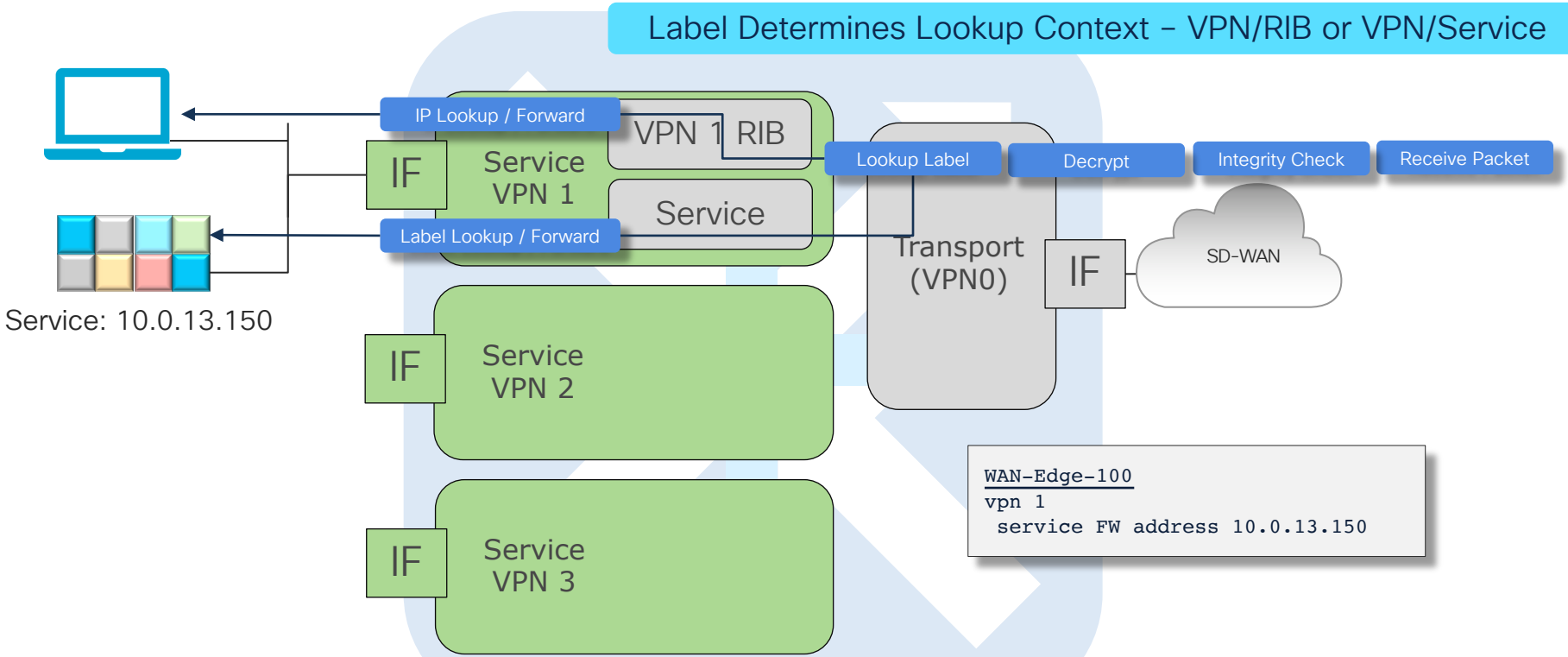
Original Advertisement from Endpoint

Un/Modified Advertisement from Controller



SD-WAN Service Chaining

WAN Edge Forwarding Paradigm



Service Chaining

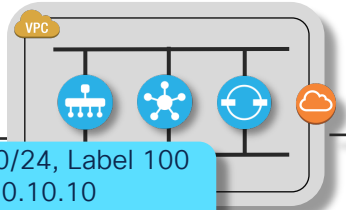
Invoking the Service – Per Direction

Legend:

- Original Advertisement from Endpoint
- Un/Modified Advertisement from Controller

```
vSmart
policy
 control-policy service-chain-upstream
  sequence 10
   match route
    tloc 20.20.20.20 color mpls
    vpn 1
   !
   action accept
    set
     service FW
!
```

```
policy
 control-policy service-chain-downstream
  sequence 10
   match route
    site-list service-chain-branches
   !
   action accept
    set
     service FW
```



VPN 1: 10.1.1.0/24, Label 100
NH: TLOC 10.10.10.10
Color: mpls

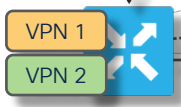
VPN 1: 20.1.1.0/24, Label 200
NH: TLOC 20.20.20.20
Color: mpls

VPN 10: 20.1.1.0/24, Label 1004
NH: TLOC 1.1.1.1
Color: mpls

VPN 10: 10.1.1.0/24, Label 1004
NH: TLOC 1.1.1.1
Color: mpls

System-IP: 1.1.1.1

SD-WAN Fabric



System-IP: 10.10.10.10
VPN 1: 10.1.1.0/24

System-IP: 20.20.20.20
VPN 1: 20.1.1.0/24

Control Policy Service Chaining:

Service not advertised to WAN Edge – Applied by Routing

Service Chaining

Invoking the Service – Using a Data Policy

Legend:

Original Advertisement from Endpoint

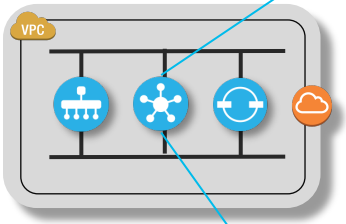
Un/Modified Advertisement from Controller

```
vEdge# show policy from-vsmart
from-vsmart data-policy Central_Security
 direction from-service
 vpn-list vpn_all
  sequence 10
   match
    protocol 6
   action accept
    set
     vpn-label 1004
     service FW
     service vpn 1
     service tloc 1.1.1.1
     service tloc color mpls
     service tloc encap ipsec
  default-action accept
from-vsmart lists vpn-list vpn_all
 vpn 1
```

Service Attributes Advertised

```
vSmart
policy
 data-policy Central_Security
  vpn-list vpn_all
   sequence 10
    match protocol 6
    !
    action accept
     set
      service FW vpn 1
     !
    !
   !
   default-action accept
```

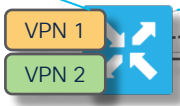
vSmart picked a Service



System-IP: 20.20.20.20

SD-WAN Fabric

System-IP: 1.1.1.1



System-IP: 10.10.10.10

Data Policy Service Chaining:

Service advertised to WAN Edge – Applied to Data Plane

Service Chaining
Additional Options

Legend:
- Original Advertisement from Endpoint
- Un/Modified Advertisement from Controller

- Using a Local Service
  - The Service Chaining framework can be used for services that are locally attached as well
  - Examples in the Data Policy section coming up
- Specify the service TLOC and priority using a TLOC list

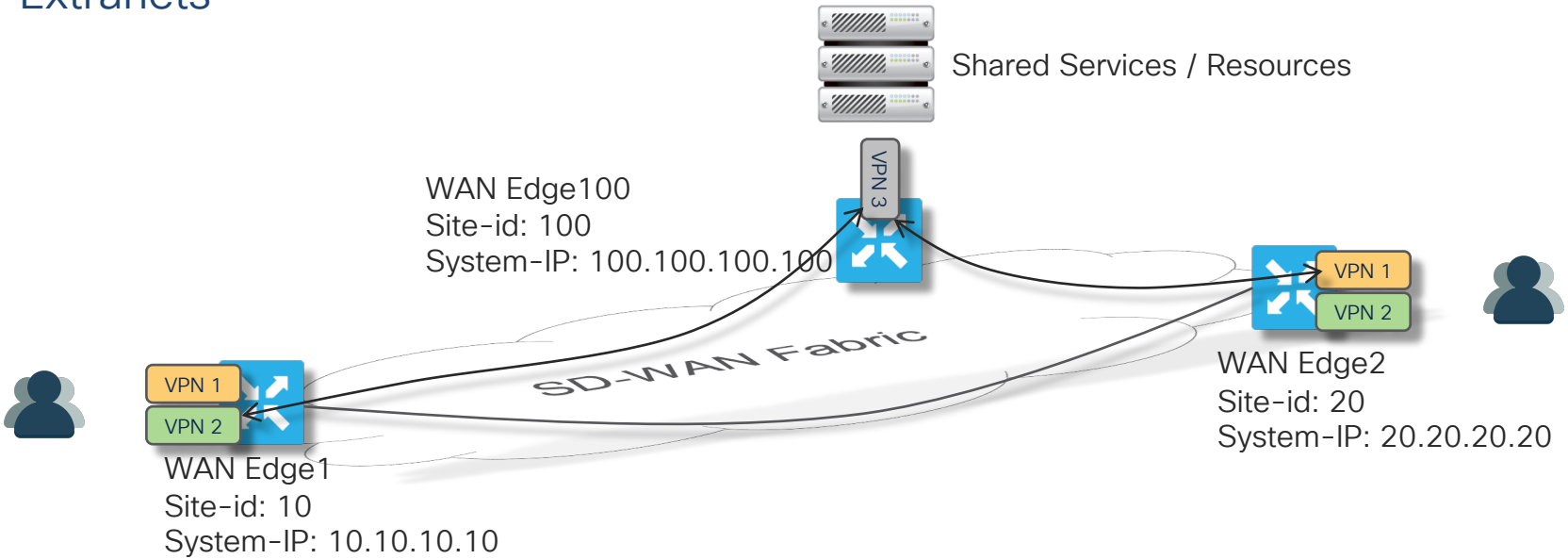
```
vSmart
policy
 control-policy service-chain-upstream
  sequence 10
   match route
    tloc 20.20.20.20 color mpls
    vpn 1
   !
   action accept
    set
     service FW tloc-list my_firewalls
!
```

```
policy
 lists
  tloc-list my_firewalls
   tloc 1.1.1.1 color mpls encap ipsec preference 100
   tloc 2.2.2.2 color mpls encap ipsec preference 100
   tloc 3.3.3.3 color mpls encap ipsec preference 50
  !
 !
!
```

Back on track

Control Policy Case #5

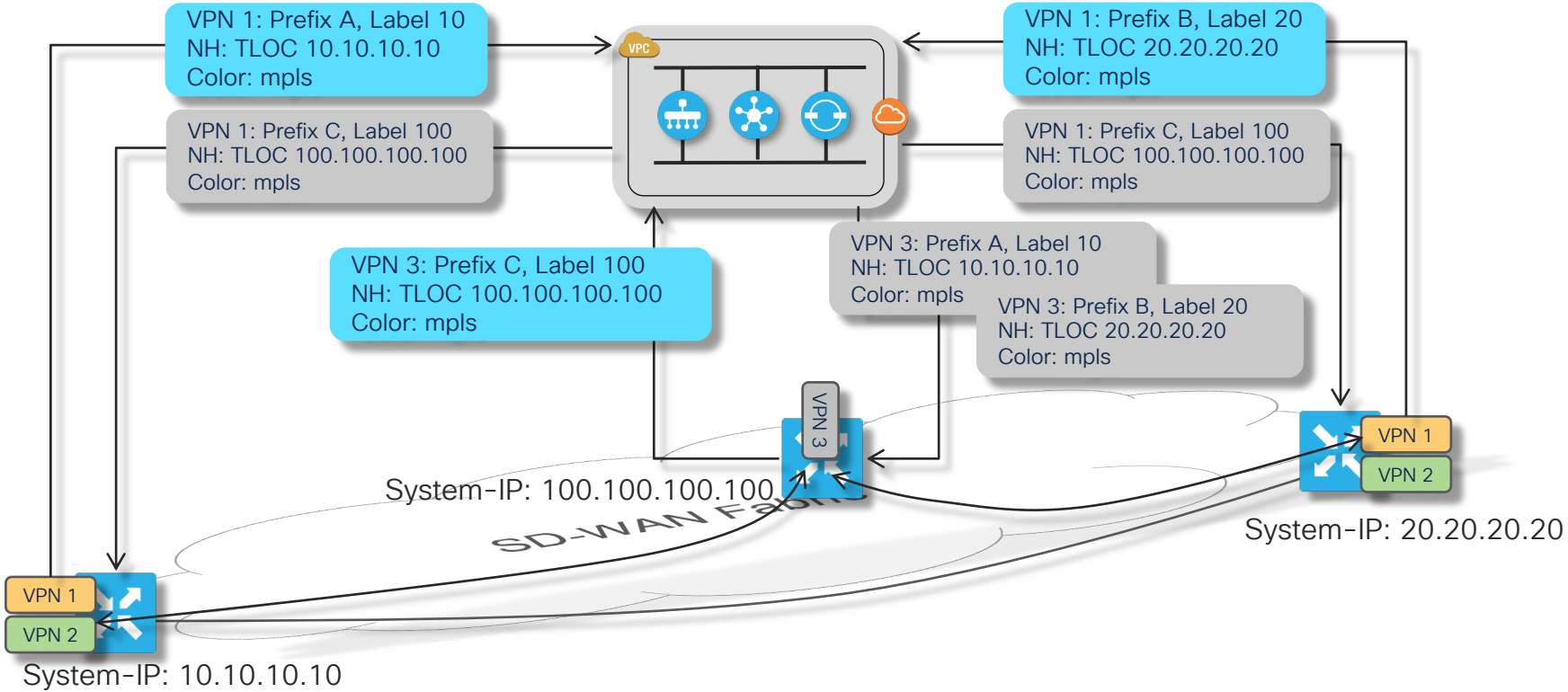
Extranets



- Problem: Shared Services to be consumed from Extranet VPN hosted location
- Solution: Provision Extranet Access from other overlay VPNs

Control Policy Case #5

Extranets



Control Policy Case #5

Extranets

For Your Reference

```
policy
 lists
  prefix-list natpools
   ip-prefix 192.168.0.0/16 le 32
  !
  site-list consumers
   site-id 3002
   site-id 3003
   site-id 3004
  !
 !
```

1 Declare Consumers

```
apply-policy
 site-list consumers
  control-policy extranet in
 !
!
```

4 Apply Control Policy

2 Export NAT Pool To Service VPN

```
policy
 control-policy extranet
  sequence 10
   match route
    prefix-list natpools
    vpn 1
   !
   action accept
    export-to
     vpn 3
    !
   !
  !
  sequence 20
   match route
    vpn 3
   !
   action accept
    export-to
     vpn 1
    !
   !
  !
  default-action accept
 !
!
```

3 Export Service Prefixes to Consumer VPN

Service Plane NAT
NAT across sites at VPN Layer

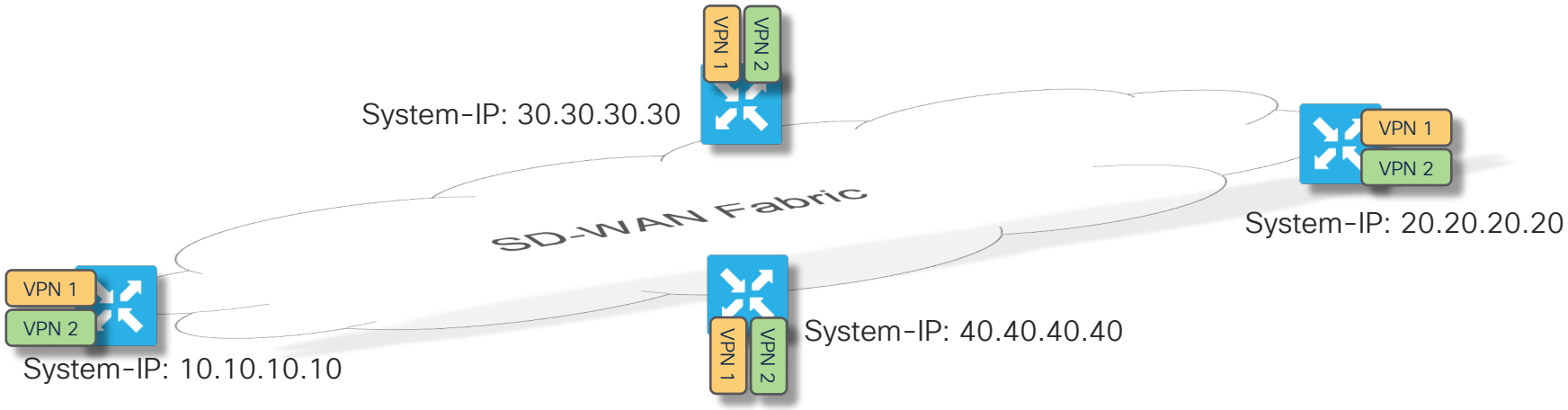
```
policy data-policy Srvc_Plane_NAT
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.1/32
    !
    action accept
     nat pool 1
    !
   !
   default-action accept
  !
```

```
WAN-Edge
vpn 1
 interface natpool1
  ip address 192.168.1.1/32
  no shutdown
 !
```

Optional Service Plane NAT

Control Policy Case #6

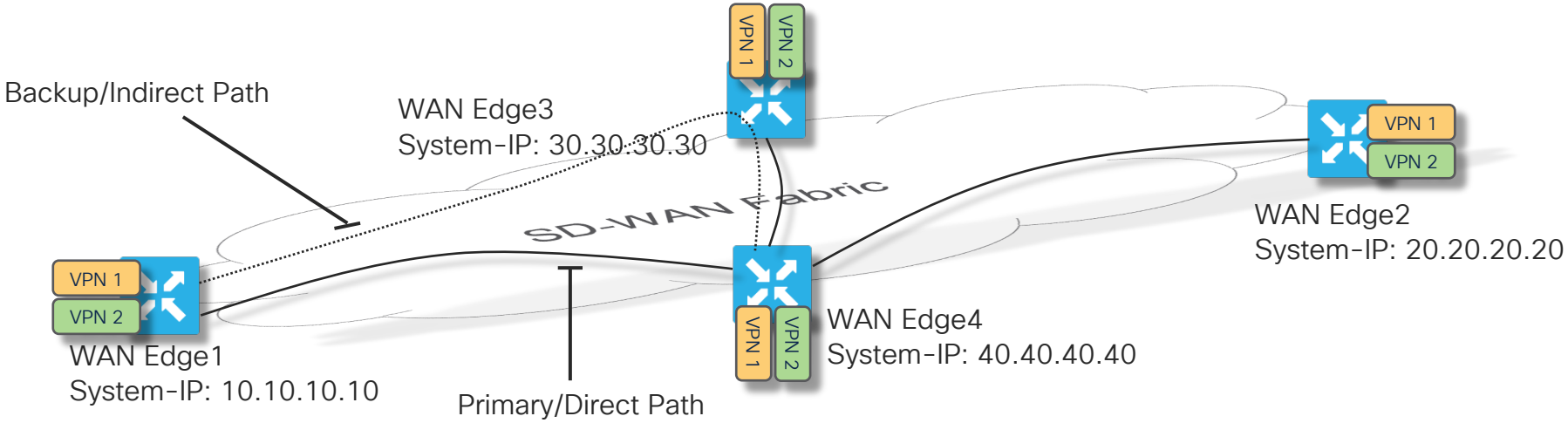
Traffic Engineering / Path Redundancy



- Problem: Backup needed for direct overlay paths to manage intermediate path issues
- Solution: Identify and Provision select indirect overlay paths for redundancy and capacity

Control Policy Case #6

Traffic Engineering / Path Redundancy



- Identify indirect paths for targeted sites
- Decide whether to use them as Primary, ECMP or Backup paths

Control Policy Case #6

Traffic Engineering / Path Redundancy

For Your Reference

```
WAN-Edge3
vpn 1
 service te
```

1 Enable TE Service for VPN 1

```
policy
 lists
  vpn-list VPN1
   vpn 1
  !
  tloc-list backup-tloc
   tloc 30.30.30.30 color mpls encap ipsec
  !
  site-list vEdge1
   site-id 10
  !
  site-list vEdge4
   site-id 40
  !
 !
!
```

2 Declare Site 3 Backup TLOC

3 Declare Application Site

4 Declare Protection Site (4)

```
apply-policy
 site-list vEdge1
  control-policy backup-node out
```

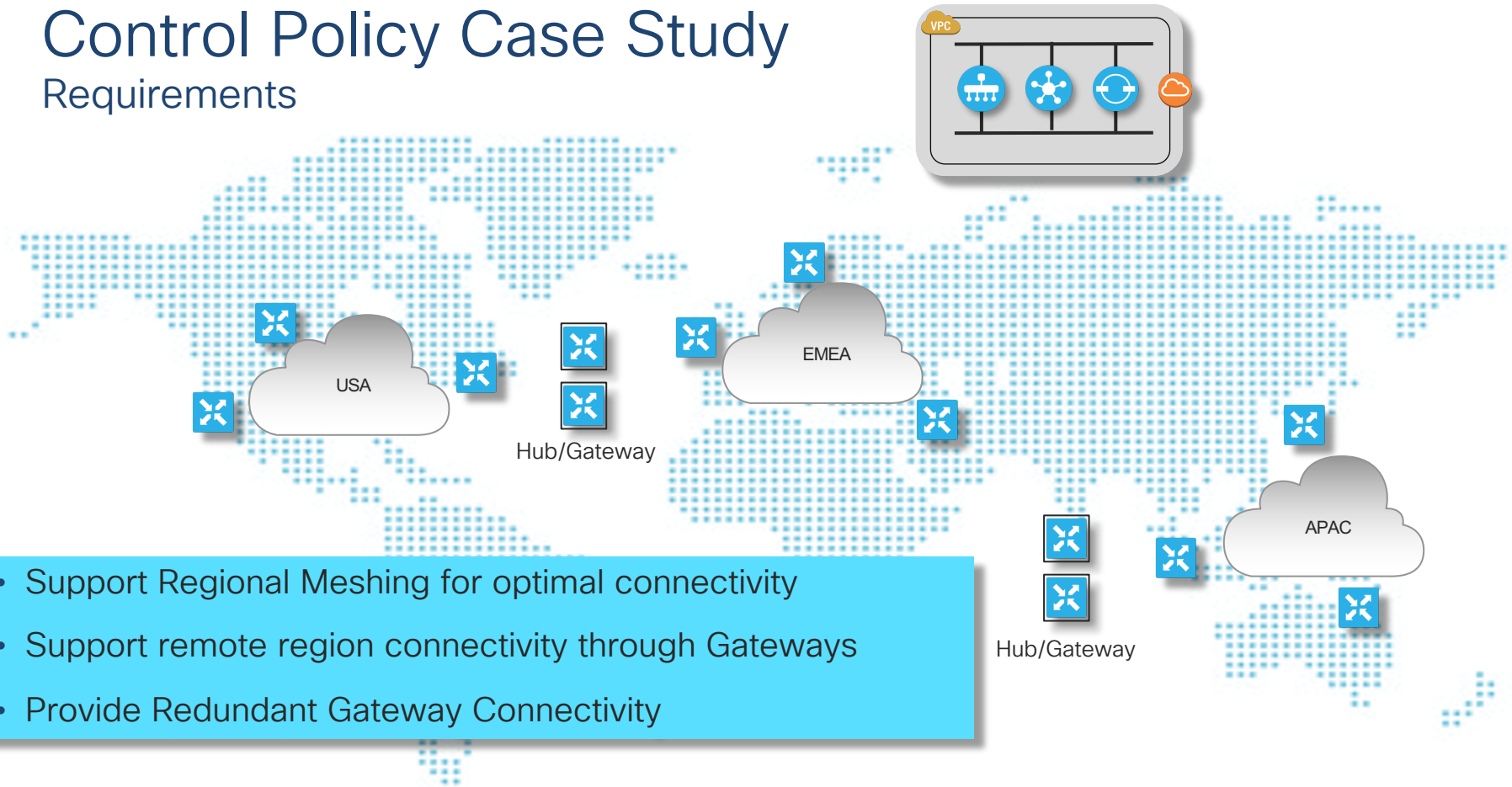
6 Apply Control Policy

5 Define Control Policy

```
policy control-policy backup-node
 sequence 10
  match route
   site-list vEdge4
   vpn-list  VPN1
  !
  action accept
   set
    tloc-action backup
    tloc-list   backup-tloc
   !
  !
 !
 default-action accept
!
```

Control Policies: Multi-domain data plane case study

Control Policy Case Study
Requirements



- Support Regional Meshing for optimal connectivity
- Support remote region connectivity through Gateways
- Provide Redundant Gateway Connectivity

Control Policy Case Study
Definitions and Dependencies

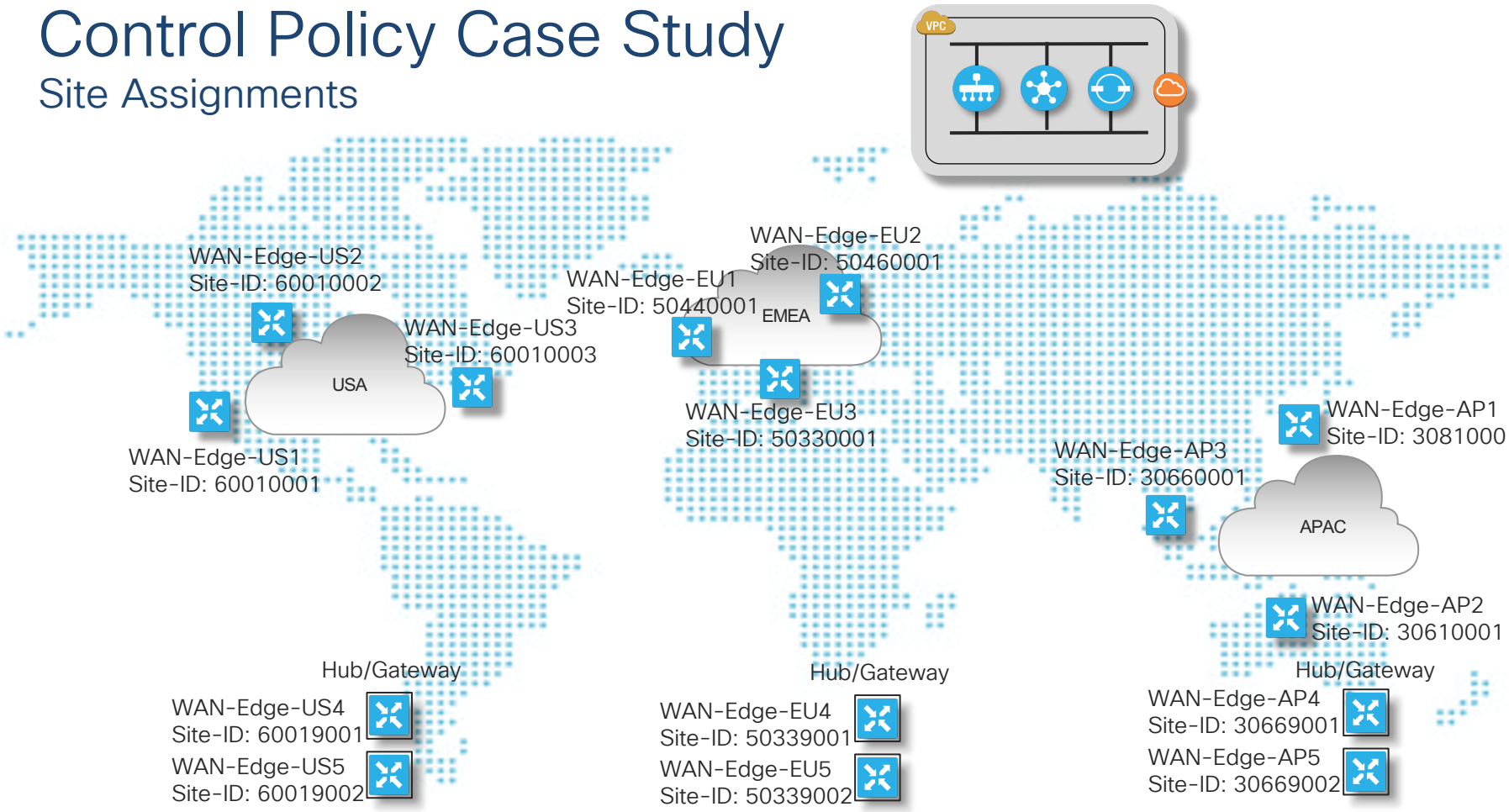
- Site-ID assignment allowing for Site identification – 32 bits

	Continent	Country	Site number
	X	YYY	ZZZZ
	1-7	1-999	1-9999
Example	Europe	Sweden	Site
	5	046	1000

- TLOC Colors illustrating how sites are attached
- System-IP identifying individual nodes

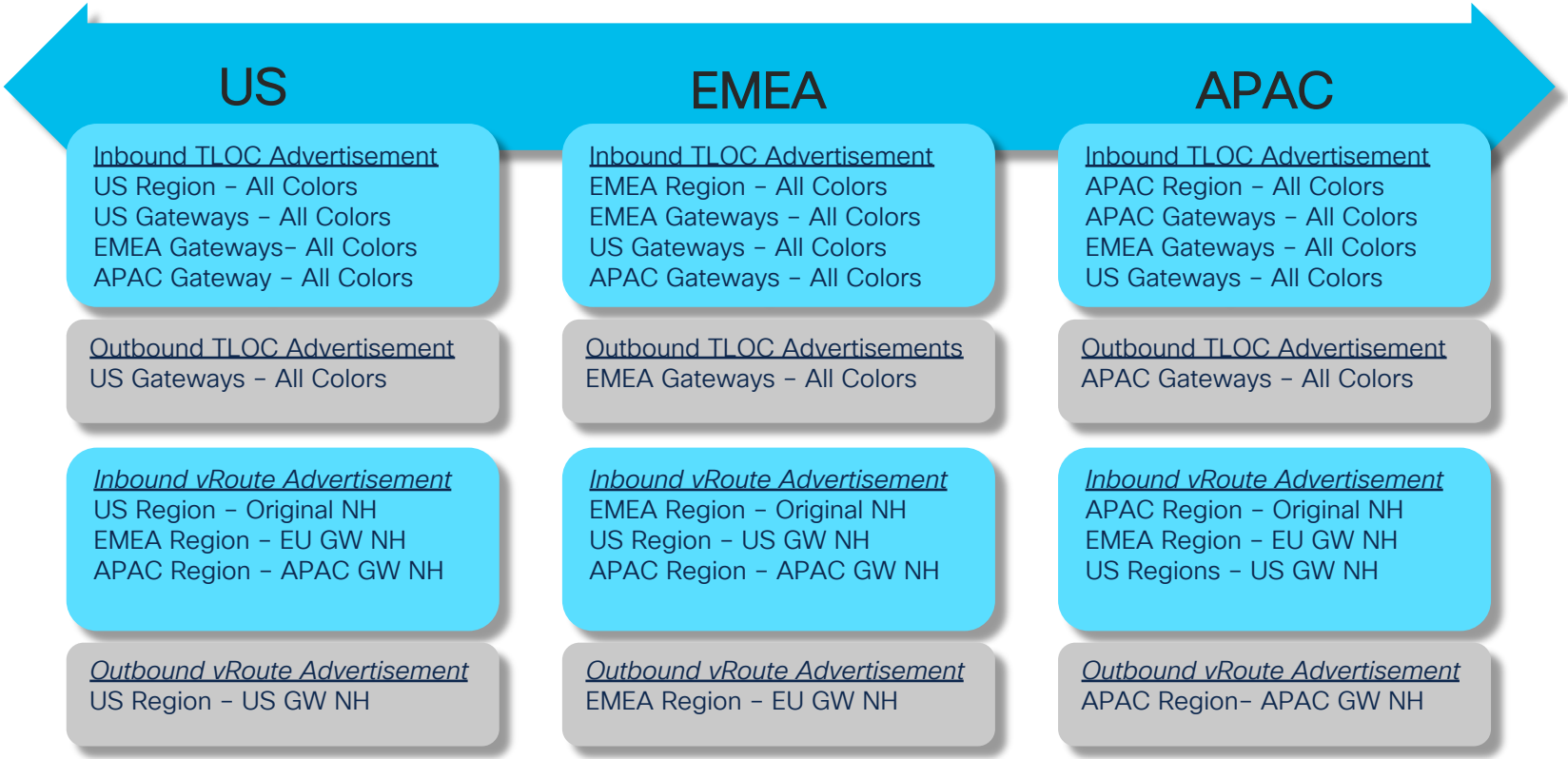
Control Policy Case Study

Site Assignments



Control Policy Case Study

Reachability Information Distribution Requirements



Control Policy Case Study

Policy Definition – Lists

For Your Reference

```
policy
 lists
  site-list US_branch_sites
   site-id 60010000-60018999
  !
  site-list US_gateway_sites
   site-id 60019000-60019999
  !
  site-list EMEA_branch_sites
   site-id 50010000-50338999
   site-id 50340000-59999999
  !
  site-list EMEA_gateway_sites
   site-id 50339000-50339999
  !
  site-list APAC_branch_sites
   site-id 30010000-30668999
   site-id 30670000-39999999
  !
  site-list APAC_gateway_sites
   site-id 30669000-30669999
  !
 !
!
```

```
policy
 lists
  tloc-list US_gateway_tlocs
   tloc 1.1.1.1 color mpls encap ipsec preference 100
   tloc 1.1.1.1 color biz-internet encap ipsec preference 100
   tloc 2.2.2.2 color mpls encap ipsec preference 50
   tloc 2.2.2.2 color biz-internet encap ipsec preference 50
  !
  tloc-list EMEA_gateway_tlocs
   tloc 3.3.3.3 color mpls encap ipsec preference 100
   tloc 3.3.3.3 color biz-internet encap ipsec preference 100
   tloc 4.4.4.4 color mpls encap ipsec preference 50
   tloc 4.4.4.4 color biz-internet encap ipsec preference 50
  !
  tloc-list APAC_gateway_tlocs
   tloc 5.5.5.5 color mpls encap ipsec preference 100
   tloc 5.5.5.5 color biz-internet encap ipsec preference 100
   tloc 6.6.6.6 color mpls encap ipsec preference 50
   tloc 6.6.6.6 color biz-internet encap ipsec preference 50
  !
 !
!
```

Control Policy Case Study

Policy Definition Cont'd – Control Policy – Applied to US Sites

For Your Reference

```
policy
 control-policy us_domain
  sequence 10
   match tloc
    site-list US_branch_sites
   !
   action accept
   !
  !
  sequence 20
   match tloc
    site-list US_gateway_sites
    SNIP … (accept)
  sequence 30
   match tloc
    site-list EMEA_gateway_sites
    SNIP … (action accept)
  sequence 40
   match tloc
    site-list APAC_gateway_sites
   !
    SNIP … (action accept)
```

```
sequence 50
 match route
  site-list US_branch_sites
 !
 action accept
 !
sequence 60
 match route
  site-list US_gateway_sites
  SNIP … (action accept)
sequence 70
 match route
  site-list EMEA_branch_sites
 !
 action accept
  set
   tloc-list EMEA_gateway_tlocs
  !
 !
!
sequence 80
 match route
  site-list EMEA_gateway_sites
  SNIP … (action accept)
```

Control Policy Case Study

Policy Definition Cont'd – Control Policy - Applied to US Sites

For Your Reference

```
  sequence 90
   match route
    site-list APAC_branch_sites
   !
   action accept
    set
     tloc-list APAC_gateway_tlocs
    !
   !
  !
  sequence 100
   match route
    site-list APAC_gateway_sites
   !
   action accept
   !
  !
  default-action accept
```

```
apply-policy
 site-list US_branch_sites
  control-policy us_domain out
 !
 site-list US_gateway_sites
  control-policy us_domain out
 !
!
```

- Policy Logic

Sequence 10: Advertise US Branch TLOCs

Sequence 20: Advertise US GW TLOCs

Sequence 30: Advertise EMEA GW TLOCs

Sequence 40: Advertise APAC GW TLOCs

Sequence 50: Advertise US Branch routes

Sequence 60: Advertise US GW routes

Sequence 70: Advertise EMEA Branch routes w/ NH of EMEA GW

Sequence 80: Advertise EMEA GW routes

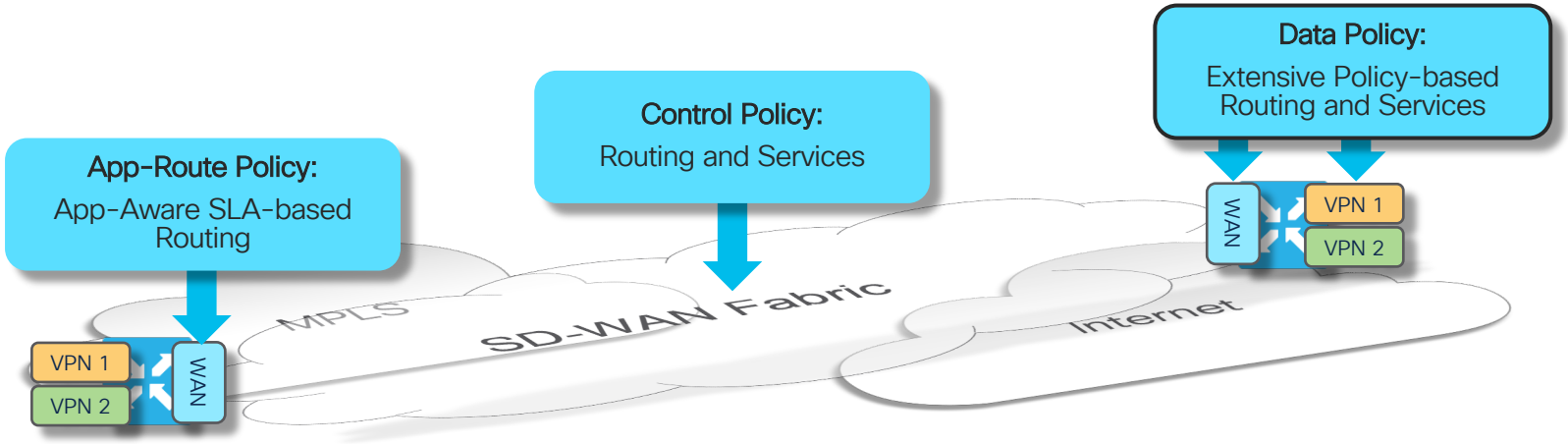
Sequence 90: Advertise APAC Branch routes w/ NH of APAC GW

Sequence 100: Advertise APAC GW Routes

Policy Framework: Data Policies

Cisco SD-WAN Policy Architecture

Suite of Policies to address different functional domains



- Control Policies are applied at vSmart: Tailors routing information advertised to WAN endpoints
- App-Route Policies are applied at WAN Edge: SLA-driven path selection for applications
- Data Policies are applied at WAN Edge: Extensive Policy driven routing

Data Policies

Policy-driven Routing and Service Enablement

- Data policies:
  - Applied on vSmart
  - Advertised to and executed on WAN Edge
- A Data policy acts on an entire VPN and is not interface-specific
- Different Data Policies can be applied to different VPNs
- Data Policies are used to enable the following functions and services:
  - Application Pinning
  - NAT/DIA
  - Classification, Policing and Marking
  - and more …
- Use a Data Policy for any type of data plane centered traffic management

Data Policies

Policy Structure

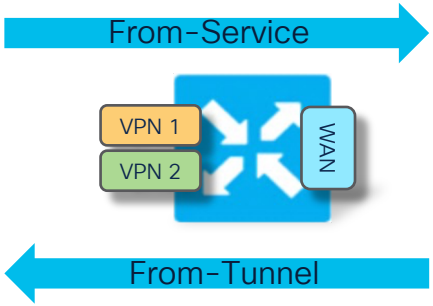
```
data-policy <name>
  vpn-list <name>
    sequence <n>
      match
        app-list <name>
        destination-data-ipv6-prefix-list <name>
        destination-data-prefix-list <name>
        destination-ip <ip-address>
        destination-ipv6 <ipv6-address>
        destination-port <port>
        dns request | response
        dns app-list <name>
        dscp <dscp>
        packet-length <length>
        plp <plp>
        protocol <protocol>
        source-data-ipv6-prefix-list <name>
        source-data-ip-prefix-list <name>
        source-ip <ip-address>
        source-ipv6 <ipv6-address>
        source-port <port>
        tcp-syn
       !
      !
```

```
      action
        accept
          set
            dscp <dscp>
            forwarding-class <name>
            local-tloc <tloc>
            local-tloc-list <list>
            next-hop <ip-address>
            next-hop-ipv6 <ipv6-address>
            policer <name>
            service <name>
            tloc <tloc>
            tloc-list <name>
            vpn <vpn-id>
          cflowd
          count <counter>
          drop
          log
          loss-protect-fec-always
          loss-protect-fec-adaptive
          loss-protect-packet-dup
          nat-pool <nat-pool>
          nat use-vpn <vpn-id>
          redirect dns
          tcp-optimization
         !
        !
       !
      !
     !
    !
   !
  default-action accept
 !
```

Data Policy Application
Direction of Processing

- A Data Policy can be applied in three modes:
  - From-service (Upstream)
  - From-tunnel (Downstream)
  - All (Up and Downstream)
- Different Data-policies can be applied to the same site if they apply to different directions

Upstream Traffic matched by Data-policy

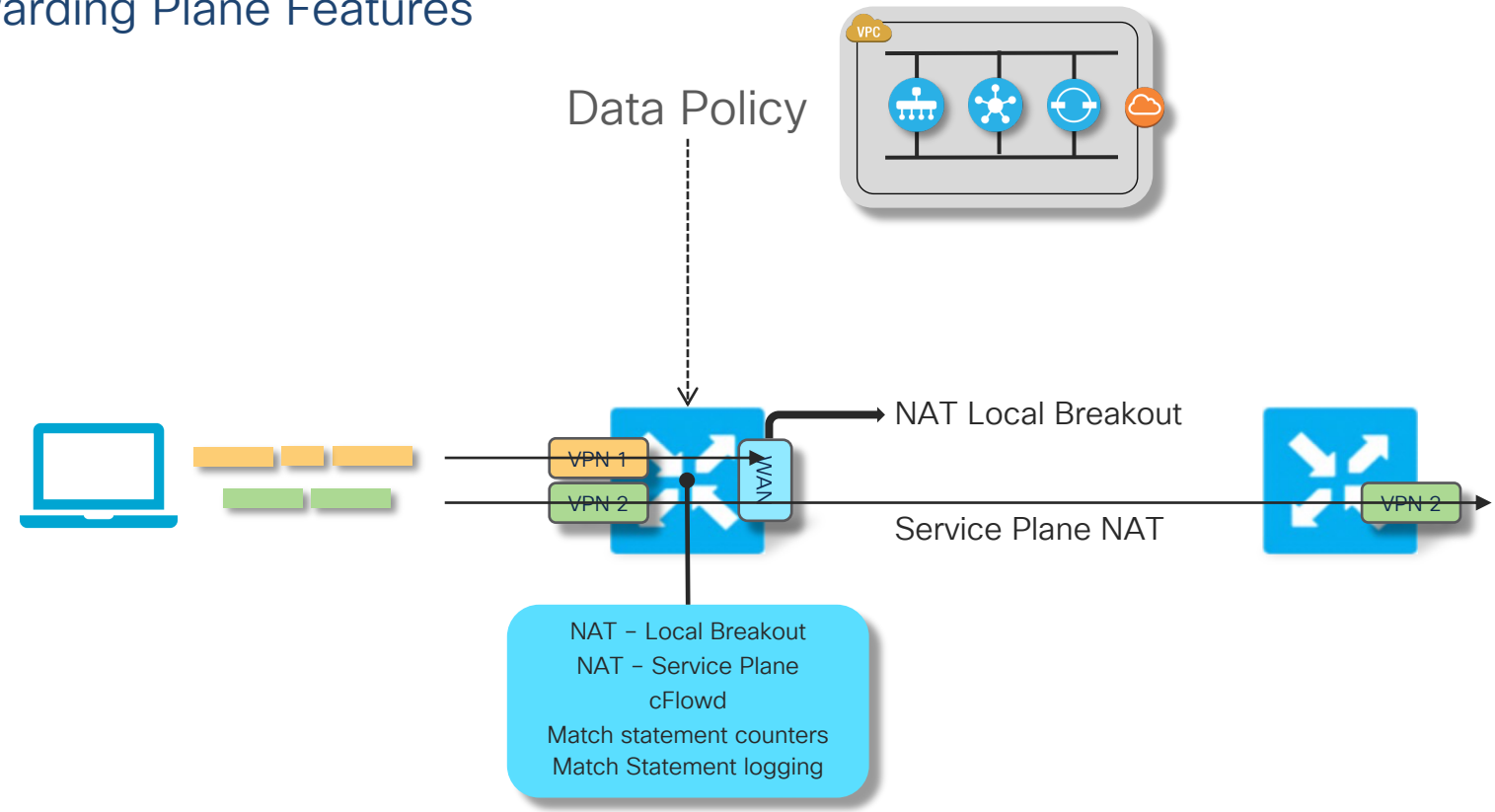


Downstream Traffic matched by Data-policy

```
apply-policy site-list <name>
  data-policy <name> all | from-service | from-tunnel
```

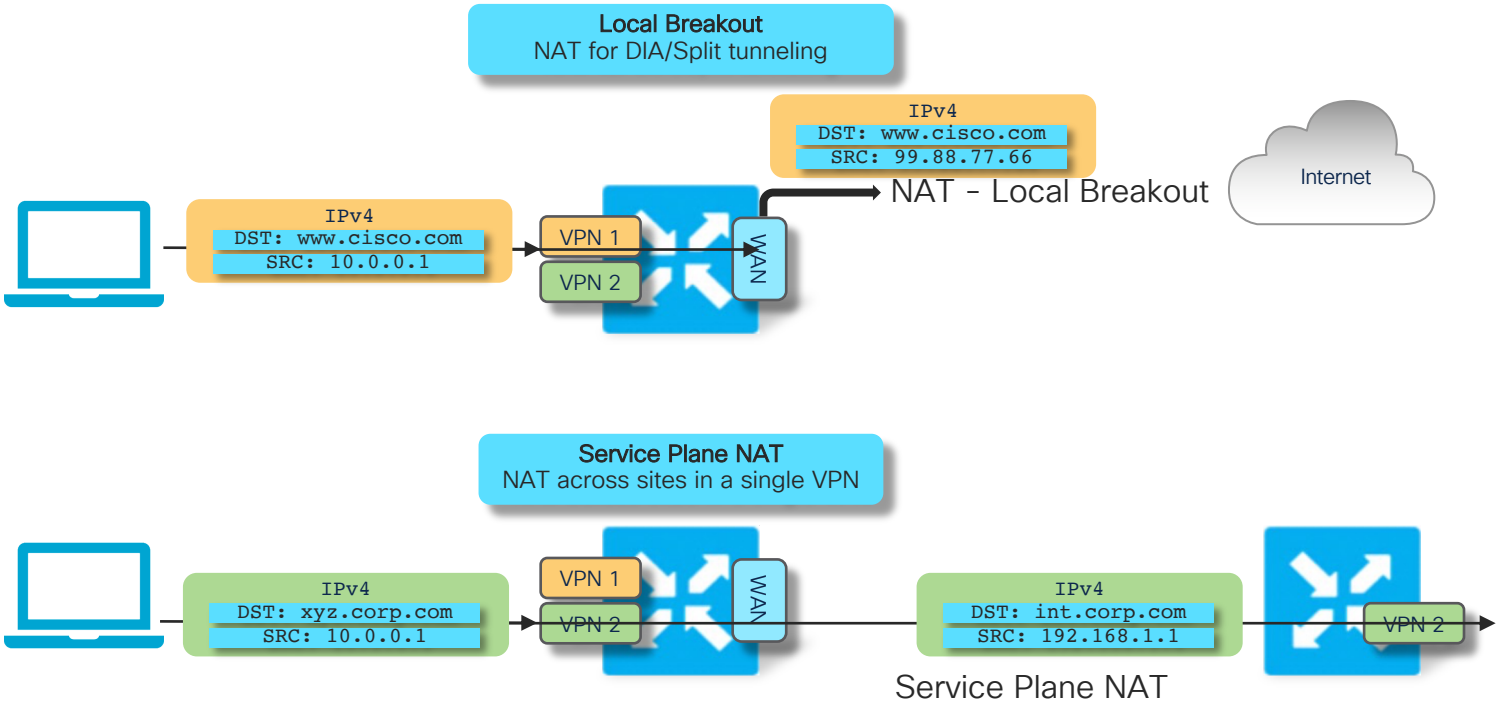
Data Policy Case #1

Forwarding Plane Features



Data Policy Case #1

Forwarding Plane Features – NAT for DIA and Service VPN



Data Policy Case #1

Forwarding Plane Feature Enablement – Policy Structure

For Your Reference

Service Plane NAT
NAT across sites in a single VPN

```
policy data-policy Srvc_Plane_NAT
  vpn-list VPN2
   sequence 10
    match source-ip 10.0.0.1/32
    !
    action accept
     nat pool 1
    !
   !
   default-action accept
  !
```

```
WAN-Edge
vpn 2
 interface natpool1
  ip address 192.168.1.1/32
  no shutdown
 !
```

Local Breakout
NAT for DIA/Split tunneling

```
policy data-policy DIA_NAT
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.1/32
    !
    action accept
     nat use-vpn 0
    !
   !
   default-action accept
  !
```

```
WAN-Edge
vpn 0
 interface ge0/0
  ip address 99.88.77.66/32
  no shutdown
  nat
 !
```

Data Policy Case #1

Forwarding Plane Feature Enablement – Policy Structure

For Your Reference

Local Breakout
cFlowd and Counting

```
policy data-policy DIA_NAT
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.1/32
    !
    action accept
     cflowd
     count local-breakout-traffic
     nat use-vpn 0
    !
   !
   default-action accept
  !
```

Local Breakout
Logging breakout traffic

```
policy data-policy DIA_NAT
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.1/32
    !
    action accept
     log
     nat use-vpn 0
    !
   !
   default-action accept
  !
```

```
WAN Edge
System
 logging
  server syslog.company.com
   vpn 1
   source-interface loopback1
  exit
 !
```

```
WAN Edge
policy
 log-frequency <number>*
```

* Default is every 1000 packets

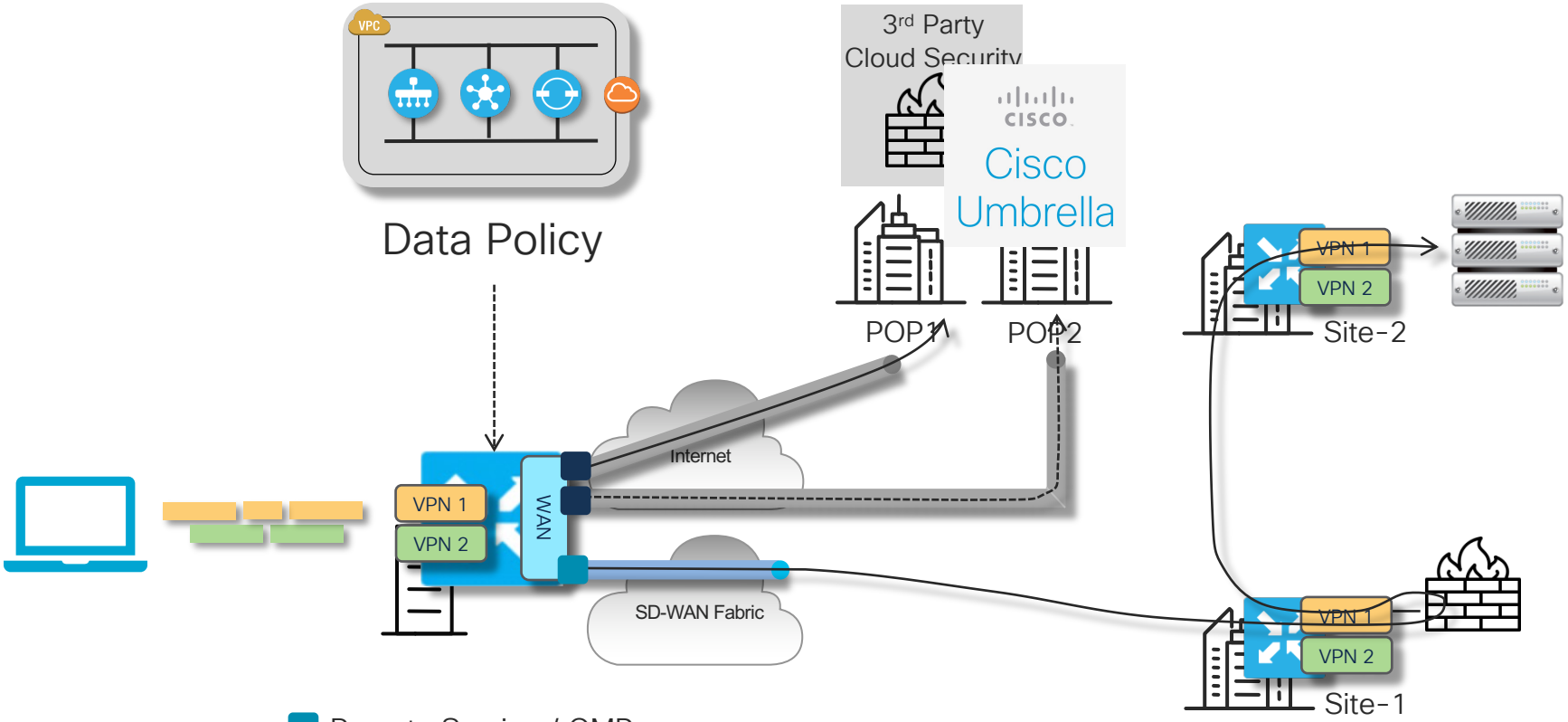
- Counters visible using GUI/Realtime or via CLI

```
show policy data-policy-filter
```

- Use cflowd template for export-destination configuration

Data Policy Case #2

Service Chaining – Local and Remote Services



Remote Service / OMP

Local Service

Data Policy Case #2

Service Chaining – Local Services – Policy Structure

For Your Reference

```
vSmart
policy
 data-policy Cloud_Security
  vpn-list vpn_all
   sequence 10
    match protocol 6
    match destination-port 80 443
    !
    action accept
     set
      service FW local
     !
    !
   !
   default-action accept
```

2 Match Traffic

3 Apply Local Service

```
WAN Edge
vpn 1
 service FW interface gre1 gre2
vpn 0
 interface ge0/0
  ip address 99.88.77.66/32
  no shutdown
  nat
 !
 interface gre1
  ip address 12.13.14.15/24
  tunnel-source-interface ge0/0
  tunnel-destination 123.123.123.123
  no shutdown
 !
 interface gre2
  ip address 16.17.18.19/24
  tunnel-source-interface ge0/0
  tunnel-destination 124.124.124.124
  no shutdown
```

1 Define Local Service FW

Primary Tunnel

Backup Tunnel

- Data Policy redirection to locally configured service
- Service represented by local GRE or IPsec tunnel pre-configured on each WAN Edge

Data Policy Case #2

Service Chaining – Remote Services – Policy Structure

For Your Reference

```
vSmart
policy
 data-policy Central_Security
  vpn-list vpn_all
   sequence 10
    match protocol 6
    match destination-port 80 443
    !
    action accept
     set
      service FW vpn 1
     !
    !
   !
   default-action accept
```

2 Match Traffic

3 Apply OMP FW Service

```
WAN Edge – Site1
vpn 1
 service FW address 12.13.14.100
 !
 interface ge0/0
  ip address 12.13.14.15/24
  no shutdown
```

1 Define Service FW for OMP Announcement

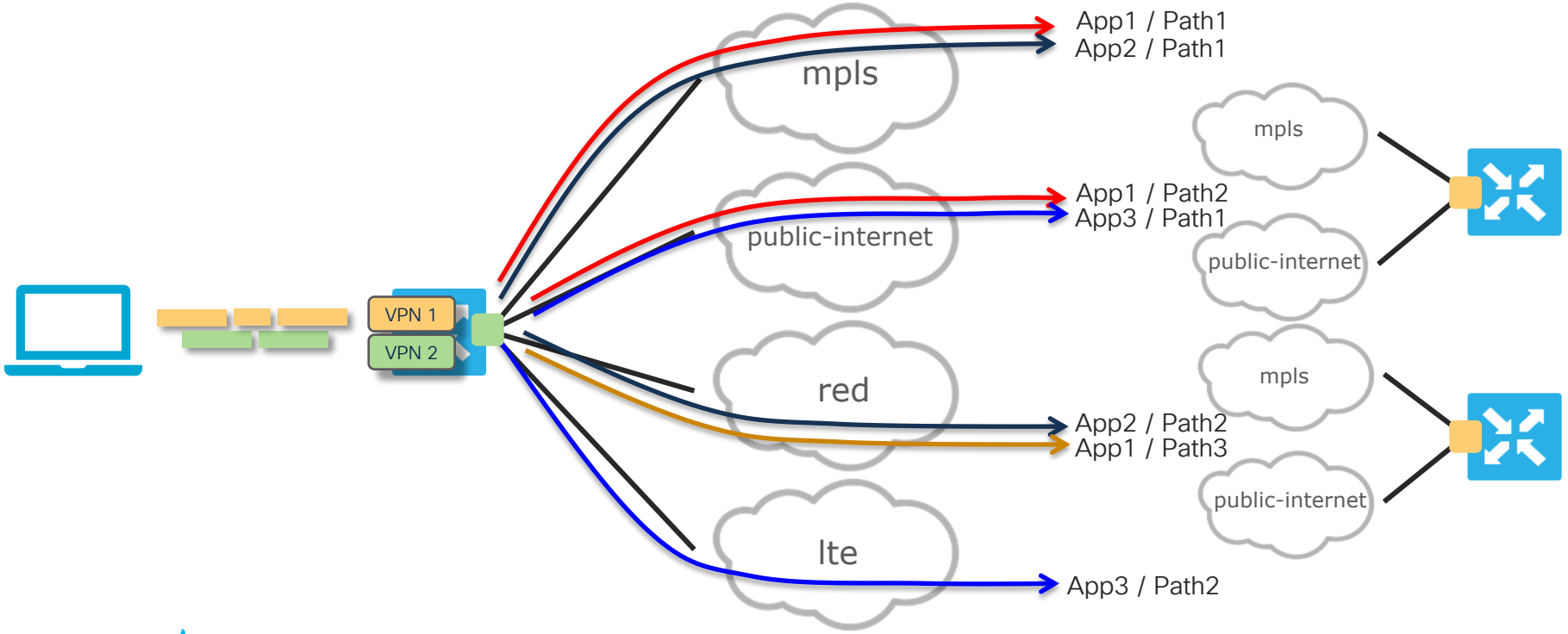
- Data Policy redirection to remotely configured service
- Service represented by OMP advertised service identifier
- Service association can be specified via TLOC or TLOC-list (with priorities) if needed

Data Policy Case #3

Application Pinning

Local TLOC Selection: Loose preference, falls back to routing upon failure

Remote TLOC Selection: Strict preference, traffic dropped upon failure



Data Policy Case #3

Application Pinning – Policy Structure

Local TLOC
Prefer Local Underlay Path

```
vSmart
policy
 data-policy local-tloc-preference
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.0/8
    !
    action accept
     local-tloc red blue
```

(Remote) TLOC
Prefer a remote Node/TLOC

```
vSmart
policy
 data-policy local-tloc-preference
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.0/8
    !
    action accept
     set
      tloc 1.1.1.1 color biz-internet

Or
    action accept
     set
      tloc-list remote-node
```

- local-tloc – Loose match that will fall back to routing if all local TLOCs in list are down
- tloc/tloc-list refer to specific remote TLOCs and will not fall back to routing

```
policy
 lists
  tloc-list remote-node
   tloc 1.1.1.1 color mpls encap ipsec preference 100
   tloc 1.1.1.1 color biz-internet encap ipsec preference 50
```

Policy Framework: Internet Breakout / DIA Case Study

Internet Breakout / DIA

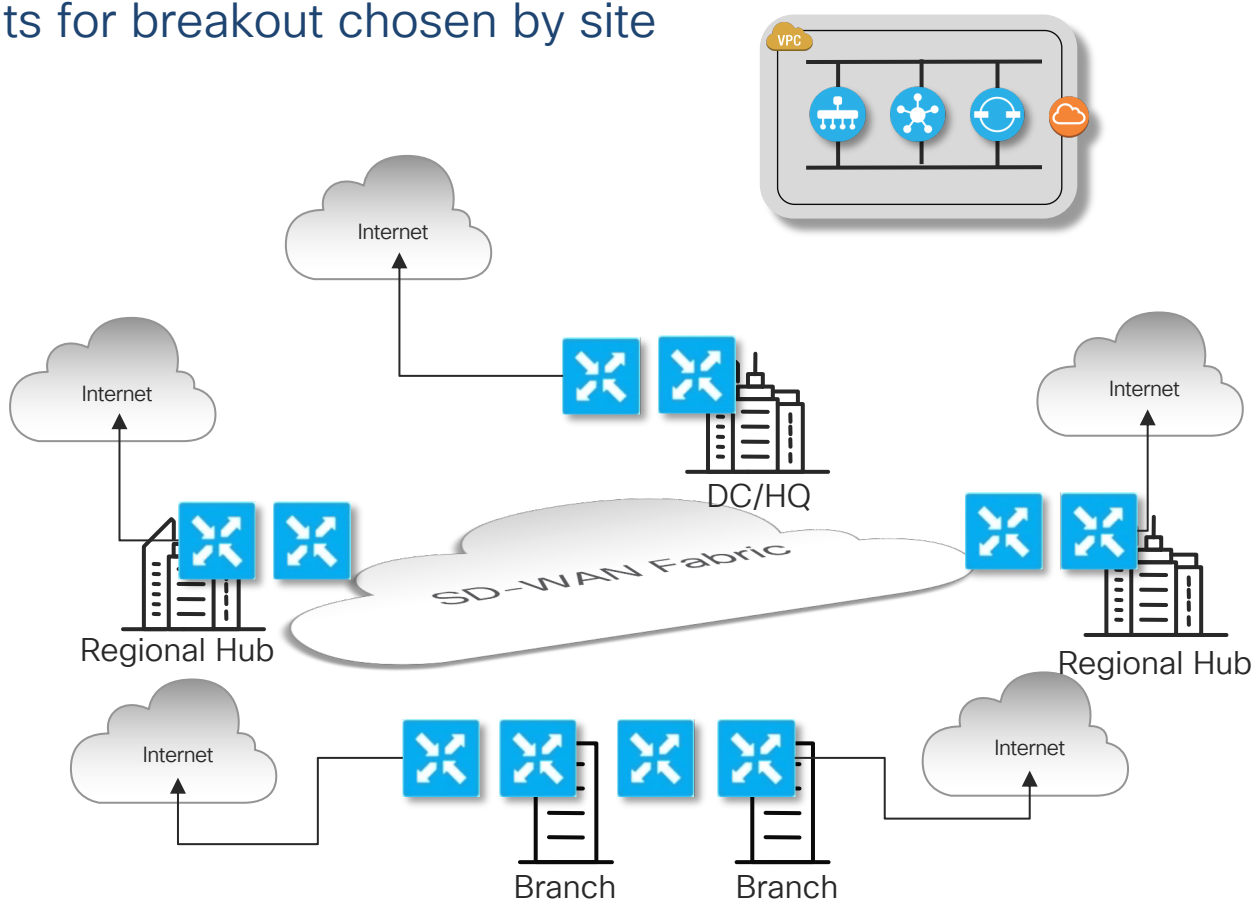
Routing and/or Policy-driven Capabilities

- The Cisco SD-WAN Architecture provides a lot of flexibility in enabling DIA
- Breakouts can be presented via:
  - Routing
  - Policy
  - In combination, with Preference and Backup options
  - Cloud-based Security as a Local Service using a Policy
- NAT is a required feature when providing a local breakout
- Service-side breakouts can be provided in case NAT is not needed or special care is needed for public addressing
- Can be deployed in combination with Service Chaining for monitoring/security/processing requirements

Internet Breakout Leverage

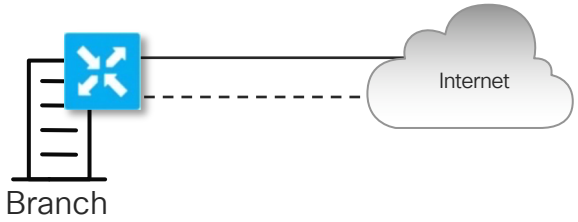
Most appropriate points for breakout chosen by site

- Enterprises can gradually progress from centralized to distributed breakouts
- Routing plane enables primary/backup as needed
- Policies further enhance selection and breakout granularity
- Align well with deployment of Cloud-based Security solutions



SD-WAN Internet Breakout Options

Local Breakout using a Default Route



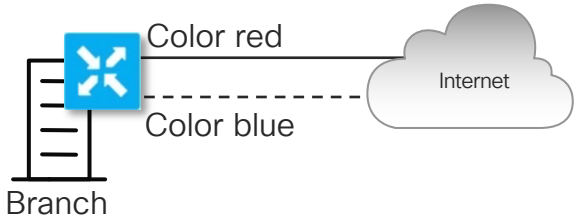

```
vpn 0
 interface ge0/0
  nat
  tracker my_tracker
 !
vpn 1
 ip route 0.0.0.0/0 vpn 0
```

```
System
 tracker my_tracker
 endpoint-ip 1.2.3.4
 Interval 5
 Multiplier 3
 Threshold 500
```

- Static route in Service VPN
  - Can be default or more granular
- Redirects traffic to interfaces in VPN 0:
  - Interfaces must have NAT enabled
  - Multiple interfaces enables per-flow load-sharing
  - Relies on VPN 0 routing table
- Can be complemented with a Tracker to monitor Internet availability beyond first hop gateway

SD-WAN Internet Breakout Options

Local Breakout using Data Policy




```
WAN Edge
vpn 0
 interface ge0/0
  nat
```

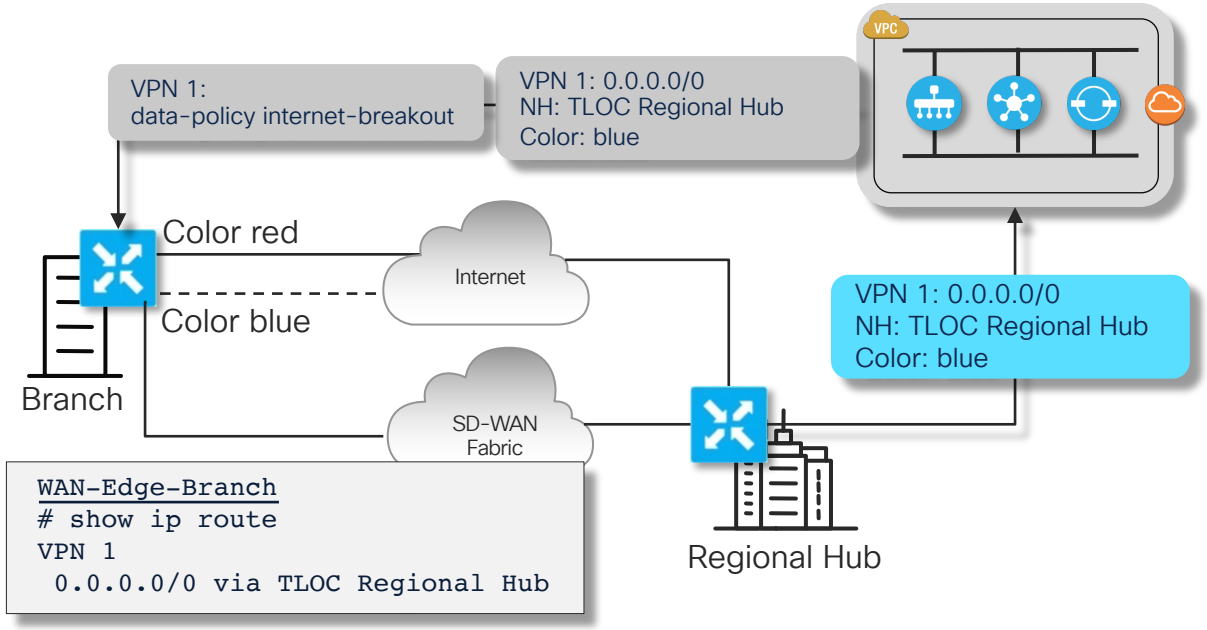
```
vSmart
policy
 data-policy internet-breakout
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.0/8
    !
    action accept
     nat use-vpn 0
     local-tloc public-internet
```

- Policy now redirects instead of static route
  - In case local exit fails, lookup can fall back to local service VPN routing table
- Redirects traffic to interfaces in VPN 0:
  - Interfaces must have NAT enabled
  - Multiple interfaces enables per-flow load-sharing
  - Relies on VPN 0 routing table
- Can be complemented with a Tracker to monitor Internet availability beyond first hop gateway (ref: previous slide)
- Local TLOC to be used can be specified

SD-WAN Internet Breakout Options

Joint Local and Regional Breakout using Data Policy + Routing

Legend:
- Original Advertisement from Endpoint
- Un/Modified Advertisement from Controller



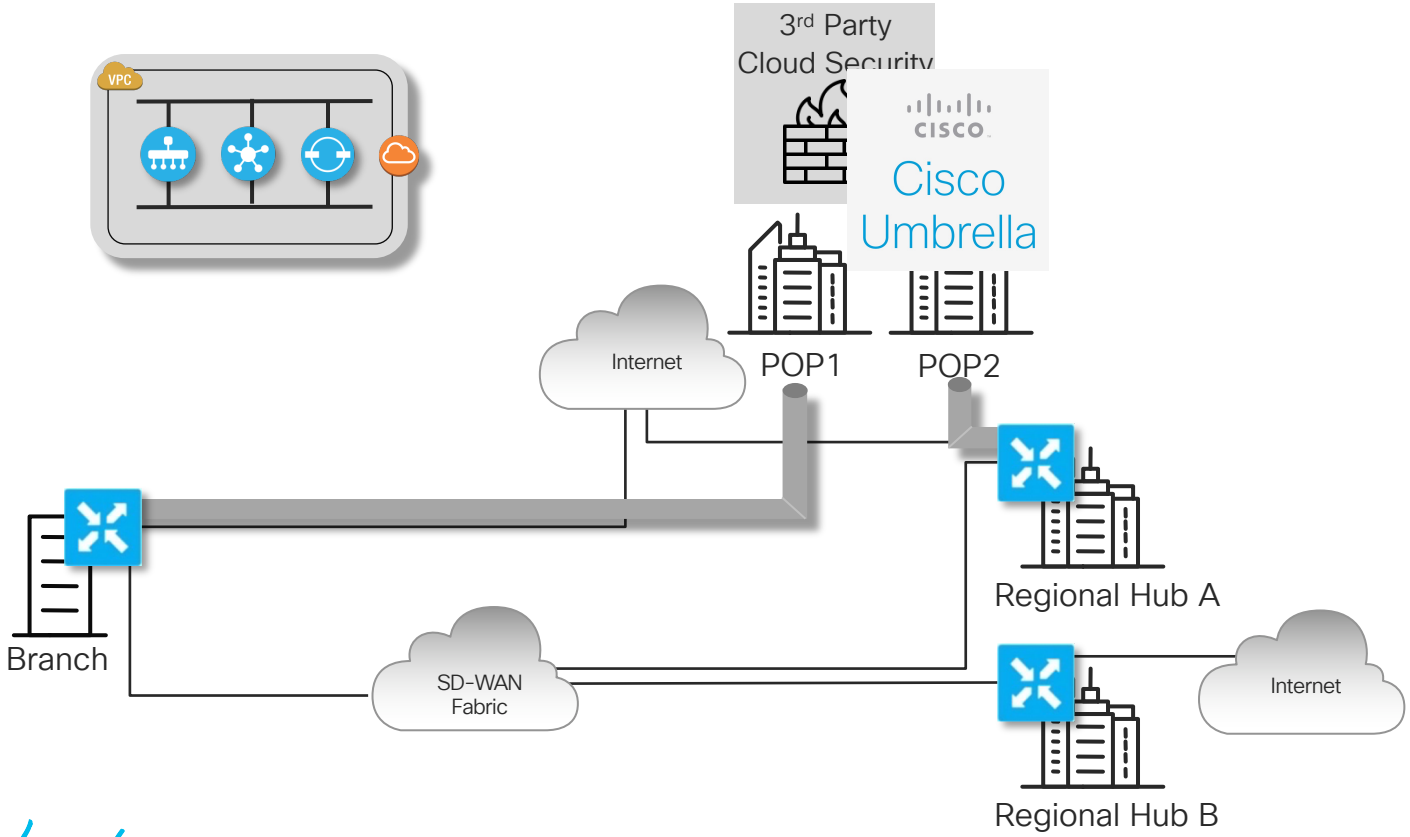

```
vSmart
policy
 data-policy internet-breakout
  vpn-list VPN1
   sequence 10
    match source-ip 10.0.0.0/8
    !
    action accept
     nat use-vpn 0
     local-tloc red blue
```

```
WAN-Edge-Regional Hub
VPN 1
 ip route 0.0.0.0/0 null0 or
 default from OSPF/BGP
```

- Data Policy allows for granular breakout policy matching L3/L4/L7 information
  - Data Policy takes precedence
  - Default route from Regional Hub acts as backup in case TLOC Red & Blue are both down

SD-WAN Internet Breakout Options

Joint Local and Regional Breakout using Data Policy and Cloud Security + Routing Preference



SD-WAN Internet Breakout Options

Joint Local and Regional Breakout using Data Policy and Cloud Security + Routing Preference

For Your Reference

```
vSmart
policy
 data-policy Cloud_Security
  vpn-list vpn_all
   sequence 10
    match
     destination-data-prefix-list internal-prefixes
    !
    action accept
    !
   !
   sequence 20
    match
    !
    action accept
     count count_fw
     set
      service FW local [restrict]
     !
```

Exclude Internal Prefixes from Internet Breakout

Any other traffic sent to Internet Breakout

Drop Traffic if Service Down

```
policy
 lists
  data-prefix-list internal-prefixes
   ip-prefix 10.0.0.0/8
   ip-prefix 172.16.0.0/12
   ip-prefix 192.168.0.0/16
```

```
WAN-Edge-Branch
vpn 1
 service FW interface gre1
vpn 0
 interface gre1
  ip address 12.13.14.15/24
  tunnel-source-interface ge0/0
  tunnel-destination 123.123.123.123
  no shutdown
```

```
WAN-Edge-Regional Hub A
vpn 1
 service FW interface gre1
 ! ip route 0.0.0.0/0 null0 or
 ! default from OSPF/BGP
```

```
WAN-Edge-Regional Hub B
vpn 1
 ! ip route 0.0.0.0/0 null0 or
 ! default from OSPF/BGP
```

SD-WAN Internet Breakout Options

Joint Local and Regional Breakout using Data Policy and Cloud Security + Routing Preference

For Your Reference

vSmart Control Policy

```
vSmart
Policy
 lists
  prefix-list default_route
   ip-prefix 0.0.0.0/0
  !
 !
 control-policy default_priority
  sequence 10
   match route
    prefix-list default_route
    site-id Regional Hub A
    !
    action accept
     set
      preference 100
    !
   !
  !
  default-action accept
```

Default from Hub A gets higher preference

WAN Edge Static TLOC preference

```
WAN-Edge-Regional Hub A
vpn 0
 interface ge0/0
  tunnel-interface
   encapsulation ipsec preference 100
!
vpn 1
 ! ip route 0.0.0.0/0 null0 or
 ! default from OSPF/BGP
```

```
WAN-Edge-Regional Hub B
vpn 0
 interface ge0/0
  tunnel-interface
vpn 1
 ! ip route 0.0.0.0/0 null0 or
 ! default from OSPF/BGP
```

SD-WAN Internet Breakout Options

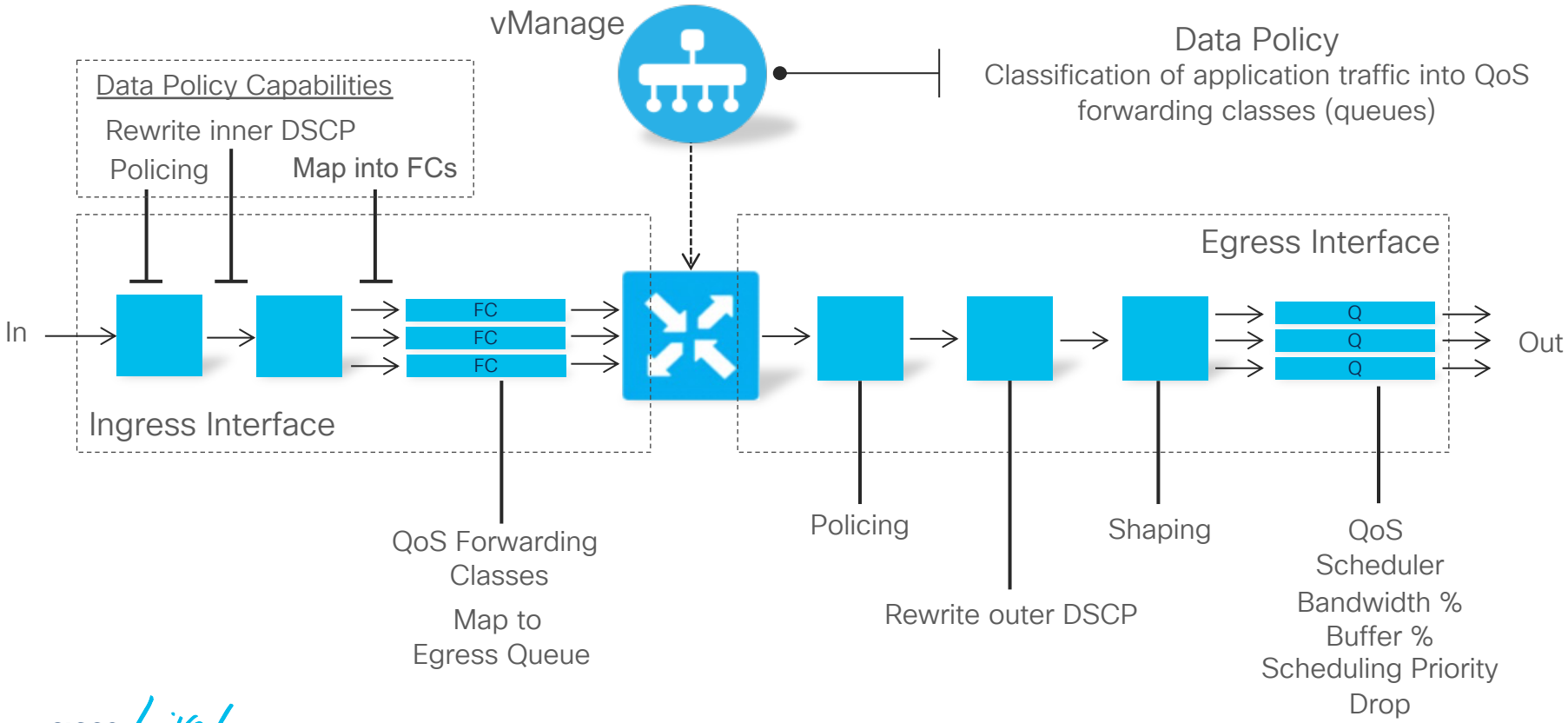
Application Specific Breakout

- The Data Policy construct can also be used to locally breakout specific applications with defined DPI signatures (e.g. O365, FaceBook, Youtube)
- Example:
  - Office365 to be locally broken out
  - All other Internet traffic via regional exit
- Arrangements required for supporting O365
  - Cloud On-Ramp SaaS recommended for breaking out locally
  - Default route from regional exit for two purposes:
    - Breakout for all non O365 traffic
    - O365 session establishment involves quite a few protocols beyond the core O365 protocols – A default route from somewhere is required to deal with those applications and allow for successful O365 operations
- SD-AVC support required to provide Application Recognition from the first packet

Quality of Service

WAN Edge Router Device QoS Overview

WAN Edge Router



Data Policy for QoS

Quality of Service – Policy Structure

For Your Reference

```
policy
 data-policy enterprise_traffic
  vpn-list VPN1
   sequence 10
    match app-list audio-video
    !
    action accept
     set
      dscp 46
      forwarding-class EF-class
     !
    !
   !
  !
 data-policy DIA
  vpn-list VPN10
   sequence 10
    match source-ip 10.0.0.0/8
    !
    action accept
     set
      policer police_DIA
     !
    !
   !
   default-action accept
  !
```

- App-list consists of DPI signature references
- Forwarding-class referring to configured QoS-class

  (Ref: qos-group in Cisco IOS)

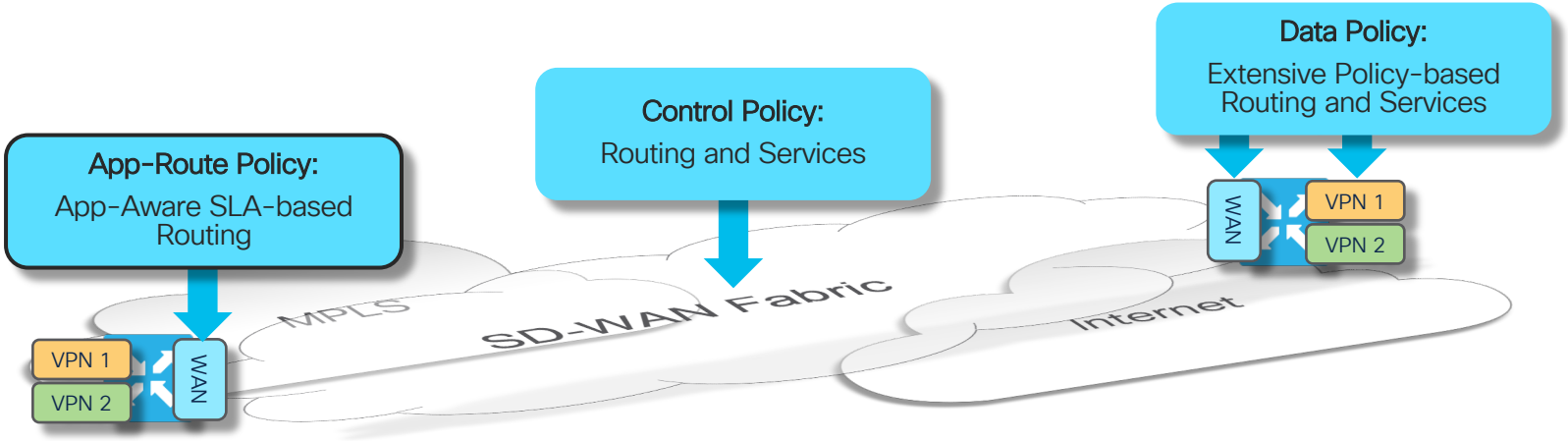
```
policy
  policer police_DIA
  rate    10000000
  burst   1000000
  exceed drop
 !
!
```

Policer configured as part of Policy

Policy Framework: App-Route Policies

Cisco SD-WAN Policy Architecture

Suite of Policies to address different functional domains



- Control Policies are applied at vSmart: Tailors routing information advertised to WAN endpoints
- App-Route Policies are applied at WAN Edge: SLA-driven path selection for applications
- Data Policies are applied at WAN Edge: Extensive Policy driven routing

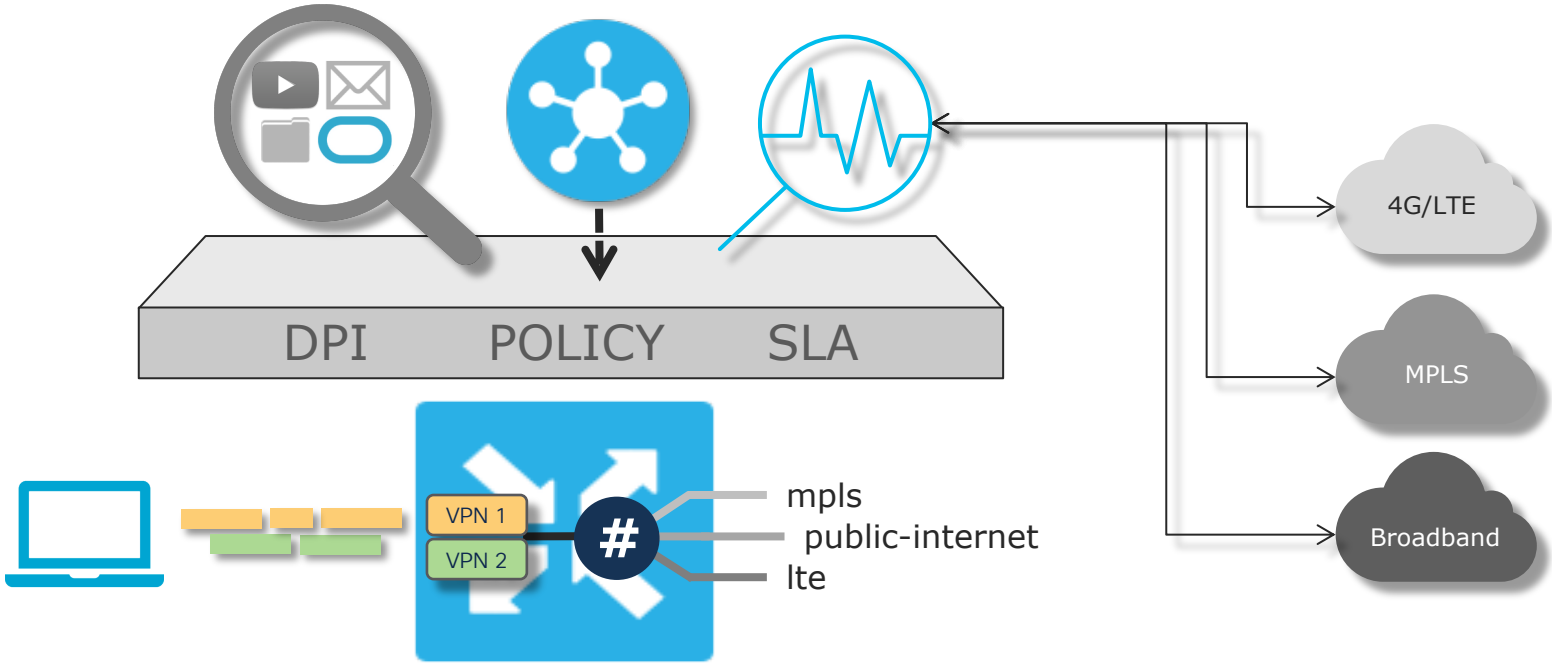
App-Route Policies

Centralized Policy for enabling SLA-driven routing on WAN Edge endpoints

- App-route policies:
  - Applied on vSmart
  - Advertised to and executed on vEdge
- Monitors SLAs for active overlay paths to direct Applications along qualified paths
- Allows for the use of L3/L4 keys or DPI Signatures for application identification
- Delivers a fully distributed SLA-driven routing mechanism

App-Aware Routing Policies

SLA-Driven Routing / Performance Routing



App-Route Policies

App-route Components and Dependencies / Configuration

BFD Settings
BFD rx_interval and multiplier settings
(only rx_interval is relevant to AAR)

```
bfd
 color <color>
  hello-interval <msec>
  multiplier <number>
```

App-route algorithm configuration
Define how SLA data is used to influence path selection

```
bfd
 app-route
  multiplier <number>
  poll-interval <msec>
```

App-route Policy Definition
Define SLA-classes, Application associations, VPN applicability and Policy actions/preferences

```
SLA-classes
Policy Construct
 match
 action
```

DPI Engine Enablement
AAR relies on DPI for L7 signatures

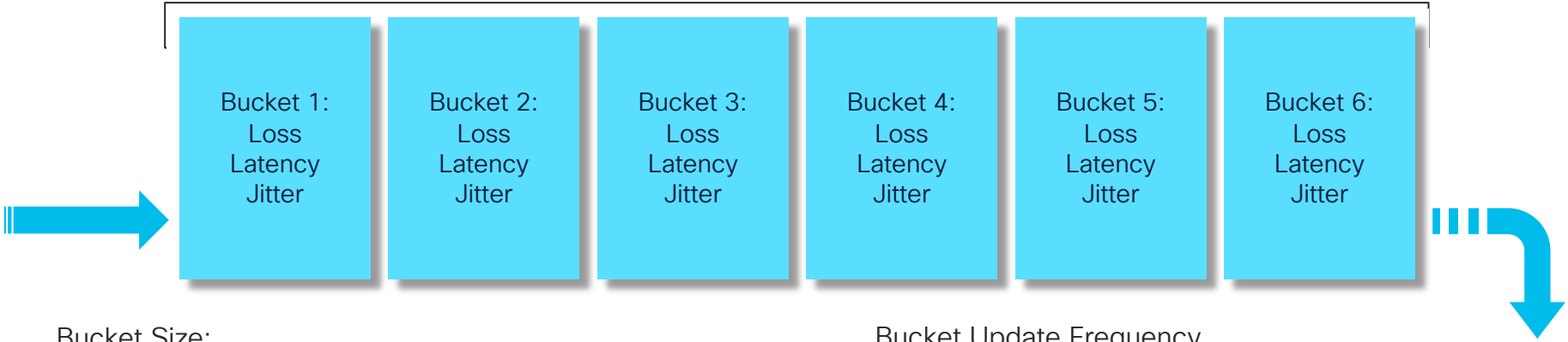
```
policy
 app-visibility
```

*https://docs.viptela.com/Product_Documentation/Software_Features/Release_18.2/07Policy_Applications/01Application-Aware_Routing/01Configuring_Application-Aware_Routing

App-Route Policies

App-route Algorithm

Avg (B1 + B2 + B3 + B4 + B5 + B6) = Mean
Mean recalculated every Bucket completion cycle



Bucket Size:

```
bfd
 app-route poll-interval
```
(default 600,000 ms)

# of Buckets:

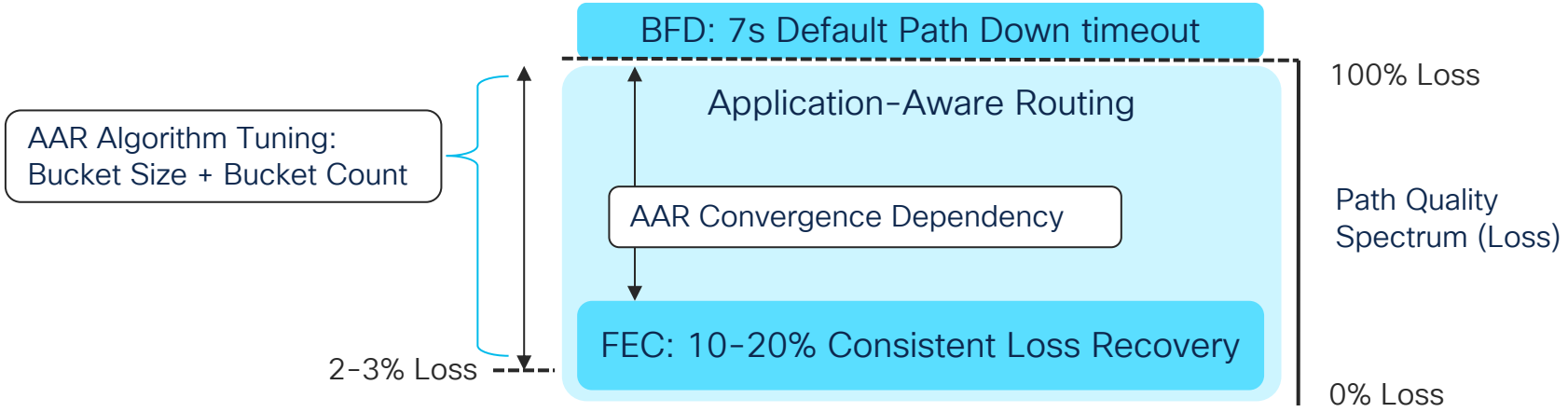
```
bfd
 app-route multiplier
```
(default 6)

Bucket Update Frequency

```
bfd
 hello-interval
```
(default 1000ms)

App-Route Policies

Path Blackout / Brownout Management

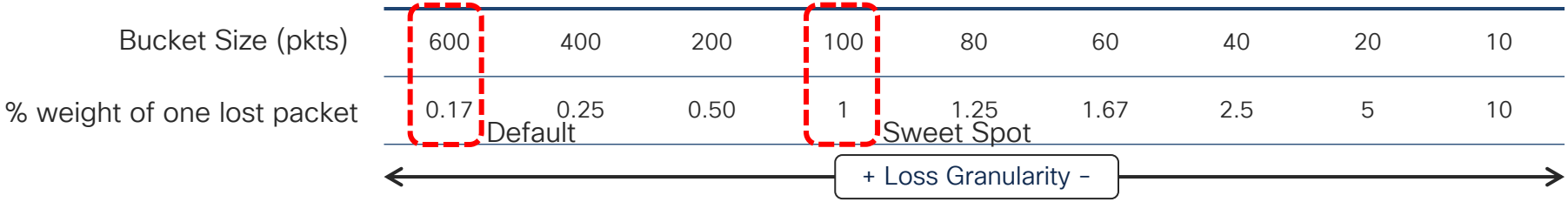


- Three Components in Complementary Working Order – BFD + FEC + AAR
- Consider Downsides of Traffic Sloshing vs Instant Convergence away from Brownout

App-Route Policies

App Route Algorithm Configuration

- Bucket Size in Packets = app-route poll-interval / hello-interval
- Consider bucket size (packets) impact on recalculation of Mean:



Bucket Size:

```
bfd
 app-route poll-interval  (default 600,000 ms)
```

Bucket Update Frequency

```
bfd
 hello-interval  (default 1000ms)
```

- Mean Loss / Latency / Jitter calculated across app-route-multiplier buckets

# of Buckets:

```
bfd
 app-route multiplier  (default 6)
```

Weight of new bucket relative to multiplier: 1/6, 1/4, 1/3 etc

App-Route Policies

App-route Policy Definition

SLA Classes
Loss, Latency, Jitter per Class

```
Policy
 sla-class <name>
  jitter <msec>
  latency <msec>
  loss <percentage>
```

App-list
Use L3/L4 or DPI Signatures

```
Policy
 lists
  app-list <name>
   app <name> | app-family <family>
```

App-route Policy
VPN applicability and Policy actions/preferences

App-route Logging
Enable logging of packet headers

App-Route Policies

App-route Policy Definition

SLA Classes
Loss, Latency, Jitter per Class

App-list
Use L3/L4 or DPI Signatures

App-route Policy
VPN applicability and Policy actions/preferences

App-route Logging
Enable logging of packet headers

1. For traffic not explicitly matched in policy
2. For traffic with an SLA-class disqualified across all links
3. Drop traffic if SLA-class is disqualified
4. One or more preferred colors if multiple links qualify

```
Policy
 app-route-policy <name>
  vpn-list <vpn-list>
   default-action sla-class <name>          1
   sequence <number>
    match
     …
    action
     backup-sla-preferred-color [list]      2
     count <name>
     log
     sla-class <name> [strict] [preferred-color [list]]
                              3              4
```

App-Route Policies

Policy Example

For Your Reference

```
policy
 lists
  vpn-list VPN1
   vpn 1
  !
  site-list app-route-sites
   site-id 3003
  !
  app-list AVV
   app-family audio_video
  !
  app-list SFDC
    app salesforce
  !
```

1 Declare app-lists for policy match

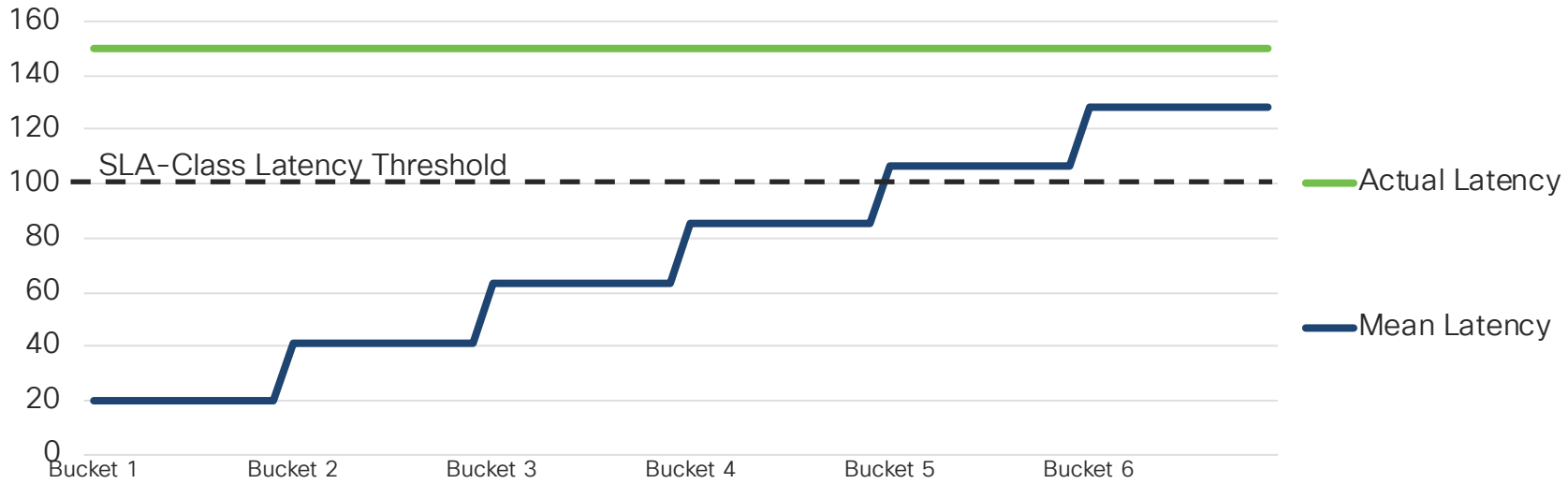
```
apply-policy
 site-list app-route-sites
  app-route-policy SLA-Routing
```

```
Policy
 sla-class EF
  loss    1
  latency 100
 !
 sla-class Biz-apps
  loss    2
  latency 150
 !
 app-route-policy SLA-Routing
  vpn-list VPN1
   sequence 10
    match app-list AVV
    !
    action
     sla-class EF
    !
   !
   sequence 20
    match app-list SFDC
    !
    action
     sla-class Biz-apps
    !
   !
```

2 Define SLA classes and thresholds

3 Map app-lists to SLA classes and other actions

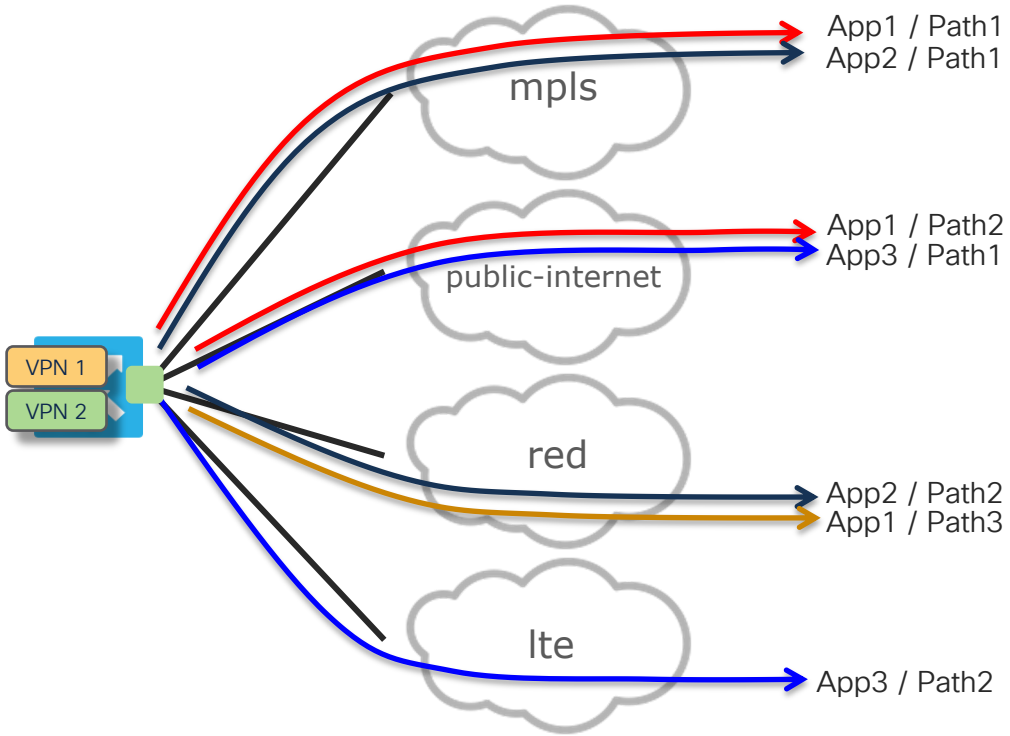
App-route Policy Path Convergence



Current Mean Latency is 20ms, when Latency jumps to 150ms as Bucket 1 collection starts

AAR Policy Use Case

Application Pinning with SLA



- App1
  - SLA-class: Business
  - MPLS / Public-Internet: Primary – Load-share
  - Red: Backup
  - Fall back to Routing
- App2
  - SLA-class: EF
  - MPLS: Primary
  - Red: Primary
  - Drop on Path Unavailability
- App3
  - SLA-class: POS
  - Public-Internet: Primary
  - LTE: Backup
- Other Apps
  - SLA-Class: Default

App-Route Policies

Application Pinning with SLA

For Your Reference

```
policy
 lists
  vpn-list VPN1
   vpn 1
  !
  site-list app-route-sites
   site-id 3003
  !
  app-list App1
   app-family <name>
  !
  app-list App2
    app <name>
  !
  app-list App3
    app <name>
  !
```

```
Policy
 sla-class EF
  loss    1
  latency 100
 !
 sla-class Business
  loss    2
  latency 150
 !
 sla-class POS
  loss 1
  latency 200
 !
 sla-class Default
  loss 5
  latency 300
 !
```

```
apply-policy
 site-list app-route-sites
  app-route-policy SLA-Routing
```

```
Policy
app-route-policy SLA-Routing
  vpn-list VPN1
   sequence 10
    match app-list App1
    !
    action
     backup-sla-preferred-color red
     sla-class Business preferred-color mpls public-internet
    !
   !
   sequence 20
    match app-list App2
    !
    action
     sla-class EF strict preferred-color mpls red
    !
   !
   sequence 30
    match app-list App3
    !
    action
     backup-sla-preferred-color lte
     sla-class POS preferred-color public-internet
    !
   !
   sequence 40
    match
    !
    action
     sla-class Default
    !
   !
```

Primary: mpls + public-internet
Backup: red

Primary: mpls + red
Backup: None - Drop

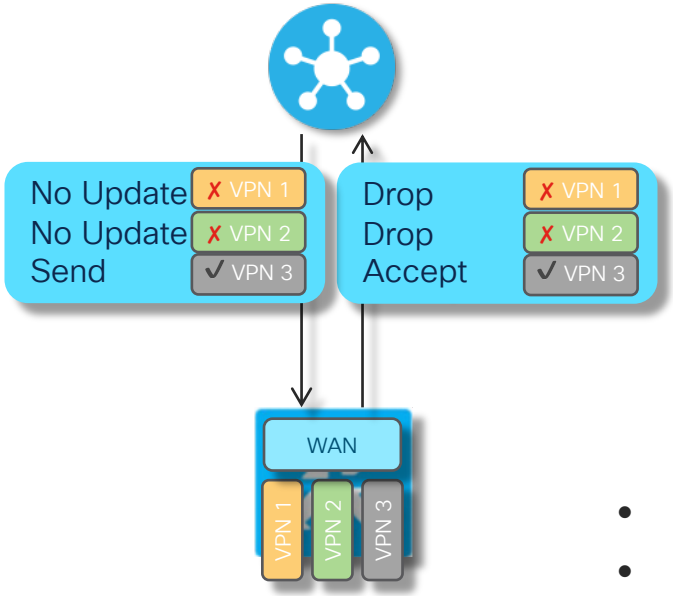
Primary: public-internet
Backup: lte

Primary: Any link meeting SLA
Backup: Any other link

Other Centralized Policies:
VPN Membership
cFlowd

VPN Membership Policies

VPN Service filtering between vEdge and vSmart




```
Policy
 lists
  vpn-list restricted_vpns
   vpn 1, 2
  !
 !
 vpn-membership acme_1
  sequence 10
   match vpn-list restricted_vpns
   action reject
   !
  !
  default-action accept
 !
!
```

- Restricted VPNs become islands on hosting vEdge
- Outbound vSmart updates are not generated
- White-listing or Black-listing possible

cFlowd / Netflow Template

Configuring the cFlowd Cache and Collectors

Max Collectors: 4
Flow-active-timeout: Default 600s
Flow-inactive-timeout: Default 60s
Flow-sampling-interval: Default 0
Template-refresh: Default 90s

```
policy
 cflowd-template cflowd_temp
 collector vpn 100 address 1.1.1.1 port 4739 transport transport_udp
  flow-active-timeout   60
  flow-inactive-timeout 60
  flow-sampling-interval
  template-refresh
 !
!
```

- cFlowd enabled by policy / flow-visibility configuration Applied on vSmart
  - Populates local flow-cache only
- cFlowd Template required to configure and enable export

Tips and Tricks

Useful Policy Features

For Your Reference

Generic Policy Features

Function	Description	Comment

Elimination statement	Use Match without an action in a sequence
	`Sequence 10`
	`match route`
	`!`
	`action accept`
		Useful for ensuring that certain objects are eliminated from further policy processing

Catchall statement	Use 'action accept' without a match in a sequence
	`Sequence 10`
	`action accept`
		Useful to ensure all traffic is matched and to allow for use of 'set' or other action

Color-List	Match any color using color-list
	`color-list colors`
	`color red`
	`color blue`
		Useful in control policies to match a selection of TLOCs with different colors or routes originating from TLOCs of different colors

Counter	Extremely useful for troubleshooting and policy verification
	`action accept`
	`count <name>`
		To display, use:
		Show policy app-route-policy-filter
		Show policy data-policy-filter

Default-action	Applied to any traffic not matched by another statement in the policy `default-action reject`	Default-action is set to reject or drop by default. It is always visible in the policy

Enable DPI	vEdge and IOS-XE:
	`Policy`
	`app-visibility`
		IOS-XE will automatically have added:
		`Interface x/y/z`
		`ip nbar protocol discovery`

Useful Policy Features

For Your Reference

Generic Policy Features

Function	Description	Comment

Match logic	Match protocol AND ANY entry in prefix-list:
	`Match`
	`protocol 6`
	`destination-data-prefix-list`
		Lists are used to matched any entry (or)
		Entries in match statement are match all (and)

Match Route vs TLOC	Match statements for routes and TLOCs have different match criteria and also allow 'set' of different attributes	Related to the specific attributes associated with each
Omp-tag	Control-policy: Match and Set Local Policy: Match and Set	Equivalent to a BGP community for OMP for generically tagging and identifying routes and TLOCs

Policy Application

Rules and Restrictions

- The minimum granularity for policy application is the Site-ID
  - Multiple devices sharing the same Site–ID is subject to the same policies being applied
- Any given Site-ID is restricted to a single policy of each type, per direction
- Example, given Site-ID 100:
  - Control-Policy 1 in or out, or both
  - Control-Policy 2 in or out, or both – where ever Control-Policy 1 is not applied
  - App-route-policy 1 (only applied outbound – transport facing)
  - Data-policy 1 from-service or from-tunnel, or all
  - Data-policy 2 from-service or from-tunnel, or all (where Data-policy 1 is not applied)
- Different App-route policies and Data-policies can be applied per VPN

Regional Internet Access via Transport

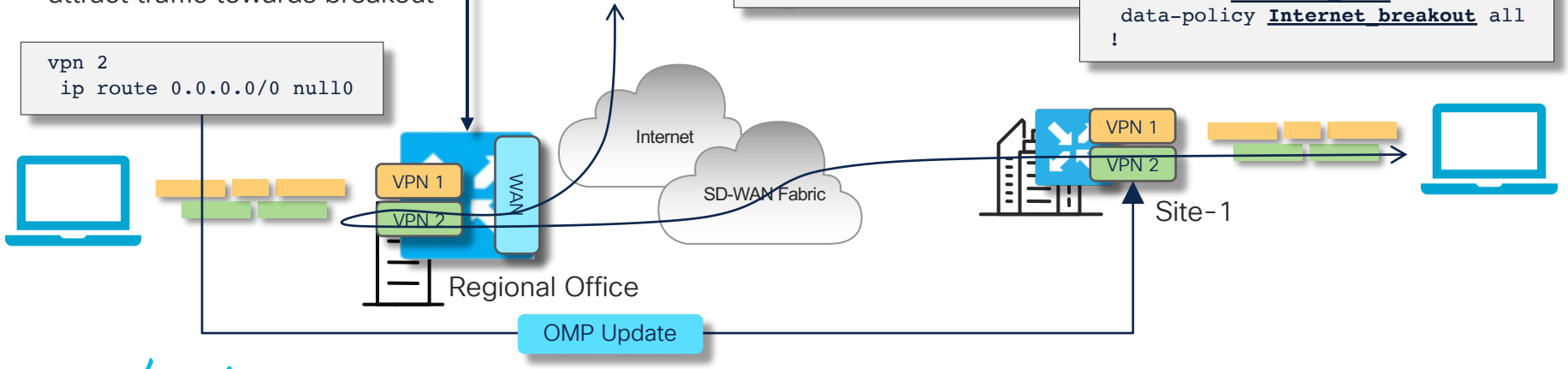
Hair-pinning via Transport

- Data-policy Sequence 10
  Allow standard routing for internal prefixes
- Data-policy Sequence 20
  Direct all other traffic to DIA
- Apply Data-policy in both directions to service up and downstream traffic
- Originate a default route to attract traffic towards breakout

```
data-policy Internet_breakout
  vpn-list vpn_all
   sequence 10
    match
     destination-data-prefix-list internal-pfx
    !
    action accept
   !
   sequence 20
    match
    !
    action accept
     local-tloc public-internet [restrict]
    !
  default-action accept
 !
```

```
apply-policy
 site-list regional_exit
  data-policy Internet_breakout all
 !
```

```
vpn 2
 ip route 0.0.0.0/0 null0
```



Cisco Umbrella Integration

Policy Generated via vManage Security Policy Configuration

```
policy
 lists
  local-domain-list exclude-domains
    cisco.com
   !
  !
 !
security
 umbrella
  token 1234567890ABCDEF
  dnscrypt
 !
!
vpn matchAllVpn
 dns-redirect umbrella match-local-domain-to-bypass
```

Domains to exclude for redirection of DNS lookups and subsequent flows

DNSCrypt (eDNS) allows for tracking the origin of DNS requests, in addition to encryption

DNS set to use Umbrella for all VPNs.

Platform Support and Scalability

Policy Scalability and Performance

Policy Construction Guidelines

- Not different from most other parsing processes
- Eliminate objects / traffic in early and target simple policy statements
  - Good example is to exclude internal prefixes from further processing in first sequence
- Simple Match statements are better
  - Single Prefixes, Ports, DSCP, Protocol Ports, App-IDs
  - Avoid placing long prefix lists and port lists early
  - Ranges are better than lists if possible
- Fewer Set statements are better
  - Forwarding redirection better than header modifications (Set Next-Hop vs set DSCP)

Policy Scalability and Performance

Policy Construction Guidelines

- Control Policies, VPN Membership
  - Processed on vSmart for routing updates only
  - Structure is less critical
- cFlowd Template
  - Simple and sent on application and update only
- App-aware Routing and Data Policies
  - Affects all traffic traversing the device (in enabled VPNs)
  - Policy Structure is imperative to minimize any performance impact

Policy Scalability and Memory Consumption

Policy Construction Guidelines

- Platforms are limited in how many entities can be supported
  - Policy Instances
  - Sequence Instances
  - Shared Memory Pools or TCAM used for Match / Set
- Memory consumption is challenging to determine upfront
- Hidden command being exposed in following releases

  `show policy filter-memory-usage`

  vEdge: 19.3 (Dec ‘19)

  cEdge: 17.2.1 (Mar ’20)

Policy Scalability – The Numbers

Forwarding Plane Policies

Element	vEdge-100	vEdge-1/2/5K	ISR	ASR
Policy Instances	256	512	512	512
Policy Sequences	Filter Block Dependent	Filter Block Dependent	Policy Memory Chunk Dependent	TCAM Dependent
Filter Block	6/16/64 * 1024 (Model dependent)	1024 x 1024	N/A	N/A
Policy Memory Chunks	N/A	N/A	64K	N/A
TCAM	N/A (Next-Gen Models=10-20MB)	N/A	N/A	20-80MB (Platform dependent)
Match Statement	>= 1 Filter Block depending on construct	>= 1 Filter Block depending on construct	>= 1 Policy Chunk depending on construct	>=1 160b Entry depending on construct
Action Statement	>= 1 Filter Block depending on construct	>= 1 Filter Block depending on construct	No Limit	No Limit

Policy Feature Support

For Your Reference

Control Policy

Function	Description	vEdge	IOS-XE
Match / Route / Color	Match Routes of a given color	vSmart Only 14.1	vSmart Only 16.9
Color-List	Match routes of any color in the list	vSmart Only 15.4	vSmart Only 16.9
Ipv6-prefix-list	Match routes present in the prefix-list	vSmart Only 18.4	vSmart Only 16.9
Omp-tag	Match routes with the specific omp-tag	vSmart Only 15.4	TBD
origin	Match routes with the specified origin protocol (Connected, Static, eBGP, OSPF Intra, OSPF Inter, OSPF External, iBGP, Unknown/Unset)	vSmart Only 14.1	vSmart Only 16.9
originator	Match routes that originated from specified system-IP (as in originating vEdge)	vSmart Only 14.1	vSmart Only 16.9
preference	Match routes with the specified preference	vSmart Only 14.1	vSmart Only 16.9
Prefix-list	Match routes present in the prefix-list	vSmart Only 14.1	vSmart Only 16.9
Site-id	Match routes originating from the specified site-id	vSmart Only 14.1	vSmart Only 16.9

Policy Feature Support

For Your Reference

Control Policy

Function	Description	vEdge	IOS-XE
Site-list	Match Routes from any site present in the list	vSmart Only 14.1	vSmart Only 16.9
tloc	Match routes from the specified TLOC	vSmart Only 14.1	vSmart Only 16.9
Tloc-list	Match routes from any TLOC in the list	vSmart Only 14.1	vSmart Only 16.9
vpn	Match routes belonging to the specified VPN	vSmart Only 14.1	vSmart Only 16.9
Vpn-list	Match routes belonging to any VPN in the list	vSmart Only 14.1	vSmart Only 16.9
Match / Tloc / Carrier	Match TLOCs with the specified carrier	vSmart Only 14.2	TBD
color	Match TLOCs with the specified color	vSmart Only 14.1	vSmart Only 16.9
Color-list	Match TLOCs with any color present in the list	vSmart Only 15.4	vSmart Only 16.9
Domain-id	Match TLOCs originating from the specified domain-id	Not currently implemented	Not currently implemented

Policy Feature Support

For Your Reference

Control Policy

Function	Description	vEdge	IOS-XE
Group-id	Match TLOCs with the specified Group-id	vSmart Only 15.1	TBD
Omp-tag	Match TLOCs with the specified OMP-tag	vSmart Only 15.4	TBD
originator	Match TLOCs originating from the specific System-IP	vSmart Only 14.1	vSmart Only 16.9
preference	Match TLOCs with the specified preference	vSmart Only 14.1	vSmart Only 16.9
Site-id	Match TLOCs originating from the specified Site-ID	vSmart Only 14.1	vSmart Only 16.9
Site-list	Match TLOCS originating from any site in the list	vSmart Only 14.1	vSmart Only 16.9
tloc	Match the specified TLOC	vSmart Only 14.1	vSmart Only 16.9
Tloc-list	Match any TLOC in the list	vSmart Only 14.1	vSmart Only 16.9

Policy Feature Support

For Your Reference

Control Policy

Function	Description	vEdge	IOS-XE
Action / Accept (applicable to Match / Route)	Accept matched route and install in RIB without further action	vSmart Only 14.1	vSmart Only 16.9
Export-to vpn | vpn-list	Export the matched route into the specified VPN | List	vSmart Only 14.1	vSmart Only 16.9
Set omp-tag	Set an OMP-tag on the matched route	vSmart Only 15.4	TBD
Set preference	Set the preference on the matched route	vSmart Only 14.1	vSmart Only 16.9
Set Service <type>	Associate a service with the matched route to enable service chaining	14.1	TBD
Set service <type> [tloc]	Associate the service advertised from the specified TLOC with the matched route	16.3	TBD
Set service <type> [tloc-list]	Associate the service advertised from a TLOC in the specified list with the matched route	16.3	TBD
Set service <type> [vpn]	Associate a service advertised from the specified VPN with the matched route	16.3	TBD

Policy Feature Support

For Your Reference

Control Policy

Function	Description	vEdge	IOS-XE
Set tloc	Reset the TLOC on the matched route	vSmart Only 14.1	vSmart Only 16.9
Set tloc-action backup | ecmp | primary | strict	Set a TLOC action for the matched route to enable overlay Traffic Engineering using Service TE	16.3	TBD
Set tloc-list	Reset the TLOC to a list of TLOCs on the matched route	vSmart Only 14.1	vSmart Only 16.9
Action / Accept (applicable to Match / TLOC)	Accept matched TLOC and install into RIB without further action	vSmart Only 14.1	vSmart Only 16.9
Set omp-tag	Set OMP-tag on the matched TLOC	vSmart Only 15.4	TBD
Set preference	Set preference on the matched TLOC	vSmart Only 15.4	vSmart Only 16.9

Policy Feature Support

For Your Reference

Data Policy

Function	Description	vEdge	IOS-XE
Match / App-list	Match DPI application signature(s) specified in App-list	15.4	16.9
Destination-data-ipv6-prefix-list	Match packet destination IP to any prefix specified in prefix-list	TBD	16.10
Destination-data-prefix-list	Match packet destination IP to any prefix specified in prefix-list	14.1	16.9
Destination-ip	Match packet destination IP to IP-address / Prefix specified	14.1	16.9
Destination-ipv6	Match packet destination IP to IP-address / Prefix specified	TBD	16.10
Destination-port	Match packet destination-port	14.1	16.9
Dns request | response	Match on DNS traffic for intercept / redirect	17.2	16.9
Dns-app-list	Match on DNS traffic for the specified set of applications for intercept / redirect	17.2	16.9
dscp	Match on packet DSCP	14.1	16.9

Policy Feature Support

For Your Reference

Data Policy

Function	Description	vEdge	IOS-XE
Packet-length	Match on packet length	14.1	16.9
plp	Match packet PLP	16.3	TBD
protocol	Match packet protocol	14.1	16.9
Source-data-ipv6-prefix-list	Match packet source IP to any prefix specified in prefix-list	TBD	16.10
Source-data-prefix-list	Match packet source IP to any prefix specified in prefix-list	14.1	16.9
Source-ip	Match packet destination IP to IP-address / Prefix specified	14.1	16.9
Source-ipv6	Match packet destination IP to IP-address / Prefix specified	18.4	16.10
Source-port	Match packet source port	14.1	16.9
Tcp syn	Match packet TCP flag	14.1	16.9

Policy Feature Support

For Your Reference

Data Policy

Function	Description	vEdge	IOS-XE
Action / Accept	Accept any matching packet for forwarding	14.1	16.9
Set dscp	Set the DSCP on the matched packet	15.1	16.9
Set forwarding-class	Set the packet to use a specific QoS Class within the node without setting the DSCP (eq qos-group)	15.1	16.9
Set local-tloc color [encap]	Pin the matching flow/packet to the defined TLOC	16.1	17.2.1
Set local-tloc-list color [encap] [restrict]	Pin the matching flow/packet to the list of TLOCs, using ECMP for >1. Restrict will cause drop if no chosen color is operational, otherwise process falls back to RIB.	16.1	17.2.1
Set local-tloc / local-tloc-list	Pin the matching flow/packet to the defined TLOC for DIA/Split tunneling traffic	16.1	17.2.1
Set next-hop	Route the matching flow/packet to the chosen IP	14.1	16.9
Set next-hop-ipv6	Route the matching flow/packet to the chosen IP	18.4	16.10
Set policer	Apply the defined policer to the traffic	14.1	16.11

*Not yet Committed

Policy Feature Support

For Your Reference

Data Policy

Function	Description	vEdge	IOS-XE
Set service <type>	Associate a service with the matched traffic to enable service chaining	14.1	TBD
Set service local <type> [restrict] vpn <n>	Associate a local service with the matched route to enable service chaining	15.4.1	TBD
Set service tloc <system-ip> <color> <encap>	Associate the service advertised from the specified TLOC with the matched traffic	16.1	TBD
Set service tloc-list	Associate the service advertised from a TLOC in the specified list with the matched traffic	16.1	TBD
Set tloc	Route the matching traffic to a remote TLOC on a different SD-WAN Edge node across the WAN	14.1	16.12
Set tloc-list	Define a list of TLOCs to be used in preference order and with ECMP in case of multiple with equal preference	14.1	16.12
Set vpn	Define a next-hop VPN for the matching traffic	14.1	16.9
Action / cflowd	Enable flow-accounting for the matching traffic	14.3	16.9
count	Create a counter for the matching traffic	14.1	16.9

Policy Feature Support

For Your Reference

Data Policy

Function	Description	vEdge	IOS-XE
drop	Drop the matching traffic	14.1	16.9
Log *policy log-frequency 1000 (default nearest down power of 2 packet is logged, so every 512th)	Create a log entry (using the log configuration for the node) for the matching traffic	16.3	TBD
Loss-protect fec-adaptive	Enable Adaptive FEC for the matching traffic (FEC is enabled on >=2% path packet loss	18.4	TBD
Loss-protect fec-always	Enable continuous FEC for the matching traffic	18.3	16.11
Loss-protect pkt-dup	Enabled packet duplication for the matching traffic	18.4	16.12
Nat pool <name>	NAT the matching traffic using the named NAT-pool	15.3	16.9
Nat use-vpn <0> [fallback]	NAT the matching traffic as it is subject to split tunneling / DIA via VPN 0. Fallback allows for falling back to routing on NAT resource exhaustion	14.2	16.9
Nat use-vpn <0> pool <name>	NAT the matching traffic using the name NAT-pool as it is subject to split tunneling / DIA via VPN 0.	TBD	16.9

*Introduced in 16.3 / TBD

Policy Feature Support

For Your Reference

Data Policy

Function	Description	vEdge	IOS-XE
Redirect-dns <ip>	Redirect the intercepted DNS request to the server residing at IP	17.2	16.9
Redirect-dns host	Redirect the intercepted DNS request for resolution locally on the node	TBD	TBD
Redirect-dns umbrella	Redirect the intercepted DNS request to Umbrella / Open DNS	TBD	16.10
Tcp-optimization	Enable TCP-optimization for the matching traffic	17.2	16.12

Policy Feature Support

For Your Reference

App-Route Policy

Function	Description	vEdge	IOS-XE
Match / app-list	Match DPI application signature(s) specified in App-list	14.2	16.9
Cloud-saas-app-list	Used for Cloud On-Ramp SaaS (orchestrated by vManage)	16.3	17.2.1
Destination-data-ipv6-prefix-list	Match packet destination IP to any prefix specified in prefix-list	TBD	16.10
Destination-data-prefix-list	Match packet destination IP to any prefix specified in prefix-list	14.2	16.9
Destination-ip	Match packet destination IP to IP-address / Prefix specified	14.2	16.9
Destination-ipv6	Match packet destination IP to IP-address / Prefix specified	TBD	16.10
Destination-port	Match packet destination-port	14.2	16.9
Dns request | response	Match on DNS traffic for intercept / redirect	17.2	16.9
Dns-app-list	Match on DNS traffic for the specified set of applications for intercept / redirect	17.2	16.9

*Not yet Committed

Policy Feature Support

For Your Reference

App-Route Policy

Function	Description	vEdge	IOS-XE
dscp	Match on packet DSCP	14.2	16.9
plp	Match packet PLP	16.3	TBD
protocol	Match packet protocol	14.2	16.9
Source-data-ipv6-prefix-list	Match packet source IP to any prefix specified in prefix-list	TBD	16.10
Source-data-prefix-list	Match packet source IP to any prefix specified in prefix-list	14.2	16.9
Source-ip	Match packet destination IP to IP-address / Prefix specified	14.2	16.9
Source-ipv6	Match packet destination IP to IP-address / Prefix specified	14.2	16.10
Source-port	Match packet source port	14.2	16.9

Policy Feature Support

For Your Reference

App-Route Policy

Function	Description	vEdge	IOS-XE
Action / backup-sla-preferred-color	Specify the TLOC to use for traffic in an SLA-class disqualified across all links	16.3	17.2.1
Cloud-saas	Used for Cloud On-Ramp SaaS (orchestrated by vManage)	16.3	17.2.1
count	Create a counter for the matching traffic	14.2	16.9
Log *policy log-frequency 1000 (default nearest down power of 2 packet is logged, so every 512th)	Create a log entry (using the log configuration for the node) for the matching traffic	16.3	TBD
Sla-class <name>	Associate the matching traffic with a defined SLA-class	14.2	16.9
Sla-class <name> preferred-color <n> [<n>] ...	Configure a preferred TLOC for the traffic being associated to the SLA-class (multiple for ECMP)	15.2 / 17.1^ (^multiple colors)	16.9 / 16.9
Sla-class <name> strict	Drop the traffic being associated with the SLA-class in case there's no path meeting the SLA threshold(s)	14.2	16.9
Default-action sla-class	Define SLA for traffic not explicitly matched in a sequence	14.2	16.9

*Introduced in 16.3 / TBD **Not yet Committed

Thank you

Possibilities

#CiscoLive