cisco Live!

Let's go

The bridge to possible

Harnessing the Capabilities of the Cisco Catalyst SD-WAN Policy Framework

Architecture, Building Blocks and Case Studies

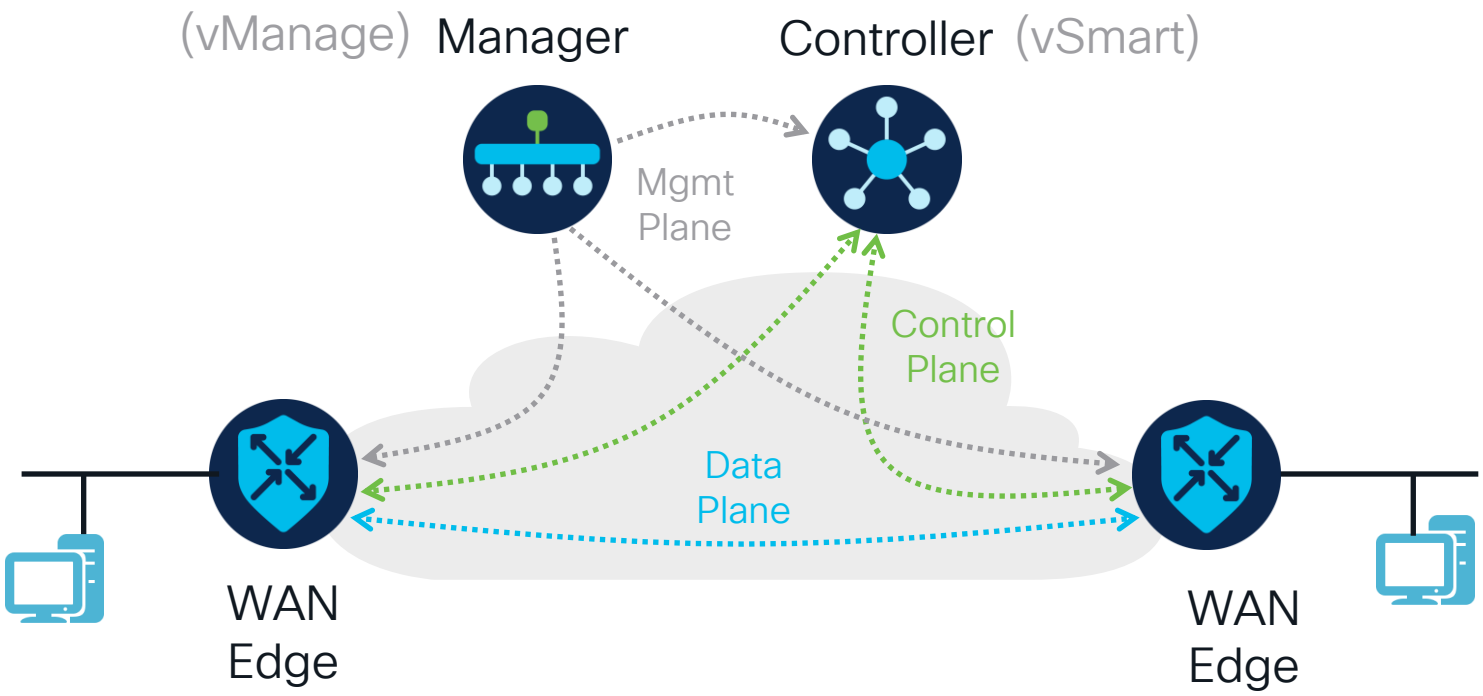
Kazuo Yamamoto, Global Solutions Engineer, CCIE #5644

Session Objectives

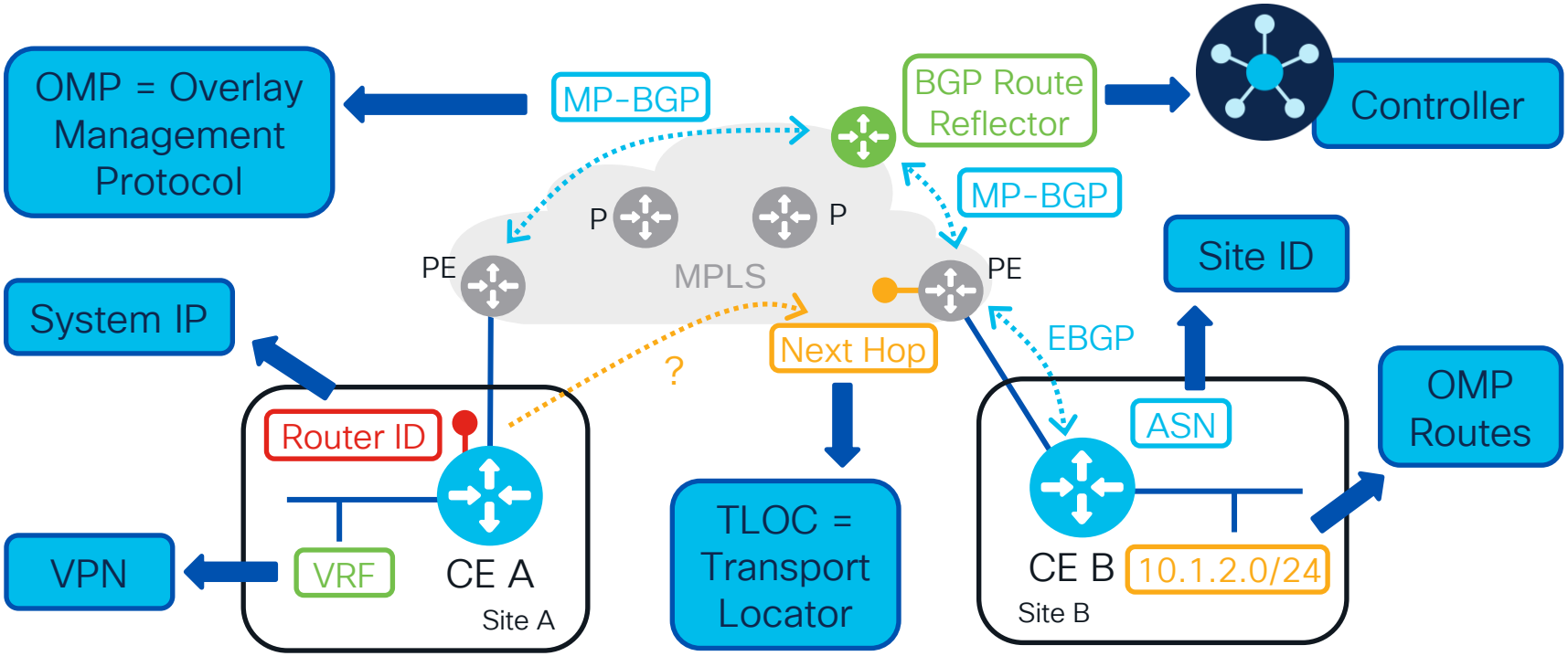
Based on the Abstract

- Examine the Cisco Catalyst SD-WAN policy structure and components, accompanied by real-world scenarios and practical applications that illustrate the significant potential of policies within the SD-WAN fabric.
- Equip you with the necessary knowledge and tools to optimize performance and security through the design and implementation of effective SD-WAN policies.

Catalyst SD-WAN: A High-Level Overview



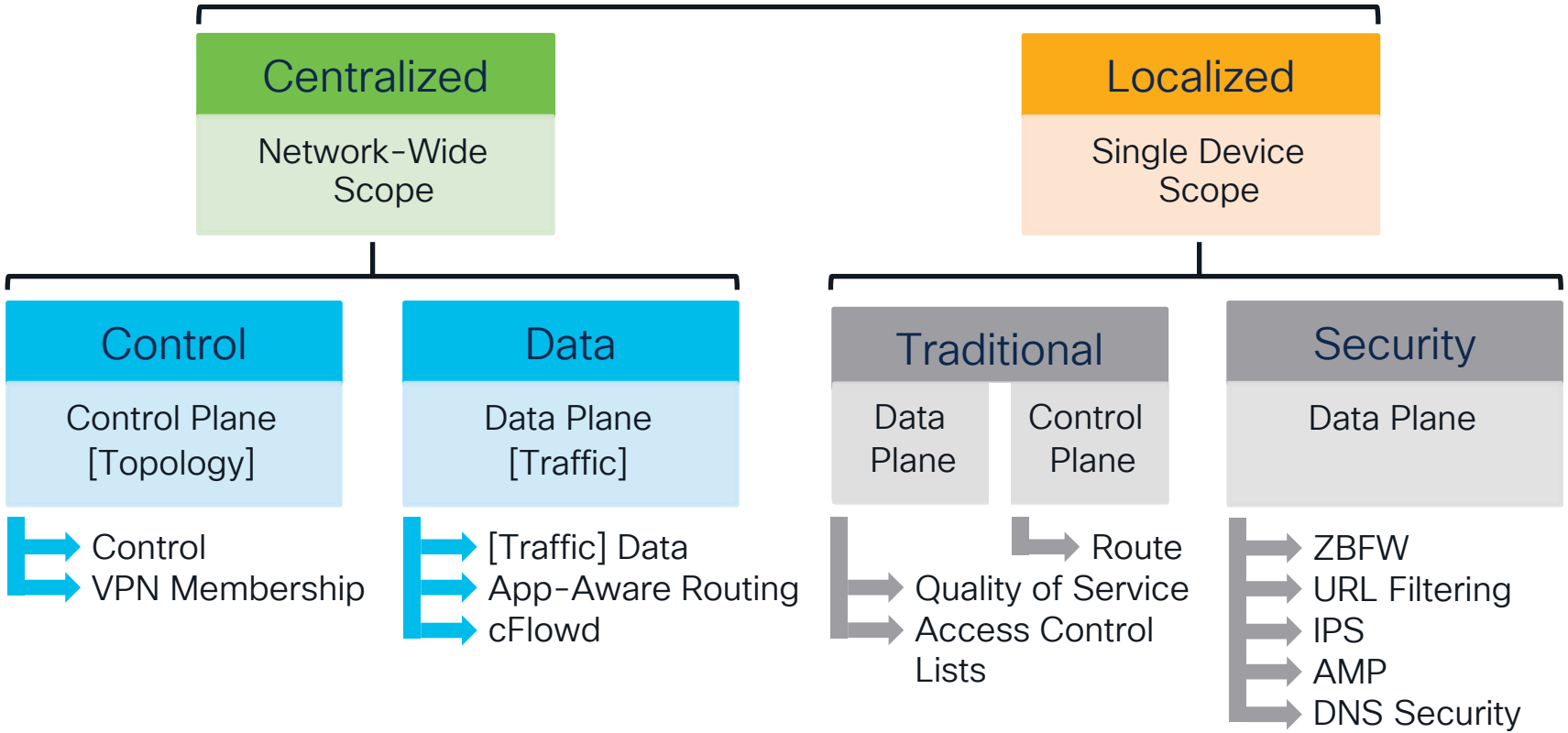
A Networking Analogy: MPLS VPN*



* Analogy = correspondence or similarity (not a synonym)

Policy Introduction

Catalyst SD-WAN Policy Architecture

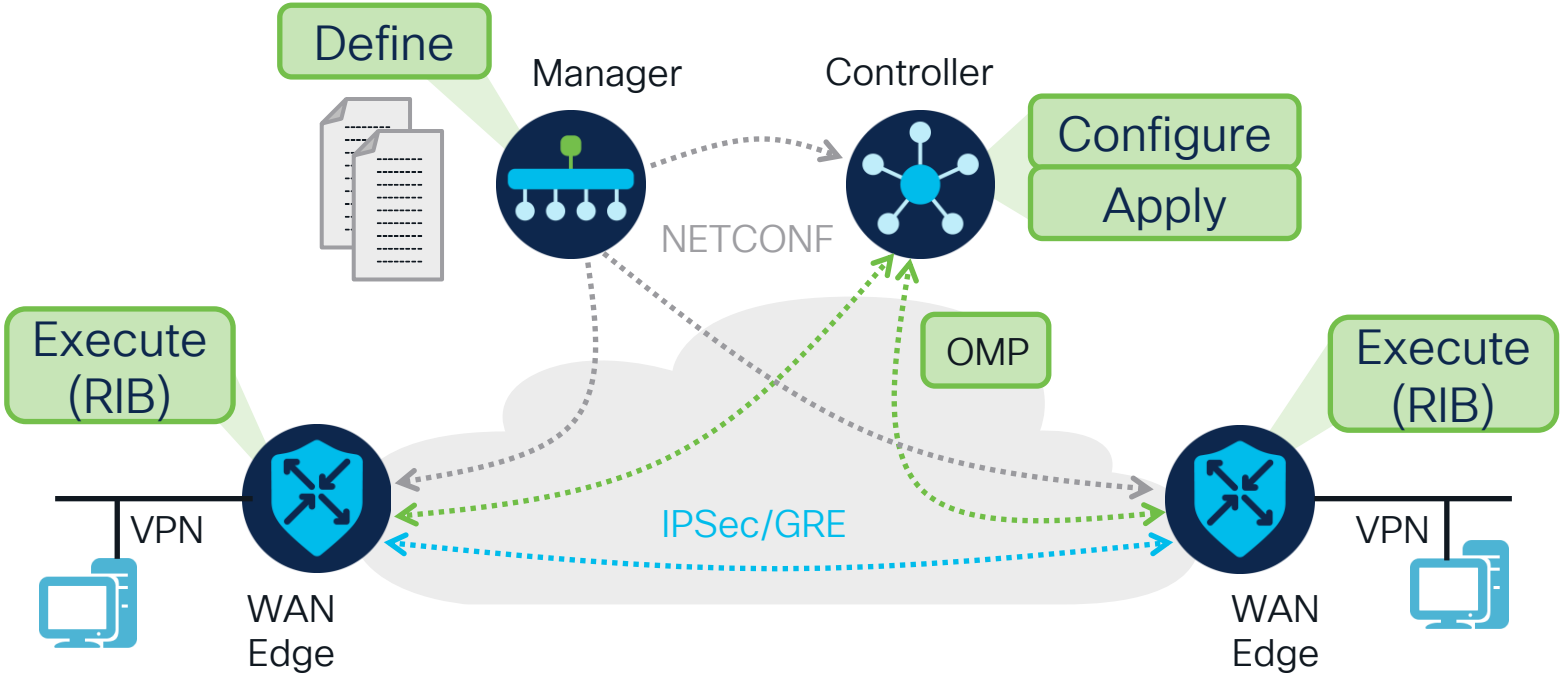


For Your Reference

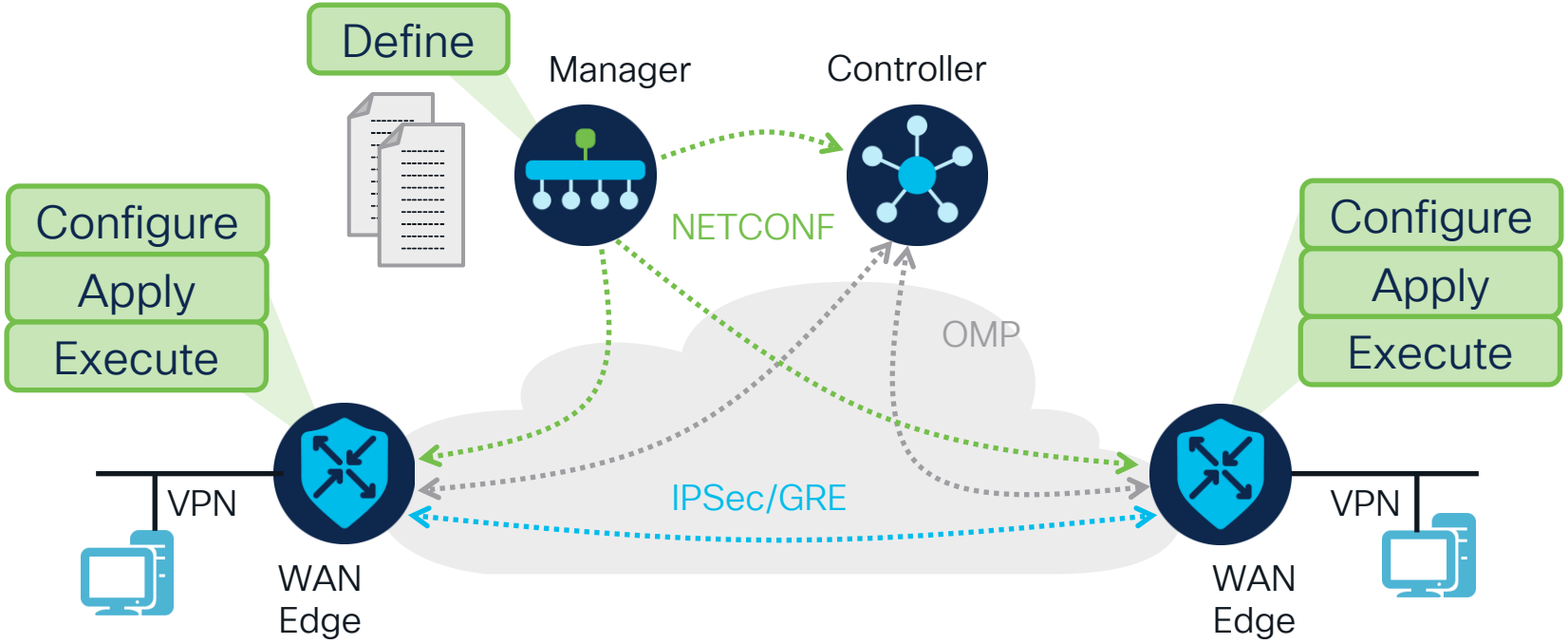
Define vs. Configure vs. Apply vs. Execute

Element	Action	Centralized Control	Centralized Data	Localized Control	Localized Data	Localized Security
Manager	Define/Adm	✓	✓	✓	✓	✓
Controller	Configure	✓	✓			
	Apply	✓	✓			
	Execute	✓				
WAN Edge	Configure			✓	✓	✓
	Apply			✓	✓	✓
	Execute		✓ (RIB)	✓	✓	✓

A Practical Example – Centralized Data Policy



A Practical Example – Localized Data Policy



A Traditional Routing Policy in IOS

```
ip prefix-list 1 permit 172.16.0.0/16
ip prefix-list 2 permit 192.168.1.0/24
!
```

```
route-map ROUTE-MAP-NAME permit 10
 match ip address 1
 set community 10:1
 !
!
route-map ROUTE-MAP-NAME permit 20
 match ip address 2
 set as-path prepend 10 10
 !
!
```

```
router bgp 50000
 neighbor 10.0.0.1 remote-as 50000
 address-family ipv4 unicast
  neighbor 10.0.0.1 route-map ROUTE-MAP-NAME in
 !
!
```

Building Catalyst SD-WAN Policies

A three-step process

Lists

```
lists
 site-list Sites_300_400_500
  site-id 300
  site-id 400
  site-id 500
 !
 tloc-list Site100_200_TLOC_All
  tloc 1.1.10.1 color mpls encap ipsec
  tloc 1.1.10.1 color biz-internet encap ipsec
  tloc 1.1.10.2 color mpls encap ipsec
  tloc 1.1.10.2 color biz-internet encap ipsec
  tloc 1.1.20.1 color mpls encap ipsec
  tloc 1.1.20.1 color biz-internet encap ipsec
  tloc 1.1.20.2 color mpls encap ipsec
  tloc 1.1.20.2 color biz-internet encap ipsec
 !
 vpn-list VPN11
  vpn 11
 !
 prefix-list _AnyIpv4PrefixList
  ip-prefix 0.0.0.0/0 le 32
```

Policy

```
control-policy VPN11_Hub_and_Spoke_Topology
    sequence 1
     match route
      site-list Sites_300_400_500
      vpn-list VPN11
      prefix-list _AnyIpv4PrefixList
     !
     action accept
      set
       tloc-list Site100_200_TLOC_All
      !
     !
    !
  default-action accept
```

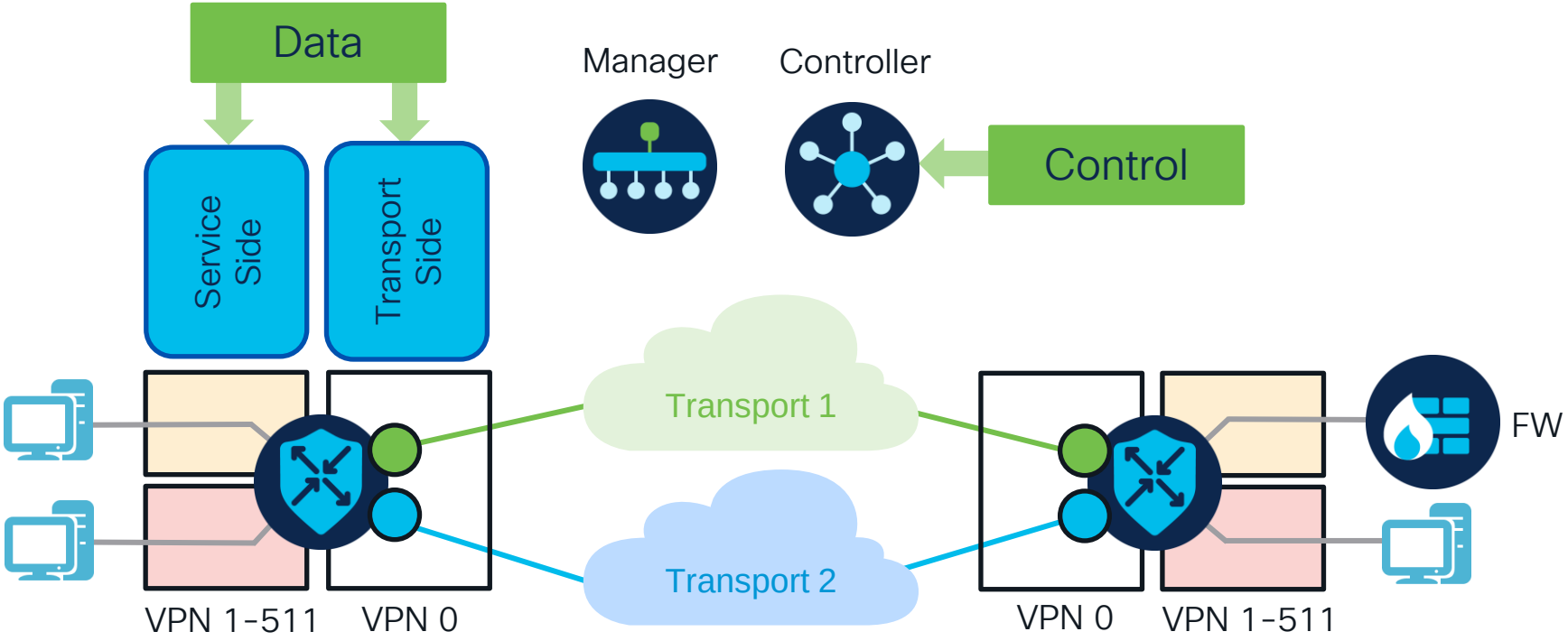
Apply

```
!
apply-policy
 site-list Sites_300_400_500
  control-policy VPN11_Hub_and_Spoke_Topology out
 !
```

Centralized Policies

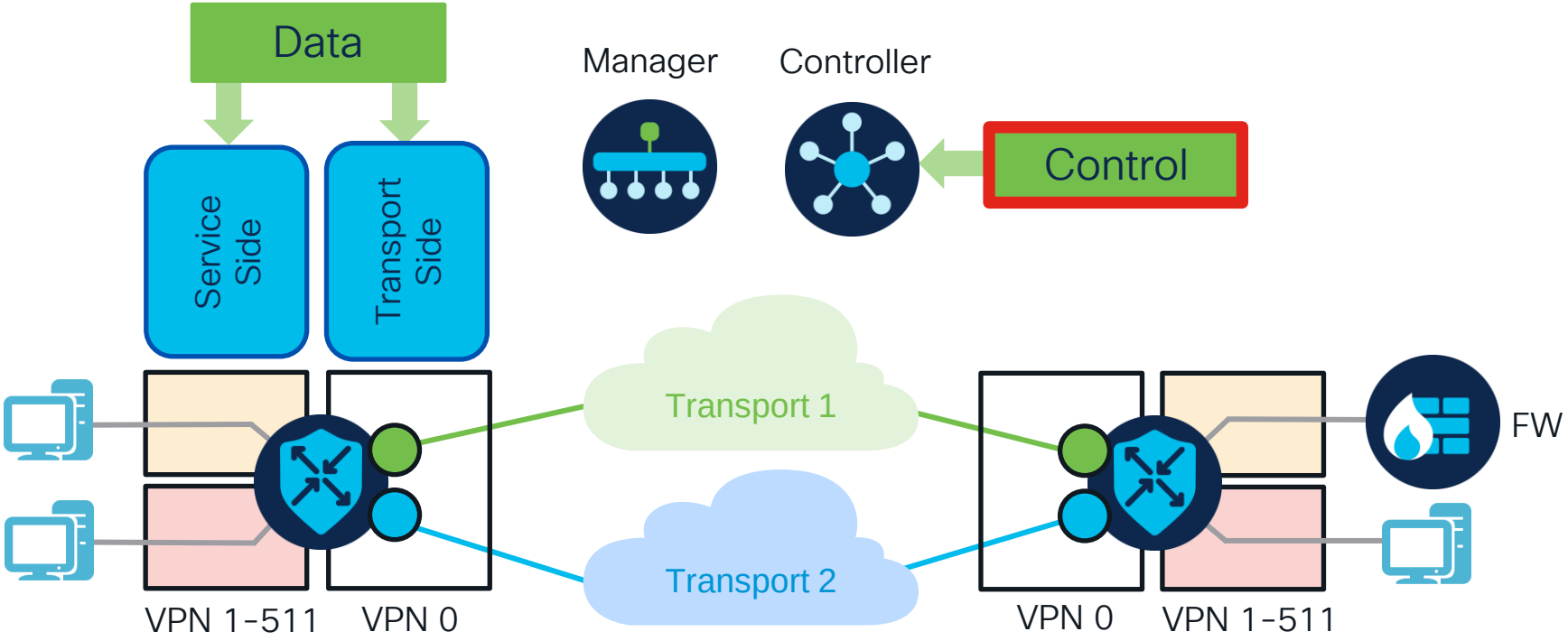
Centralized Policies – Network-Wide Scope

Executed in Different Places



Centralized Policies – Network-Wide Scope

Executed in Different Places



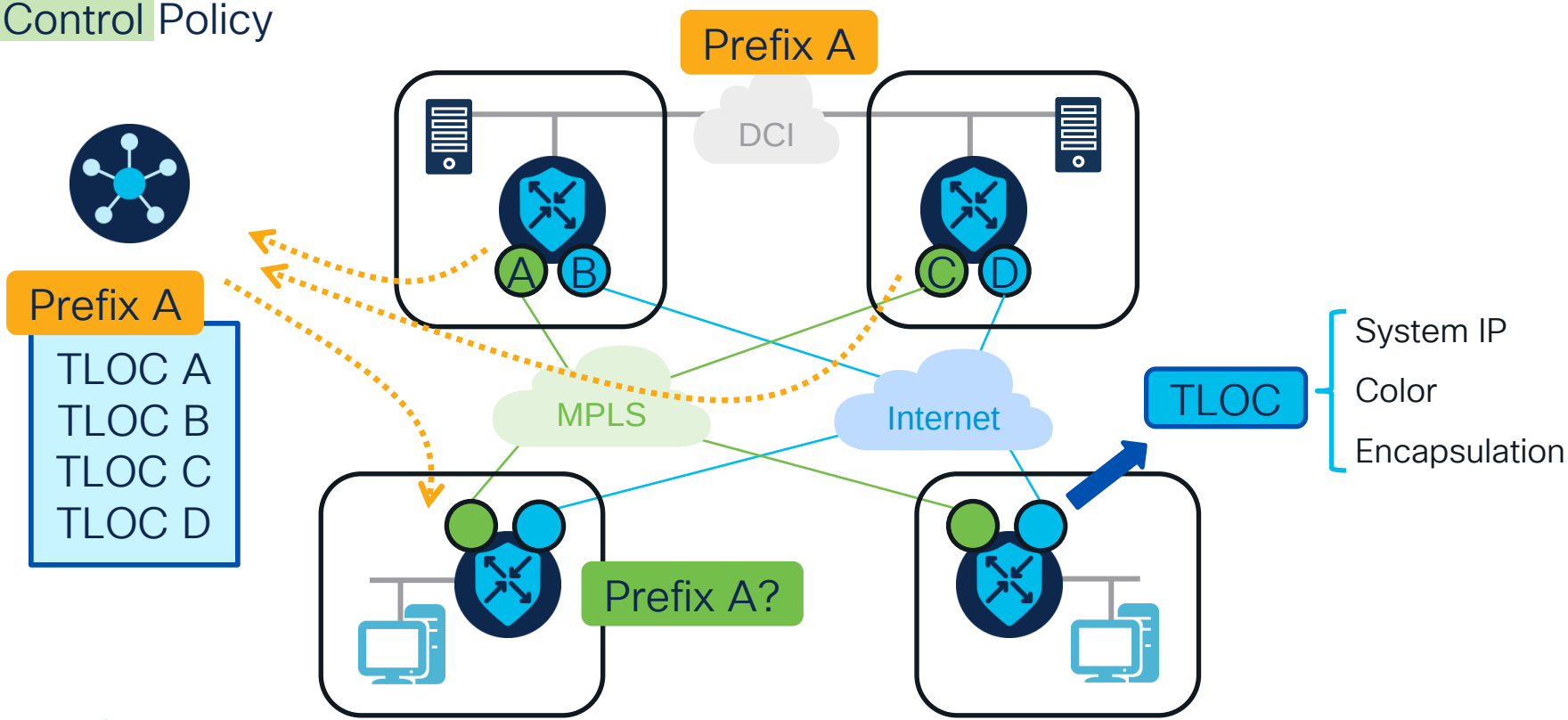
Control Policy – Filter/Manipulate OMP Routing

One of the Most Powerful Tools in the SD-WAN Toolbox

Path Selection	Service Insertion	Traffic Engineering	Extranet
Shared Services	Service and Path Affinity	Arbitrary VPN Topologies	Traffic Segmentation

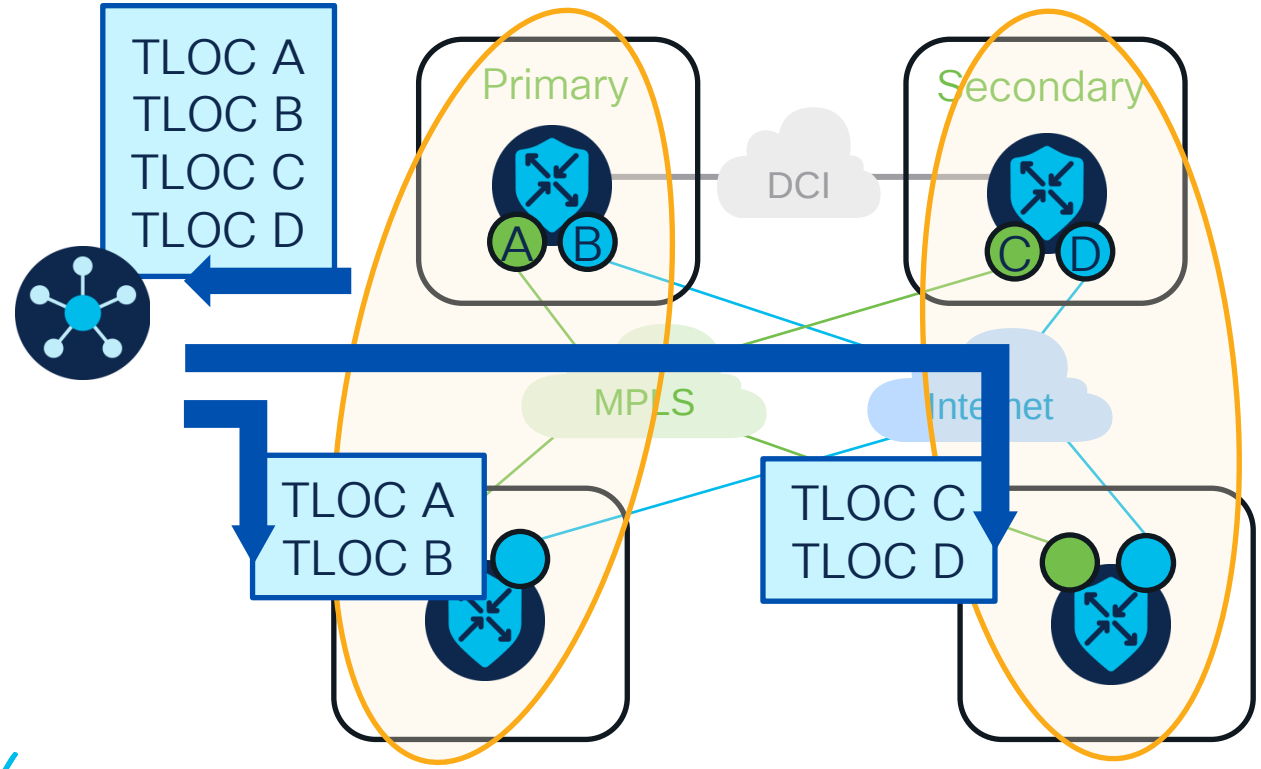
Data Center Preference

Control Policy



Data Center Preference

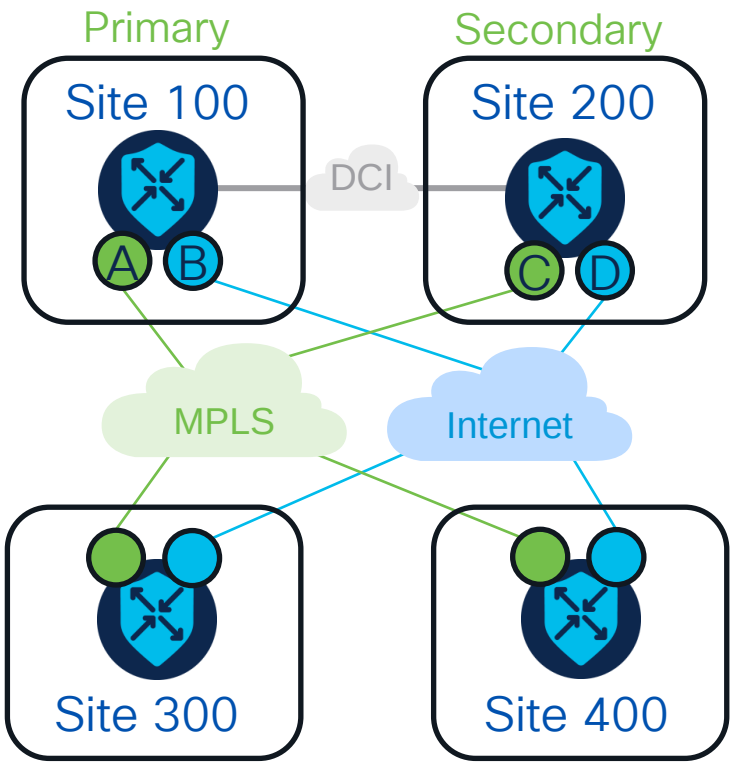
Control Policy – Identify Regions and Define DC Preferences



Data Center Preference – An Example

Control Policy – Define Site Lists

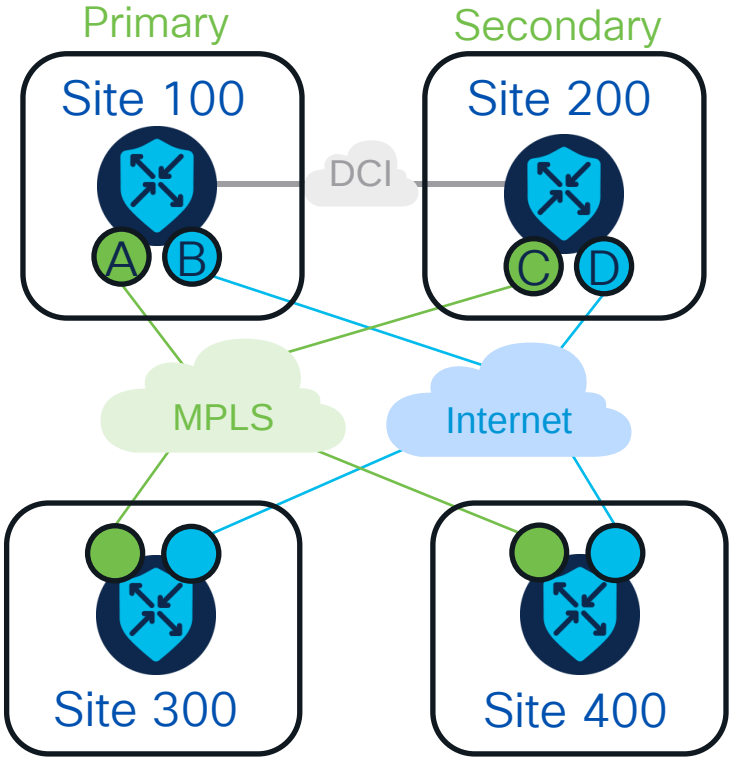
```
lists
 site-list Site300
  site-id 300
 !
 site-list Site400
  site-id 400
 !
 site-list Sites_100_200
  site-id 100
  site-id 200
 !
 !
 prefix-list _AnyIpv4PrefixList
  ip-prefix 0.0.0.0/0 le 32
```



Data Center Preference – An Example

Control Policy – Define TLOC Lists with DC Preference

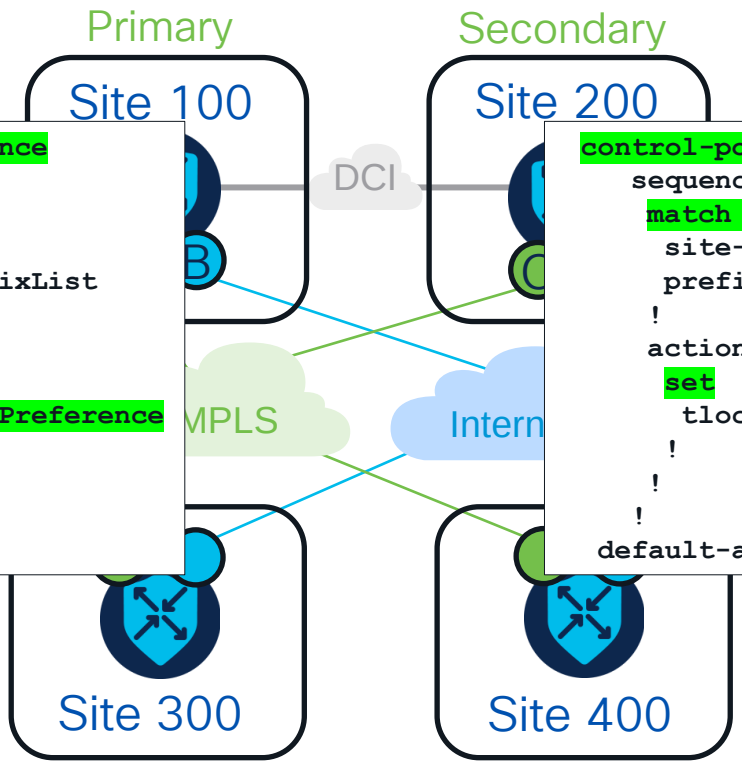
```
tloc-list TLOC_Site100_Preference
 tloc 1.1.10.1 color mpls encap ipsec preference 100
 tloc 1.1.10.1 color biz-internet encap ipsec preference 100
 tloc 1.1.10.2 color mpls encap ipsec preference 100
 tloc 1.1.10.2 color biz-internet encap ipsec preference 100
 tloc 1.1.20.1 color mpls encap ipsec preference 50
 tloc 1.1.20.1 color biz-internet encap ipsec preference 50
 tloc 1.1.20.2 color mpls encap ipsec preference 50
 tloc 1.1.20.2 color biz-internet encap ipsec preference 50
!

tloc-list TLOC_Site200_Preference
 tloc 1.1.10.1 color mpls encap ipsec preference 50
 tloc 1.1.10.1 color biz-internet encap ipsec preference 50
 tloc 1.1.10.2 color mpls encap ipsec preference 50
 tloc 1.1.10.2 color biz-internet encap ipsec preference 50
 tloc 1.1.20.1 color mpls encap ipsec preference 100
 tloc 1.1.20.1 color biz-internet encap ipsec preference 100
 tloc 1.1.20.2 color mpls encap ipsec preference 100
 tloc 1.1.20.2 color biz-internet encap ipsec preference 100
```



Data Center Preference – An Example

Control Policy – Define Policy

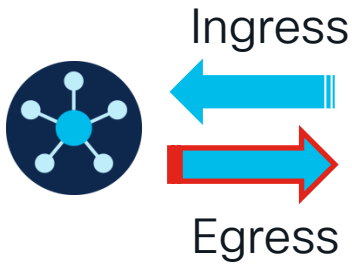
```
control-policy Site100_Preference
    sequence 1
     match route
      site-list Sites_100_200
      prefix-list _AnyIpv4PrefixList
     !
     action accept
      set
       tloc-list TLOC_Site100_Preference
      !
     !
    !
  default-action accept
```



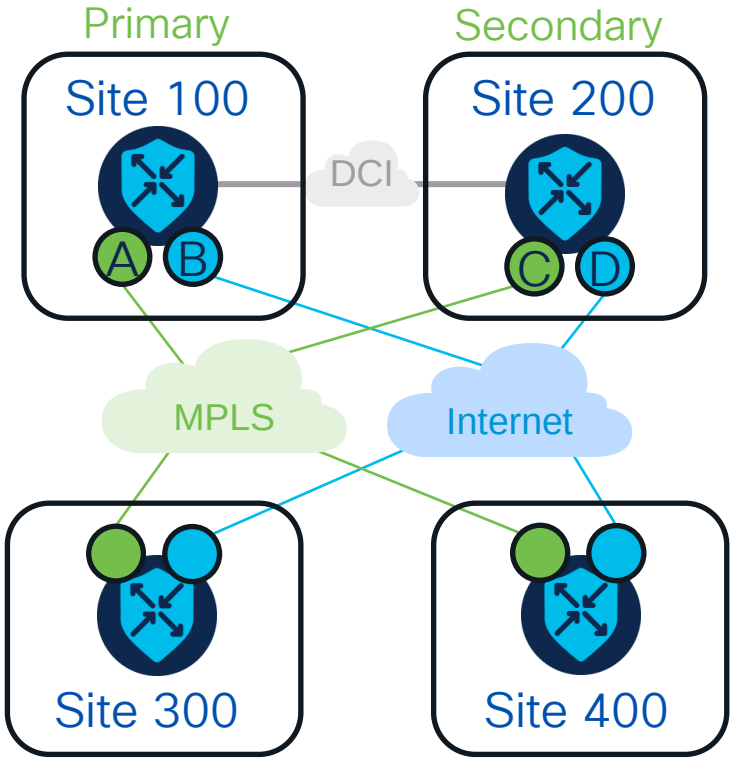

```
control-policy Site200_Preference
    sequence 1
     match route
      site-list Sites_100_200
      prefix-list _AnyIpv4PrefixList
     !
     action accept
      set
       tloc-list TLOC_Site200_Preference
      !
     !
    !
  default-action accept
```

Data Center Preference – An Example

Control Policy – Apply Policy




```
apply-policy
 site-list Site400
  control-policy Site200_Preference out
 !
 site-list Site300
  control-policy Site100_Preference out
 !
```



Data Center Preference – An Example

Control Policy – How it looks at the GUI

Sequence Rule | Drag and drop to re-arrange rules

Match Conditions

Site List: Sites_100_200

Site ID: 0-4294967295

Actions

Accept: Enabled

TLOC List: TLOC_Site100_Preference

TLOC IP: Example: 10.0.0.1

Color: Select a color list

Encapsulation: Select an encapsulation

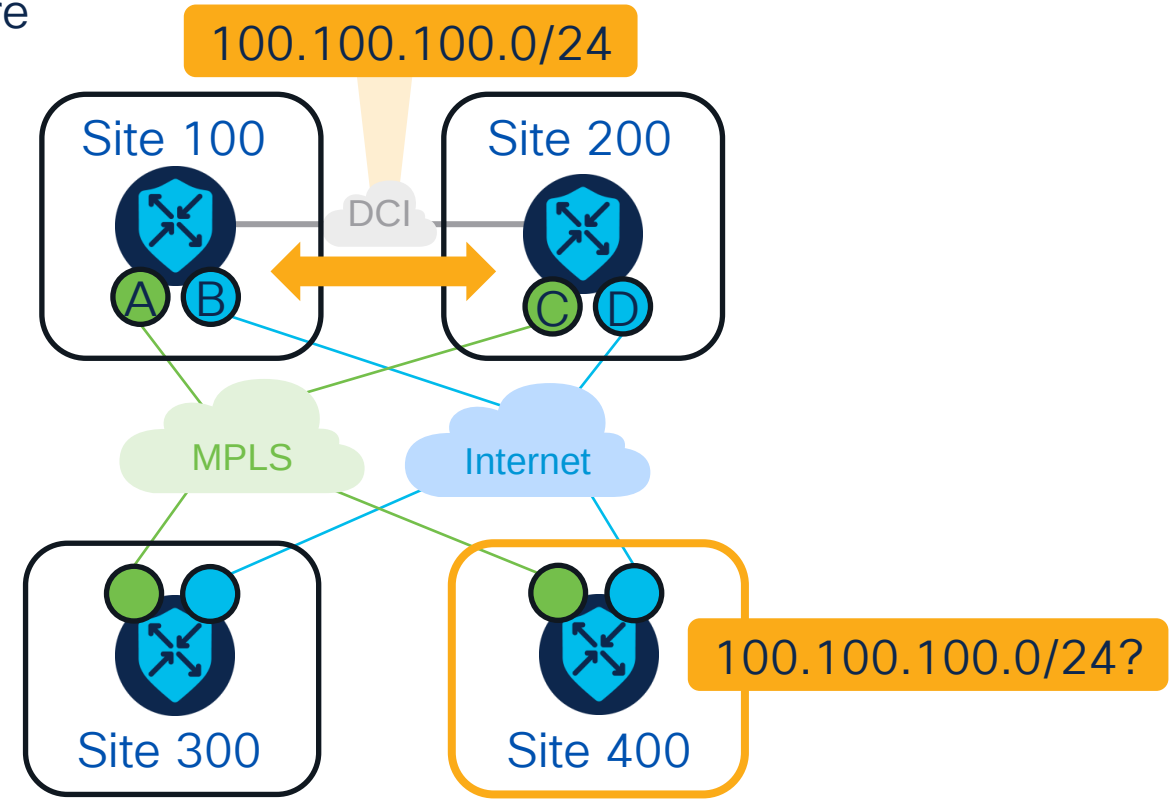
Site200_Preference

New Site/Region List

Direction	Site/Region List
out	Site400

Data Center Preference – An Example

Control Policy – Before



Data Center Preference – An Example

Control Policy – Before

Site400-cE1 | 1.1.40.1 Site Name 400 Device Model: C8000v

Device Options: OMP Received Routes

Filter Prefix: 100.100.100.0/24 Export

Search

Total Rows: 16

Last Update...	VPN ID	Prefix	Tenant ID	From Peer	Label	Status	Attribute Type	Tloc IP	Tloc Color	T
29 Jan 2024 ...10		100.100.100.0/24	0	1.1.1.3	1003	C I R	installed	A 1.1.10.1	biz-internet	
29 Jan 2024 ...10		100.100.100.0/24	0	1.1.1.3	1003	C I R	installed	B 1.1.10.1	mpls	
29 Jan 2024 ...10		100.100.100.0/24	0	1.1.1.3	1003	C I R	installed	C 1.1.20.1	mpls	
29 Jan 2024 ...10		100.100.100.0/24	0	1.1.1.3	1003	C I R	installed	D 1.1.20.1	biz-internet	

Data Center Preference – An Example

Control Policy – After

Site400-cE1 | 1.1.40.1 Site Name 400 Device Model: C8000v

Device Options: OMP Received Routes

Filter Prefix: 100.100.100.0/24

Export

Search

Total Rows: 16

Last Update...	VPN ID	Prefix	Tenant ID	From Peer	Label	Status	Attribute Type	Tloc IP	Tloc Color	Tloc Enc
29 Jan 2024 ...	10	100.100.100.0/24	0	1.1.1.3	1003	C I R	installed	1.1.20.1	mpls	ipsec
29 Jan 2024 ...	10	100.100.100.0/24	0	1.1.1.3	1003	C I R	installed	1.1.20.1	biz-internet	ipsec

Policy Processing Logic

Policies are processed sequentially. Order is important!

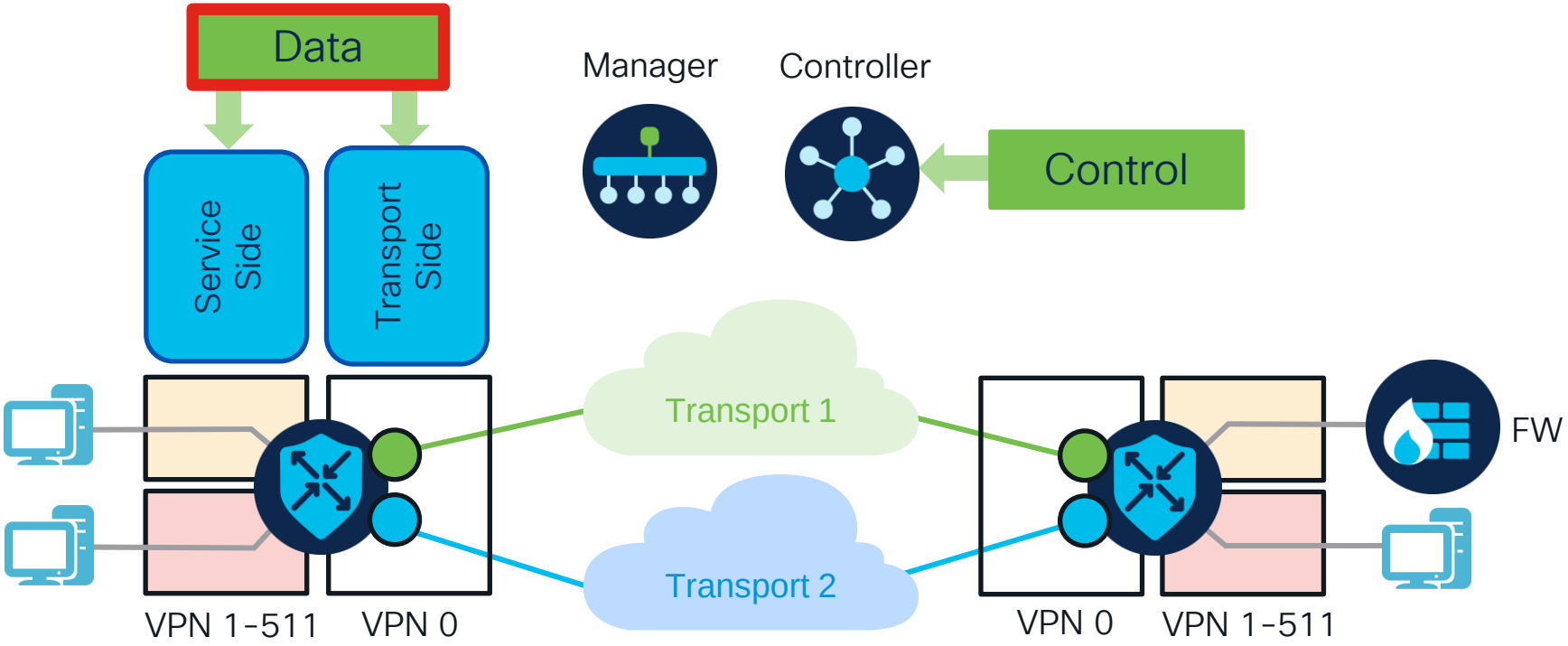
When a match occurs, the matched entity is subject to the sequence's configured action and is no longer subject to continued processing.

Entity not matched in a sequence is subject to default action for the policy.

Any node will make use of all available routing information.

Centralized Policies – Network-Wide Scope

Executed in Different Places



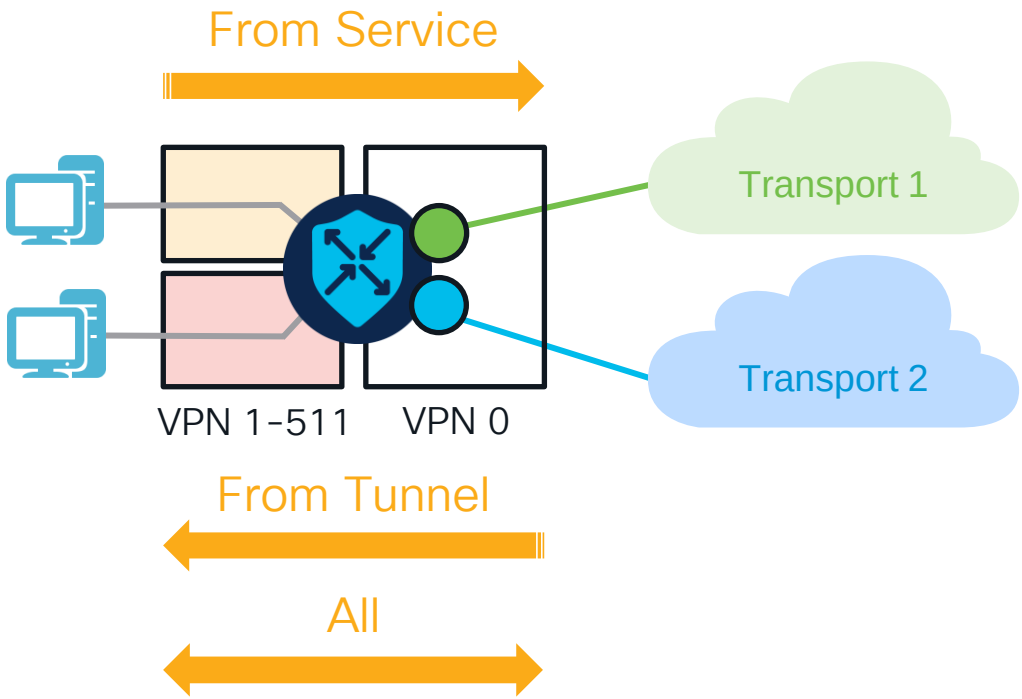
Data Policy – Manipulate Data Plane

Specify a Set of Actions for the Traffic

- Application Pinning
- Direct Internet Access
- App-Aware Routing
- Service Insertion
- App-Based Traffic Engineering
- Direct Cloud Access
- Forward Error Correction
- cFlowd

Data Policy Structure

Policy Processing

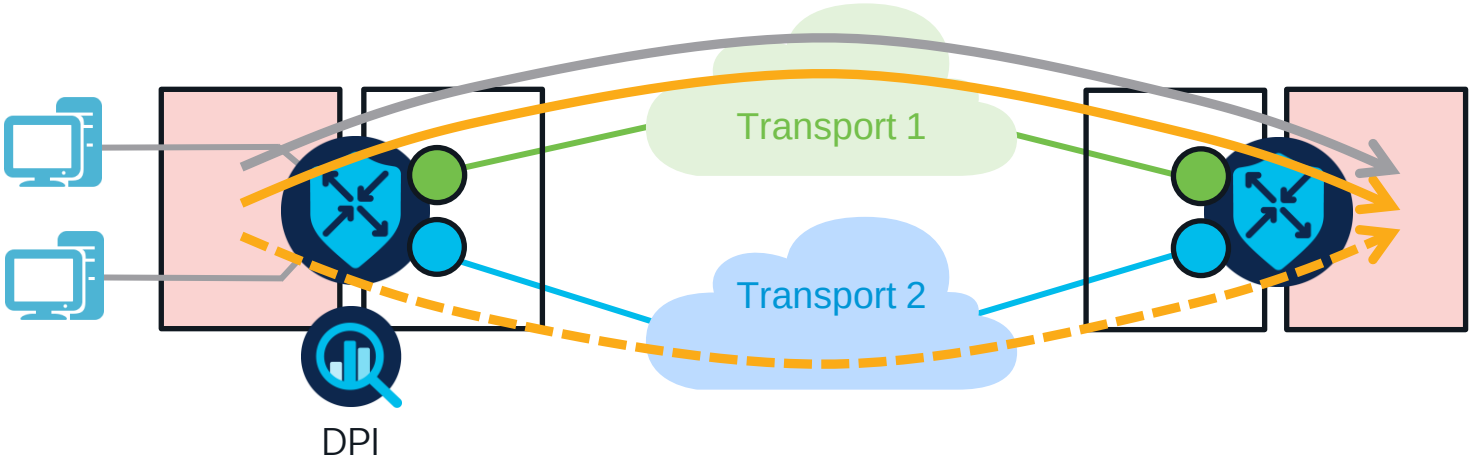


App-Based Traffic Engineering

Data Policy

App A: Primary Transport 1, Loose Preference

App B: Primary Transport 1, Strict Preference

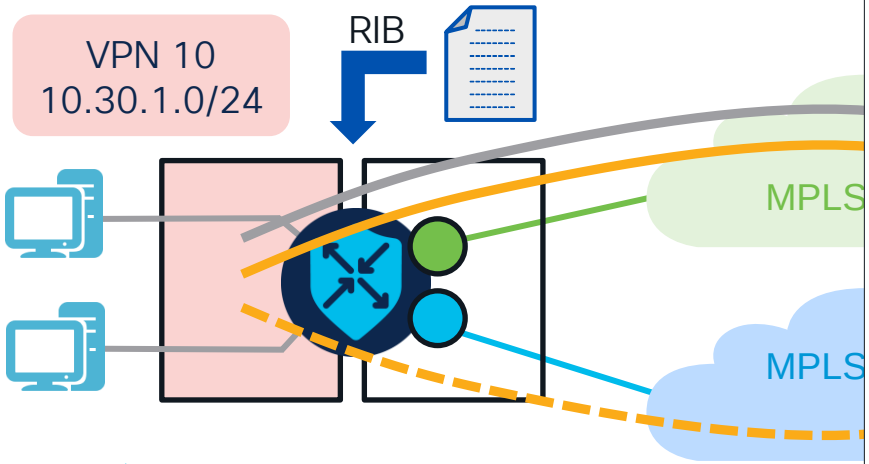


App-Based Traffic Engineering – An Example

Data Policy - Application Pinning

AWS: Primary MPLS 1, Loose Preference (Fallback to Routing)

YouTube: Primary MPLS 1, Strict Preference (Drop Upon Failure)




```
data-policy _VPN10_AppBasedTEPolicy
  vpn-list VPN10
    sequence 1
     match
      source-data-prefix-list VPN10_Site300_Prefixes
      app-list Amazon_AWS
     !
     action accept
      set
       local-tloc-list
        color mpls
        encap ipsec
    !
    sequence 11
     match
      source-data-prefix-list VPN10_Site300_Prefixes
      app-list YouTube
     !
     action accept
      set
       vpn 10
       tloc-list REMOTE_TLOC
    !
  default-action accept
```

SLA-Based Routing – An Example

AAR Policy – Define SLA and Path Behavior

Webex

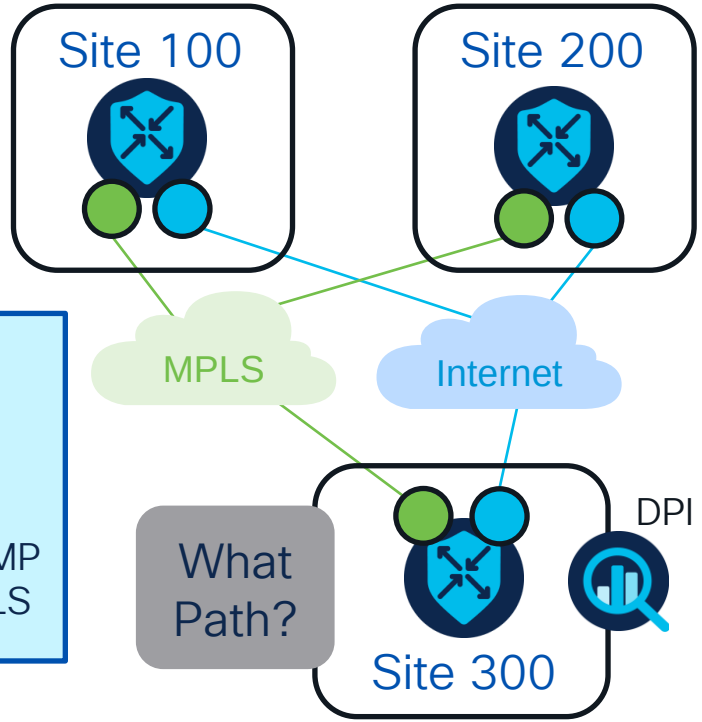
2% Loss
50 ms Latency
100 ms Jitter
Pref: MPLS
SLA not met: ECMP

SAP

7% Loss
150 ms Latency
100 ms Jitter
SLA met: ECMP
SLA not met: ECMP

SIP

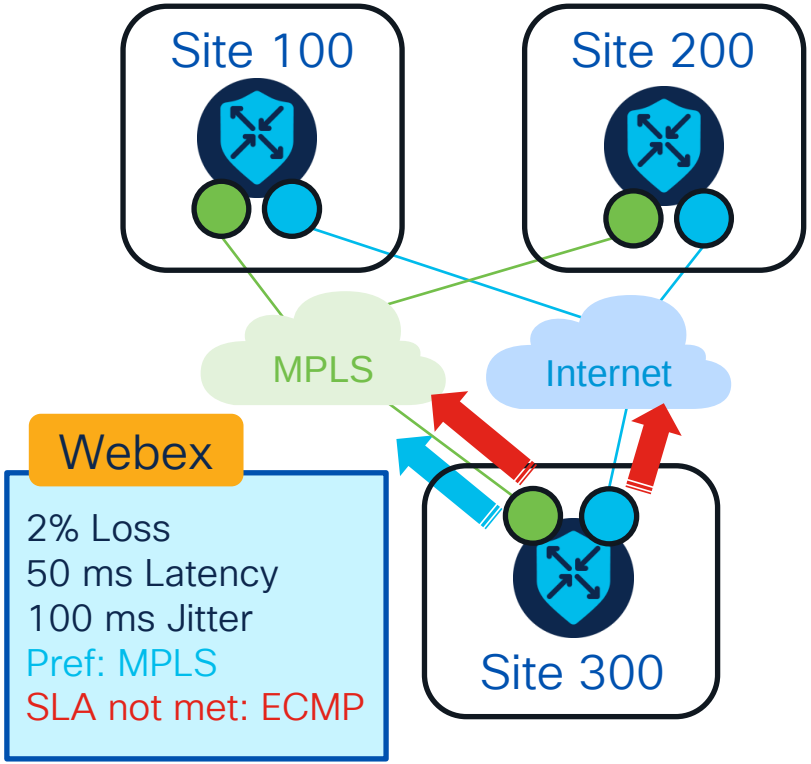
2% Loss
50 ms Latency
100 ms Jitter
Pref: Internet
SLA not met: ECMP
Backup Pref: MPLS



SLA-Based Routing – An Example

AAR Policy – Policy Snippet (Details Omitted)

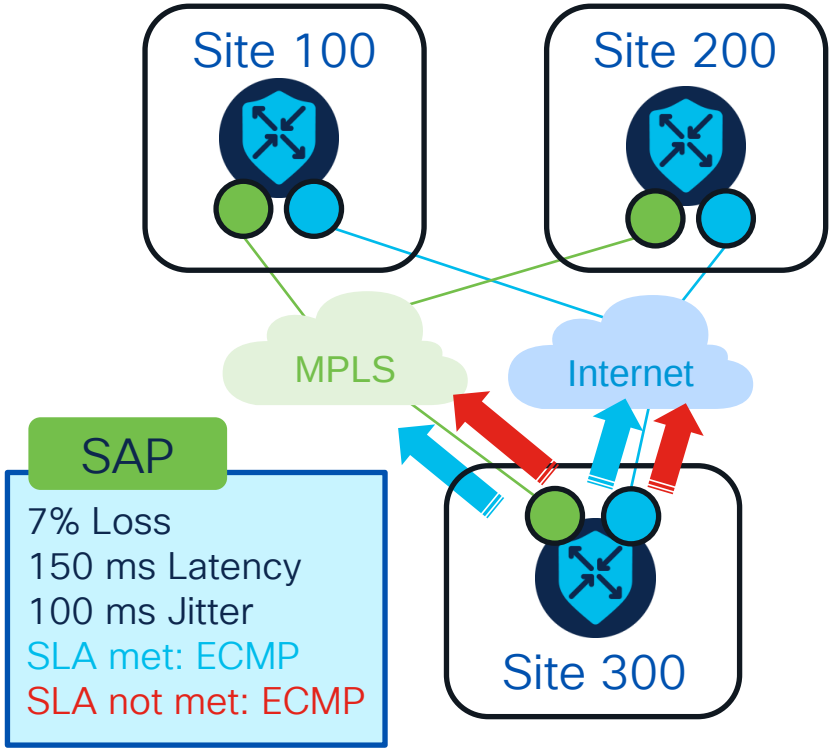
```
sla-class Critical_SLA
    latency 50
    loss 2
    jitter 100
  !
app-route-policy _VPN10_VPN10_AAR
  vpn-list VPN10
    sequence 1
     match
      source-data-prefix-list VPN10_Site300_Prefixes
      app-list webex_apps
     !
     action
      sla-class Critical_SLA preferred-color mpls
     !
    !
apply-policy
 site-list AllSites
  app-route-policy _VPN10_VPN10_AAR
```



SLA-Based Routing – An Example

AAR Policy – Policy Snippet (Details Omitted)

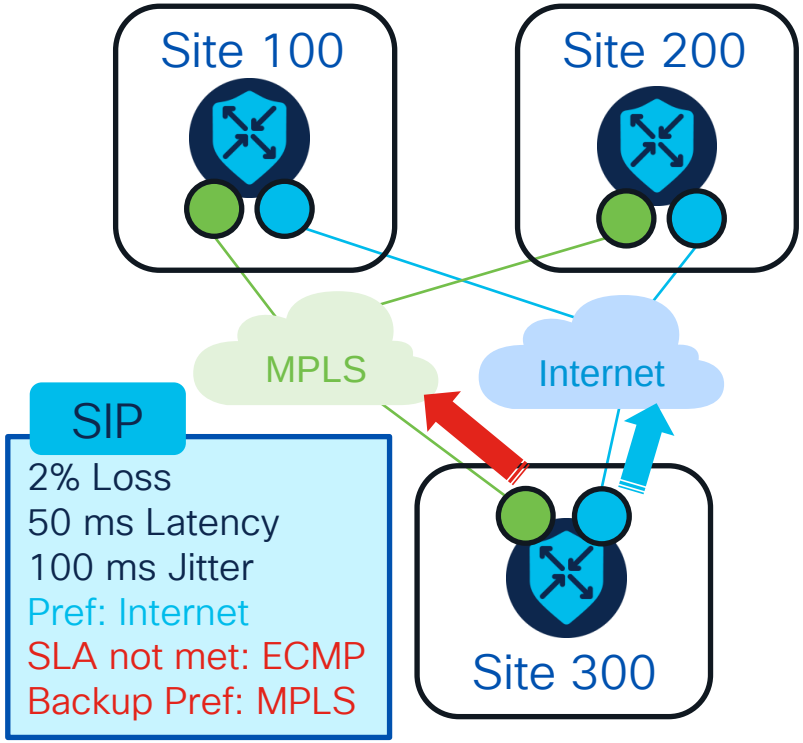
```
sla-class Priority_SLA
    latency 150
    loss 7
    jitter 100
   !
app-route-policy _VPN10_VPN10_AAR
  vpn-list VPN10
    sequence 11
     match
      app-list SAP
      source-ip 0.0.0.0/0
     !
     action
      sla-class Priority_SLA
     !
    !
apply-policy
 site-list AllSites
  app-route-policy _VPN10_VPN10_AAR
 !
```



SLA-Based Routing – An Example

AAR Policy – Policy Snippet (Details Omitted)

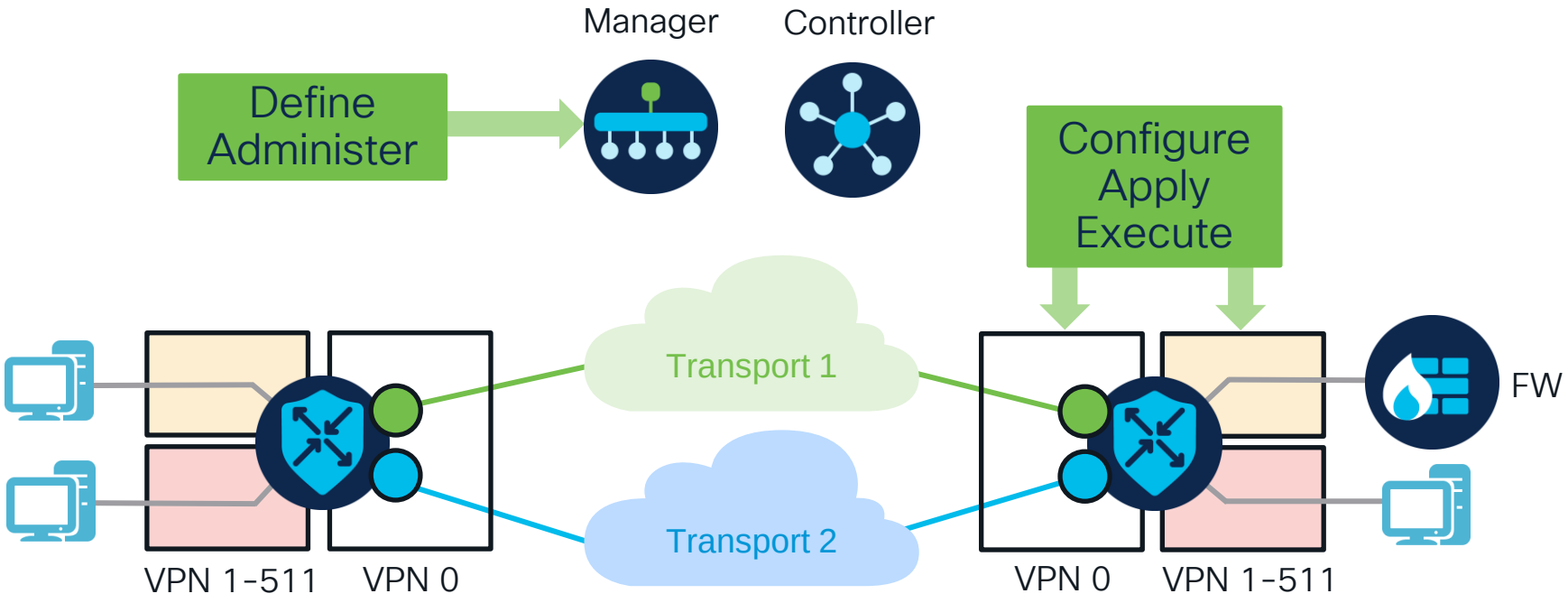
```
sla-class Critical_SLA
    latency 50
    loss 2
    jitter 100
   !
app-route-policy _VPN10_VPN10_AAR
  vpn-list VPN10
    sequence 21
     match
      app-list SIP
      source-ip 0.0.0.0/0
     !
     action
      sla-class Critical_SLA preferred-color biz-internet
      backup-sla-preferred-color mpls
     !
    !
apply-policy
 site-list AllSites
  app-route-policy _VPN10_VPN10_AAR
 !
```



Localized Policies

Localized Policies – Single-Device Scope

Can be Distributed to Multiple Devices via Template



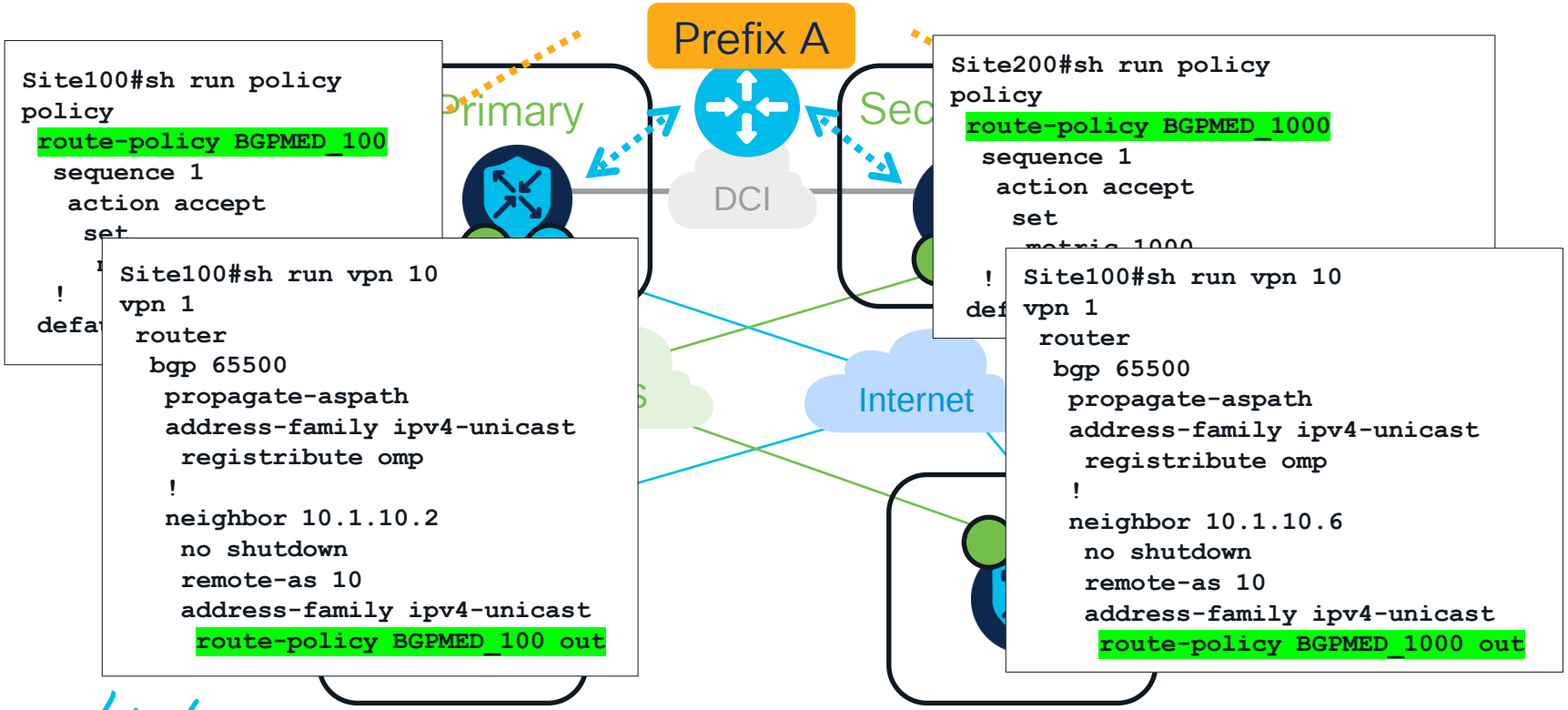
Localized Policies

Granularity and Flexibility

Control	Data	Security
▪ Manipulate Routing Attributes ▪ Filter Routes	▪ Manipulate Individual Packets or Flows of Data Traffic Into and Out of the Interfaces ▪ Access Control Lists ▪ Quality of Service	▪ Apply appropriate security mechanisms in the branch, such as firewalling, intrusion prevention, URL filtering, and malware protection.

Data Center Preference – An Example

Control Policy to Optimize Outbound Routing - Policy Snippet



Conclusion

What To Do Next?

1. Think About Your Own Policy Scenarios/Possibilities
2. Run/Reserve a Lab and Practice (dCloud, Capture the Flag)
3. Explore More (SD-WAN Learning Map, Cisco SD-WAN Book)

The bridge to possible

Thank you

cisco Live!

cisco Live!

Let's go