
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Avoid SD-WAN Deployment Mistakes

Lessons learned and best practices

Prashant Tripathi, Global Technical Solutions Architect
Andraz Piletic, Technical Solutions Architect / Instructor

BRKENT-2018

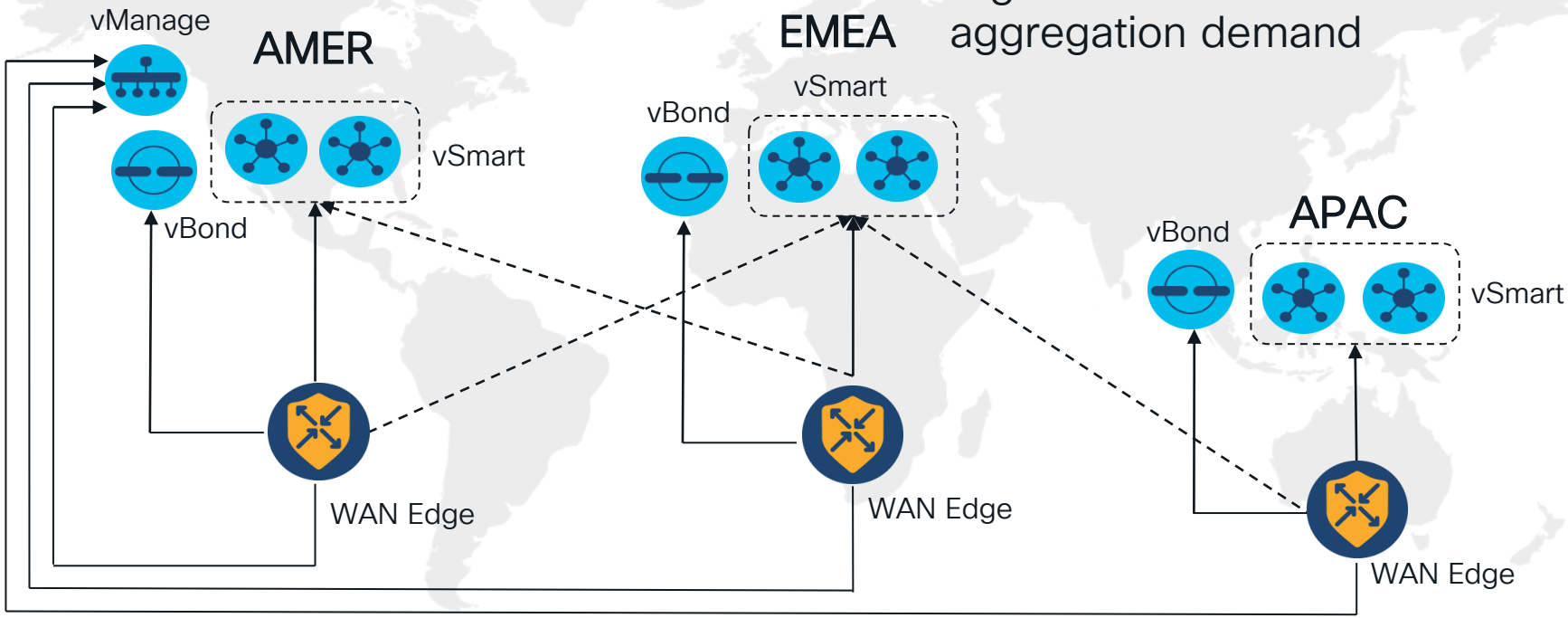
Agenda

- Scaling – Get It Right First Time
- Make Your Service Side HA
- Service Chaining Done Properly
- Avoid Breaking The Internet Breakout
- Scale Your SASE

Scaling – Get It Right First Time

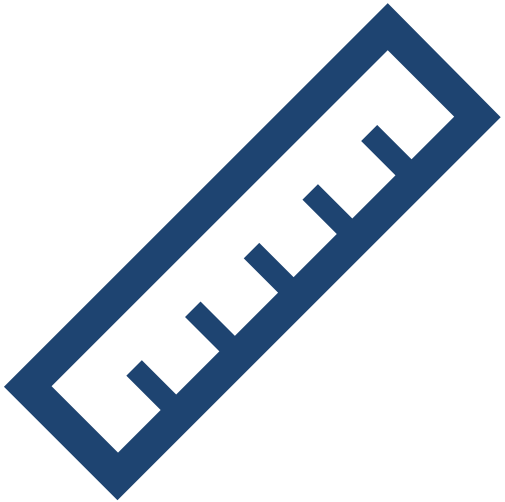
Global Financial Company

- Multi-region DC deployment
- Large scale head-end tunnel aggregation demand
- High head-end bandwidth aggregation demand



When Do We Consider Scale Out in SD-WAN?

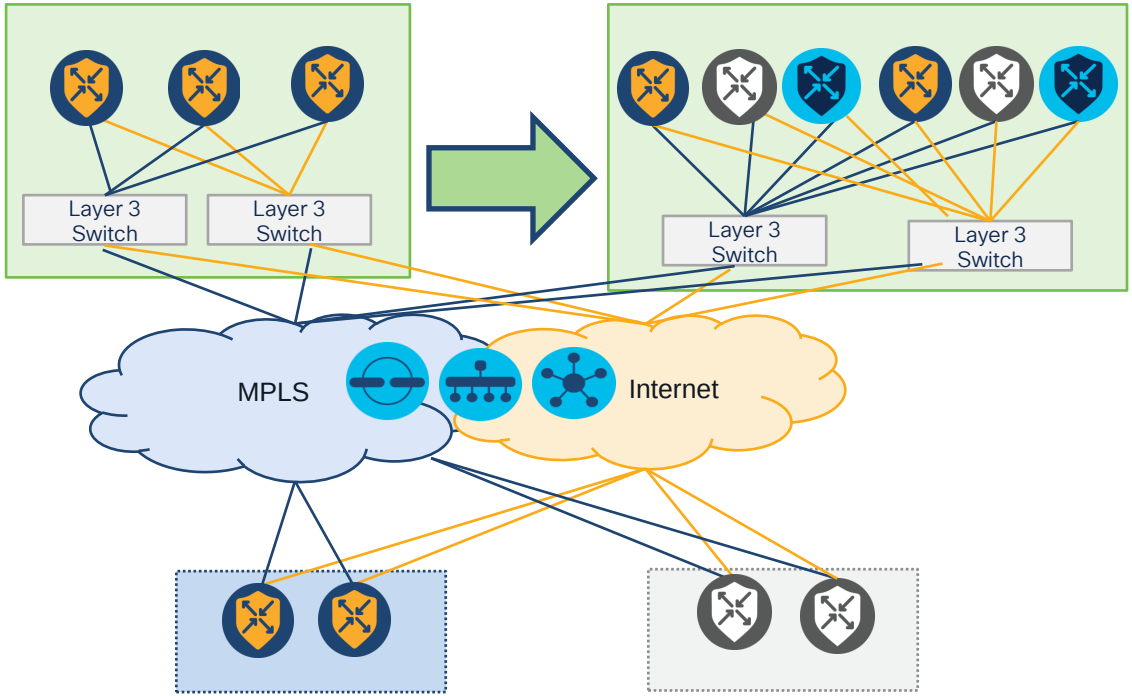
THROUGHPUT SCALE



TUNNEL SCALE

Scale Out Design – Throughput Scale

- Horizontally scale aggregation site and deploy them in active/active state
- Site specific settings remain unchanged
- Take care of traffic (a)symmetry
- Manage number of tunnels



SD-WAN Data Plane Design

Tools and Techniques for defining data plane connectivity

Color Restrict

- Limit Data Plane Establishment to TLOCs of the Same Color
- Simple configuration knob that effectively limits data plane connectivity

Control Policy

- A control policy allows for TLOC filtering and reassignments
- Can be combined with TLOC Groups and Restrict if needed
- Ultimate control over TLOC distribution, visibility, preference and connectivity model

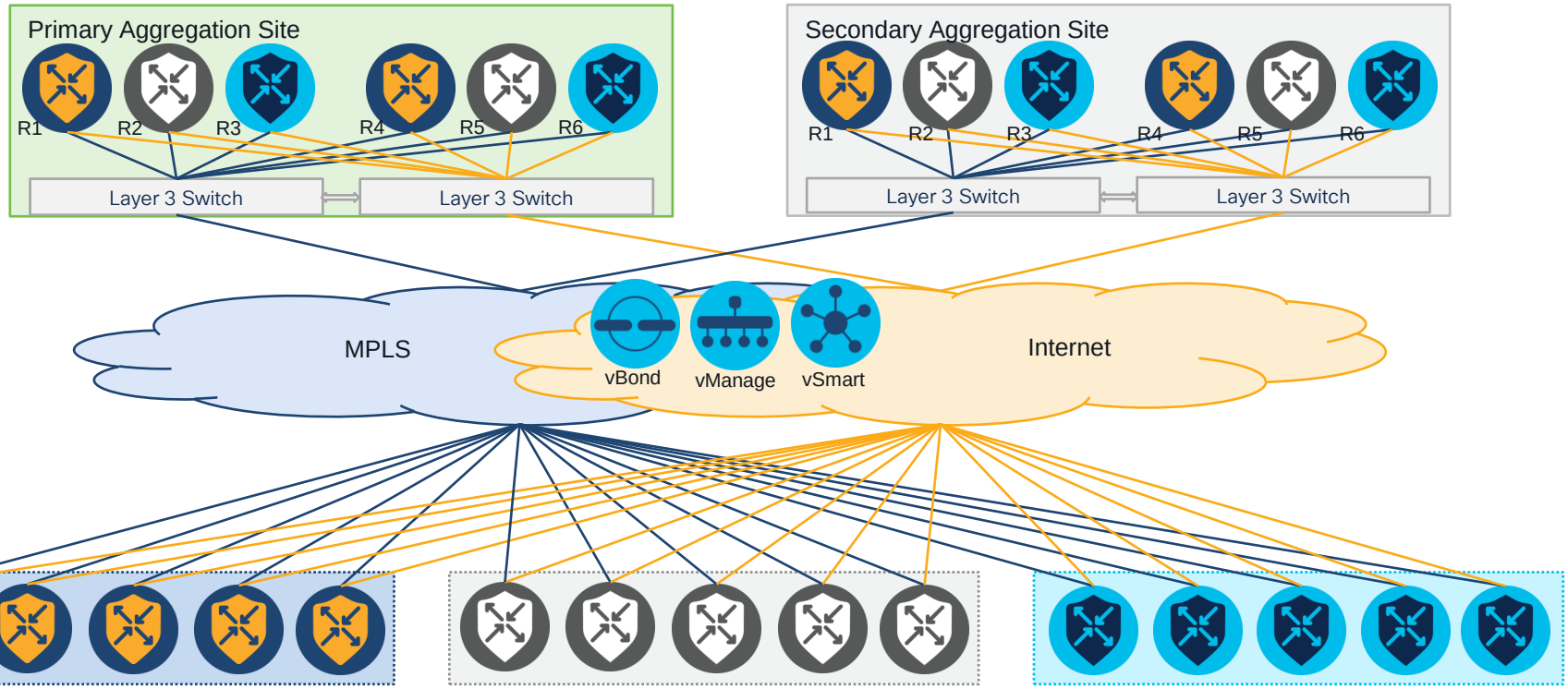
TLOC Groups

- Configure groups that determine actual data plane topology
- Can be combined with restrict
- Define groups based on site type and connectivity requirements for scalable rollout

Administrating Number of Tunnels – Option 1

Control Policy based on Site-IDs

- R1&R4 : Blue Edge Grp
- R2&R5: Gray Edge Grp
- R3&R6: Sky Blue Edge Grp



Administrating Number of Tunnels – Option 1

1 Declare Branches

```
lists
  site-list CL-Group-A
   site-id 10
   site-id 100-150
```

2 Define the Control Policy

```
Policy
 control-policy CL-Group-A
    sequence 1
     match tloc
      site-list CL-Group-A
     !
     action accept
     !
    !
    sequence 11
     match route
      site-list CL-Group-A
      prefix-list _AnyIpv4PrefixList
     !
     action accept
     !
    !
  default-action reject
```

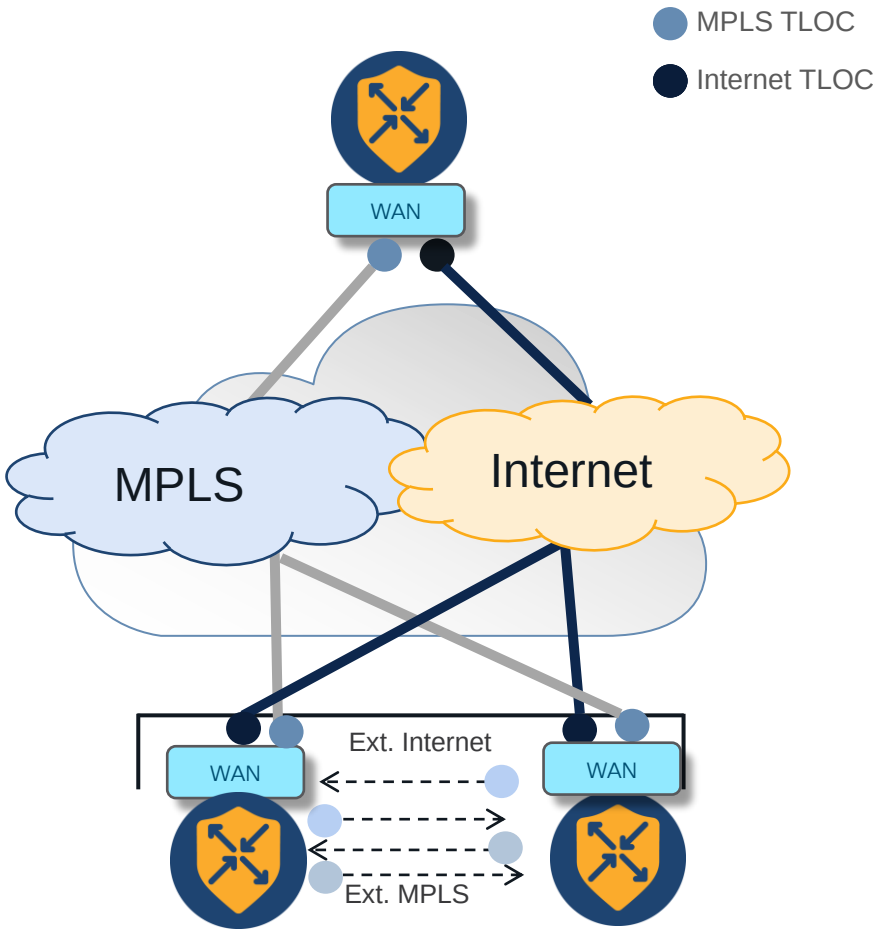
Advertise Hub TLOCs

Hub & Branch Prefixes

Drop rest Hub/Branch

3 Apply Policy to the target site-list

```
apply-policy
site-list CL-Group-A
  control-policy CL-Group-A out
 !
```



Administrating Number of Tunnels – Option 1

```
lists
  site-list CL-Group-B
   site-id 20
   site-id 200-250
```

1 Declare Branches

```
Policy
 control-policy CL-Group-B
    sequence 1
     match tloc
      site-list CL-Group-B
     !
     action accept
     !
    !
    sequence 11
     match route
      site-list CL-Group-B
      prefix-list _AnyIpv4PrefixList
     !
     action accept
     !
    !
  default-action reject
```

2 Define the Control Policy

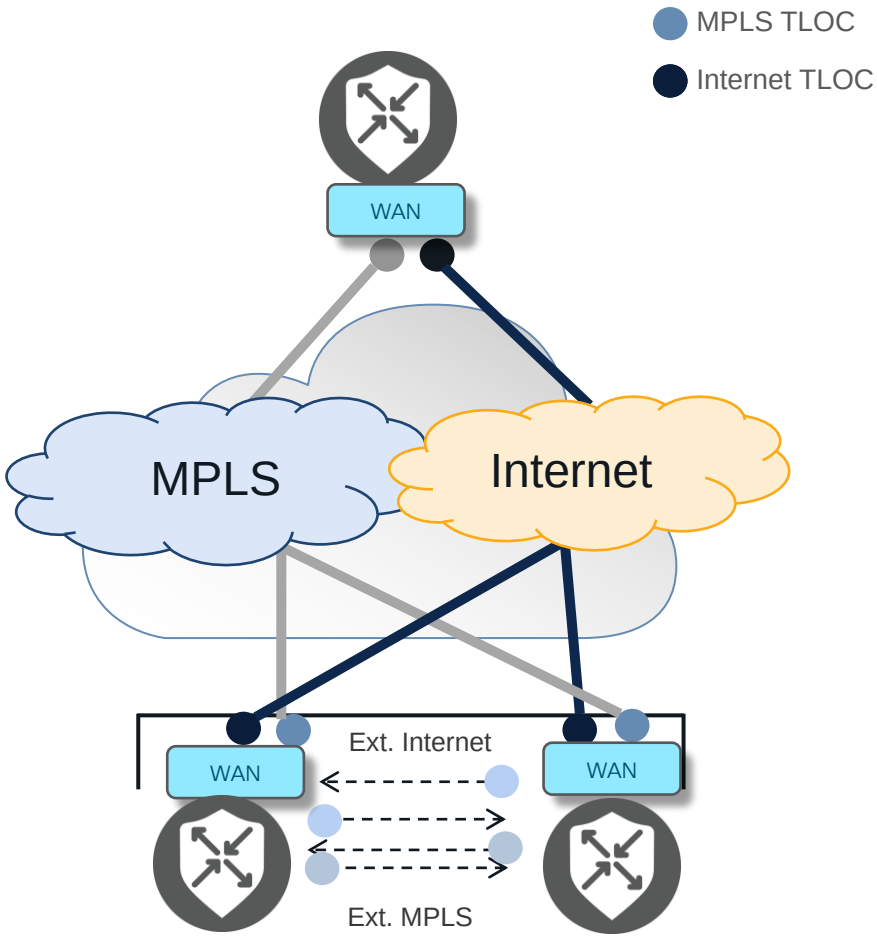
Advertise Hub TLOCs

Hub & Branch Prefixes

Drop rest Hub/Branch

```
apply-policy
site-list CL-Group-B
  control-policy CL-Group-B out
 !
```

3 Apply Policy to the target site-list



Administrating Number of Tunnels – Option 1

```
lists
  site-list CL-Group-C
   site-id 30
   site-id 300-350
```

1 Declare Branches

```
Policy
 control-policy CL-Group-C
    sequence 1
     match tloc
      site-list CL-Group-C
     !
     action accept
     !
    !
    sequence 11
     match route
      site-list CL-Group-C
      prefix-list _AnyIpv4PrefixList
     !
     action accept
     !
    !
  default-action reject
```

2 Define the Control Policy

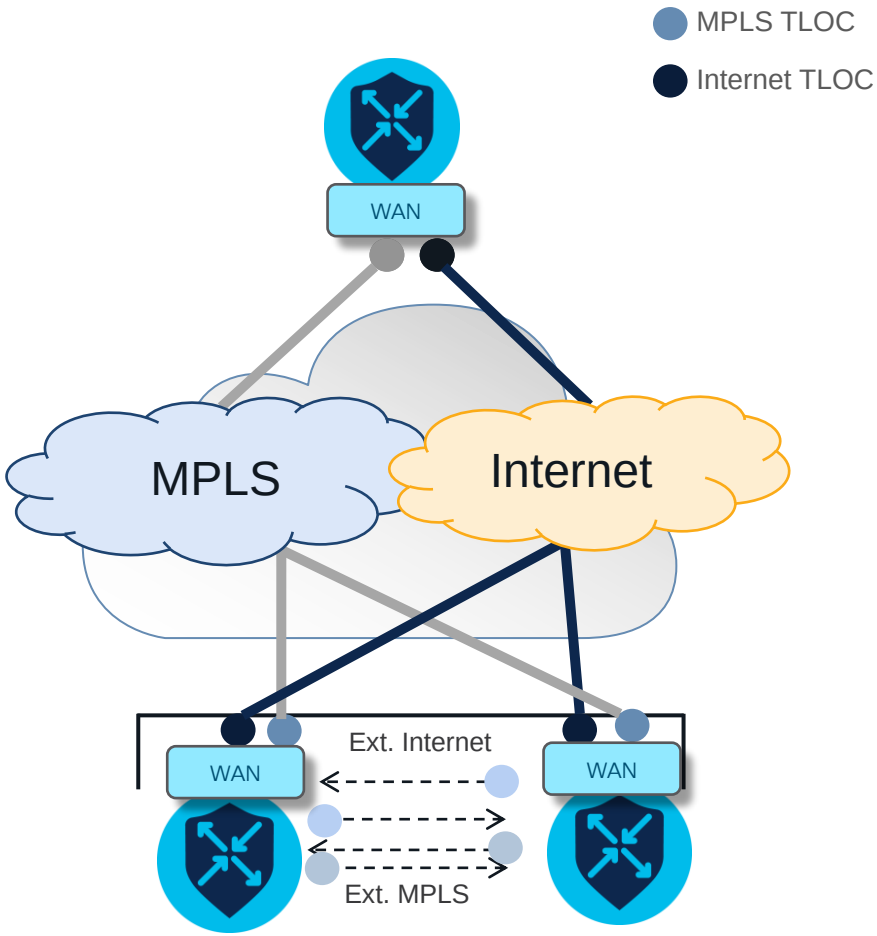
Advertise Hub TLOCs

Hub & Branch Prefixes

Drop rest Hub/Branch

```
apply-policy
site-list CL-Group-C
  control-policy CL-Group-C out
 !
```

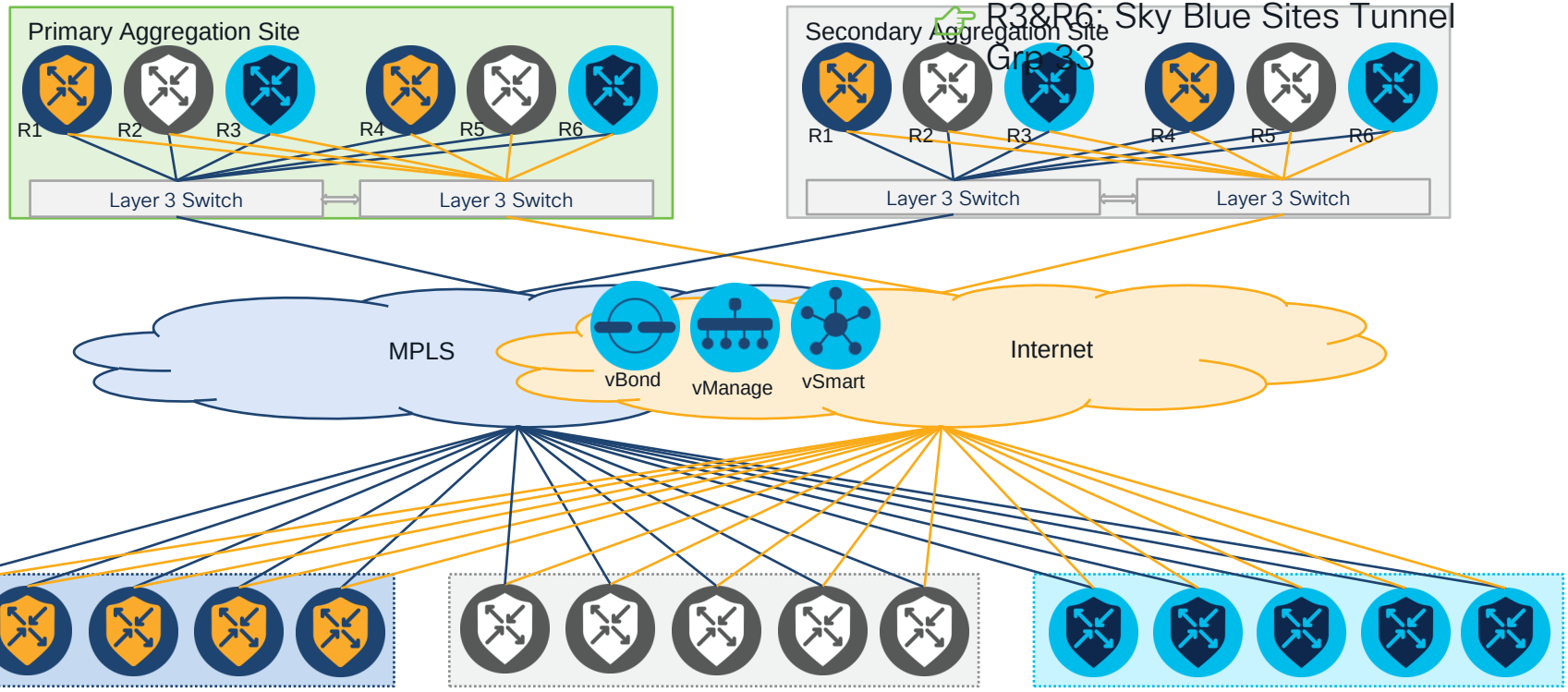
3 Apply Policy to the target site-list



Administrating Number of Tunnels – Option 2

Tunnel Group Overlay

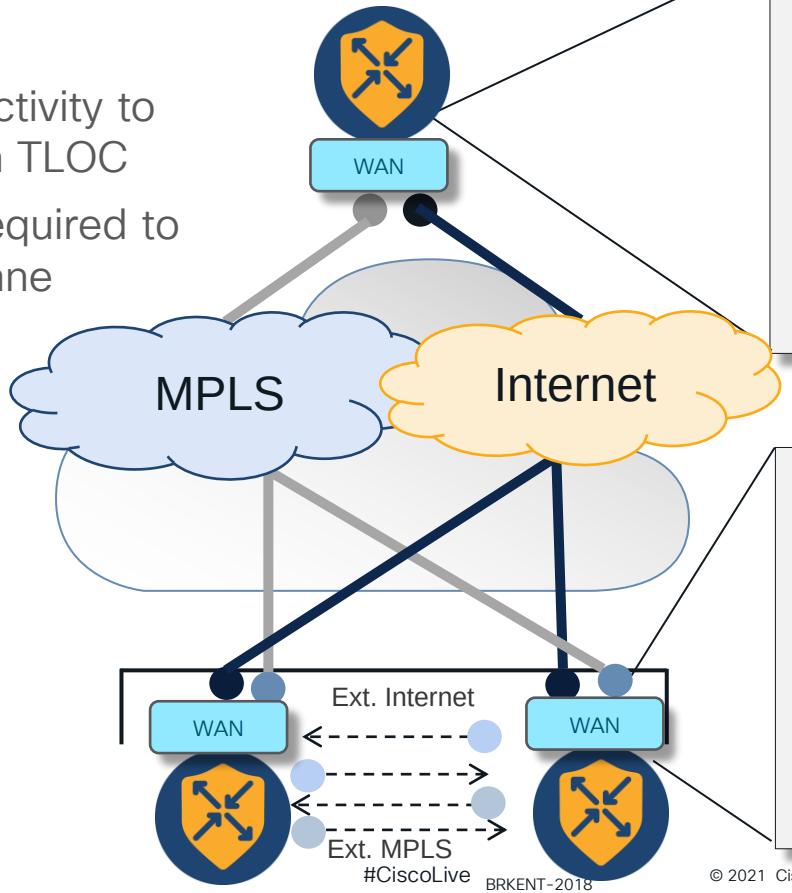
- R1&R4: Blue Sites Tunnel Grp 11
- R2&R5: Gray Sites Tunnel Grp 22
- R3&R6: Sky Blue Sites Tunnel Grp 33



Administrating Number of Tunnels – Option 2

TLOC Groups

- Limits data plane connectivity to identified group on each TLOC
- Provides the flexibility required to build any model data plane




```
sdwan
 interface GigabitEthernetx
  tunnel-interface
  encapsulation ipsec weight 1
   group 11
    color mpls
!
 interface GigabitEthernetx
  tunnel-interface
  encapsulation ipsec weight 1
   group 11
    color public-internet
```

```
sdwan
 interface GigabitEthernetx
  tunnel-interface
  encapsulation ipsec weight 1
   group 11
    color mpls
!
 interface GigabitEthernetx
  tunnel-interface
  encapsulation ipsec weight 1
   group 11
    color public-internet
```

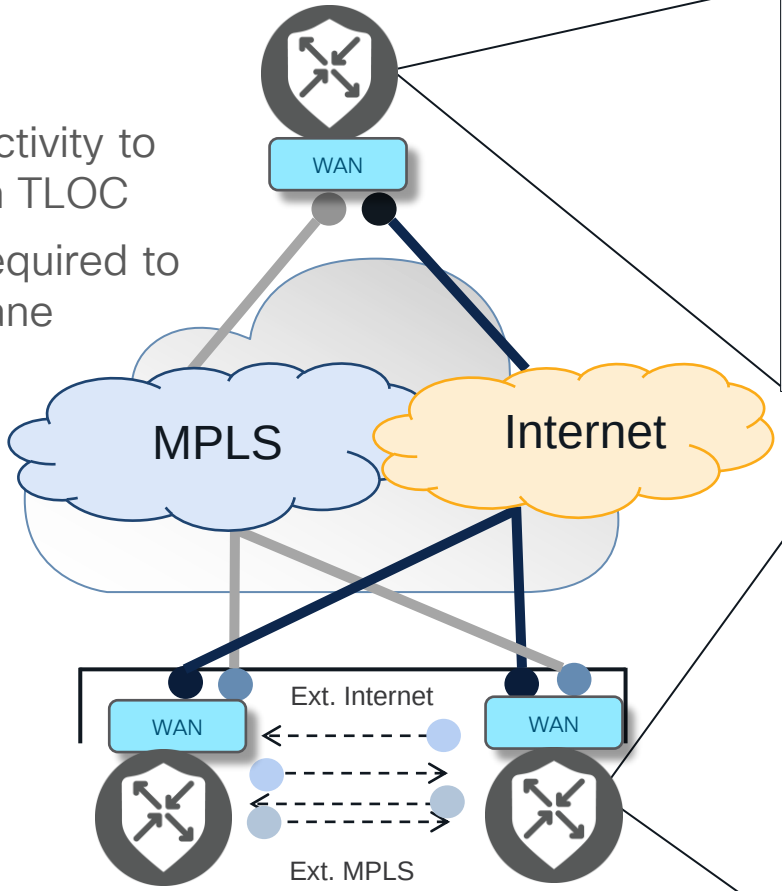
R1&R4: Blue Sites

- MPLS Group 11
- Internet – Group 11

Administrating Number of Tunnels – Option 2

TLOC Groups

- Limits data plane connectivity to identified group on each TLOC
- Provides the flexibility required to build any model data plane




```
sdwan
 interface GigabitEthernetx
  tunnel-interface
  encapsulation ipsec weight 1
   group 22
   color mpls
!
 interface GigabitEthernetx
  tunnel-interface
  encapsulation ipsec weight 1
   group 22
   color public-internet
```

```
Sdwan
 interface GigabitEthernetx
  tunnel-interface
   encapsulation ipsec weight 1
   group 22
   color mpls
!
 interface GigabitEthernetx
  tunnel-interface
   encapsulation ipsec weight 1
   group 22
   color public-internet
```

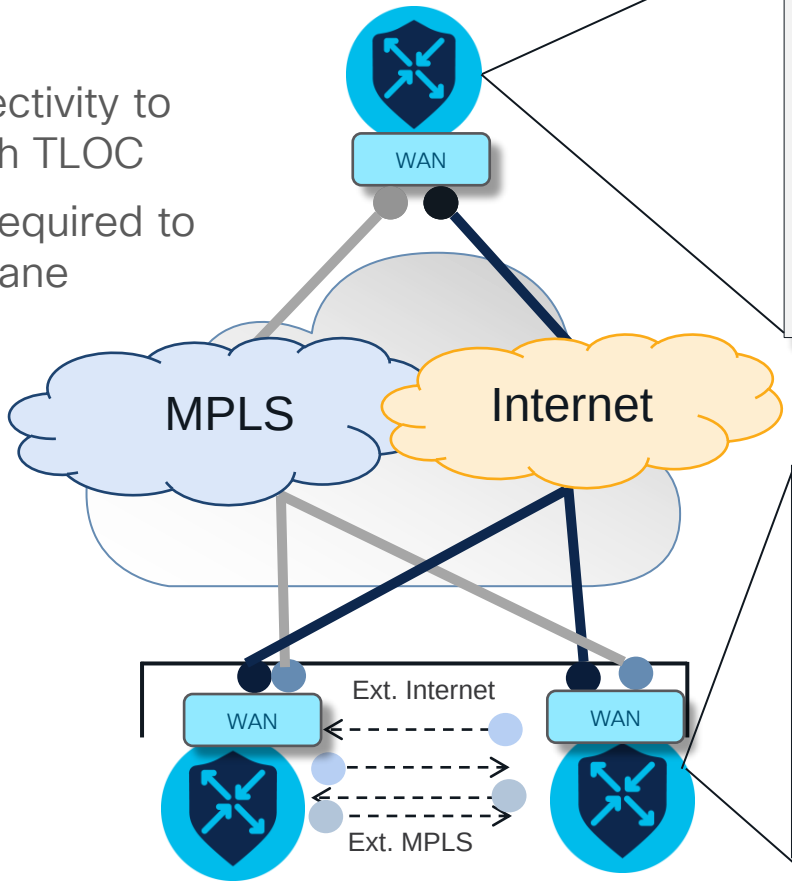
R2 Group Router

- MPLS Group 22
- Internet – Group 22

Administrating Number of Tunnels – Option 2

TLOC Groups

- Limits data plane connectivity to identified group on each TLOC
- Provides the flexibility required to build any model data plane




```
sdwan
 interface GigabitEthernetx
  tunnel-interface
  encapsulation ipsec weight 1
   group 33
   color mpls
!
 interface GigabitEthernetx
  tunnel-interface
   encapsulation ipsec weight 1
   group 33
   color public-internet
```

```
sdwan
 interface GigabitEthernetx
  tunnel-interface
  encapsulation ipsec weight 1
   group 33
   color mpls
!
 interface GigabitEthernetx
  tunnel-interface
   encapsulation ipsec weight 1
   group 33
   color public-internet
```

R3 Group Router

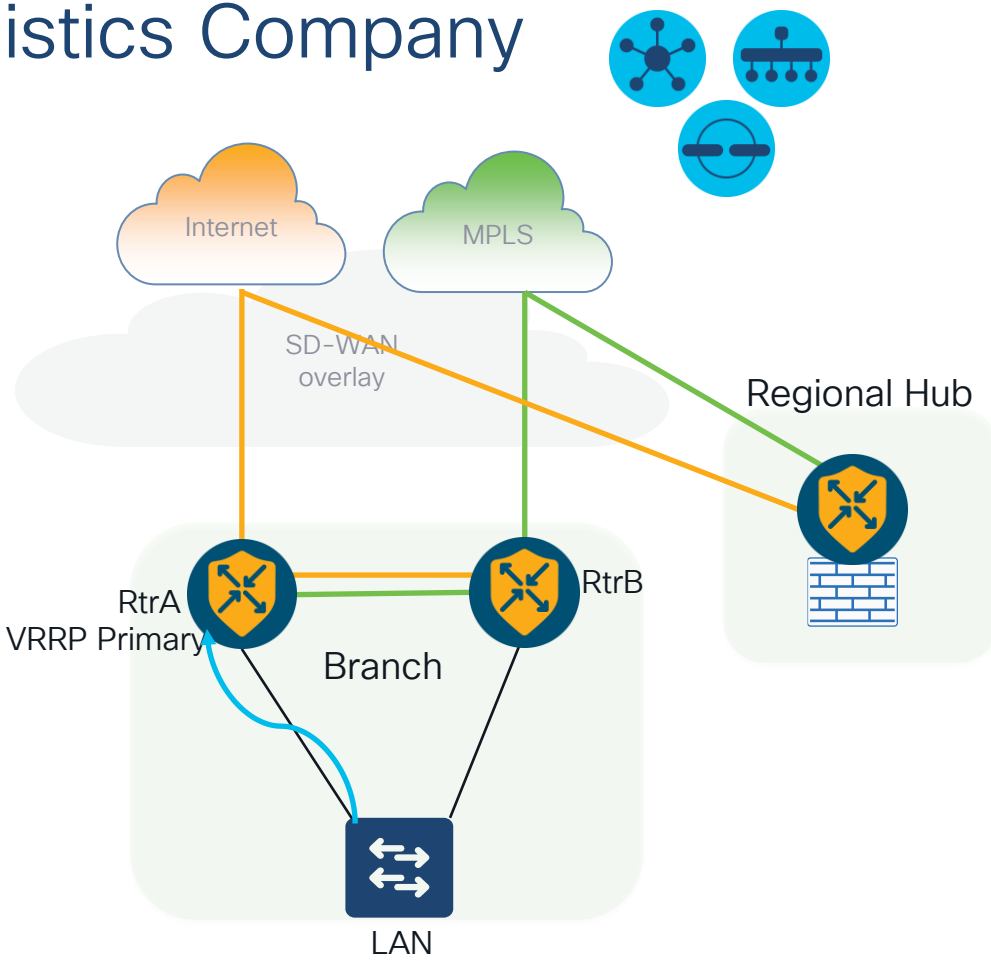
- MPLS Group 33
- Internet – Group 33

Make Your Service Side HA

Global Transport and Logistics Company

Design requirement:

- Resilient branch gateway
- RFC5798 Compliant
- Layer 2 Site uses VRRP per Segment
- In an event of Link, Router or Control plane failure the traffic shouldn't blackhole

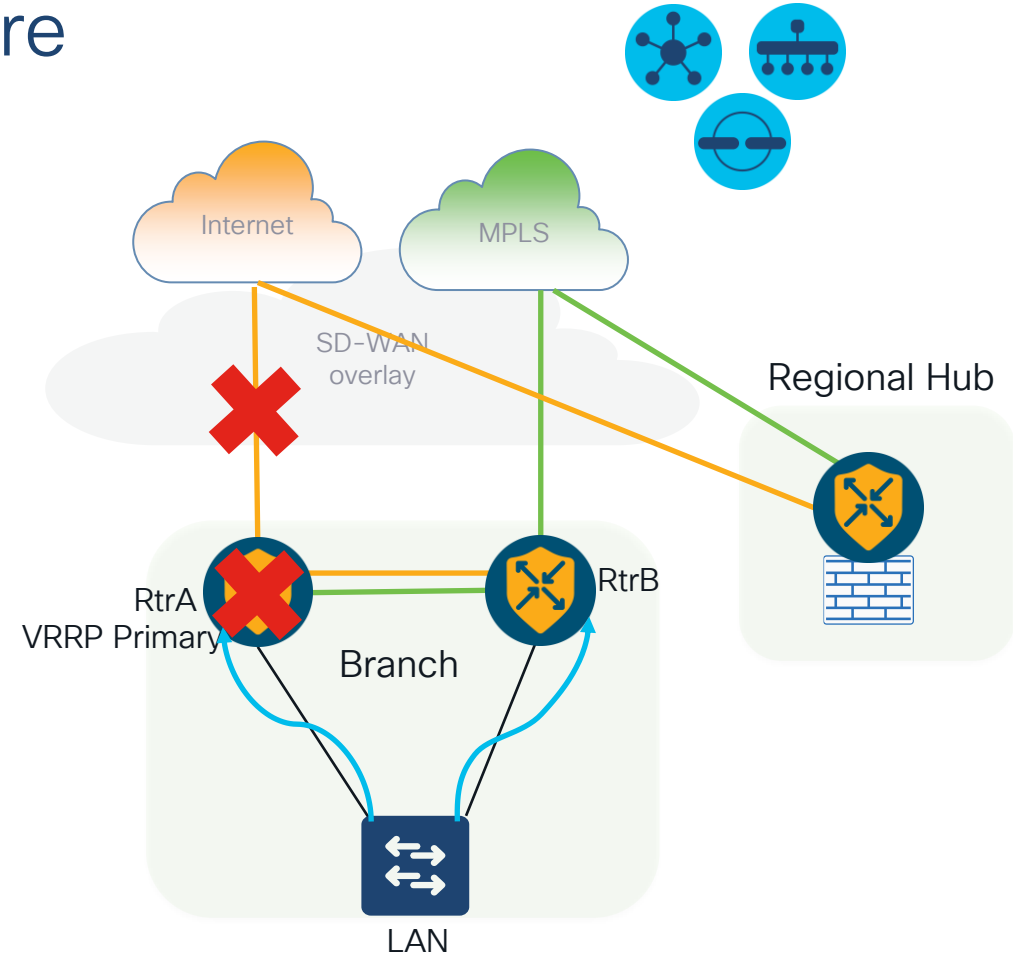


Transport or Router Failure

```
interface GigabitEthernetX
vrf forwarding x
vrrp 100 address-family ipv4
vrrpv2
address 192.168.1.2
priority 110
timers advertise 100
track omp shutdown
```

VRRP Primary

Track OMP Status

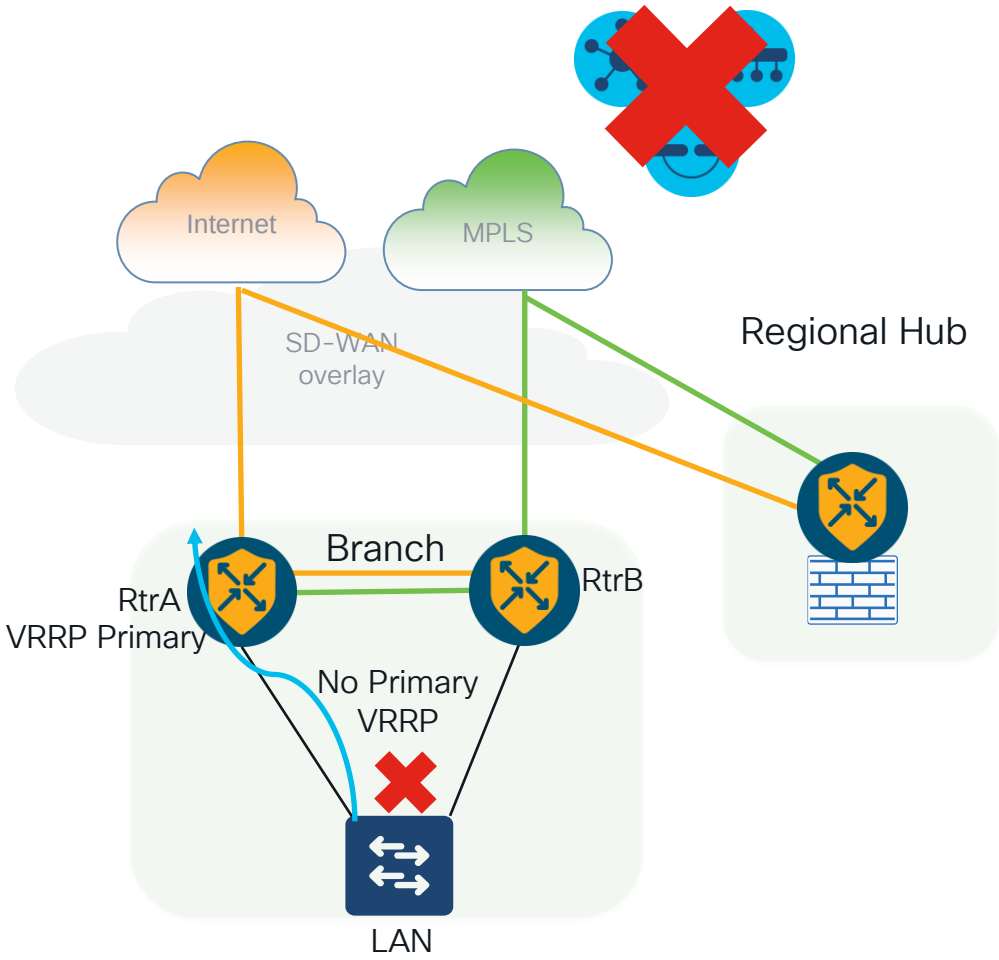


Controller Failure

```
interface GigabitEthernetX
vrf forwarding x
vrrp 100 address-family ipv4
vrrpv2
address 192.168.1.2
priority 110
timers advertise 100
track omp shutdown
```

VRRP Primary

Track OMP Status

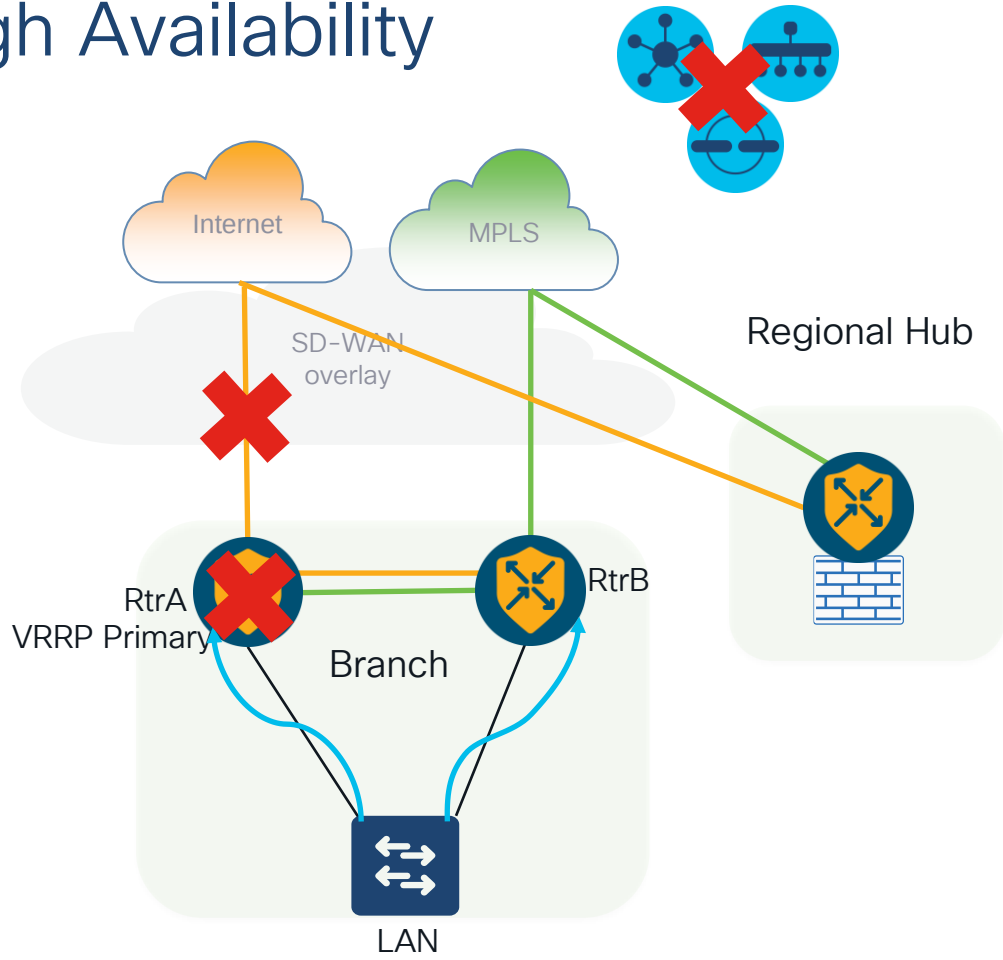


Resiliant Service Side High Availability

```
interface GigabitEthernetX
vrf forwarding x
vrrp 100 address-family ipv4
vrrpv2
address 192.168.1.2
priority 110
timers advertise 100
track 1 shutdown
!
track 1
 object 2
!
track 2 ip route 100.100.100.100
255.255.255.255
ip vrf 1
!
ip prefix-list CL-VRRP seq 5 permit
100.100.100.100/32
```

VRRP Primary

OMP Prefix upstream tracking

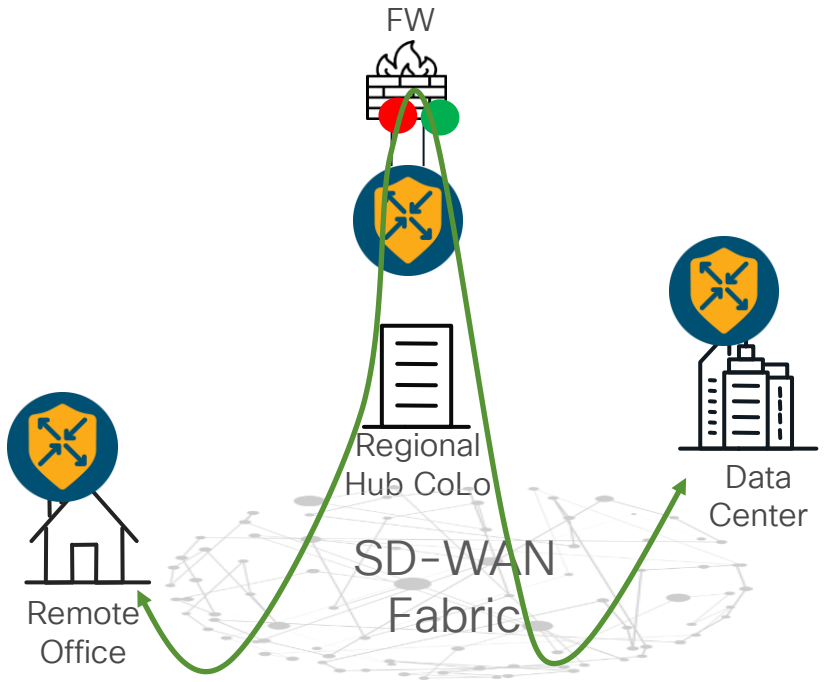


Service Chaining Done Properly

cisco Live!

Global Retail Company

- Requirement: all branch traffic must go through security inspection due to compliance
- Common approach: utilizing service chaining to redirect traffic through security appliances
- Design challenge: resiliency

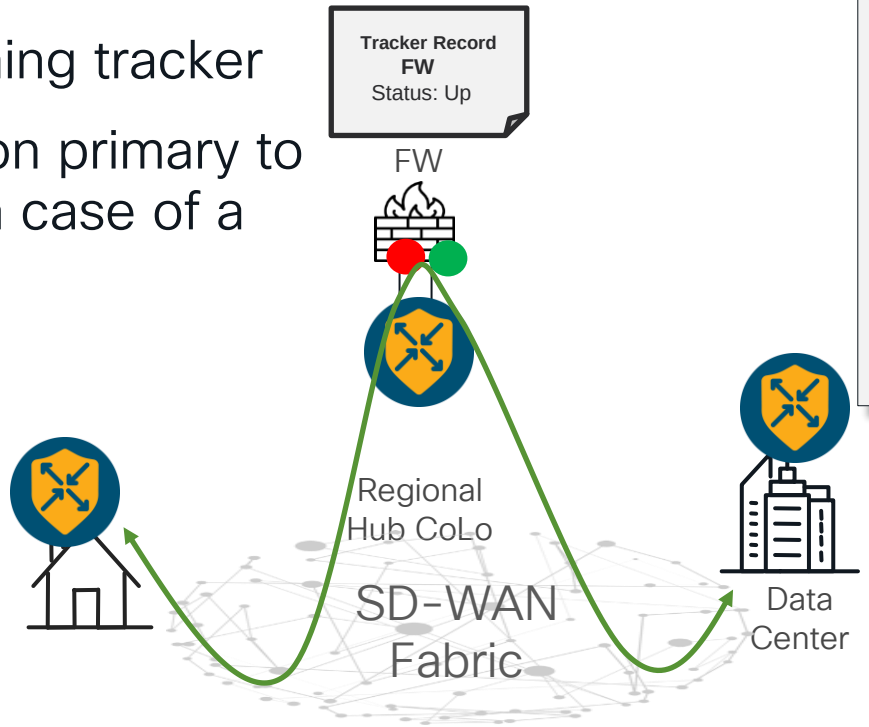


Improving Service Chaining Resiliency – Single Security Appliance

- Define SC service in the Hub site
- Utilize service chaining tracker
- Configure tloc-action primary to failover to routing in case of a tracker failure

```
sdwan
 service firewall vrf x
  track-enable
   ipv4 address 192.168.1.1
```

```
control-policy firewall-
service
  sequence 10
   match route
    site-list Branches
   !
   action accept
    set
     tloc-action primary
     service FW
    !
  default-action accept
 !
```

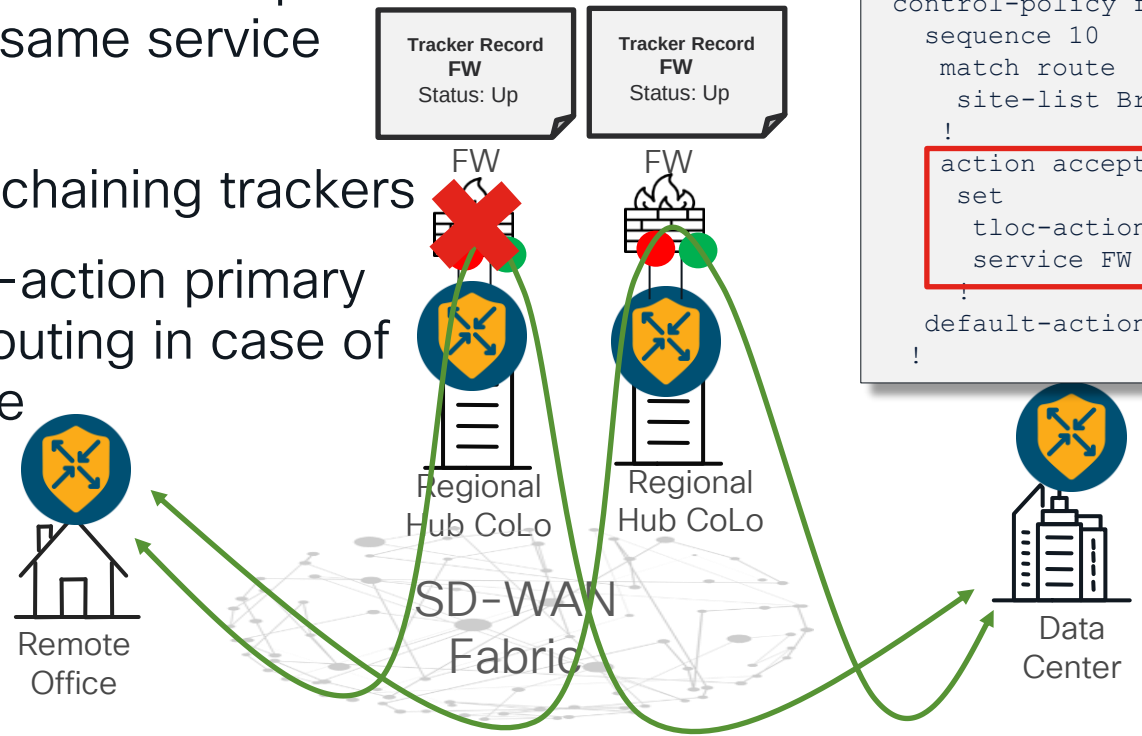


Improving Service Chaining Resiliency – Multiple Security Appliances

- Define SC service in multiple Hubs with the same service name
- Utilize service chaining trackers
- Configure tloc-action primary to failover to routing in case of a tracker failure

```
sdwan
 service firewall vrf x
  track-enable
   ipv4 address 192.168.1.1
```

```
control-policy firewall-service
  sequence 10
   match route
    site-list Branches
   !
   action accept
    set
     tloc-action primary
     service FW
    !
  default-action accept
 !
```



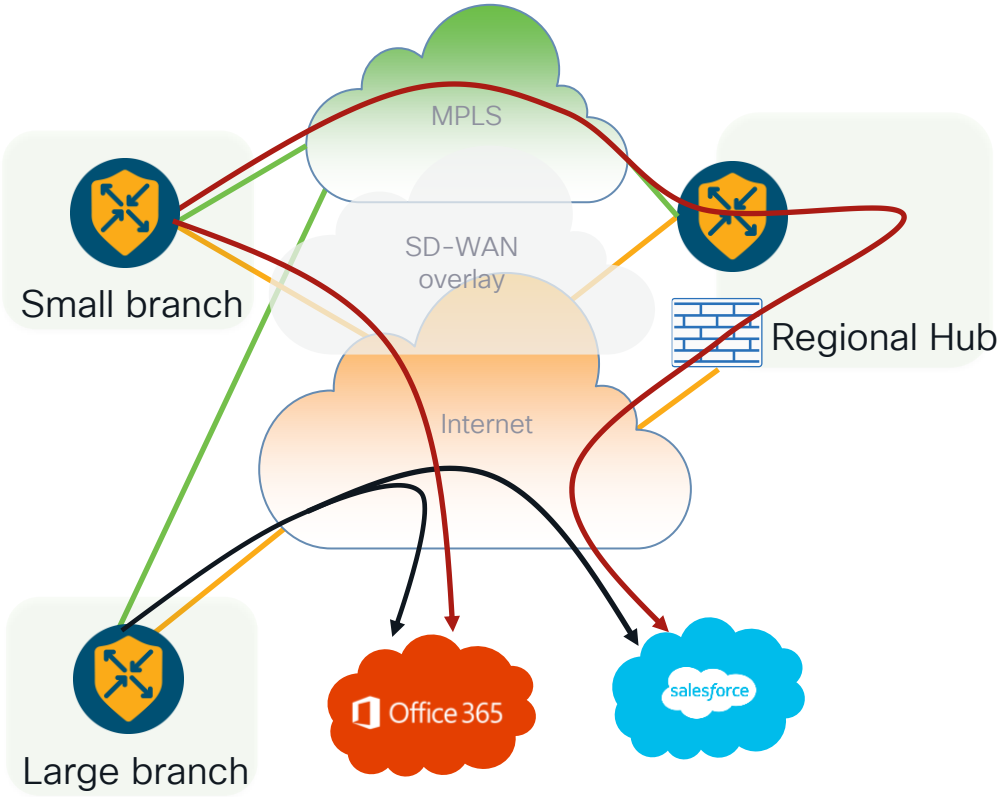
Avoid Breaking The Internet Breakout

cisco Live!

Global Manufacturing Company

- Small branches utilize selective DIA, remaining traffic flows via preferred hub
- In case of a local DIA failure, all traffic should go via the hub

- Large branches utilize local DIA for all traffic
- In case of a local DIA failure, traffic should go via the preferred Hub



Configuring Fallback Internet Routing – Large Branch – Full DIA

- Enable NAT on the interface
- Configure interface tracker
- Configure NAT default route
- Advertise alternative default route from the preferred hub

```
!
interface GigabitEthernet1/0/1
 ip nat outside
 endpoint-tracker dia
!
ip nat inside source list nat-dia-vpn-hop-
access-list interface GigabitEthernet1/0/1
overload
!
endpoint-tracker dia
 endpoint-dns-name www.ciscolive.com
 tracker-type interface
!
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
!
```

Configuring Fallback Internet Routing – Small Branch – Selective DIA

- Define interface tracker
- Configure selective DIA using Data policy with the help of local-tloc
- Configure NAT fallback as part of the Data policy
- Advertise default route from the preferred hub

```
endpoint-tracker dia
 endpoint-dns-name www.ciscolive.com
 tracker-type interface
!
interface GigabitEthernet1/0/1
 ip nat outside
 endpoint-tracker dia
!
policy
 data-policy office365-local-exit
   sequence 10
    match
     app-list microsoft_office365
    !
    action accept
     nat use-vpn 0
     nat fallback
     set
     local-tloc-list
      color public-internet
       encap ipsec
     !
    !
    default-action accept
```

Scale Your SASE

cisco Live!

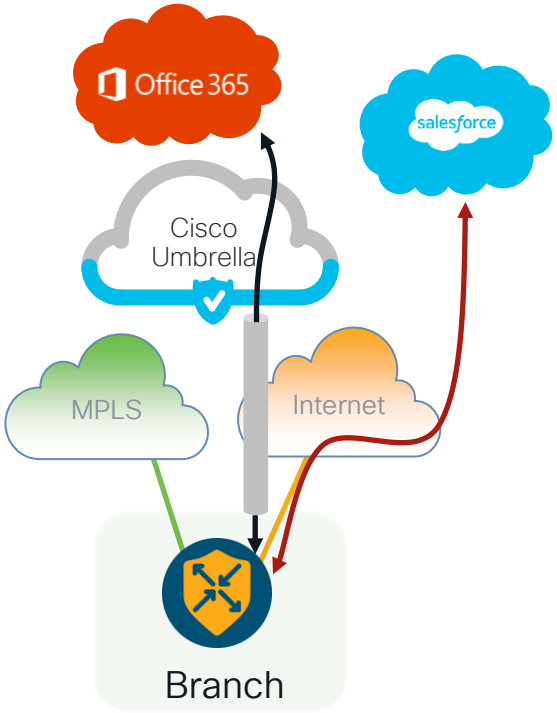
European Supermarket

- Presence all over EMEA
- Cloud security for critical applications
- 500Mbps to 1Gbps Business Internet link and a MPLS

Design requirement

- Priority apps should go to internet via SIG tunnels
- Capability to bypass SIG for certain apps which may pick DIA or DC
- Throughput requirement to SIG is 1 GB for certain branches

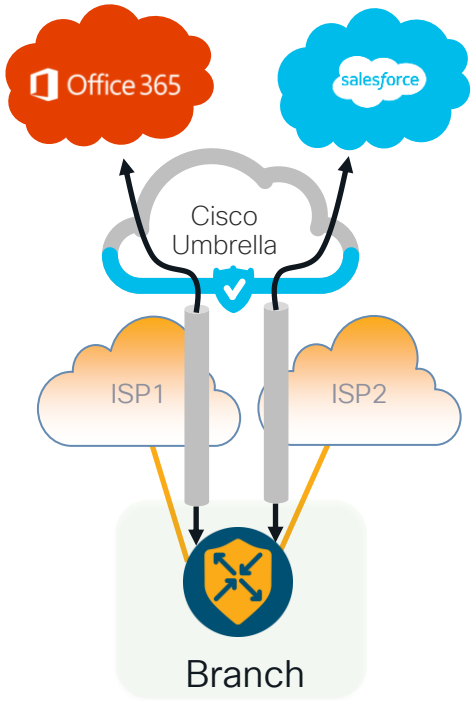
Utilizing Policy Based Path Selection




```
 data-policy Split-SIG
  vpn-list VPN1
    sequence 1
     match
      app-list microsoft_office365
       source-ip 0.0.0.0/0
     !
     action accept
      sig
     !
default-action accept
 !
 site-list Branch
   site-id 200
!
apply-policy
 site-list Branch
  data-policy Split-SIG from-service
!
```

Equal Cost Multi-Path Across Multiple Uplinks

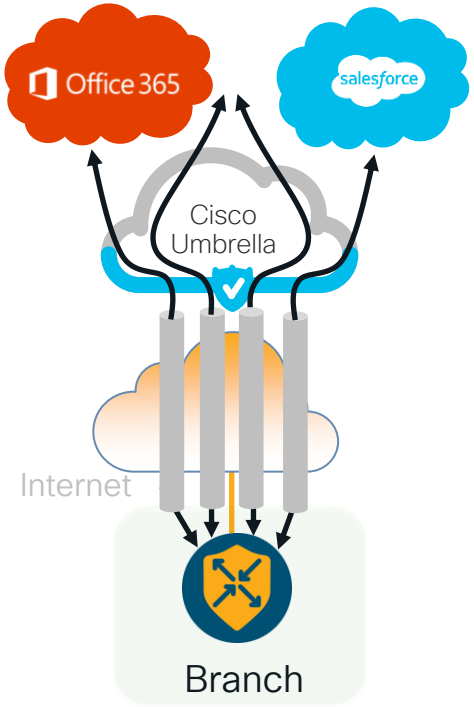
- Load balancing is supported across up to four different equal cost paths
- From individual transport interface single SIG tunnel can be establish
- Limitation: number of Internet uplinks
- Solution: Source tunnel from the loopback



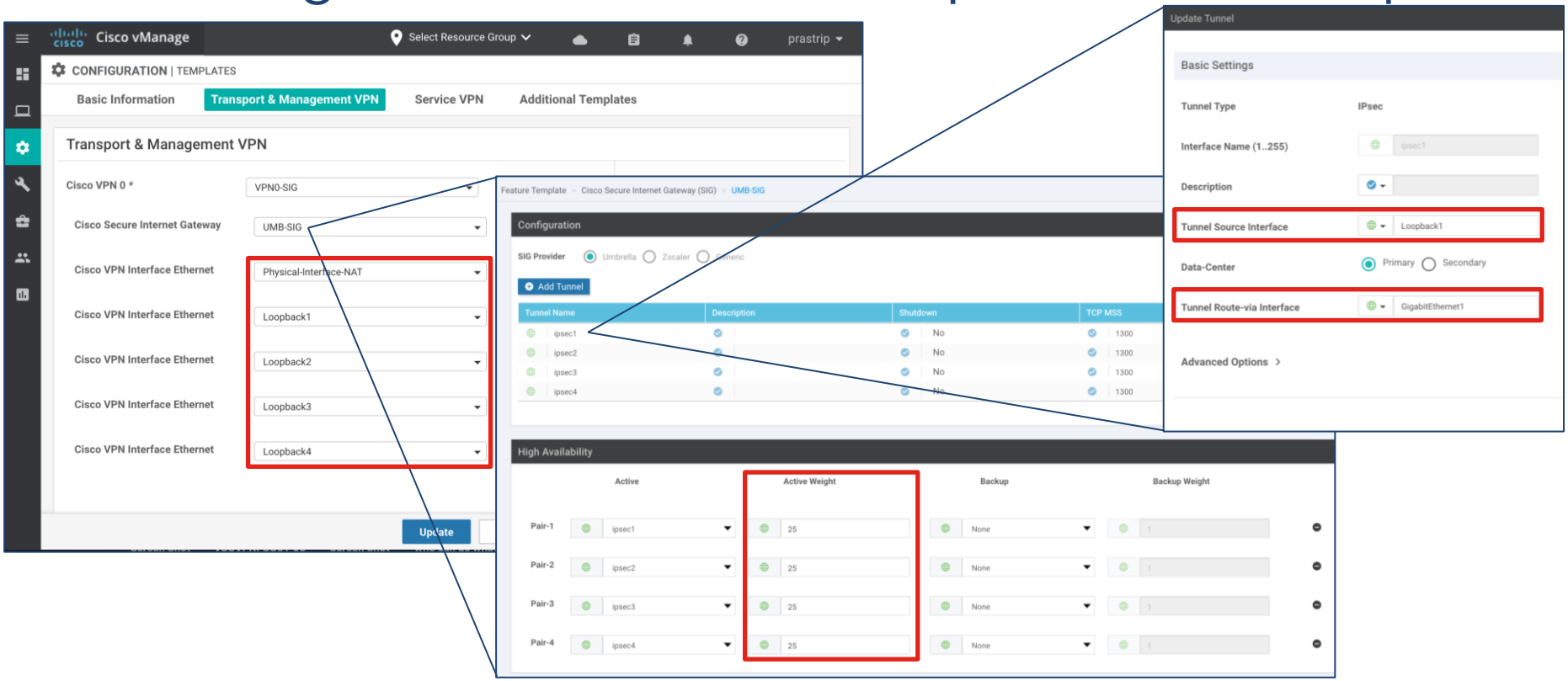
Increasing Throughput Using Multiple SIG Tunnels

- Sourcing SIG tunnels from loopback interfaces supports up to 4 active SIG tunnels with ECMP

- Multiple tunnels can be established from a singe public IP address (NAT-T)



Sourcing SIG Tunnel from Loopbacks - Example



The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive