
cisco Live!
ALL IN

The bridge to possible

Simplifying Network Service Chaining and Load-balancing with Nexus Elastic Services Redirection

Krithika Krishna Moorthy, Lead Technical Marketing Engineer
kritkris@cisco.com
BRKDCN-2879

Cisco Webex App

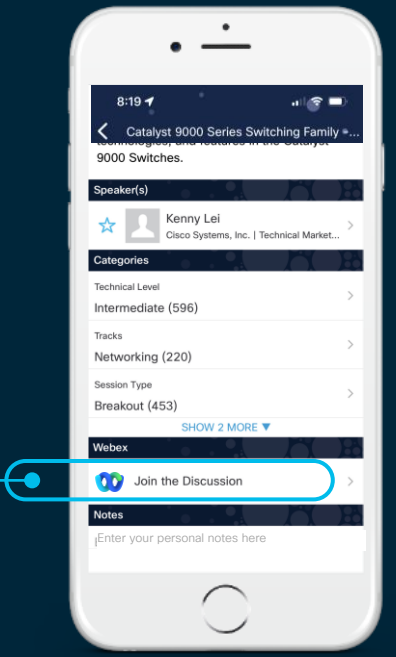
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-2879

Session abstract

In today's Virtualized Data center across Enterprise and Service Provider networks, there is need to deploy services such as firewall, load-balancers, proxies , TCP optimizers for security, compliance and optimization reasons. This introduces an evolving requirement for service chaining , selective traffic redirection and load-balancing amongst these service nodes.

This session aims at providing an overview of two powerful Cisco Nexus 9000 features namely Intelligent Traffic Director (ITD) and enhanced Policy Based Redirect (ePBR) that can be leveraged to meet these requirements. This session includes discussions around various use cases and deployment models that ITD and ePBR supports across the data center deployments.

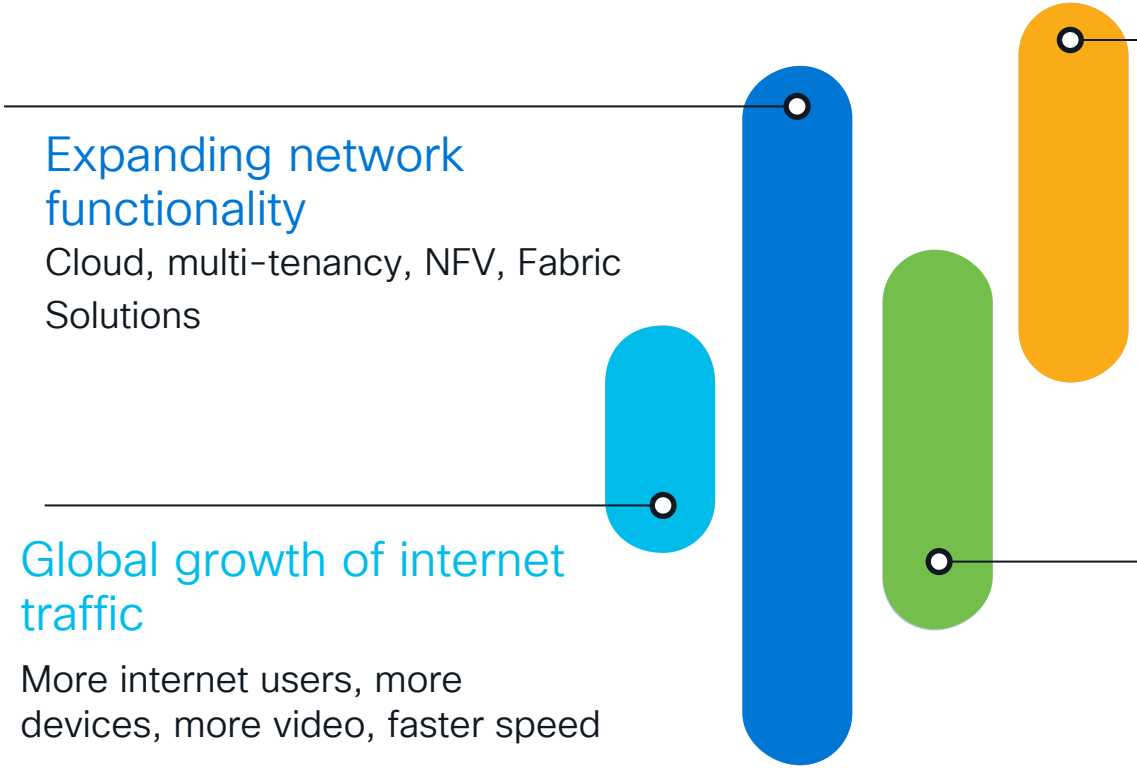
Participants will learn how Elastic Services Redirection(ESR) features - ITD and ePBR can be used to seamlessly integrate these service nodes within their data center and accomplish service chaining and load-balancing functionalities at line rate switching

Agenda

- Introduction to ESR
- Intelligent Traffic Director(ITD) Overview
- ITD Use cases
- Enhanced Policy-based Redirect(ePBR) Overview
- ePBR Use cases
- Conclusion

Introduction to ESR

Current Industry Trends



Expanding network functionality

Cloud, multi-tenancy, NFV, Fabric Solutions

Global growth of internet traffic

More internet users, more devices, more video, faster speed

Service nodes are becoming bottle necks

Not scalable

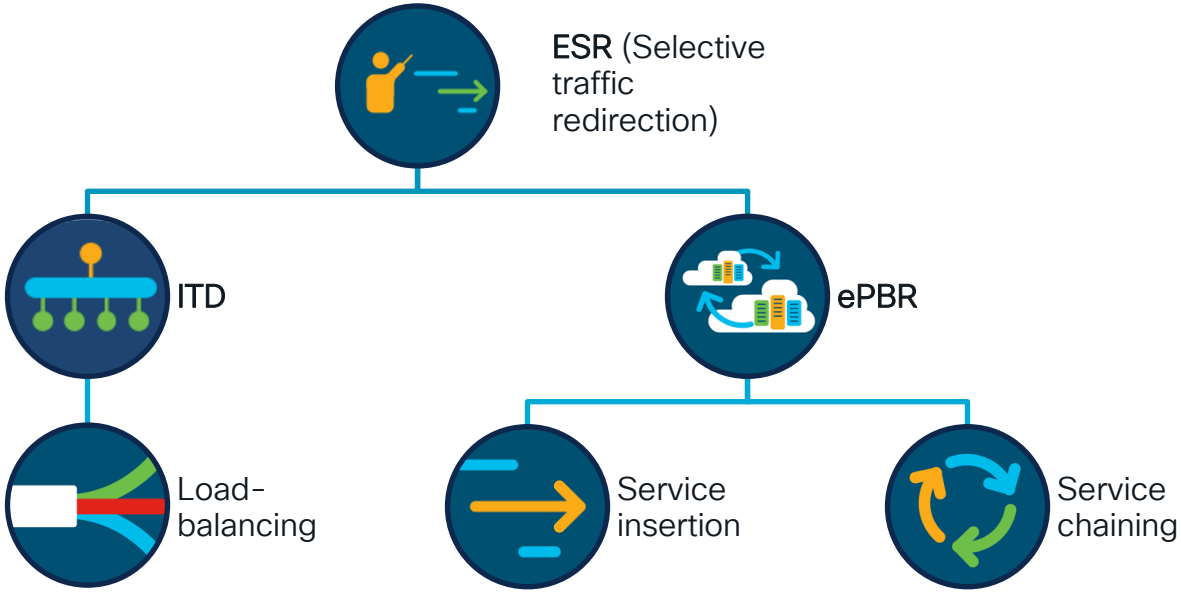
Need extra capacity

Not easy to troubleshoot.

Services deployment

FW, IPS, IDS, Video Caches, WAE, Proxies, TCP optimizers

What is Elastic Services Redirection (ESR) ?

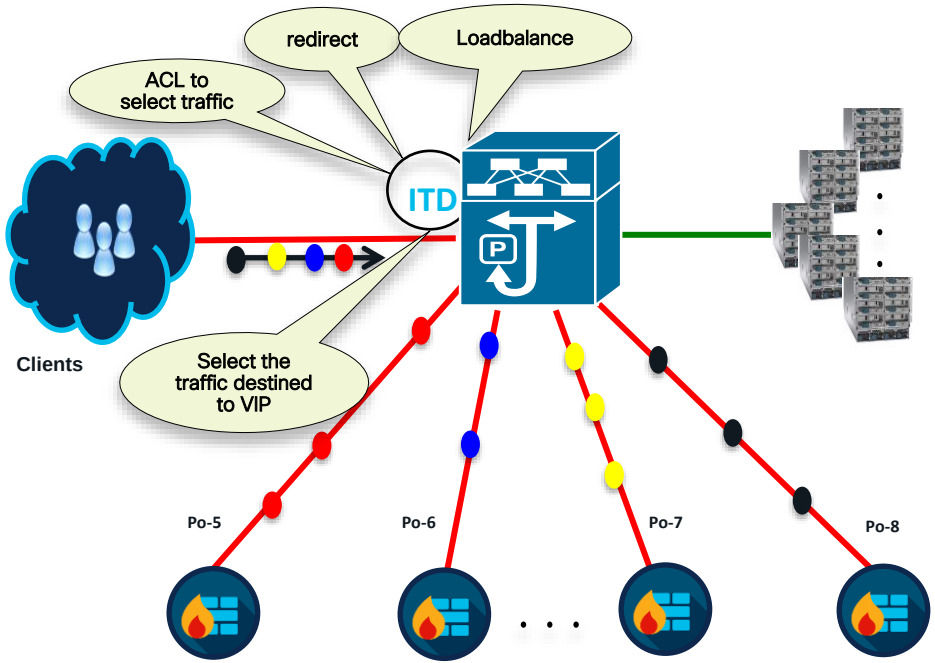


Intelligent Traffic Director (ITD) Overview

ITD ?

- Hardware based Multi-terabit L3/L4 network load-balancing solution at wire-speed
- Addresses growing demand for High-Capacity Traffic Distribution
- ITD eliminates the need to provision and manage another external expensive load-balancer (L3/L4)

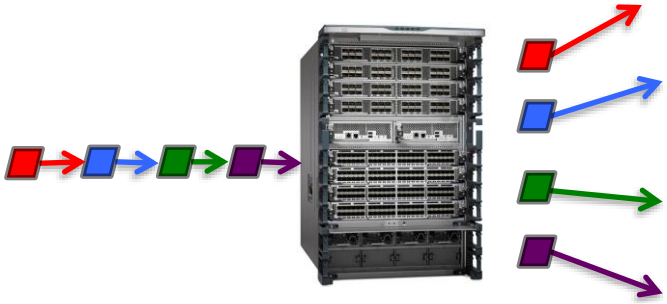
ITD: Intelligent Traffic Director



- Maintains IP stickiness & Flow symmetry
- IPv4,IPV6 and VRF Aware
- Health Monitoring
- Resilient and supports failure handling
- High availability, standby support
- Flexible deployment options
- Appliance agnostic

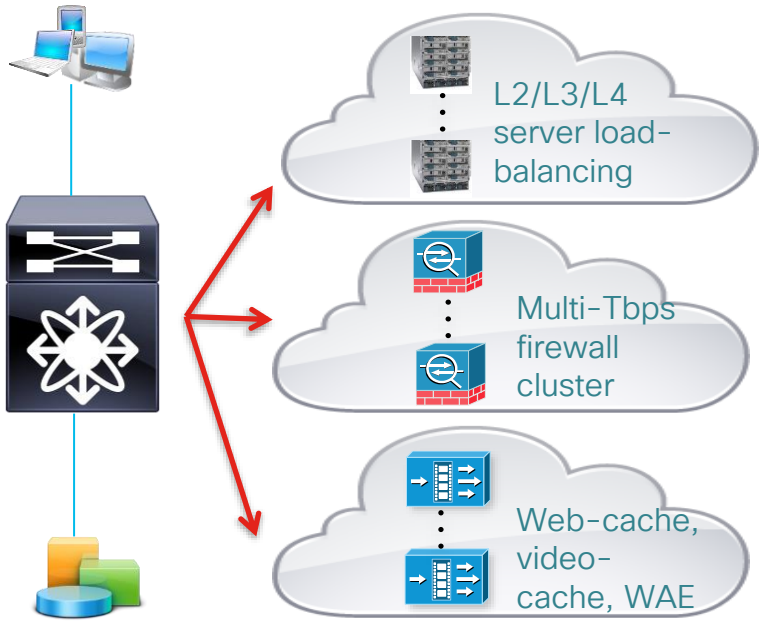
ITD Capabilities

- ✓ Supports load-balancing using Src/Dst ip and L4 port
- ✓ Supports Selective traffic load-balancing
  - VIP based SLB – (VIP/Protocol/Port)
  - ACL based
- ✓ Supports NAT & PAT (non-DSR mode)
- ✓ Weighted load-balancing
- ✓ Flexible Probe options - (ICMP/TCP/UDP/HTTP/DNS/Custom)
- ✓ Non-disruptively add and delete service nodes + ACL selection
- ✓ Sub second Convergence



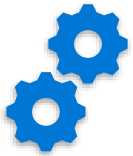
ITD Deployments

Server LB	Server farms, Application servers, Web Servers
Network Function LB	Firewall, IDS, IPS, WAF, L4-L7 Load balancers, Sandwich Deployment
Traffic Steering & Redirection	Web Acceleration Engine (WAE), Web Caches , WCCP replacement



ITD Solution details

Device group Definition



- Service Nodes / Service Appliances IP
- Probes
- Weights
- Standby (backup nodes)

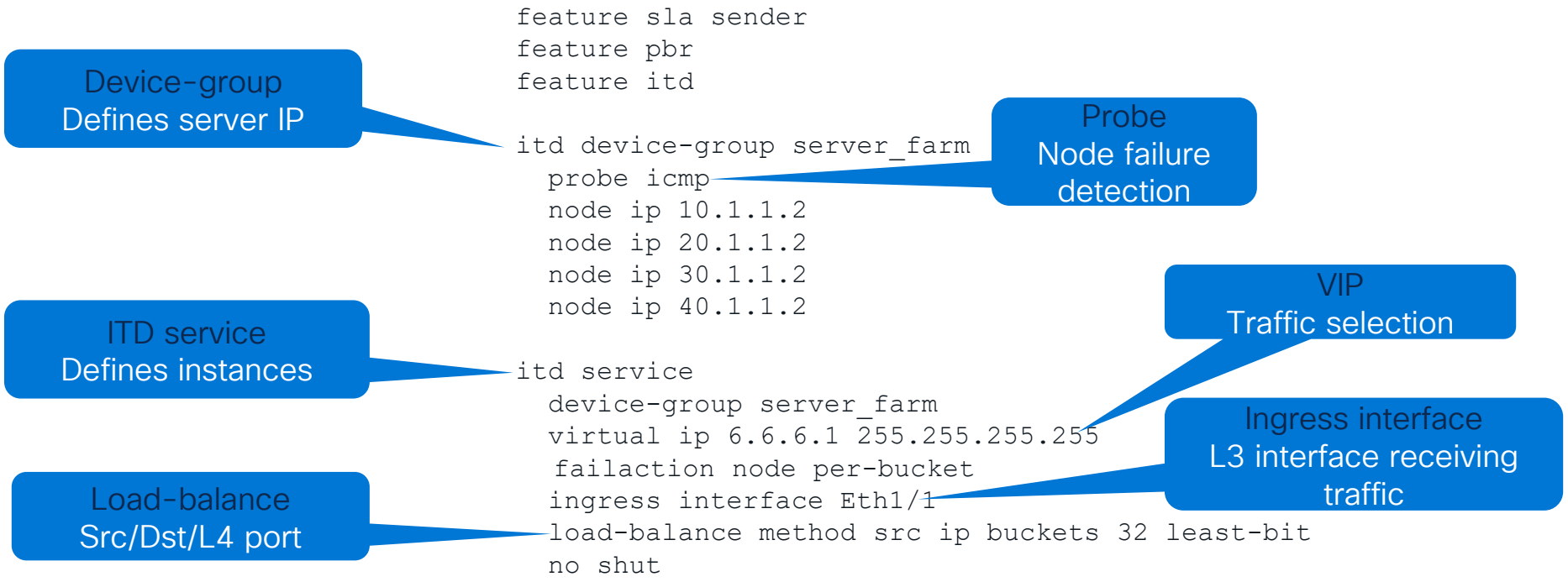
Service Definition

- Attach device-group
- Ingress-interface
- Virtual IP Address
- Traffic Filtering / selection ACL
- Load-balancing options
- Failover options

Service Bring up

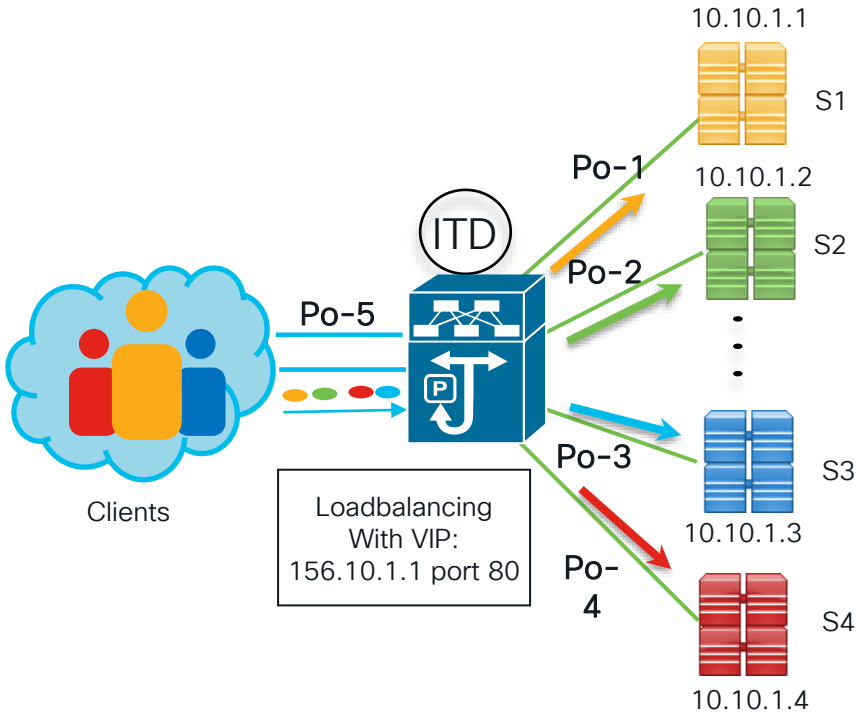
- Bring up the ITD service with ‘no shut’ for the policy to be applied on the interface

ITD config example



ITD Use cases

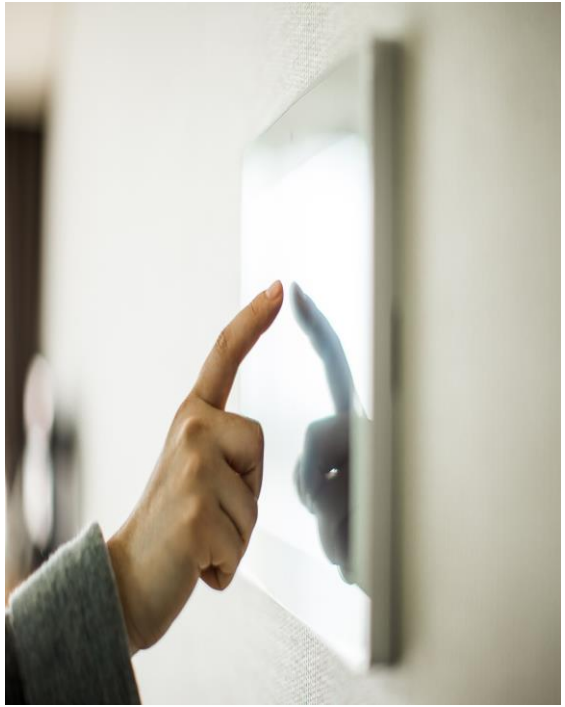
Server Load Balancing(SLB)



- Packets from client redirected and load-balanced across servers using ITD
- All servers configured with a VIP as loopback address
- Server returns the packet to client using Direct Server Return(DSR)

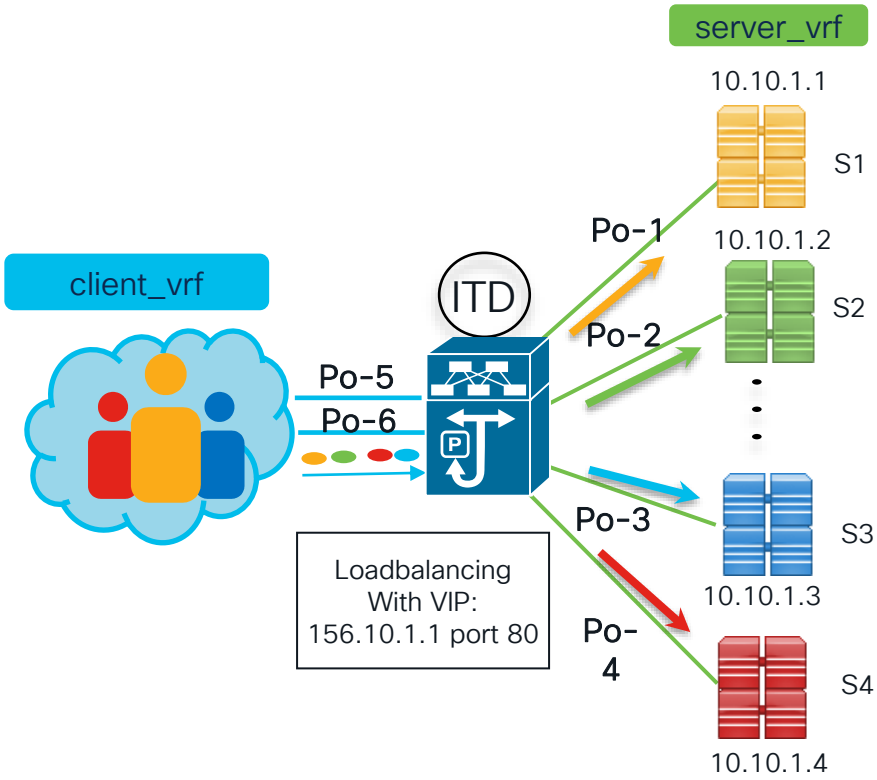
Server Load Balancing(SLB)

Configuration Example



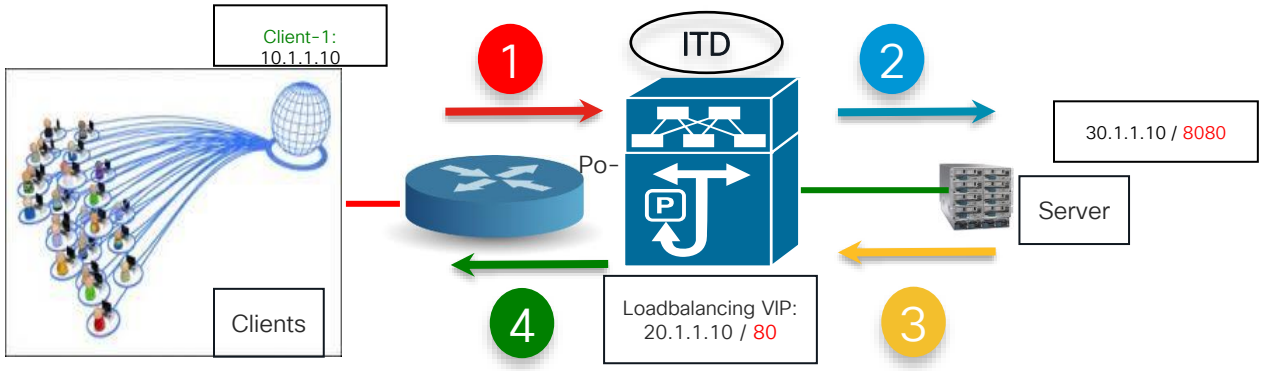
```
feature itd
feature pbr
feature sla sender

itd device-group server_farm
probe tcp port 80
  node ip 10.10.1.1
  node ip 10.10.1.2
  node ip 10.10.1.3
  node ip 10.10.1.4

itd Service-1-IPv4
  device-group server_farm
  virtual ip 156.10.1.1 255.255.255.255 tcp 80
  ingress interface po5
  ingress interface po6
  failaction node per-bucket
  load-balance method src ip buckets 16
  no shut
```

Inter-VRF Load Balancing with ITD



- Traffic from tenant belonging to one VRF can be load-balanced across service appliances present on a different VRF
- Support available starting NXOS 10.2(1)

SLB with Destination NAT & PAT



Step	dst-mac	src-mac	src-ip	dst-ip
1	N9K MAC	Router MAC	10.1.1.10	20.1.1.10:80
2	Server MAC	N9K MAC	10.1.1.10	30.1.1.10:8080
3	N9K MAC	Server MAC	30.1.1.10:8080	10.1.1.10
4	Router MAC	N9K MAC	20.1.1.10:80	10.1.1.10

- ITD NAT eliminates the need to configure a loopback on server for DSR
- In forward flow from Client to server, the N9k translates the DIP and port from VIP to real IP/Port of the server
- In reverse flow from Server back to client, N9k translates the SIP from server IP/Port to VIP/Port

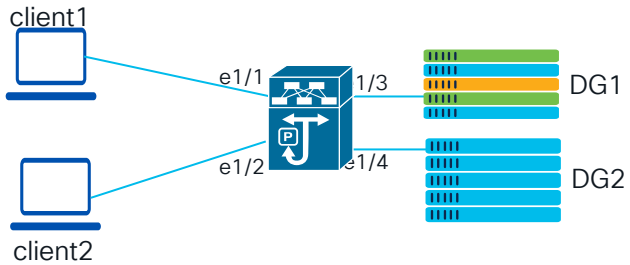
SLB with Destination NAT & PAT

Configuration Example

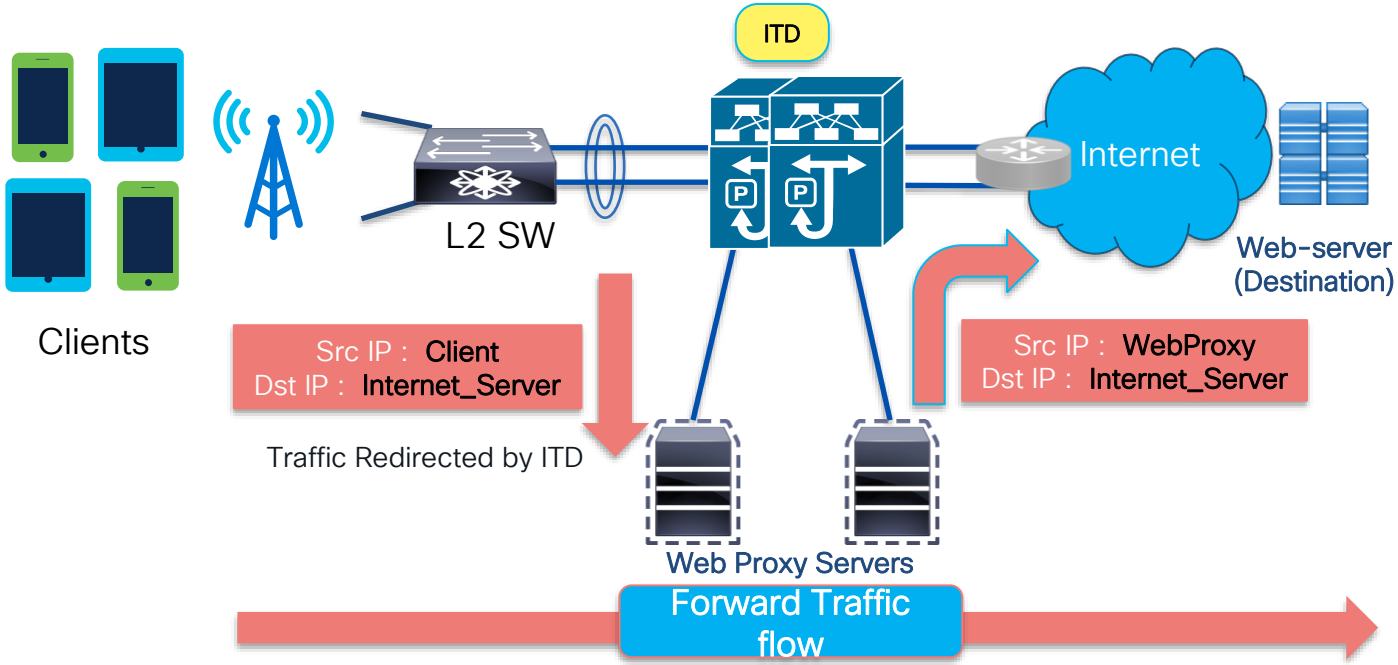
ITD NAT requires NAT tcam and feature ”NAT” to be enabled

```
hardware access-list tcam region nat 2048
feature nat
feature itd
feature sla sender

interface eth1/1-2
ip nat outside
interface e1/3-4
ip nat inside

itd device-group DG1
 probe icmp frequency 2 timeout 1
node ip 8.8.1.2
node ip 9.9.1.2
port 1000

itd device-group DG2
probe icmp
node ip 10.10.1.2
port 1000
node ip 11.11.1.3
port 2000
```

```
itd SER1
virtual ip 6.6.1.1 255.255.255.255 tcp 80 advertise enable device-
group DG1
virtual ip 6.6.1.2 255.255.255.255 tcp 90 advertise enable device-
group DG2
ingress interface e1/1
Ingress interface e1/2
nat destination
failaction node per-bucket
load-balance method src ip buckets 32
no shut
```

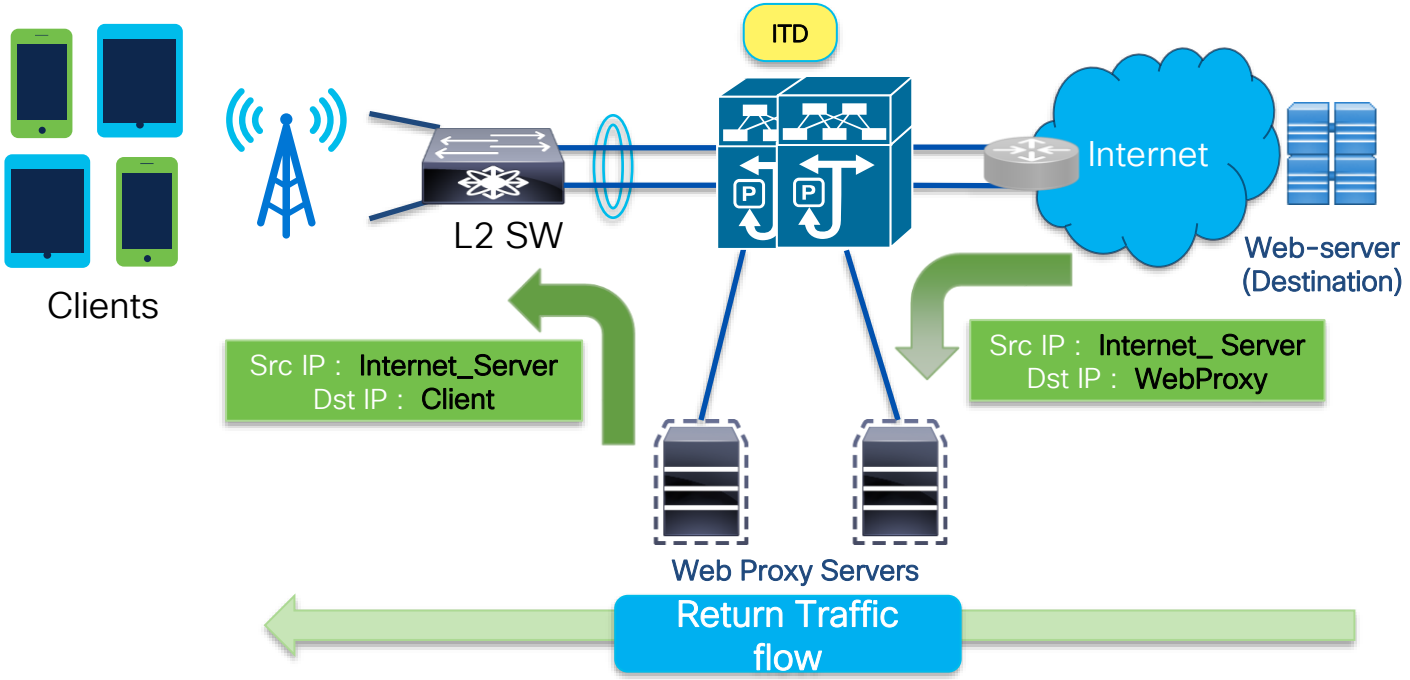


Web-Proxy Deployment



ITD redirects using **Include-ACL** and load-balances the packets across the Web-Proxy servers

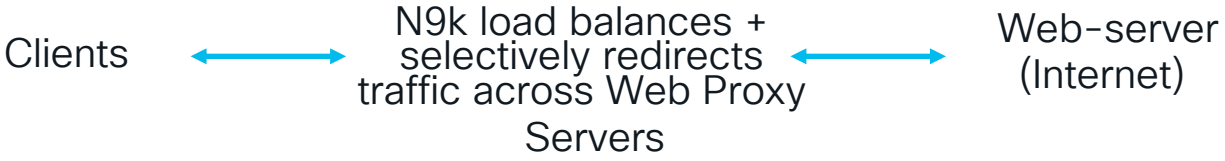
Web-Proxy Deployment (cont.)



Packets are being forwarded normally(no redirection) on the Nexus Switches.

Web-Proxy Deployment

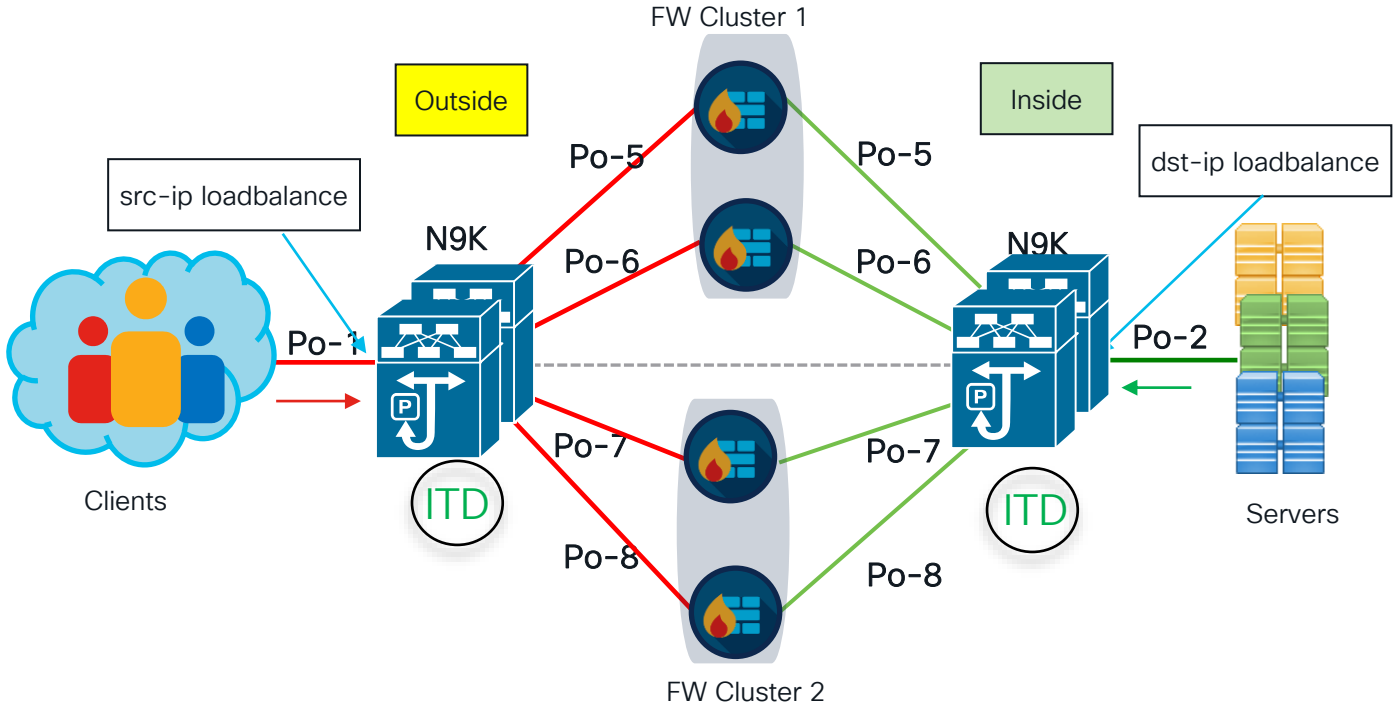
Configuration Example




```
feature itd
feature pbr
feature sla sender

ip access-list itd_exclude_ACL
  ! Exclude private IP address
  10 permit ip any 10.0.0.0/8
  20 permit ip any 192.168.0.0/16
  30 permit ip any 172.16.0.0/12

ip access-list internet-acl
  10 permit ip any any tcp 80
  20 permit ip any any tcp 443
```

```
itd device-group Web_Proxy_Servers
  probe icmp
  node ip 10.1.50.1
  node ip 10.1.50.2

itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_ACL
  access-list internet-acl
  ingress interface Vlan 10
  failaction bucket distribute
  load-balance method src ip
  no shutdown
```

Sandwich Mode Deployment

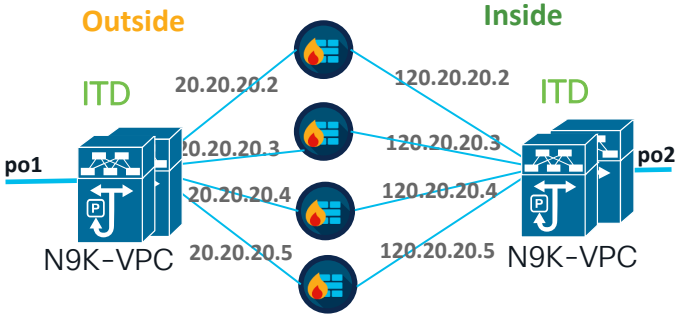


- The sandwich deployment mode provides Symmetric handling of traffic.
- Forward and reverse traffic between the client and the server flows through the same appliance.
- Appliance clustering capability

Sandwich Deployment

Configuration Example

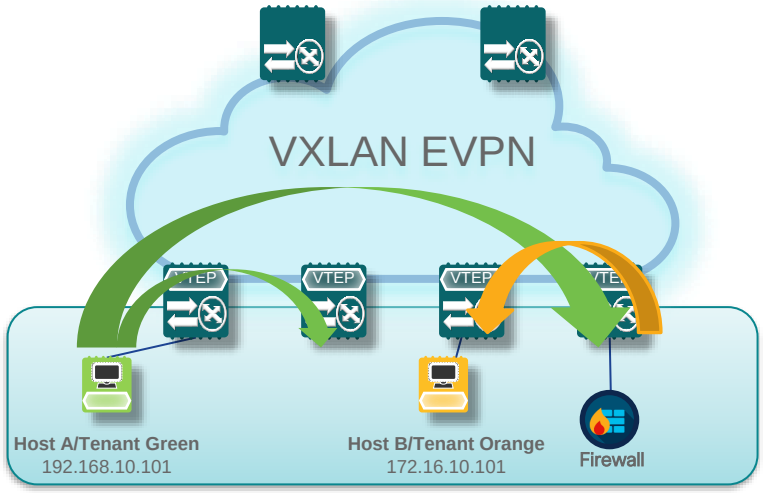
```
itd device-group FW-INSPECT
probe icmp
node ip 20.20.20.2
cluster 1
node ip 20.20.20.3
cluster 1
node ip 20.20.20.4
cluster 2
node ip 20.20.20.5
cluster 2

itd WebTraffic
Device-group FW-INSPECT
ingress interface po1
failaction bucket distribute
load-balance method src ip buckets
64
no shut
```



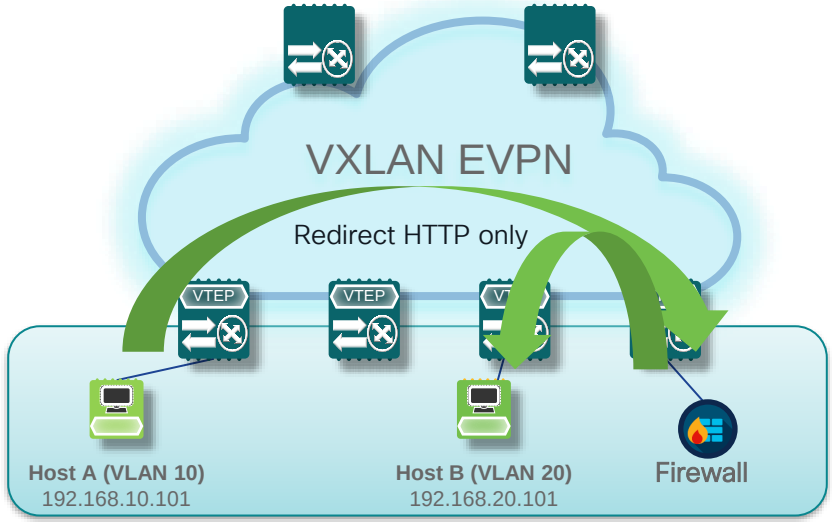

```
itd device-group FW-INSPECT
probe icmp
node ip  20.20.20.2
cluster 1
node ip 20.20.20.3
cluster 1
node ip 20.20.20.4
cluster 2
node ip 20.20.20.5
cluster 2

itd WebTraffic
Device-group FW-INSPECT
ingress interface po2
failaction bucket distribute
load-balance method dst ip buckets
64
no shut
```

Enhanced Policy-based Redirect (ePBR) Overview

How is Service Chaining Done today?



Routing rules reflect path via service devices



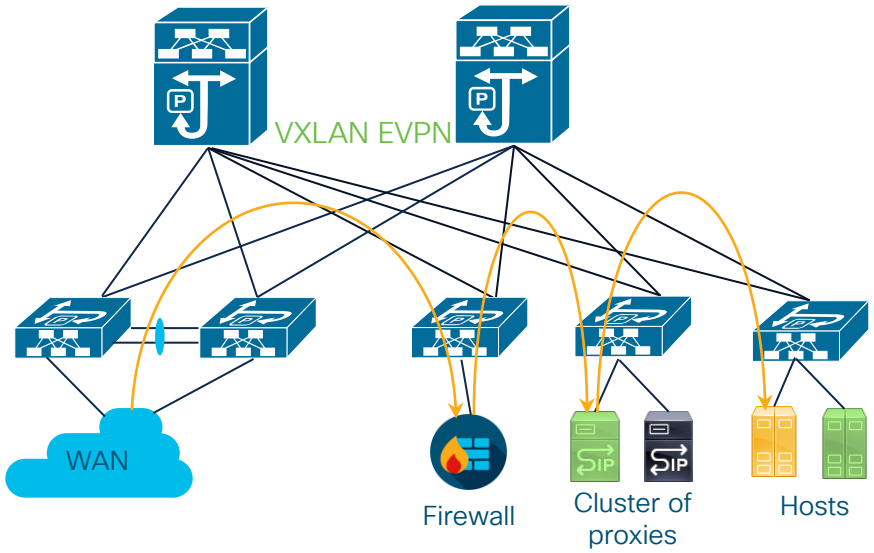
Selective Traffic Redirect using Policy Based Routing

What are the challenges with existing options?

- Service nodes becoming bottlenecks
- Static PBR policies complex to maintain
- Service redirection across multiple service nodes is complex to configure
- Options to load-balance and redirect missing
- Limited ability to monitor device health and configuring fail action based on device availability is missing
- Need to account for forward and return traffic to maintain symmetry

Enhanced Policy-based Redirect(ePBR)

- Service chaining , Selective traffic redirection & Load-balancing
- Simplified service appliance onboarding & Health Monitoring
- Service chaining across Multi-site fabrics
- Flexible deployments



ePBR Capabilities

Simplified service chain creation

- Simplified device onboarding
- Granular multi-level service policy creation

Optimized utilization of service node

- Selective traffic redirection
- L3/L4 redirect , exclude and drop options

Ability to scale

- Through symmetric load-balancing along with chaining

Health monitoring & flexible failover

- Probes - ICMP/TCP/UDP/HTTP/ DNS/Custom
- Failover - Forward / Bypass / Drop

Simplified expansion

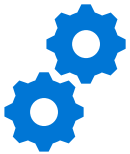
- Add/delete/modify service, policy and match ACL selection

Line Rate traffic forwarding

- No impact to throughput & performance
- No increased latency

ePBR Solution details

Onboard Service Appliance



- Service IP address
- Forward and reverse attached interface (single/dual arm)
- Probes
- VRF membership
- Additional service end-points for creating appliance cluster

Define traffic redirect Policy

- Traffic Filtering or selection ACL
- Service-chain creation
- Load-balancing options(src/dst and buckets)
- Failover options (forward/bypass/drop)

Apply the ePBR Policy on relevant interfaces

- Apply policy on ingress interface where chaining needs to start
- VXLAN – Apply on L3 VNI interfaces on service leaf
- Apply policy with “reverse” keyword to maintain flow symmetry

ePBR config example

Step 1: Onboard the appliances

```
epbr service FIREWALL_CLUSTER
   probe icmp source-interface loopback10
   vrf TENANT_A
   service-endpoint ip 172.16.1.200 interface VLAN100
           reverse ip 172.16.2.200 interface VLAN101
   service-endpoint ip 172.16.1.201 interface VLAN100
           reverse ip 172.16.2.201 interface VLAN101

epbr service TCP_Optimizer
   probe icmp source-interface loopback11
   vrf TENANT_A
   service-endpoint ip 172.17.1.200 interface VLAN100
           reverse ip 172.17.1.200 interface VLAN100
```

Step 2: Create traffic selection rules

```
ip access-list WEB
10 permit tcp any any eq 80
20 permit tcp any any eq 443

ip access-list APP-A
10 permit tcp 172.16.10.0/24 any eq 7800
20 permit tcp 192.168.20.0/24 any eq 7800
```

Step 3: Define ePBR traffic redirect policy

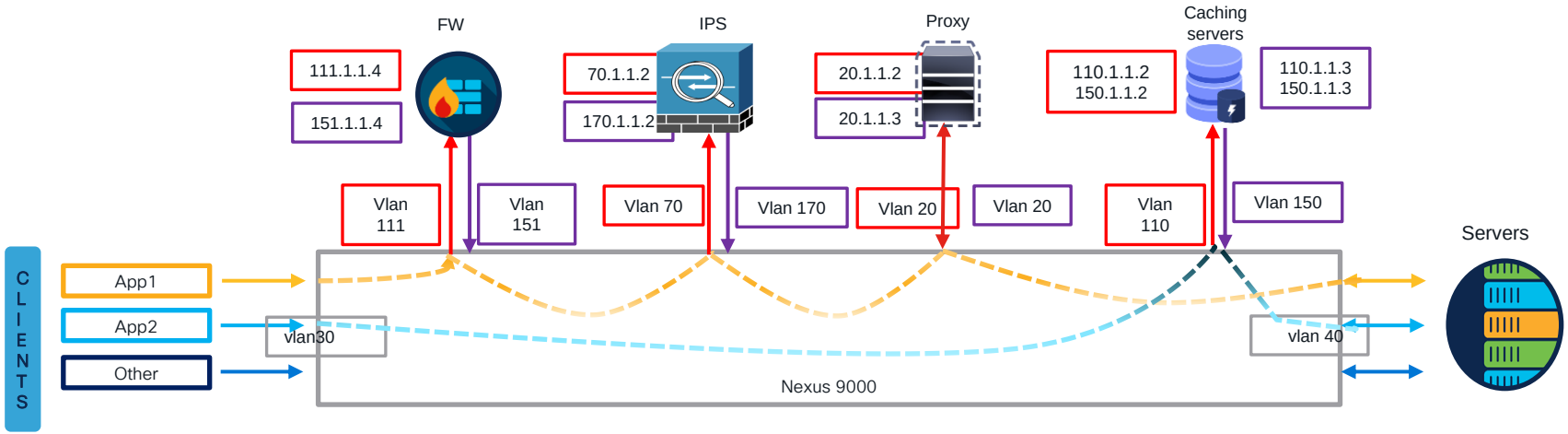
```
epbr policy Tenant_A-Redirect
   match ip address WEB
   load-balance method src-ip
    10 set service FIREWALL_CLUSTER fail-action drop
    20 set service TCP_Optimizer fail-action bypass
   match ip address APP-A
   load-balance method src-ip
    10 set service FIREWALL fail-action drop
```

Step 4: Apply the ePBR Policy on relevant ingress interfaces – Tenant SVI / L3VNI SVI / L3 interfaces

```
interface vlan 2010
  !L3 VNI SVI
  epbr ip policy Tenant_A-Redirect
  epbr ip policy Tenant_A-Redirect reverse
```

ePBR Use cases

Service chaining in Traditional deployments



- App1 traffic : firewall → IPS → Proxy
- App2 traffic : Load-balanced directly among the caching servers

Service chaining in Traditional deployments

Configuration Example

Step 1: Onboard the appliances

```
epbr service firewall
  service-end-point ip 111.1.1.4 interface Vlan111
     probe icmp source-interface loopback0
    reverse ip 151.1.1.4 interface Vlan151
       probe icmp source-interface loopback1

epbr service ips
  service-end-point ip 70.1.1.2 interface Vlan70
     probe udp 45000
    reverse ip 170.1.1.2 interface Vlan170
       probe udp 45001

epbr service proxy
  service-interface Vlan20
   probe http get index.html
  service-end-point ip 20.1.1.2
    reverse ip 20.1.1.3
```

```
epbr service caching_servers
! traffic will be load-balanced between the
servers
! server1
  service-end-point ip 110.1.1.2 interface Vlan110
     probe icmp source-interface loopback0
    reverse ip 150.1.1.2 interface Vlan150
       probe icmp source-interface loopback1
! server2
  service-end-point ip 110.1.1.3 interface Vlan110
     probe icmp source-interface loopback0
    reverse ip 150.1.1.3 interface Vlan150
       probe icmp source-interface loopback1
```

Service chaining in Traditional deployments

Configuration Example(cont.)

Step 2: Create traffic selection rules

```
ip access-list app1
        10 permit tcp 172.16.10.0/24 eq 7800 any
        20 permit tcp 192.168.20.0/24 eq 7800 any
ip access-list app2
        10 permit tcp 172.16.10.0/24 any eq www
        20 permit tcp 192.168.20.0/24 any eq www
```

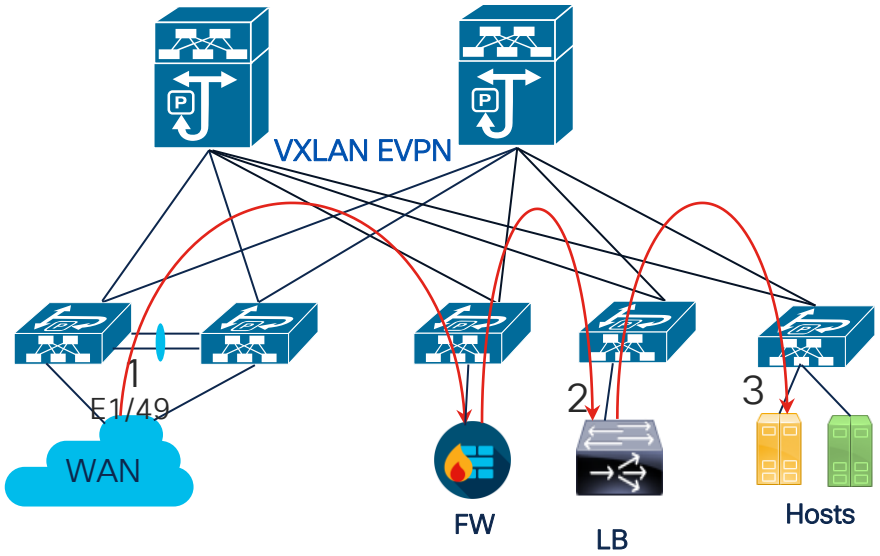
Step 3: Define ePBR traffic redirect policy

```
epbr policy redirect_and_loadbalance
  statistics
  match ip address app1
    ! Traffic matching app1 takes FW→IPS→Proxy chain
    10 set service firewall fail-action drop
    20 set service ips fail-action bypass
    30 set service proxy fail-action forward
  match ip address app2
    ! Traffic matching app2 is load-balanced across
caching servers
    load-balance buckets 8 method src-ip
    10 set service caching_servers
```

Step 4: Apply the ePBR Policy on relevant interfaces

```
interface Vlan30
  !forward policy applied to ingress interface facing
clients
  no shutdown
  ip address 30.1.1.1/24
  ipv6 address 2030::1/24
  epbr ip policy redirect_and_loadbalance

interface Vlan40
! Reverse policy applied to egress interface facing
server farm for reverse flow
  no shutdown
  ip address 40.1.1.1/24
  ipv6 address 2040::1/24
   epbr ip policy redirect_and_loadbalance reverse
```

Service chaining in VXLAN fabrics



LB in VLAN 20
FW_inside in VLAN 111 , FW_outside in VLAN 151

Chain : WAN → FW → LB → Host

- Supports Intra and Inter VRF service chaining Models of deployment
- Flexible service appliance deployment
- Service appliance mobility

Configuration Example

Step 1: Onboard the appliances

```
epbr service firewall
  vrf firewall
  service-end-point ip 111.1.1.4 interface
Vlan111
     probe icmp source-interface loopback0
    reverse ip 151.1.1.4 interface Vlan151
       probe icmp source-interface loopback1

epbr service load_balancer
  vrf load_balancer
  service-interface Vlan20
  probe http get index.html
  service-end-point ip 20.1.1.2
    reverse ip 20.1.1.3
```

Step 2: Create traffic selection rules

```
ip access-list app1
        10 permit tcp 172.16.10.0/24 any eq 7800
```

Step 3: Define ePBR traffic redirect policy

```
epbr policy chain1
  statistics
  ! Firewall → proxy → load_balancer
  match ip address app1
    10 set service firewall fail-action drop
    20 set service load_balancer fail-action forward
```

Configuration Example (contd)

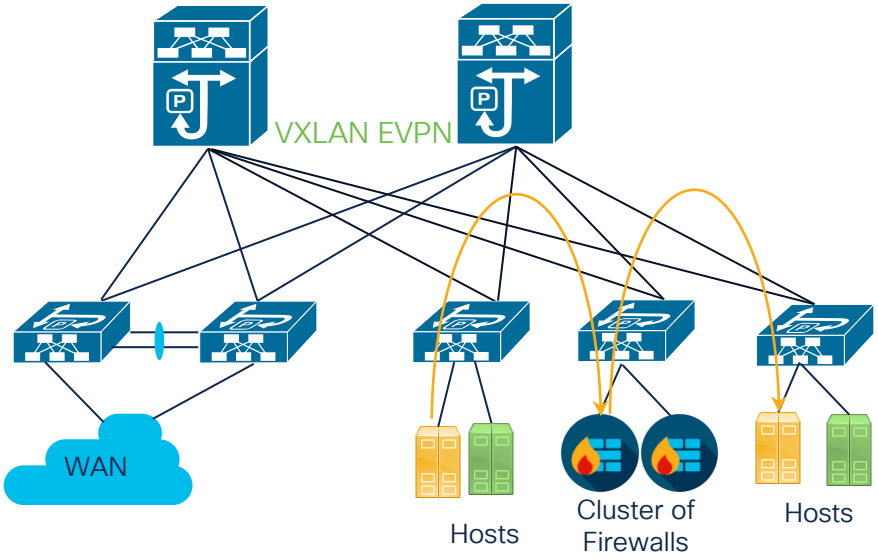
Step 4: Apply the ePBR Policy on relevant ingress interfaces

```
interface eth1/49
Vrf member tenant1
! Forward policy applied to ingress interface facing WAN in border leaf
ip address 30.1.1.1/24
epbr ip policy chain1

interface Vlan100
Vrf member firewall
! Forward policy applied to L3vni of firewall in service leaf
ip forward
no ip redirect
epbr ip policy chain1

interface Vlan102
vrf member load_balancer
! Forward policy applied to L3vni of load_balancer in service leaf
ip forward
no ip redirect
epbr ip policy chain1
```

Note1: Step1, step2 and step3 needs to be defined on all service leafs and border leaf from which traffic is ingressing onto the fabric

Note2: Leak tenant routes onto all the service VRFs in the service leafs to route packet towards destination

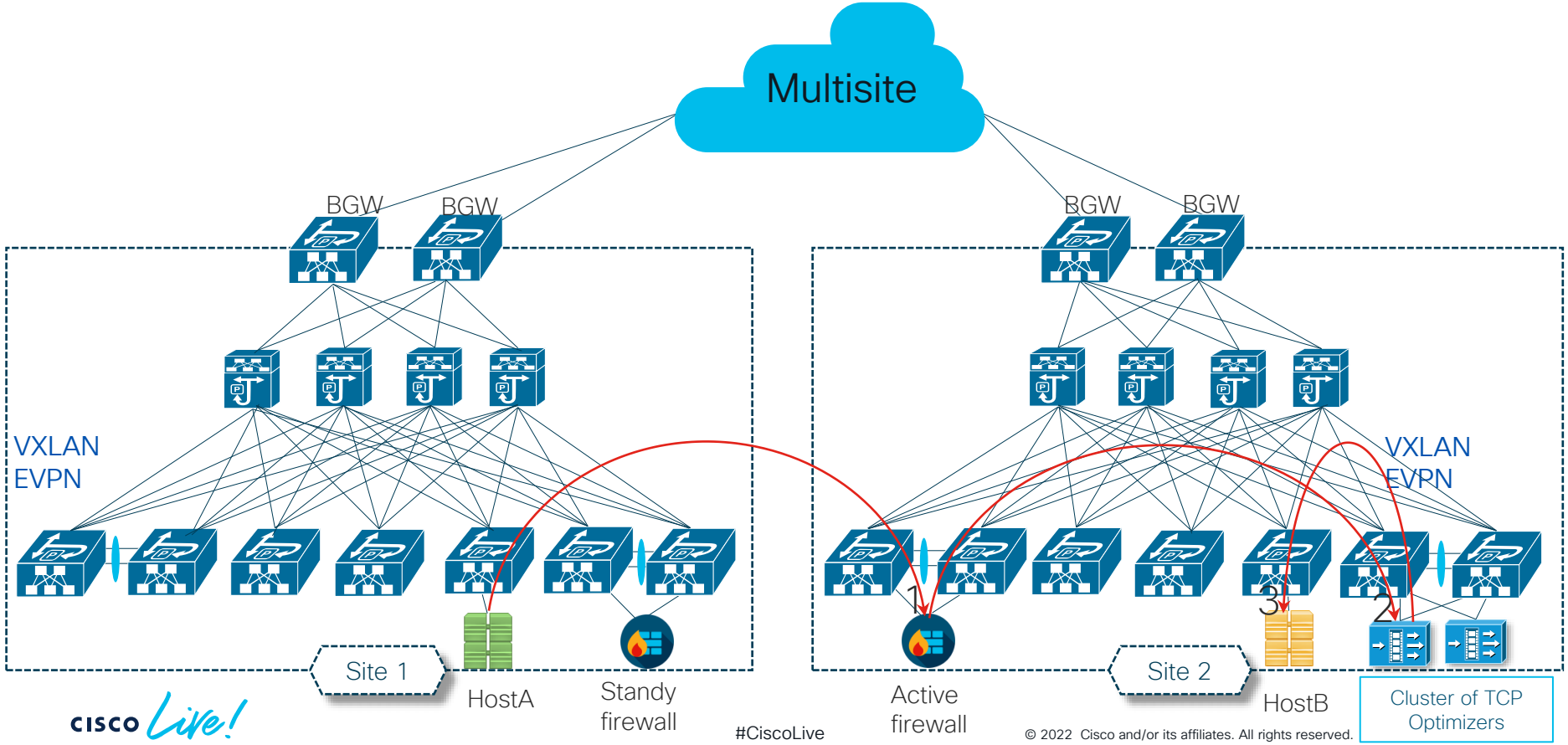
Selective traffic Load-balancing across cluster of firewalls



- Use case: Firewall as default gateway with certain flows excluded from redirection
- Load-balancing across the cluster of firewalls
- Fabric as a load-balancer
- Symmetric PBR

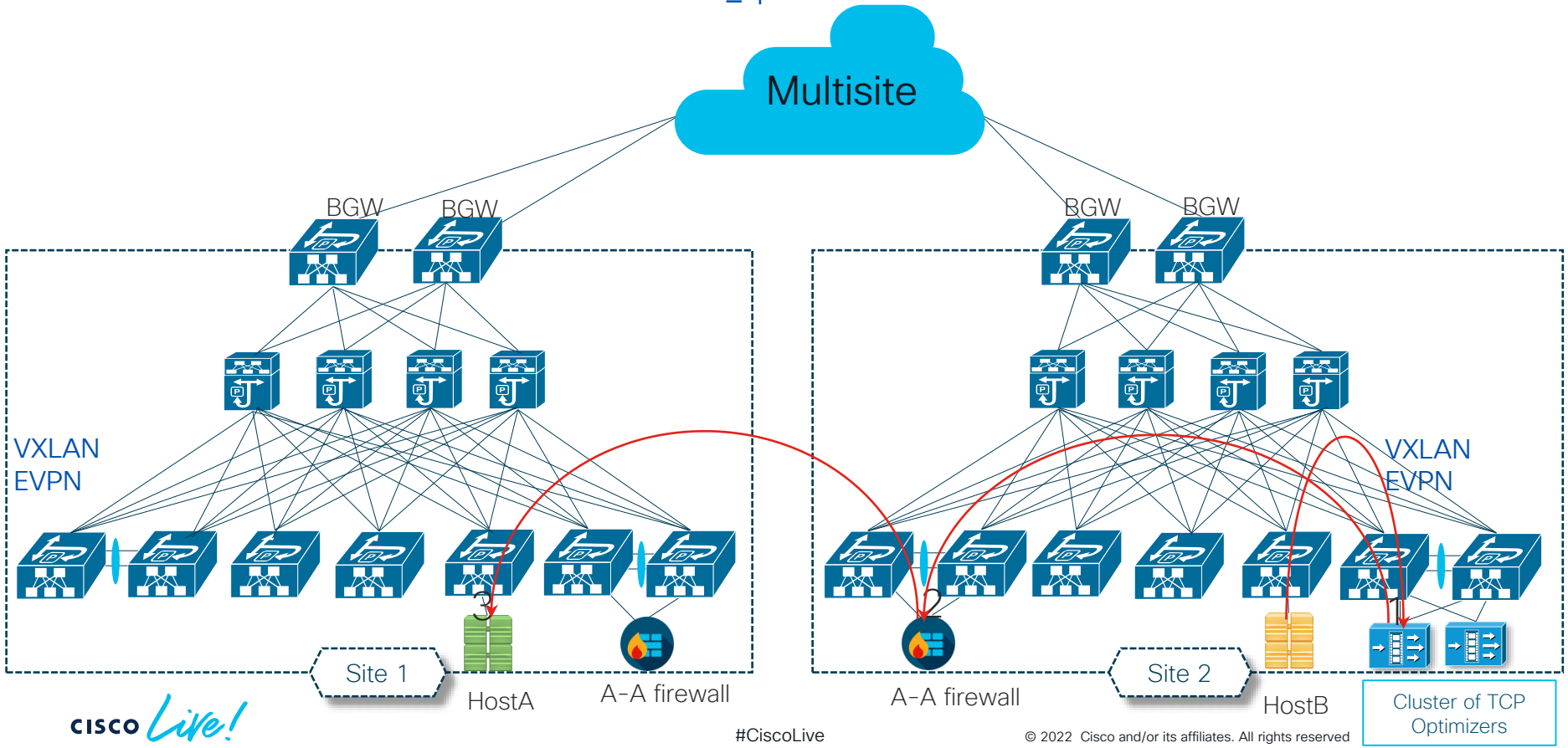
Service chaining across VXLAN Multi-site

Fwd flow : HostA -> Firewall -> TCP_optimizer cluster -> HostB



Symmetric PBR across Multisite

Rev flow : HostB -> TCP_optimizer cluster -> Firewall -> HostA



Configuration Example

Step 1: Onboard the appliances

```
epbr service firewall
  vrf firewall
  service-end-point ip 111.1.1.4 interface Vlan111
     probe icmp source-interface loopback0
    reverse ip 151.1.1.4 interface Vlan151
       probe icmp source-interface loopback1

epbr service tcp_optimizers
  vrf tcp_optimizer
!tcp_optimizer1
  service-end-point ip 110.1.1.2 interface Vlan110
     probe icmp source-interface loopback10
    reverse ip 150.1.1.2 interface Vlan150
       probe icmp source-interface loopback11
!tcp_optimizer2
  service-end-point ip 110.1.1.3 interface Vlan110
     probe icmp source-interface loopback20
    reverse ip 150.1.1.3 interface Vlan150
       probe icmp source-interface loopback21
```

Step 2: Create traffic selection rules

```
ip access-list hostA_hostB
        10 permit tcp 172.16.10.0/24 192.168.10.0 eq 7800
```

Step 3: Define ePBR traffic redirect policy

```
epbr policy service_chain
  statistics
  ! Firewall → tcp_optimizer
  match ip address hostA_hostB
    10 set service firewall fail-action drop
    20 set service tcp_optimizer fail-action forward
```

Step 4: Apply the ePBR Policy on relevant ingress interfaces

```
interface Vlan30
Vrf member tenant1
! Forward policy applied to ingress interface facing hostA
ip address 30.1.1.1/24
epbr ip policy service_chain

interface Vlan100
Vrf member firewall
! Forward policy applied to L3vni of firewall in service leaf
ip forward
no ip redirect
epbr ip policy service_chain
epbr ip policy service_chain reverse

interface Vlan101
Vrf member proxy
! Forward policy applied to L3vni of tcp_optimizer in service leaf
ip forward
no ip redirect
epbr ip policy service_chain
epbr ip policy service_chain reverse
```

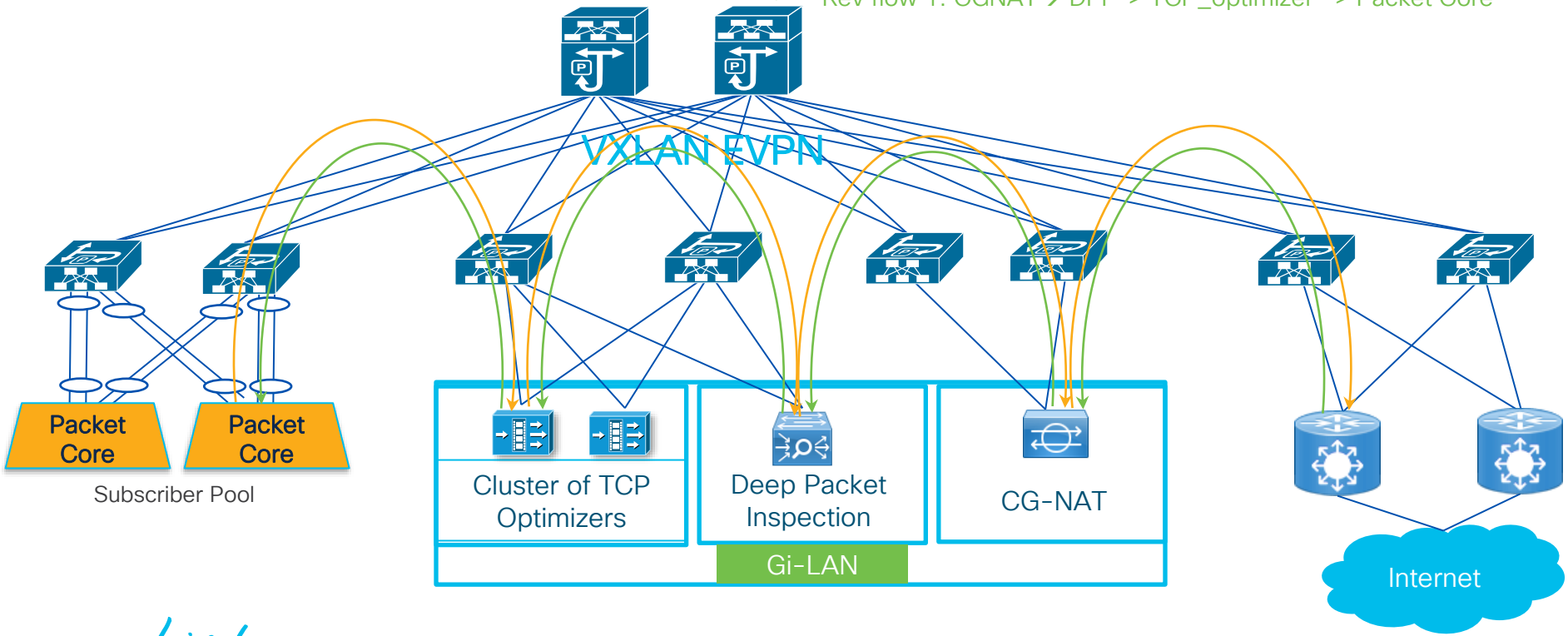
Note1: All the ePBR policy config should be enabled on service leaf hosting appliances, border leaf or border gateway acting as transit to multisite and on host leaf where traffic originates

Note2: Leak tenant routes onto all the service VRFs in the service leafs to route packet towards destination

ePBR for 5G deployments !!

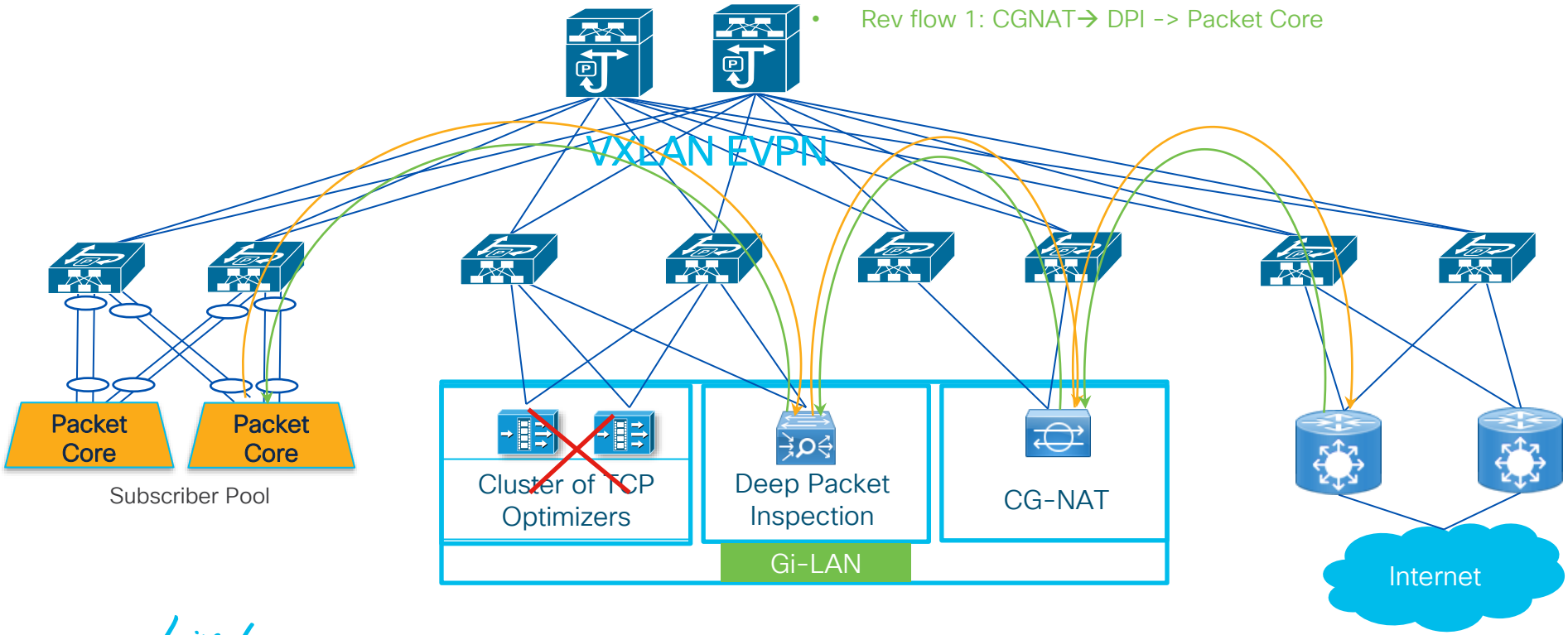
Service chaining & load-balancing across Telco DC

- Fwd flow1 : Packet Core-> TCP_optimizer -> DPI -> CG-NAT
- Rev flow 1: CGNAT→ DPI -> TCP_optimizer -> Packet Core



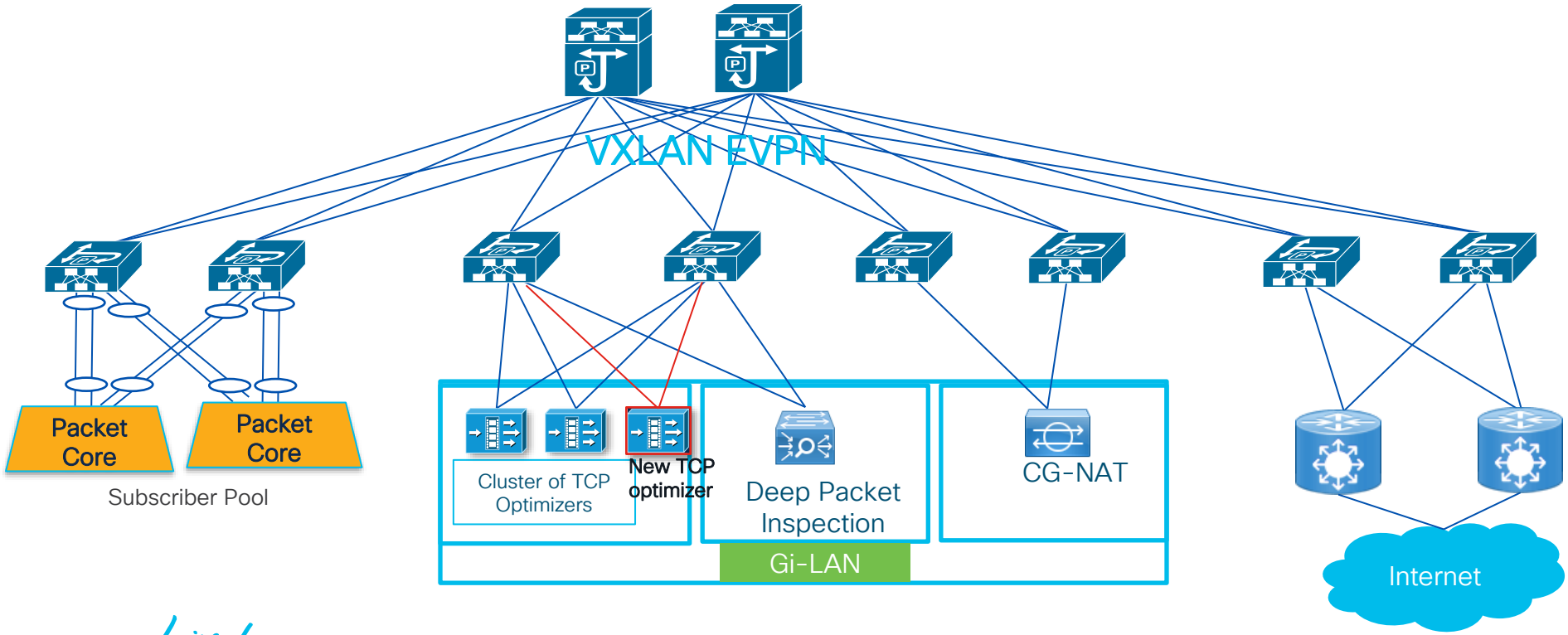
Bypass failed service node

- Fwd flow1 : Packet Core -> DPI -> CG-NAT
- Rev flow 1: CGNAT→ DPI -> Packet Core



Simplified expansion

✓ New Services and end-point can be added anywhere in fabric



ePBR for 5G deployments

Configuration Example

Step 1: Onboard the appliances

```
epbr service DPI
  service-end-point ip 111.1.1.4 interface Vlan111
     probe icmp source-interface loopback0
    reverse ip 151.1.1.4 interface Vlan151
       probe icmp source-interface loopback1

epbr service cg_nat
  service-interface Vlan20
   probe http get index.html
  service-end-point ip 20.1.1.2
    reverse ip 20.1.1.3
```

```
epbr service tcp_optimizers
! traffic will be load-balanced between the
optimizers
! optimizer1
  service-end-point ip 110.1.1.2 interface Vlan110
     probe icmp source-interface loopback0
    reverse ip 150.1.1.2 interface Vlan150
       probe icmp source-interface loopback1
! optimizer2
  service-end-point ip 110.1.1.3 interface Vlan110
     probe icmp source-interface loopback0
    reverse ip 150.1.1.3 interface Vlan150
       probe icmp source-interface loopback1
```

ePBR for 5G deployments

Configuration Example(cont.)

Step 2: Create traffic selection rules

```
ip access-list app1
        10 permit tcp 172.16.10.0/24 eq 7800 any
        20 permit tcp 192.168.20.0/24 eq 7800 any
```

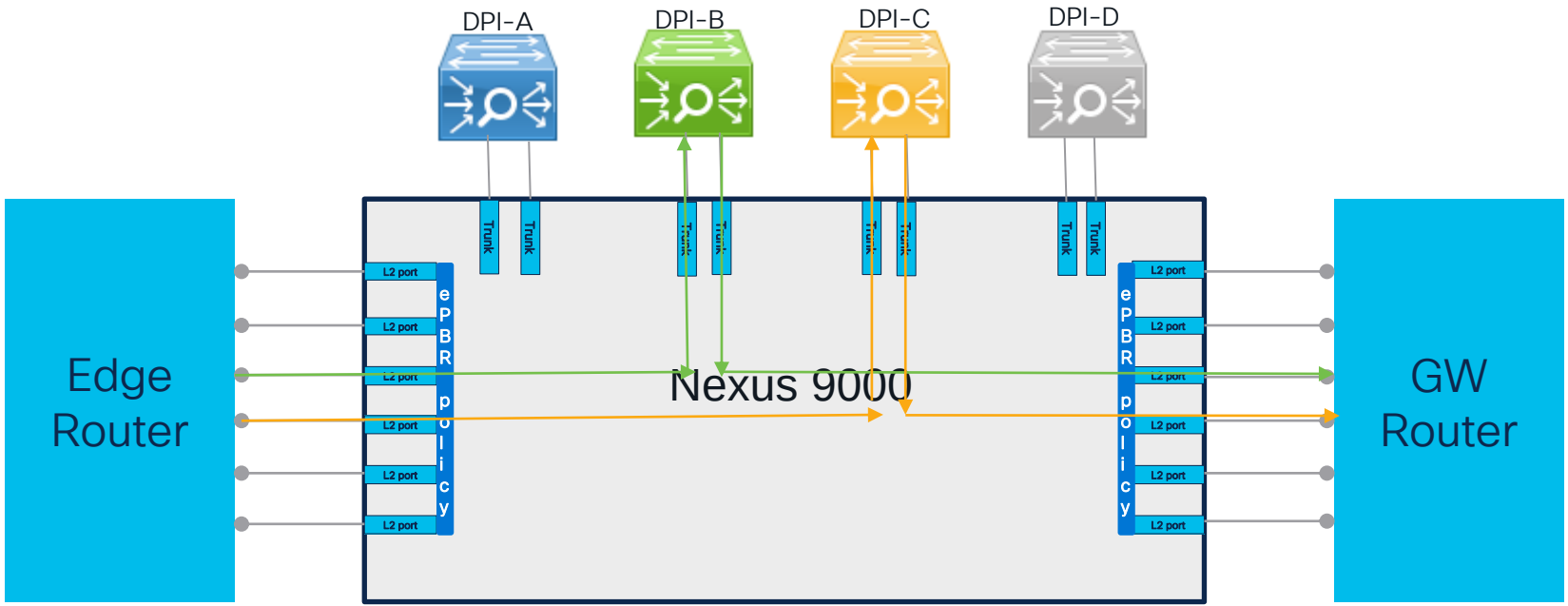
Step 3: Define ePBR traffic redirect policy

```
epbr policy servicechain_and_loadbalance
  statistics
  match ip address app1
    ! TCP optimizer→DPI→cg_nat chain
    10 set service tcp_optimizers fail-action bypass
    20 set service DPI fail-action drop
    30 set service cg_nat fail-action drop
```

Step 4: Apply the ePBR Policy on relevant interfaces

```
interface Vlan30
  !forward policy applied to ingress interface facing
classifier
  no shutdown
  ip address 30.1.1.1/24
  ipv6 address 2030::1/24
  epbr ip policy servicechain_and_loadbalance

interface Vlan40
! Reverse policy applied to egress interface facing WAN
for reverse flow
  no shutdown
  ip address 40.1.1.1/24
  ipv6 address 2040::1/24
   epbr ip policy servicechain_and_loadbalance reverse

interface vlan100
! L3vni interface on service leafs
ip forward
no ip redirect
epbr ip policy servicechain_and_loadbalance
epbr ip policy servicechain_and_loadbalance reverse
```

ePBR L2 for Inline redirection



- Transparently insert Nexus 9k on path of traffic and selectively load-balance flows towards different L1/L2 DPI devices.
- Enables Inline / Bump in the wire deployments

Conclusion

ESR Hardware Support

Nexus 9500 Series with EX, FX and GX line cards**

Nexus 9300 EX/FX/FX2/FX3/GX/GX2 Series

Nexus 3600 & 9500 R Series*

From Cisco's Data Center Portfolio

**ePBR L2 not supported, *ePBR not supported

ESR Software and Licensing requirements

ITD	NX-OS 7.0(3)I1(2)
	Essentials Package
ePBR	L3 - NX-OS 9.3(5)
	L2 - NXOS 10.2(1)
	Advantage Package

ESR Benefits

Scalability

Multi-Terabits Line Rate solutions

No CPU overhead

Scales to large number of Service Nodes

High Availability

Health Monitoring of servers/appliances

Automatic Failure Handling

N + M redundancy

OPEX Savings

Simplified provisioning & Ease of deployment

Significant reduction of Configuration Complexity

Programmable (REST, Netconf)

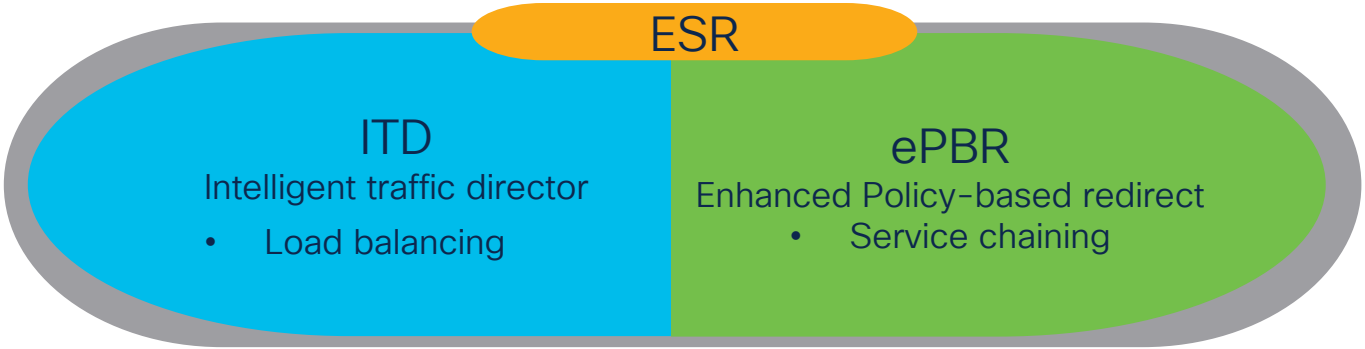
CAPEX Savings

Moving away from specialized, dedicated, expensive HW

Additional Cost savings from Wiring, Power, Rackspace

Key takeaways

- Innovative Multi-terabit line rate solutions from Nexus
- Enables high-capacity traffic distribution and selective redirection of traffic



Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

References

- ePBR config guide – https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/epbr/cisco-nexus-9000-series-nx-os-epbr-configuration-guide-102x/m-configuring-epbr.html
- ITD config guide – https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/itd/b_cisco_nexus_9000_series_nx-os_intelligent_traffic_director_configuration_guide_102_x/m-configuring-itd.html
- Verified scalability Guide – https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/scalability/cisco-nexus-9000-series-nx-os-verified-scalability-guide-1022.html
- ePBR White Paper – https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/layer4-layer7-service-redir-ply-based-redir-wp.html
- Blogs – https://blogs.cisco.com/datacenter/dynamic-service-chaining-in-a-data-center-with-nexus-infrastructure
- https://blogs.cisco.com/datacenter/continuing-our-innovations-in-service-chaining-with-nexus-enhanced-policy-based-redirect?pstdnc027110

Thank you


cisco Live!
ALL IN