cisco Live!

Let's go

The bridge to possible

Implement Direct Internet Access with Secure Firewall Threat Defense

Alejandra Páez Castro
Security Technical Leader, CX Americas
BRKSEC-2086

With Secure Firewall, Traffic can be steered through multiple active WAN links based on applications ensuring a better user application experience while keeping the network secure

Agenda

- Direct Internet Access (DIA)
  - Components
  - Configuration Walkthrough
- PBR with Path Monitoring
  - Configuration Walkthrough
- Demo
- Conclusion

Cisco Webex App

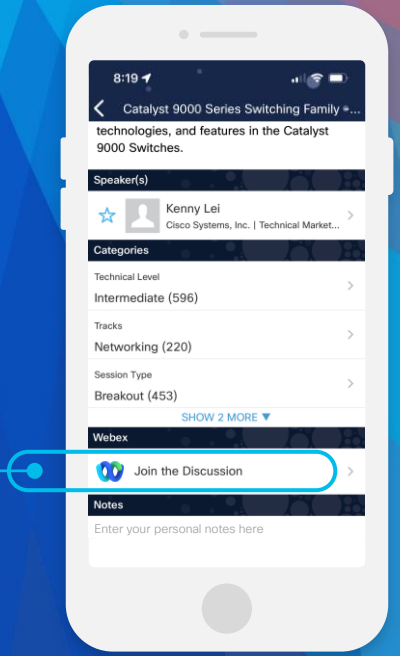
Questions?

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 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2086

Know your Presenter

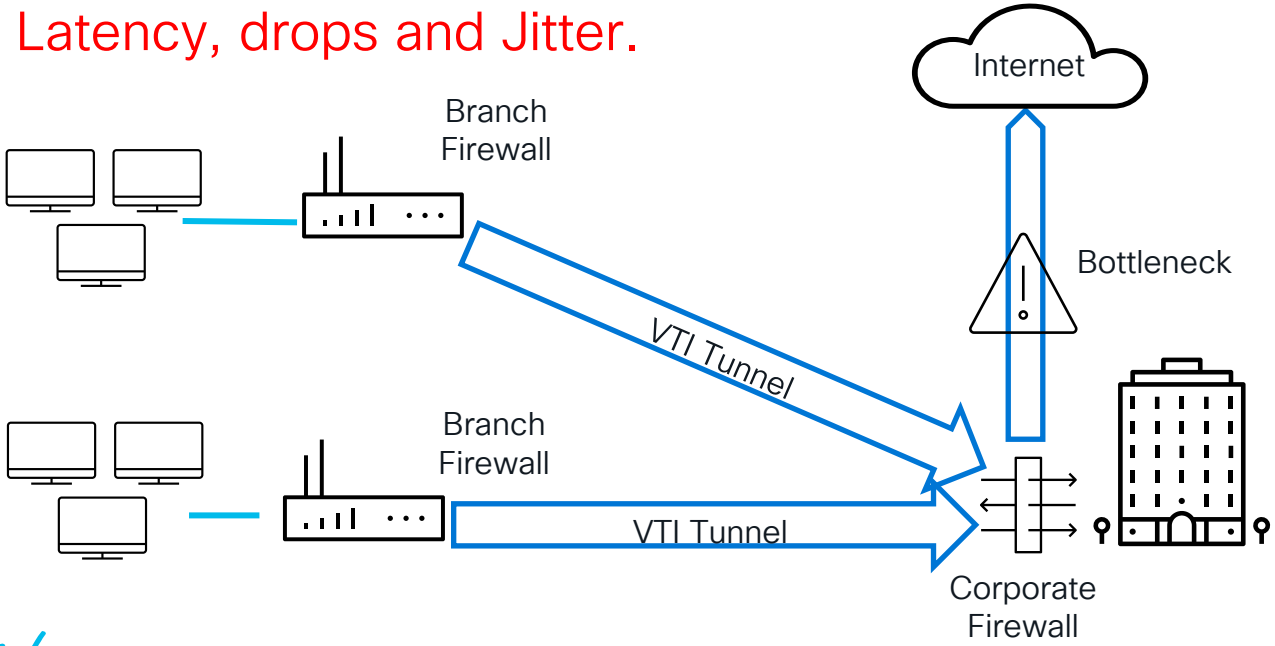
Alejandra Páez Castro

- Venezuela / Mexico
- Telecommunications Engineer
- 6 years as Technical Consulting Engineer in Firewall TAC
- 2 years+ as Security Technical Leader in CX
- Passionate about NGFW Security appliances

Direct Internet Access Introduction

Traditional WAN Architecture

Traditional WAN topology backhauls all internet traffic to the enterprise Data center, resulting in poor application experience, Packet Latency, drops and Jitter.

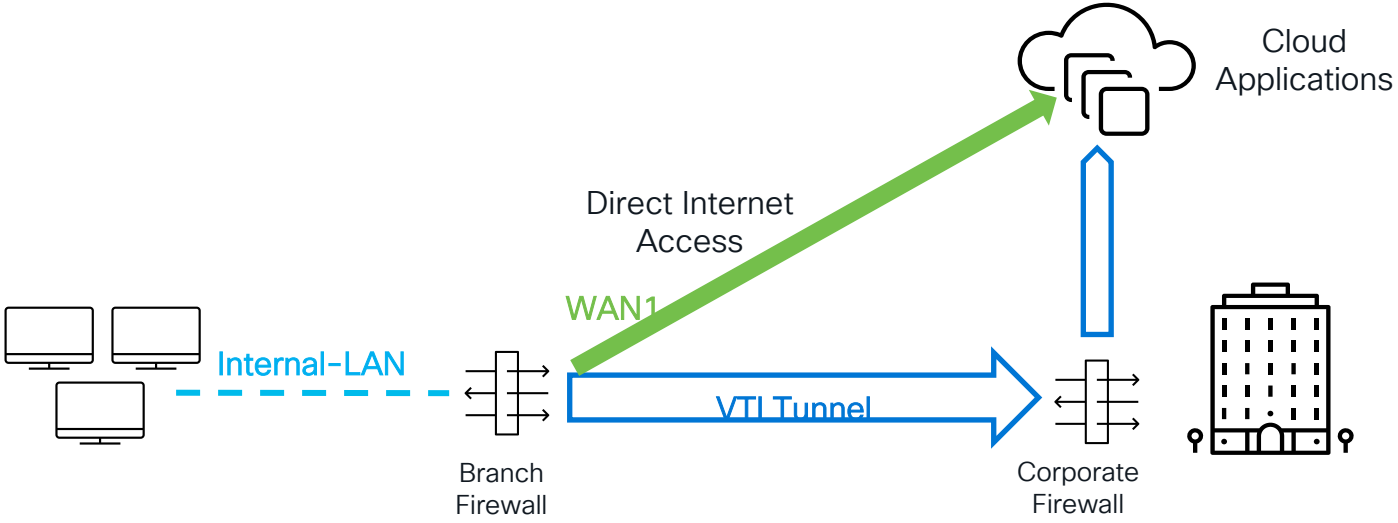


Simplified Branch Requirements

7.0	7.1	7.2
• VTI Enhancement: Active –Standby Backup VTI Tunnel configuration with SLA Monitoring	• ECMP Support from FMC UI • ECMP Support for VTI • PBR using Application as Matching Criteria (DIA)	• Adaptive traffic steering based on Path Monitoring

Direct Internet Access (DIA)

DIA gives branches the capability to send traffic directly to the internet link instead of carrying it all the way back to the centralized data center for internet access



DIA Components

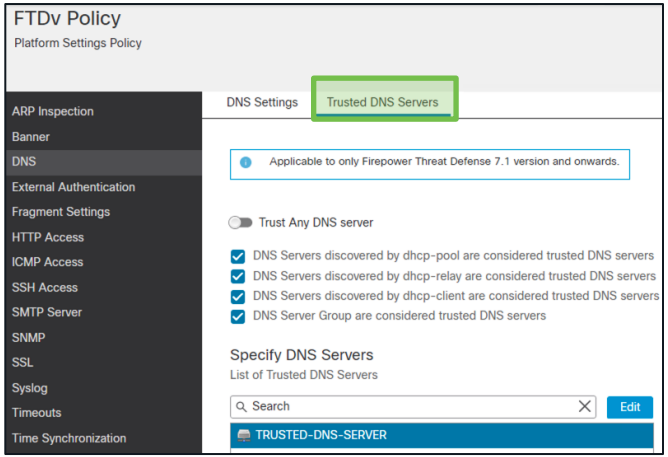
Vulnerability Database (VDB)

- VDB supplies the list of domains for application detection used by applications for DIA
  - Keep the VDB version updated

```
firepower# show object network-service
[…]
object network-service "Cisco" dynamic
 description Official website for Cisco.
 app-id 2655
 domain cisco.com (bid=1851027941) ip (hitcnt=0)
object network-service "Duo Security" dynamic
 description A user-centric access security platform that provides two-factor
 authentication, endpoint security, remote access solutions and a
 subsidiary of Cisco.
 app-id 4648
 domain duosecurity.com (bid=-2050678515) ip (hitcnt=0)
 domain duo.com (bid=-2050510683) ip (hitcnt=0)
[…]
```

Trusted DNS Server

- Application-based Policy Based Routing (PBR) uses DNS Snooping to map the application domains to IP addresses
  - Ensure DNS traffic passes through Firewall in clear text format




```
firepower# show runn dns
dns domain-lookup any
DNS server-group DNS-Group
    name-server 10.10.10.10
    domain-name cisco.com
DNS server-group DefaultDNS
dns-group DNS-Group
dns trusted-source 10.10.10.10
```

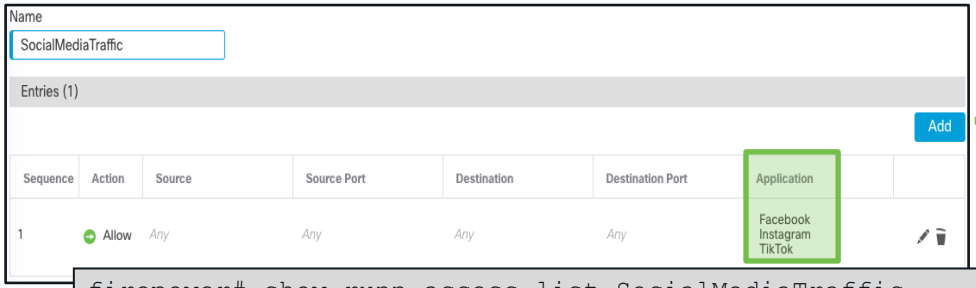
Network Service Object (NSO)

- Object associated with a particular application
  - NSOs are predefined and deployed to FTD from the FMC

```
firepower# show object id "Webex Teams"
object network-service "Webex Teams" dynamic
app-id 4080
 domain code.s4d.io (bid=839581615) ip (hitcnt=0)
 domain huron-dev.com (bid=839671741) ip (hitcnt=0)
 domain worklife.com (bid=839793477) ip (hitcnt=0)
 domain ciscospark.com (bid=839938715) ip (hitcnt=0)
 domain wbx2.com (bid=840165323) ip (hitcnt=0)
 domain idbroker.webex.com (bid=840285097) ip (hitcnt=0)
 domain teams.webex.com (bid=840320705) ip (hitcnt=0)
```

Network Service Group (NSG)

- FMC auto-generates NSG based on the Extended Access Lists configured for PBR
  - Multiple NSOs can be part of a single NSG

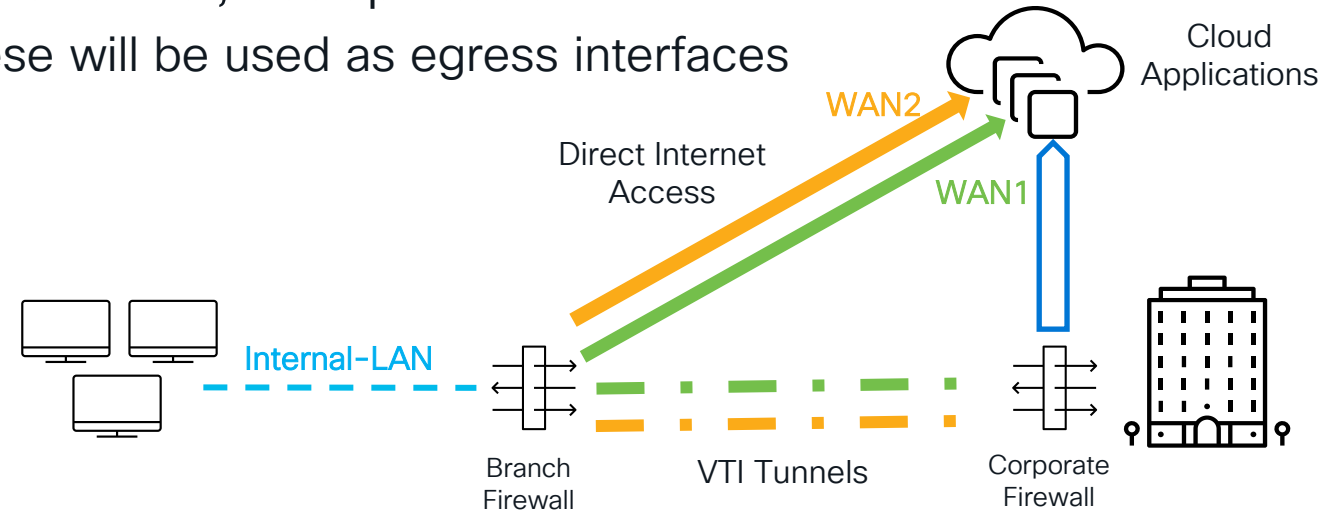



```
firepower# show runn access-list SocialMediaTraffic
access-list SocialMediaTraffic extended permit ip any object-group-network-service FMC_NSG_30064774581
firepower# show runn object-group network-service
object-group network-service FMC_NSG_30064774581
 network-service-member "Facebook"
 network-service-member "Instagram"
 network-service-member "TikTok"
```

DIA Configuration Walkthrough

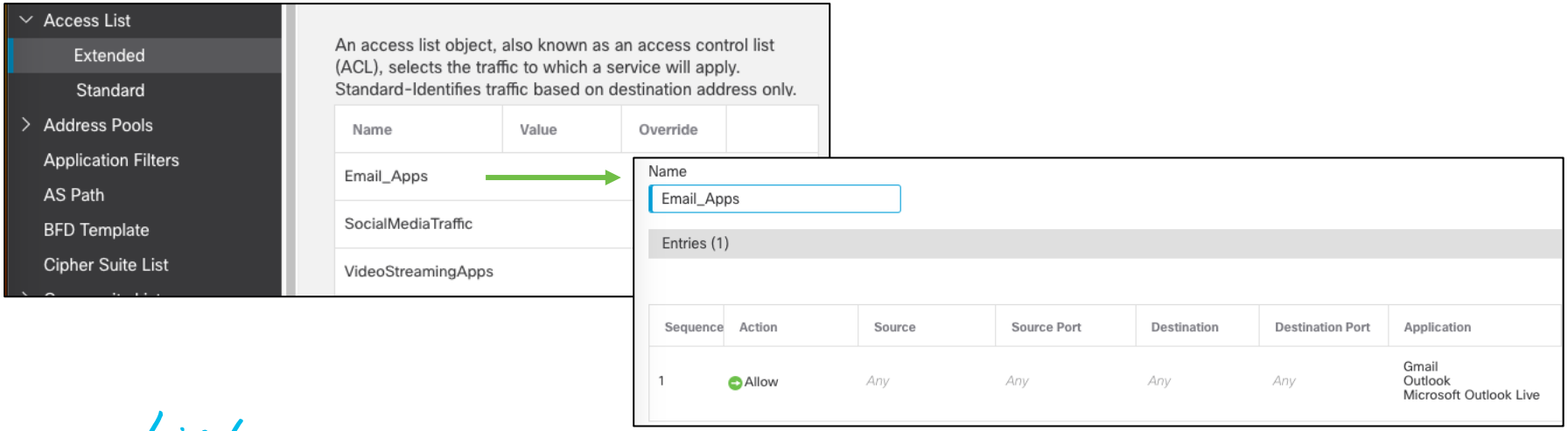
Configure interfaces

- Define and configure interfaces to be used as ingress and egress
- Assuming the PBR is going to allow access to resources behind a secure tunnel, set up Static VTIs
  - These will be used as egress interfaces



Configure the Extended Access-list

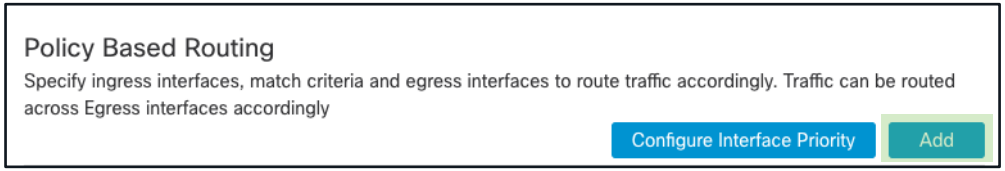
- Configure Extended Access List with Applications
  - The selected applications (NSOs) in each of the Access Control entries form an NSG
  - This NSG is used in DIA to classify traffic based on the match criteria

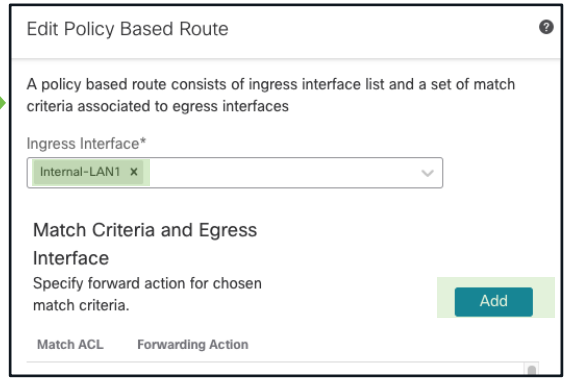


Configure Policy-Based Routing

Define Ingress interface

- PBR can be used to classify the network traffic based on applications
  - PBR policy enables you to securely breakout traffic for specific applications

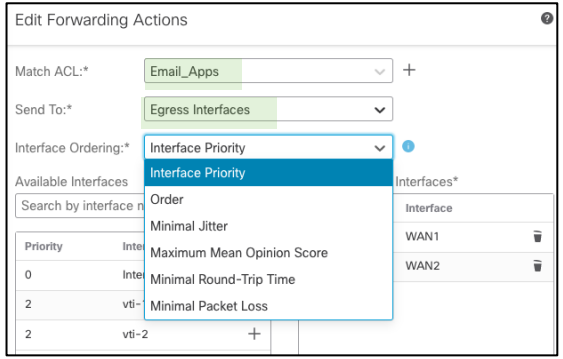


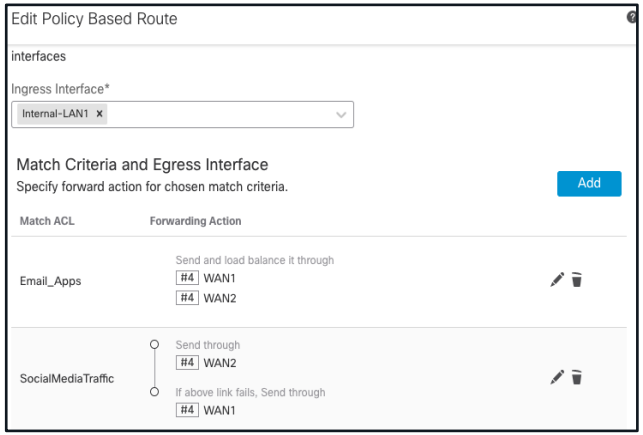


Configure Policy-Based Routing

Match Traffic Criteria and Egress Interface

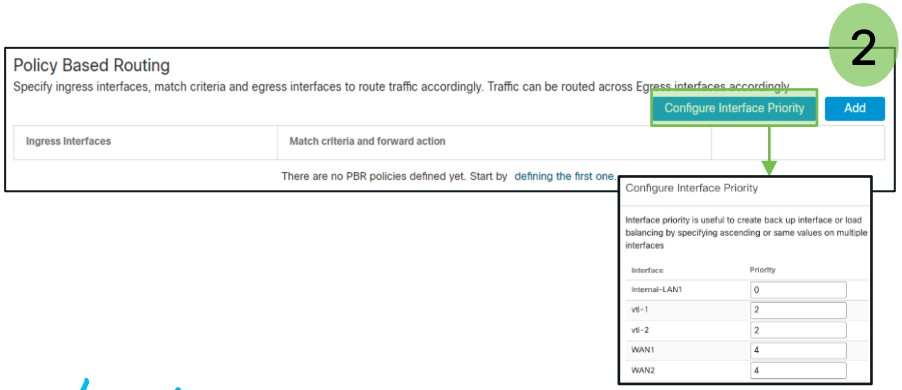
- Traffic will be forwarded through the Egress interface based on the Interface Ordering attributes:
  - Static attributes: Order, Interface Priority
  - Dynamic attributes: Round Trip Time(RTT), Jitter, Mean Opinion Score (MOS) or Packet Loss

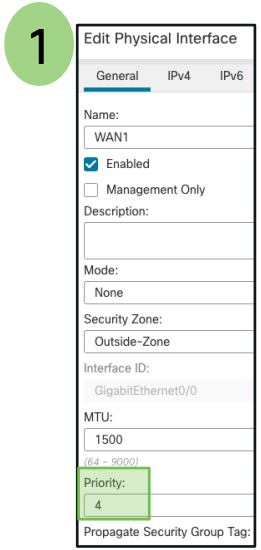




Interface Priority

- Traffic is routed to the interface with the least priority first
  - If the priority value is the same for a group of interfaces, then traffic is load balanced among them
- There are 2 ways to configure interface priority:

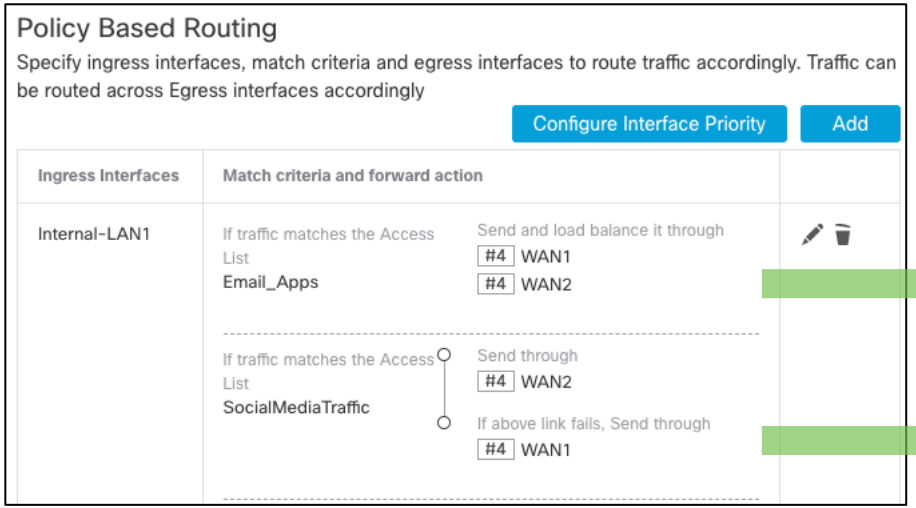




Configure Policy-Based Routing

Match Traffic Criteria and Egress Interface

- Multiple PBR Rules configured on different set of ingress interfaces



Interface Ordering
By Priority

Interface Ordering
By Order

DIA Configuration Flow

- Define egress interfaces priorities

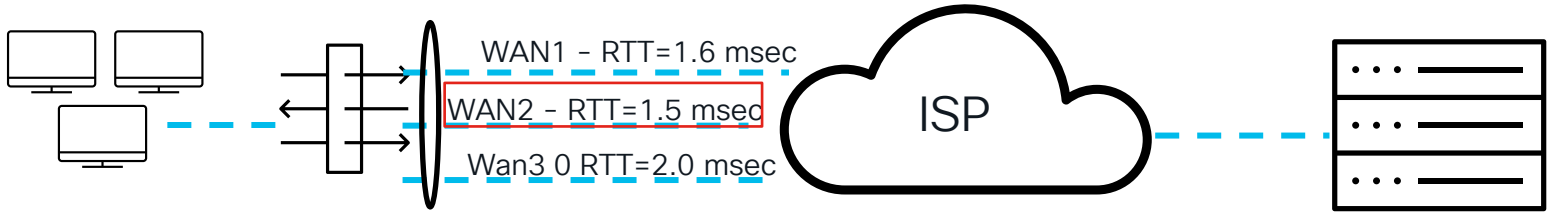
- VDB updated
- Trusted DNS
- Extended ACLs with Applications definition

- Egress Interface Selection by:
  - Static attributes
  - Dynamic attributes

PBR with Path Monitoring

PBR with Path Monitoring

- PBR with Path Monitoring steers traffic based on dynamically monitored interface statistics such as RTT, Jitter, MOS, and packet loss
  - These metrics are collected dynamically using ICMP Probe Messages



PBR with Path Monitoring

Components

Path Monitoring Module (PMM)

Responsible to collect the Link metric statistics using ICMP probes

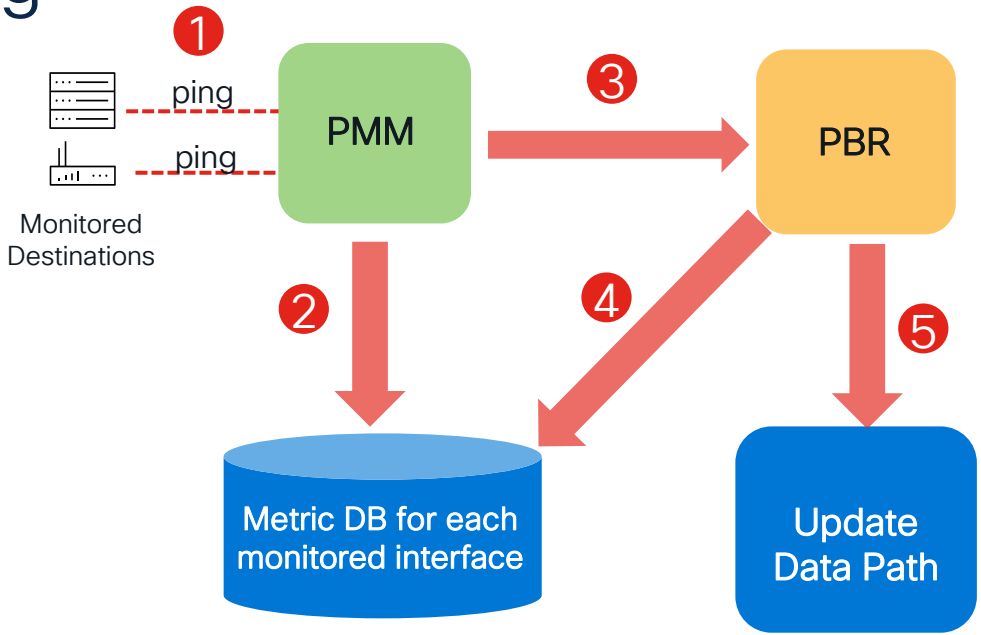
Policy-Based Routing (PBR)

Responsible to route the traffic using the egress interface as per the best metric reported by the PMM

PBR Path Monitoring

Data Flow

1. PMM sends ICMP probes to Monitored destinations
2. PMM computes and stores interface metrics
3. PMM pushes a list of interfaces that have updates to PBR
4. PBR fetches the latest available metrics from PMM internal DB
5. PBR pushes the routing updates



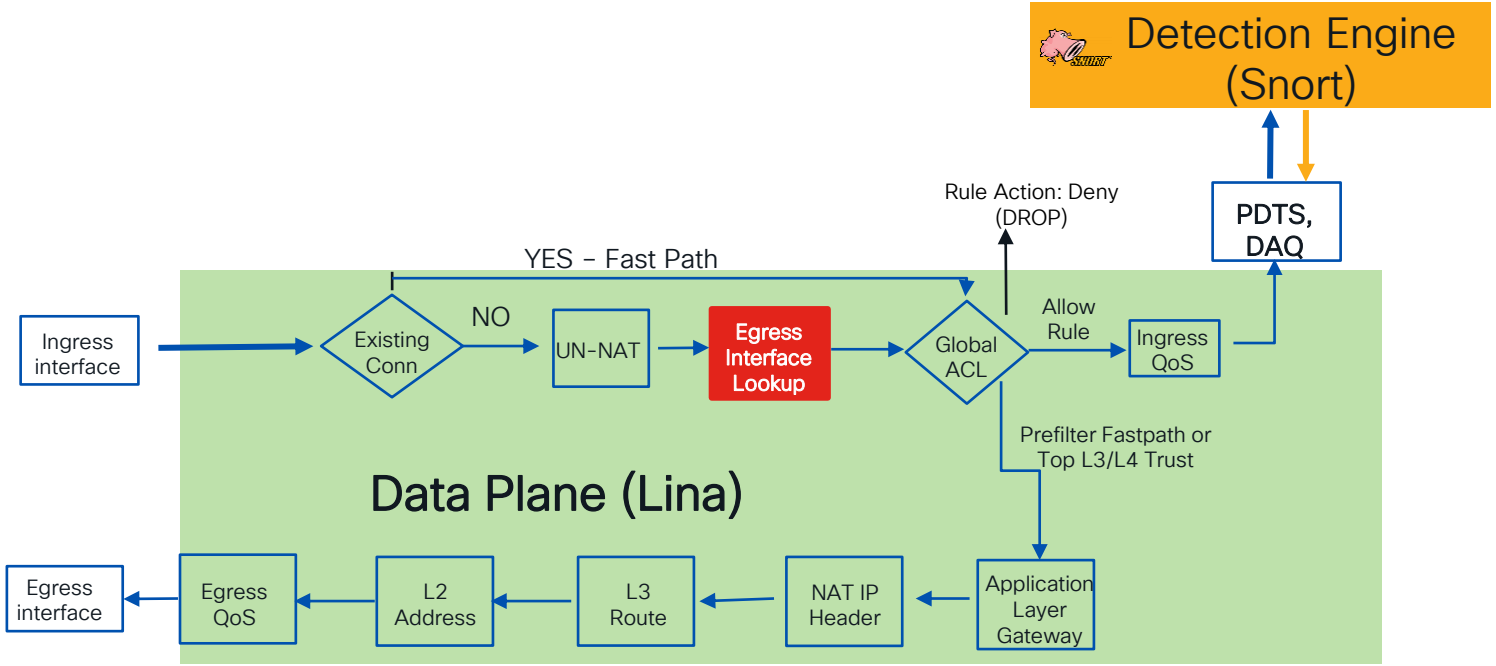
Interface: WAN1
RTT average: 1474 microsecond(s)
Jitter: 261 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 10 second(s) ago

Interface: WAN2
RTT average: 883 microsecond(s)
Jitter: 158 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 10 second(s) ago

PBR Path Monitoring

Packet flow

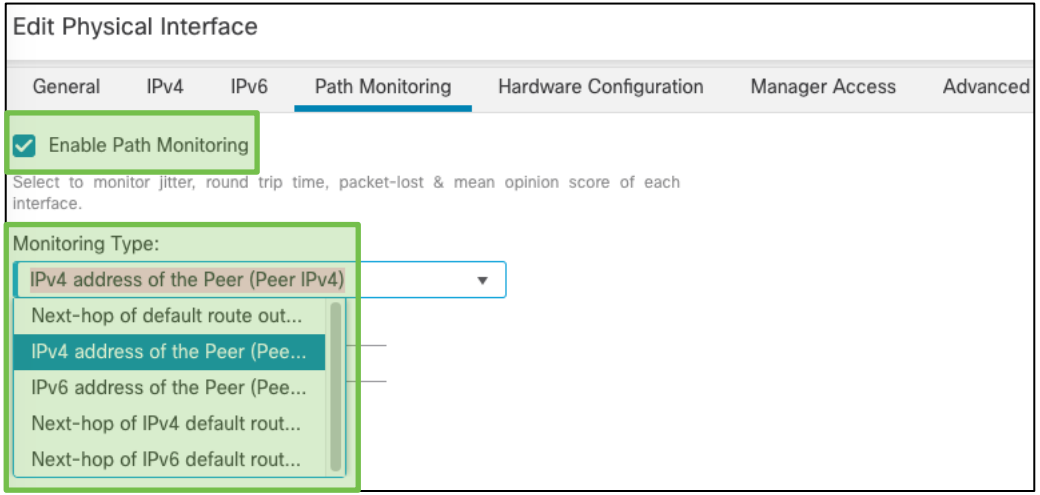
PBR is part of L3 Routing, it takes precedence over route lookup



PBR with Path Monitoring Configuration Walkthrough

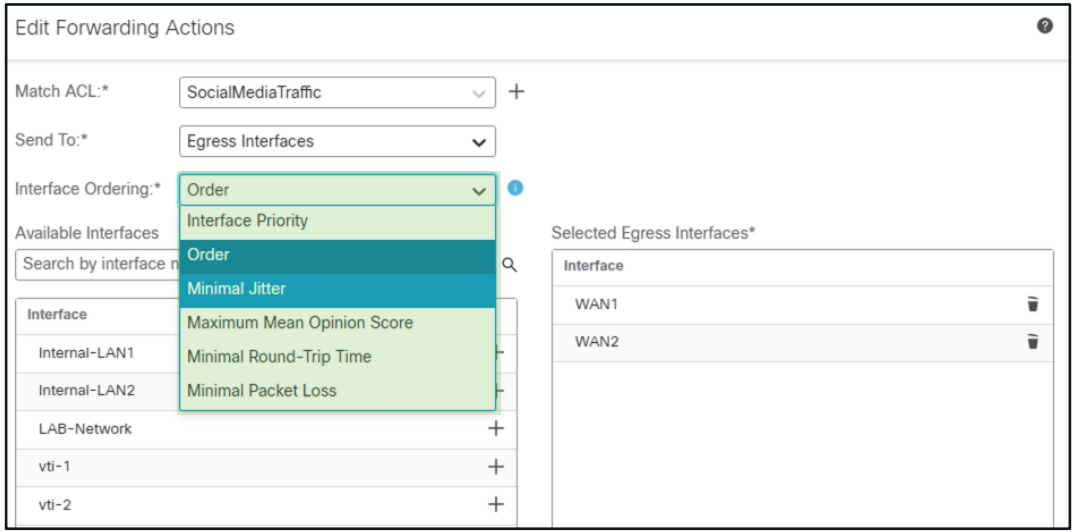
Interface Path Monitoring Configuration

- Enable Path Monitoring at the interface level
  - Link metrics determined using ICMP to either Next Hop (auto, auto4, auto6) or to the explicit IP



PBR Policy Configuration

- PBR Interface Ordering enhanced to adaptively steer traffic based on the dynamically monitored metrics of the interfaces



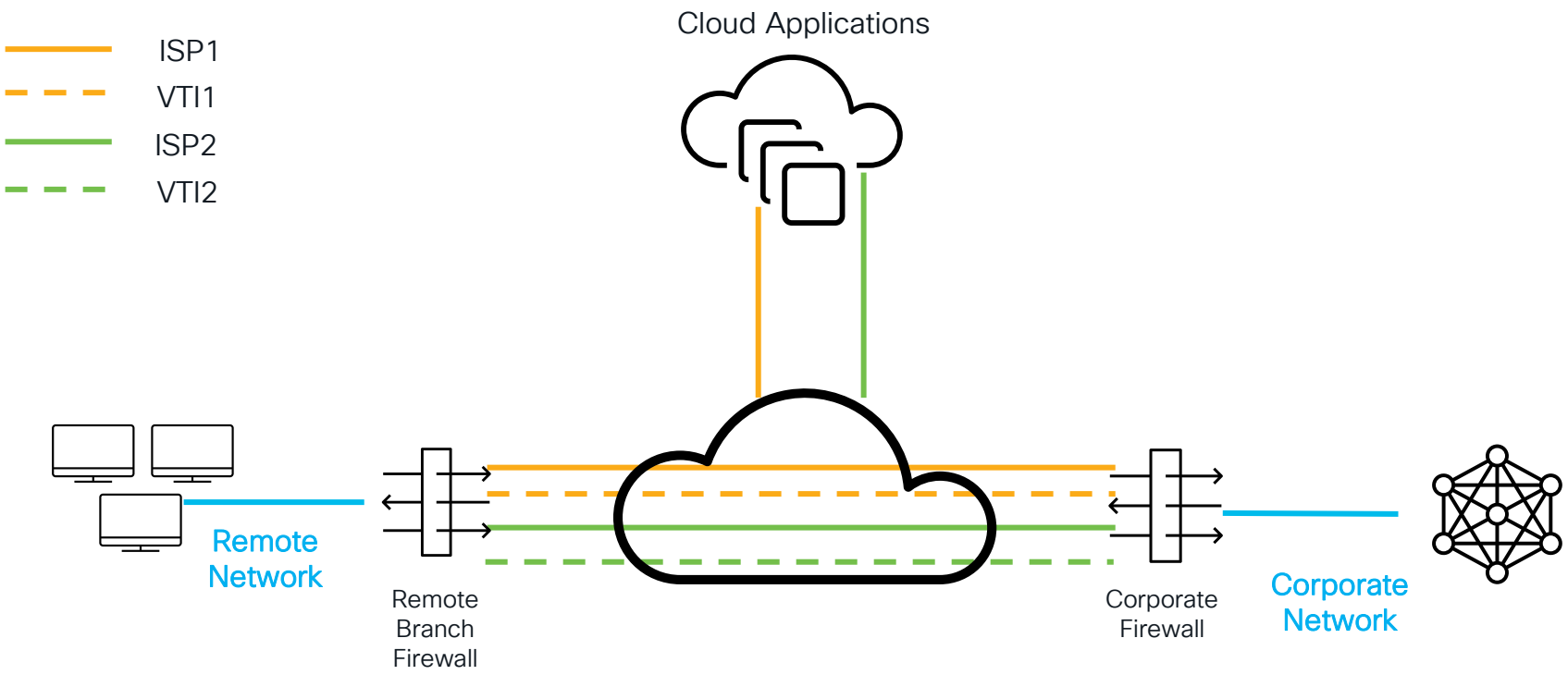
Demo

Demo 1:
DIA configuration

In this Demo we will…

- Configure Trusted DNS server
- Configure ECMP for both VTI and WAN interfaces
- Configure Extended Access List with Applications
- Configure PBR with Applications
- Initiate traffic from end-user machine to both WAN links and VTI tunnels based on applications

DIA Demo Topology

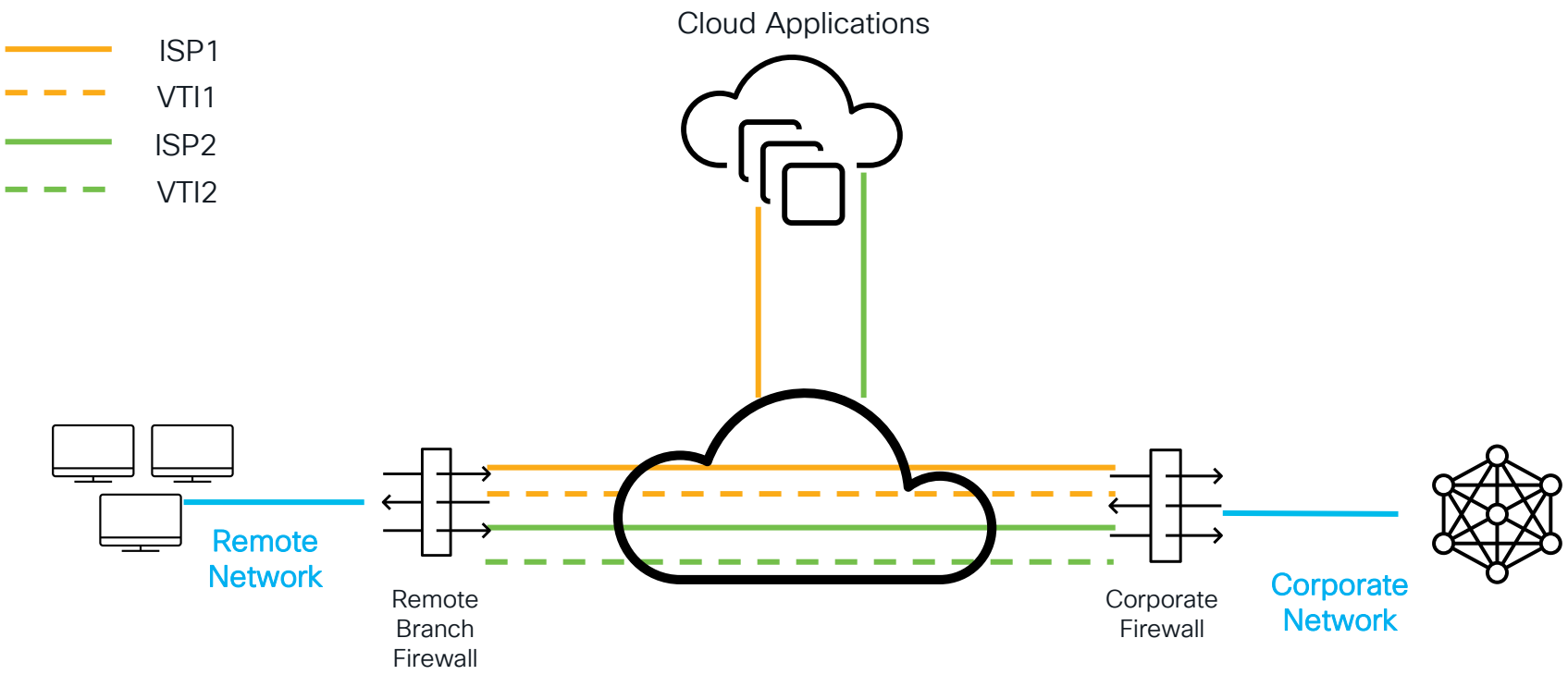


Demo 2:
PBR with Path Monitoring

In this Demo we will…

- Configure Interface Path Monitoring
- Configure PBR with flexible metric ‘Jitter’ to steer Video Streaming traffic based on the link with Minimum Jitter

DIA Demo Topology



Conclusion

With Secure Firewall, Traffic can be steered through multiple active WAN links based on applications ensuring a better user application experience, while keeping the network secure

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

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

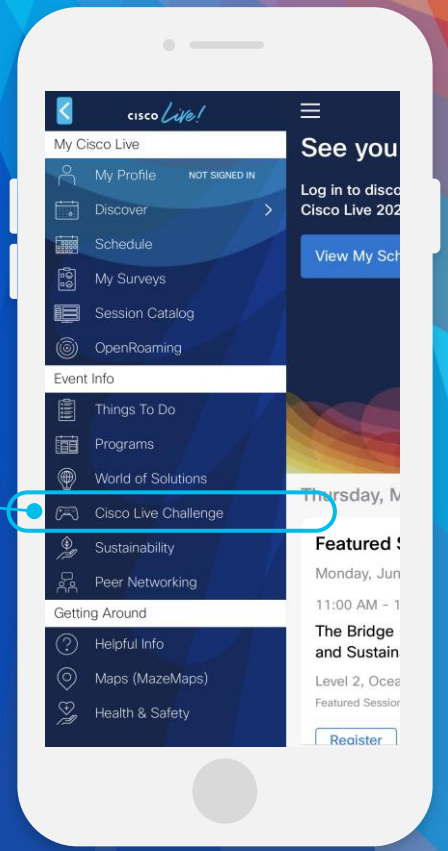
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



Thank you

cisco Live!

Let's go