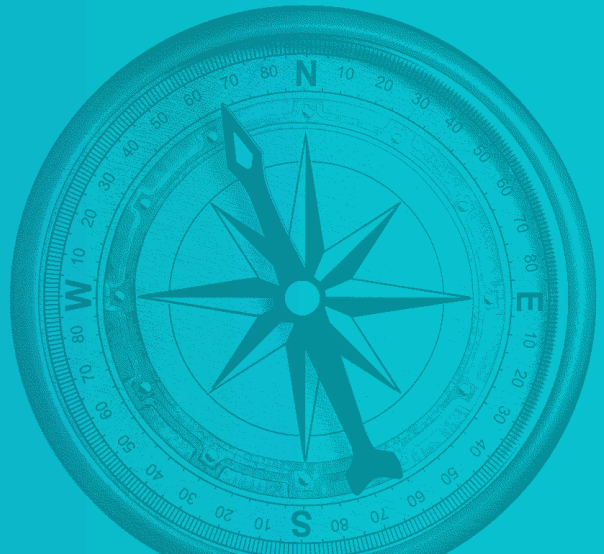
Cisco Intelligent WAN

Ľuboš Lontoš
Systems Engineer SP/R&S
ALEF NULA a.s.



ALEF

Agenda

- Cisco iWAN Architecture Overview
- Tranport Independent Design
- Intelligent Path Control- PfRv3
- Product Portfolio

ALEF

Traditional WAN vs. Hybrid iWAN design

Active/Standby WAN Paths

Primary With Backup

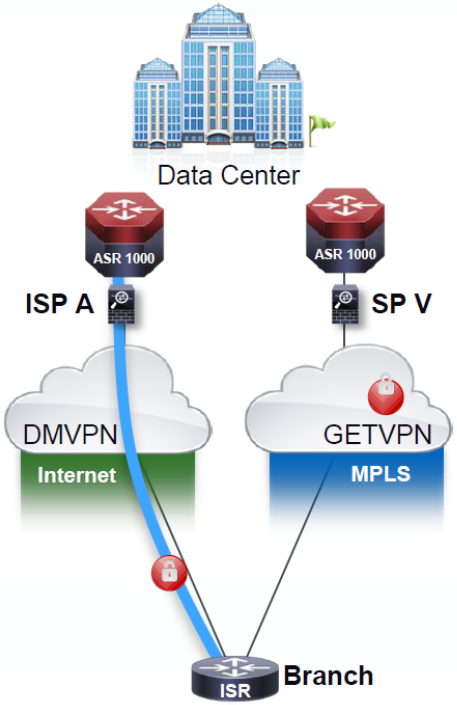
Two IPsec Technologies

GETVPN/MPLS
DMVPN/Internet

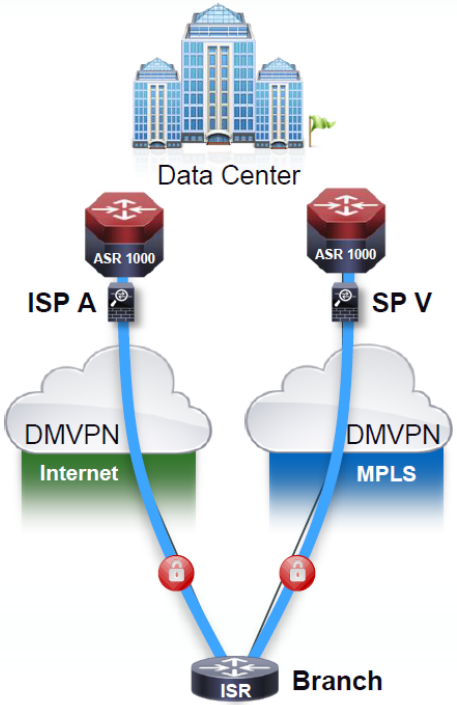
Two WAN Routing Domains

MPLS: eBGP or Static
Internet: iBGP, EIGRP or OSPF
Route Redistribution
Route Filtering Loop Prevention

TRADITIONAL HYBRID



Intelligent WAN HYBRID



Active/Active WAN Paths

One IPsec Overlay

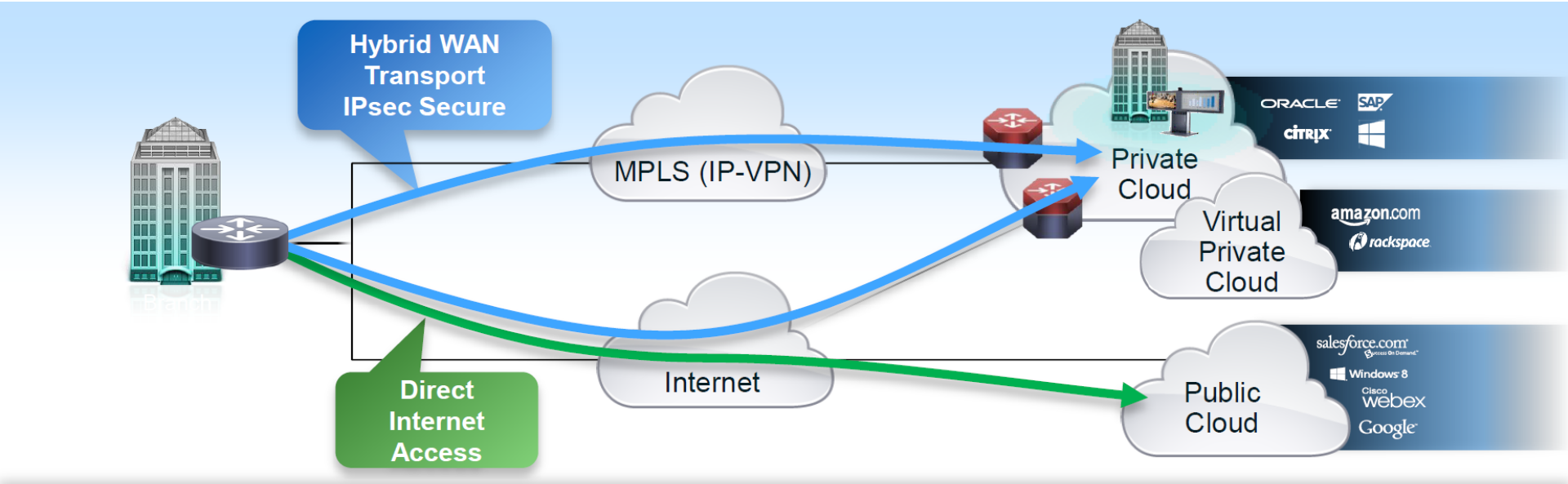
DMVPN

One WAN Routing Domain

EIGRP or iBGP

ALEF

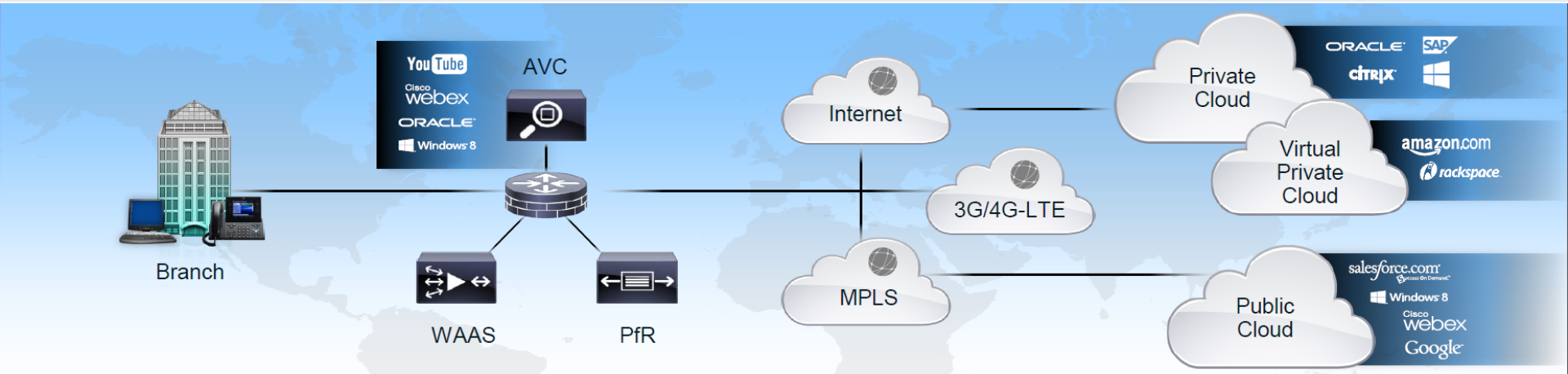
iWAN - Secure WAN Transport and Internet Access



- Secure **WAN transport** for private and virtual private cloud access
- Leverage **local Internet** path for public cloud and Internet access
- Increased WAN transport capacity and cost effectively
- Improve application performance

ALEF

Intelligent WAN Solution Components



Transport Independent

- Consistent operational model
- Simple provider migrations
- Scalable and modular design
- DMVPN IPsec overlay design

Intelligent Path Control

- Application best path based on delay, loss, jitter, path preference
- Load balancing for full utilization of all bandwidth
- Improved network availability
- Performance Routing (PfR)

Application Optimization

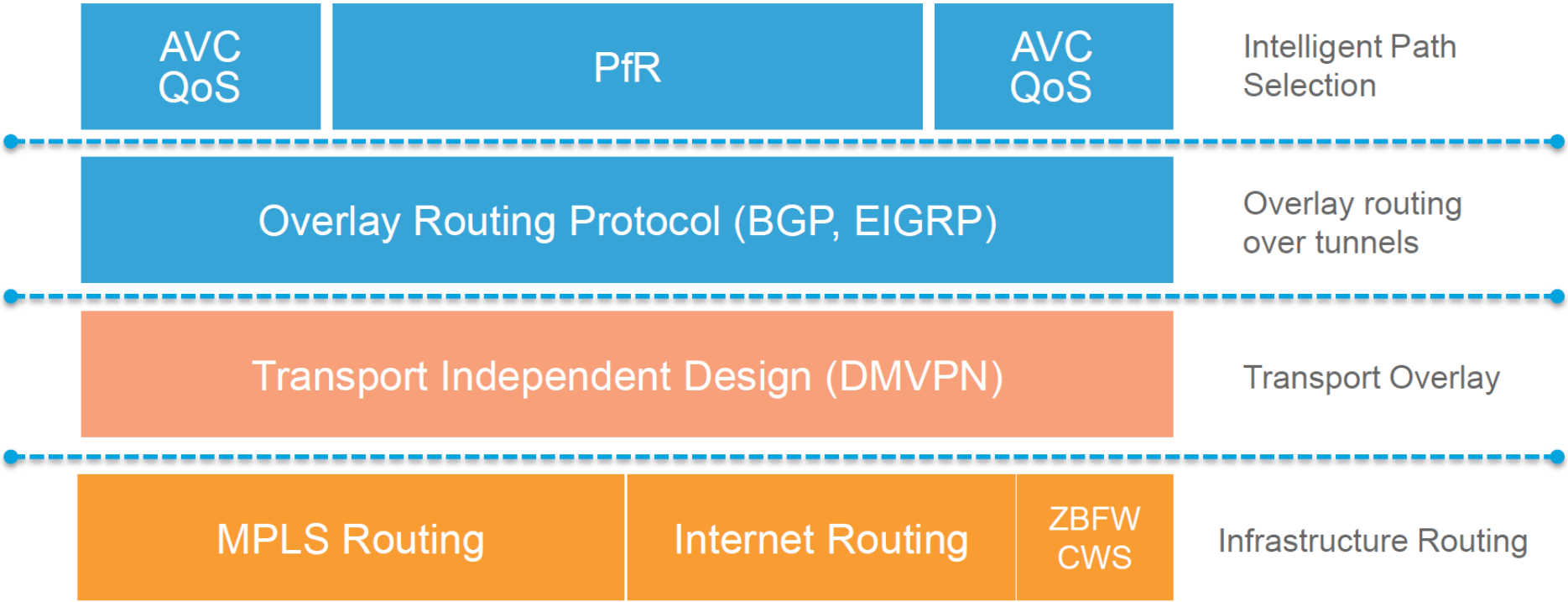
- AVC: Application monitoring with Application Visibility and Control
- Per-tunnel Hierarchical QoS
- WAAS: Application Acceleration and bandwidth savings
- WAAS: Intelligent Edge Caching with Akamai Connect

Secure Connectivity

- Certified strong encryption
- Comprehensive threat defense with ASA and IOS firewall/IPS
- Cloud Web Security (CWS) for scalable secure direct Internet access

ALEF

iWAN Layers



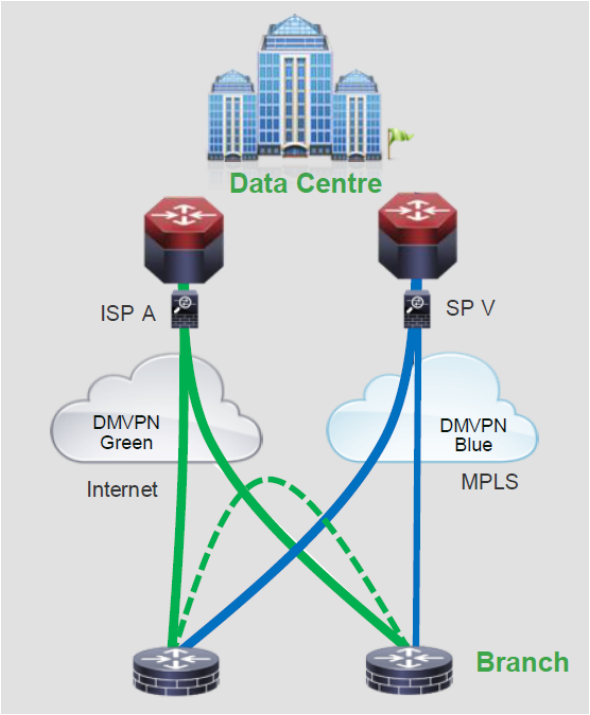
ALEF

Tranport Independent Design

ALEF

Dynamic Multipoint VPN (DMVPN)

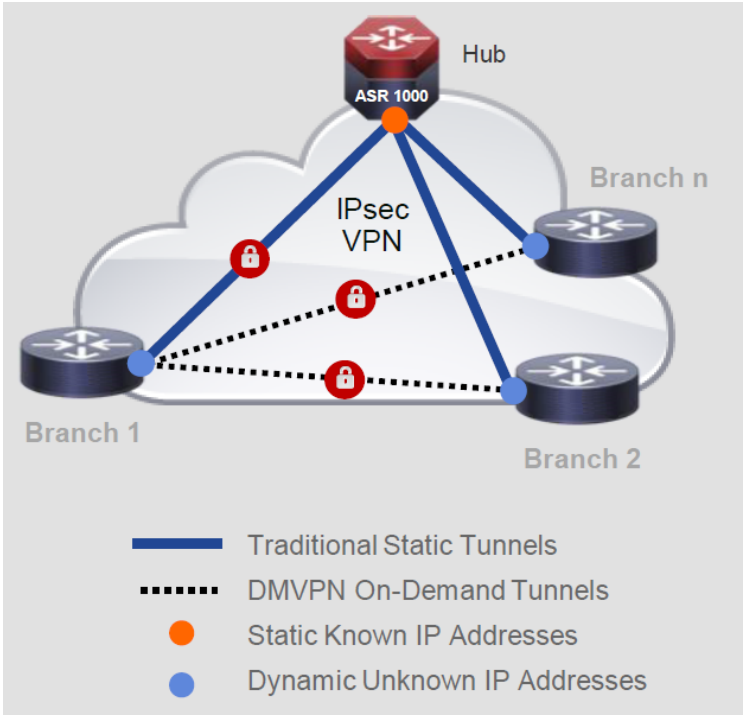
- Proven IPsec VPN technology
  - Widely deployed, large scale, standards based
  - Advanced QOS: hierarchical, per tunnel and adaptive
  - Zero-packet-loss tunnel initiation
- Flexible & Resilient
  - Overlay any transport: MPLS, Carrier Ethernet, Internet, 3G/4G,..
  - Hub-n-Spoke and Spoke-to-Spoke Topologies
  - Multiple encryption, key management, routing options
  - Multiple redundancy options: platform, hub, transports
- Secure
  - Industry Certified IPsec and Firewall
  - NG Strong Encryption: AES-GCM-256 (Suite B); IKEv2
  - IEEE 802.1AR Secure unique device identifier
- Simplified iWAN Deployments
  - Prescriptive validated IWAN designs
  - Automated provisioning –Prime, APIC, LiveAction



ALEF

Over-the-Top WAN Design

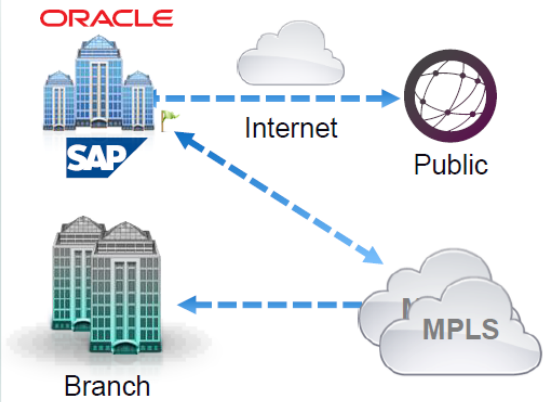
- Branch spoke sites establish a DMVPN tunnel with IPsec encryption to and register with the hub site
- IP routing exchanges prefix information for each site
- BGP or EIGRP are typically used for scalability
- WAN interface address used as the tunnel address, so provider network does not need to know or route customer internal IP prefixes
- Data traffic flows over the DMVPN tunnels
- When traffic flows between spoke sites, the hub assists the spokes to establish a site-to-site tunnel
- Per-tunnel QoS is applied to prevent hub site from overrunning spoke sites



ALEF

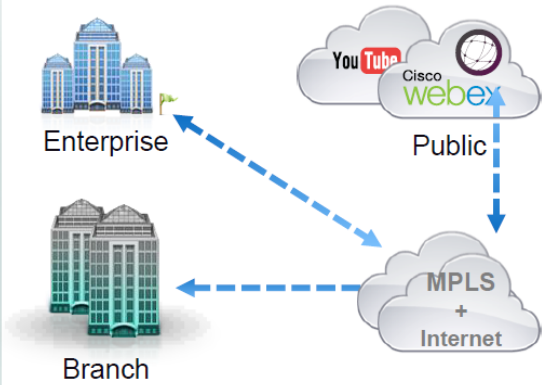
iWAN Deployment Models

Dual MPLS



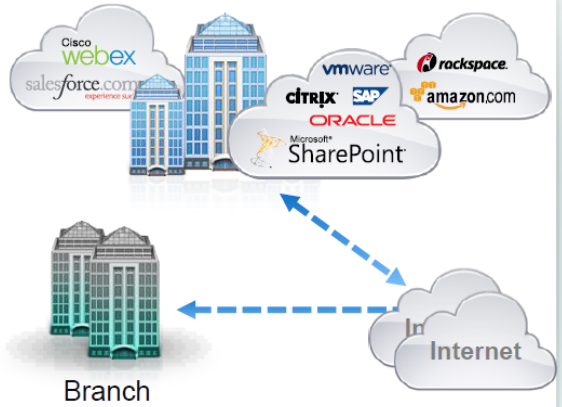
- Highest SLA guarantees
- Tightly coupled to SP
- Expensive

Hybrid



- More BW for key applications
- Balanced SLA guarantees
- Moderately priced

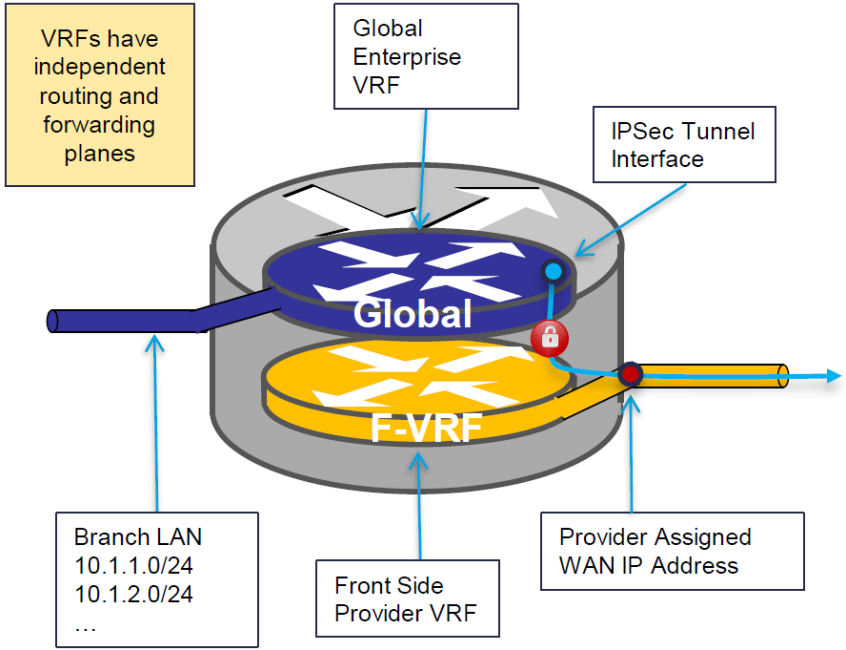
Dual Internet



- Best price/performance
- Most SP flexibility
- Enterprise responsible for SLAs

ALEF

Securing iWAN Transports



Virtual Route Forwarding (VRFs) create multiple logical routers on a single device

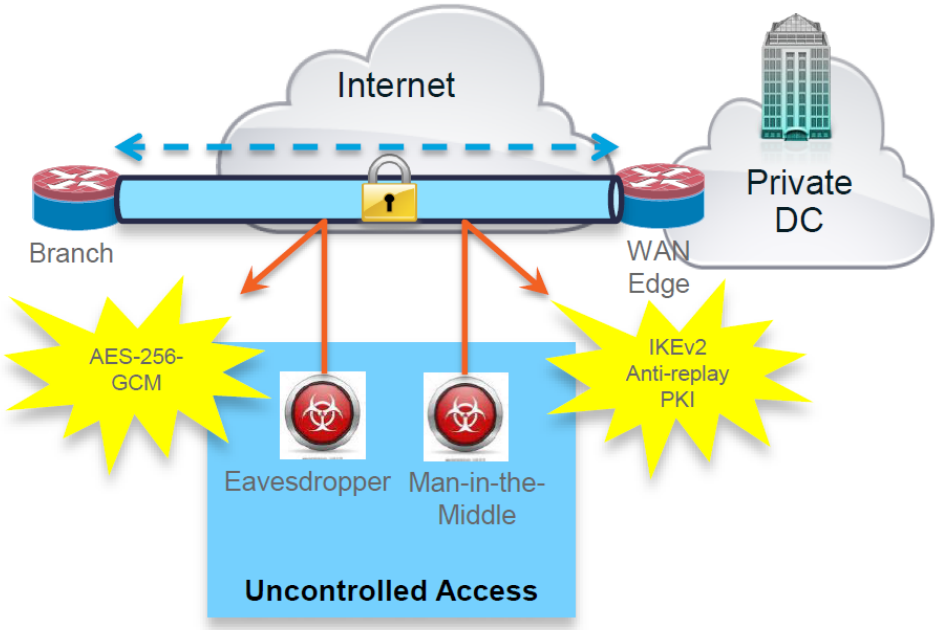
- Separate control/data planes per VRF
- No connectivity between VRFs by default
- Provider side VRF (yellow) for external networks, Global VRF (blue) for internal networks

Provider VRF minimises threat exposure

- Default routing only in Provider VRF
- Provider assigned IP addressing hides internal network
- Provider IP address used as IPSec tunnel
- Only IPSec allowed between internal Global and Provider Front Side VRFs

ALEF

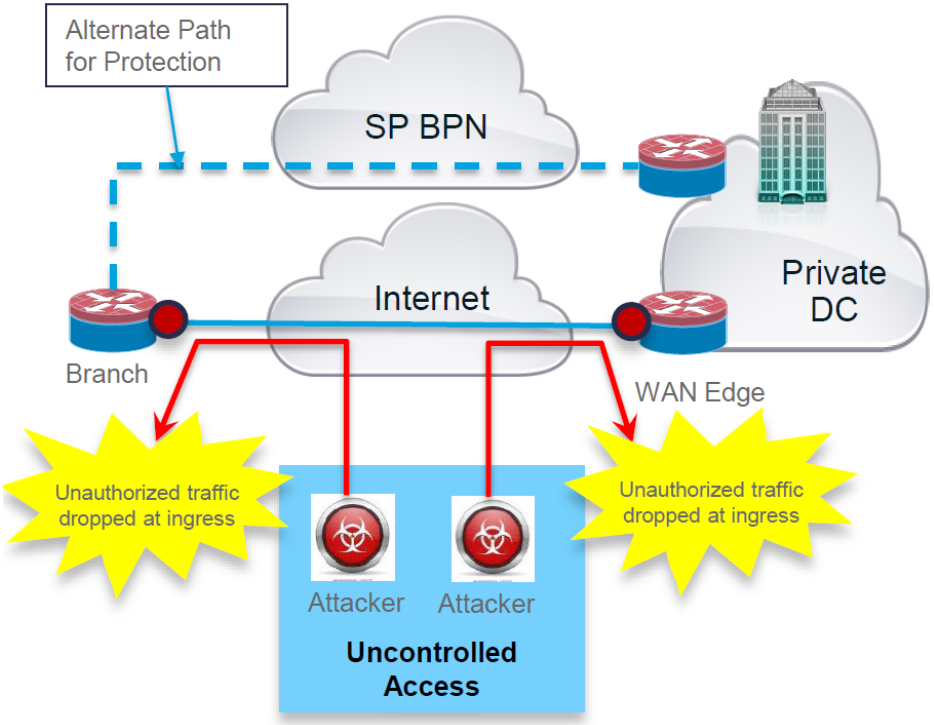
Assuring Confidentiality / IKEv2 + Strong Cryptography



- Strong, certified cryptography and IPSec architecture to protect transport
- Protects from eavesdropping and man-in-themiddle attacks
- 256-bit Advanced Encryption Standard Elliptical Curve Cryptography (AES-256-GCM) for strongest Security Level
- IKEv2 for secure, trusted transport security establishment
- Strongest authentication and Key exchange algos:
  - ECDSA, ECDH and SHA-2 (SHA-256/384)
- NSA certified for both unclassified and mostclassified information categories

ALEF

Intrusion and Attack Prevention



- Control Plane attacks are mitigated with Control Plane policing (CoPP).
- Control plane traffic is throttled and dropped to protect the control plane CPU
- Example set of Control/Mgmt Plane protocols exposed externally include;
  - DHCP
  - IPSec IKE
  - SSH, ICMP, NTP from specific hosts/subnets
- Data plane DOS attack scenario where attack points are flooded - link saturation
- Integrated ZBFW or ACL to drop all unauthorized traffic.
- Loss of BW can be mitigated with intelligent path control. PfR will detect the congestion and route traffic to alternate link.

ALEF

iWAN Routing Protocols

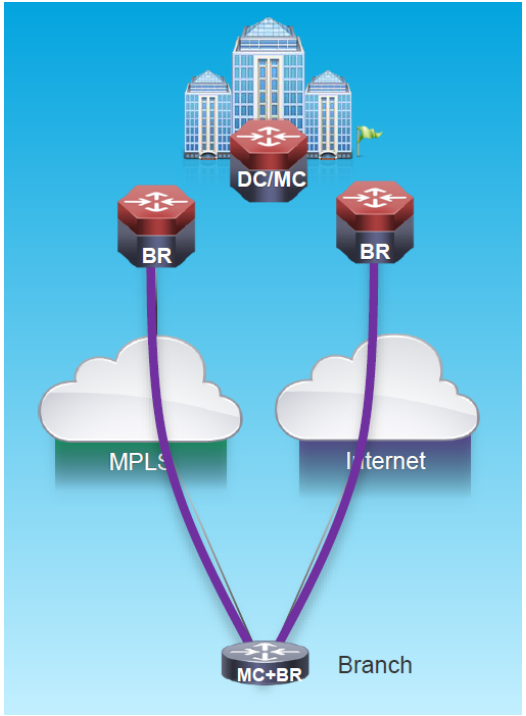
- IWAN Profiles are based upon BGP and EIGRP for scalability and optimal Intelligent Path Control
- Scalability:
  - BGP (Path Vector) and EIGRP (Advanced Distance Vector) provide best scale over large hub-and-spoke topologies like DMVPN
  - OSPF (Link State) maintains a lot of network state which **cannot** be subdivided easily in large DMVPN networks
- Intelligent Path Control:
  - PfR can be used with any routing protocols by relying on the routing table (RIB). Requires all valid WAN paths be ECMP so that each valid path is in the RIB.
  - For BGP and EIGRP, PfR can look into protocol's topology information to determine both best paths and secondary paths thus, ECMP is not required.

Intelligent Path Control – Performance Routing v3 (PfRv3)

ALEF

PfR Components

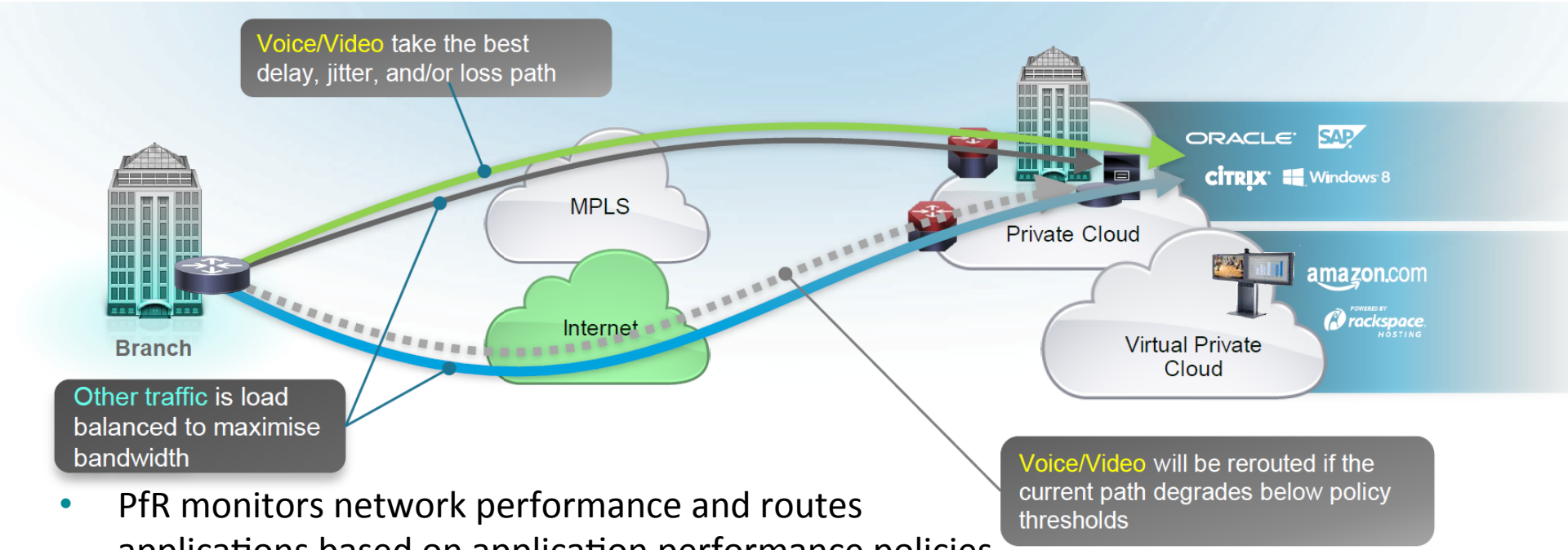
- The Policy Controller: Domain Controller (DC)
  - Discover site peers, prefixes and connected networks
  - Advertise policy and services
  - One per domain, collocated with MC
- The Decision Maker: Master Controller (MC)
  - Discover BRs, collect statistics
  - Apply policy, verification, reporting
  - No packet forwarding/inspection required
- The Forwarding Path: Border Router (BR)
  - Does all packet forwarding
  - Visibility in network performance
  - Enforce MC's decision (path enforcement)



ALEF

Intelligent Path Control with PfR

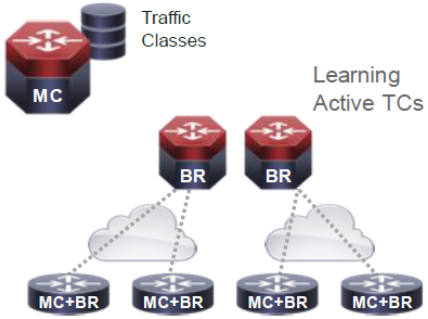
Voice and Video Use-Case

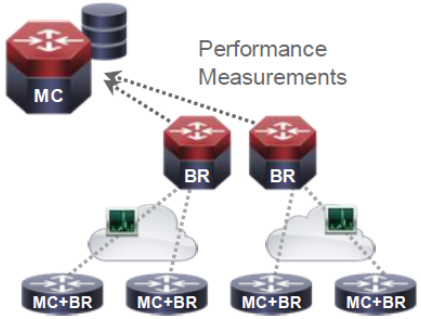


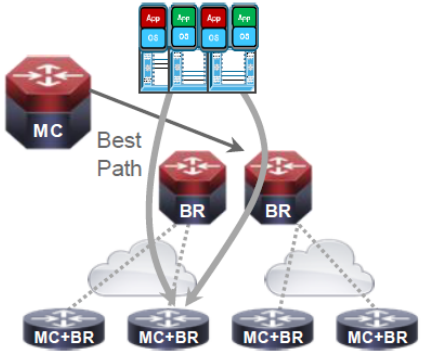
- PfR monitors network performance and routes applications based on application performance policies
- PfR load balances traffic based upon link utilization levels to efficiently utilize all available WAN bandwidth

ALEF

How PfR Works







Define Your Traffic Policy

Identify Traffic Classes based on Applications or Transport Classifiers

Learn the Traffic

ISR G2 and ASR Learn traffic classes flowing through Border Routers (BRs) based on your policy definitions

Measurement

Measure the traffic flow and network performance actively or passively and report metrics to the Master Controller

Path Enforcement

Master Controller commands path changes based on your traffic policy definitions

ALEF

iWAN Traffic Policies

- Domain policies are configured on the hub MC.
- These policies are distributed to branch MCs by using the peering infrastructure.
- All sites that are in the same domain will share the same set of PfR policies.
- Policies are created using preexisting templates, or they can be customized with manually defined thresholds for delay, loss and jitter.

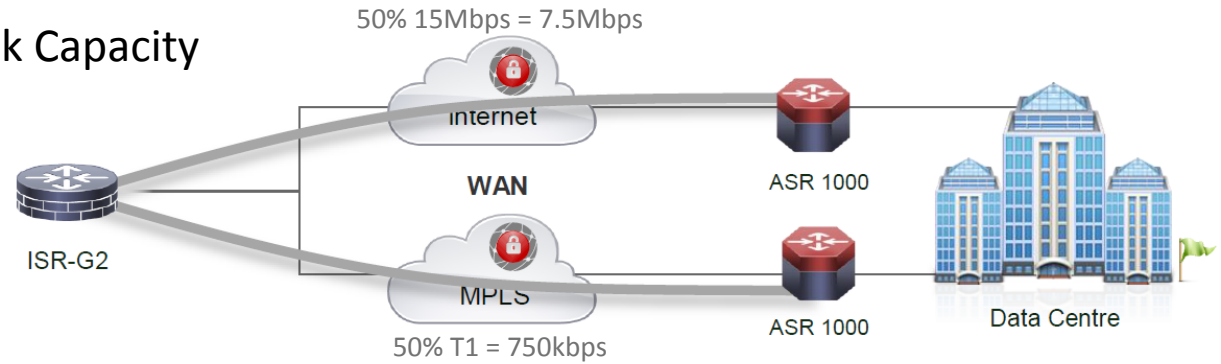
Pre-defined Template	Priority	Threshold Definition
Voice	1	one-way-delay threshold 150 msec
	2	packet-loss-rate threshold 1.0 percent
	2	byte-loss-rate threshold 1.0 percent
	3	jitter threshold 30000 usec
Real-time-video	1	packet-loss-rate threshold 1.0 percent
	1	byte-loss-rate threshold 1.0 percent
	2	one-way-delay threshold 150 msec
	3	jitter threshold 20000 usec
Low-latency-data	1	one-way-delay threshold 100 msec
	2	packet-loss-rate threshold 5.0 percent
	2	byte-loss-rate threshold 5.0 percent
Bulk-data	1	one-way-delay threshold 300 msec
	2	packet-loss-rate threshold 5.0 percent
	2	byte-loss-rate threshold 5.0 percent
Best-effort	1	one-way-delay threshold 500 msec
	2	packet-loss-rate threshold 10.0 percent
	2	byte-loss-rate threshold 10.0 percent
Scavenger	1	one-way-delay threshold 500 msec
	2	packet-loss-rate threshold 50.0 percent
	2	byte-loss-rate threshold 50.0 percent

ALEF

Load Balancing

Maximizing Link Utilization to Increase Available Bandwidth

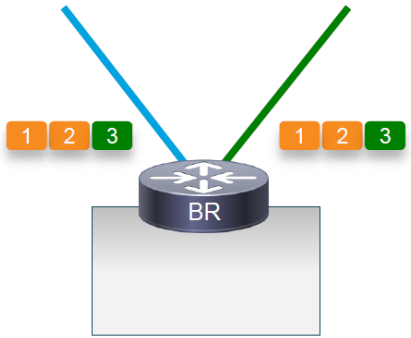
- External Link Load Balancing is enabled by default for **Default Class**
- PfR Distributes traffic across a set of links to maintain efficient utilisation levels with a diferent percentage range. Default utilisation range +/- 20%
- External links can have different available bandwidth, e.g., Int1/0=1,5Mbps, Int1/1 = 15Mbps
- Load Balancing defaults cannot be changed
  - Utilication Range 20%
  - Max Utilication = Link Capacity



ALEF

Performance Monitors

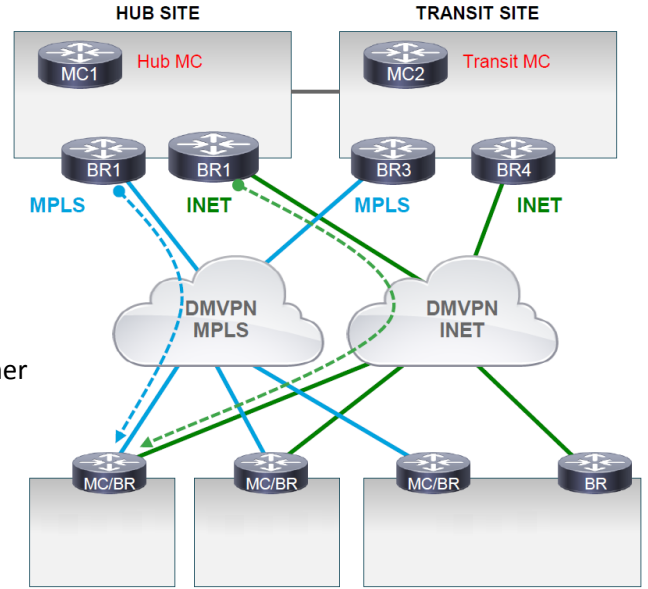
- Apply 3 Performance Monitors instances (PMI) over external interfaces
  - Monitor1–Site Prefix Learning (egress direction)
  - Monitor2–Aggregate Bandwidth per Traffic Class (egress direction)
  - Monitor3–Performance measurements (ingress direction)
- Creates a Channel



ALEF

Collecting Performance Metrics

- **User Traffic**
  - Traffic flow captured on the destination site
  - Performance Monitor collects Performance Metrics
  - Per Channel
  - Default Monitor interval is 30 sec (configurable)
- **Smart Probes**
  - Without actual traffic
    - 20 pps for channel without traffic
    - IOS-XE: BR sends 10 probes spaced 20ms apart in the first 500ms and another similar 10 probes in the next 500ms
    - IOS: BR sends one packet every 50ms
  - With actual traffic
    - Lower frequency when real traffic is observed over the channel
    - Probes sent every 1/3 of [Monitor Interval], ieevery 10 sec by default
  - Measured by Performance Monitor just like other data traffic



ALEF

Platform support

Cisco ISR G2 family

3900-AX, 2900-AX, 1900-AX, 890

as *MC, BR*

Cisco ASR 1000 family

as *MC, BR*

Cisco ISR 4000 family

4300-AX, 4400-AX

as *MC, BR*

Cisco CSR1000v

as *MC, BR(IOS-XE 3.18)*

ALEF

Intelligent WAN Summary

Transport Independent Design

- Highly available Hybrid WAN

Intelligent Path Control

- Performance Routing (PfR) to protect applicationsand load balance traffic to maximize expensive WAN bandwidth

Application Optimization

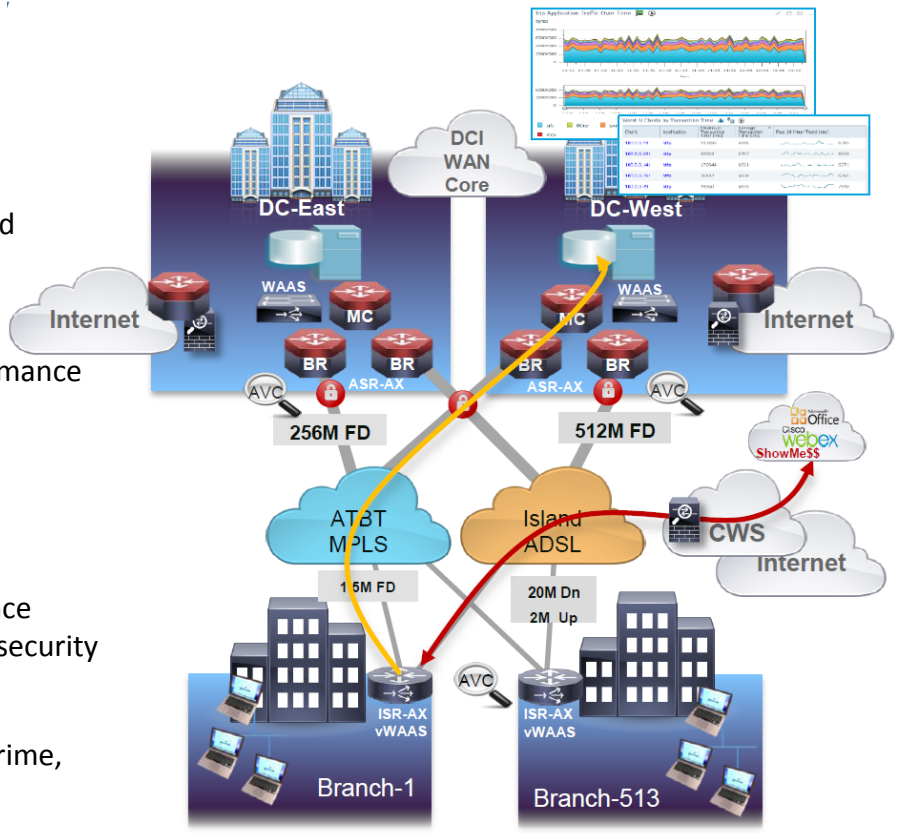
- Application Visibility and Control (AVC) to monitor performance
- WAAS + Akamai to reduce bandwidth consumption while improving application experience

Secure Connectivity

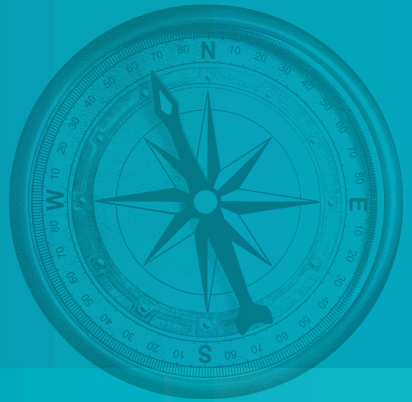
- Secure the network from outside threats
- Cloud Web Security (CWS) for improved Cloud performance whilefreeing up WAN bandwidth, without compromising security

iWAN Management

- Cisco and Ecosystem Partner tools APIC-EM iWAN-APP, Prime, LiveAction, GlueWare, and more



ALEF



Thank you

ALEF