Cisco Connect
Seoul, Korea
April 1-2, 2015

IWAN과 함께하는 Smart Branch Design

조두권 차장
ducho@cisco.com
Cisco Systems Korea, Enterprise SE

AGENDA

Cisco Connect
Seoul, Korea
April 1-2, 2015

1. Intelligent WAN Overview
2. Transport Independent Design
3. Intelligent Path Control
4. Application Optimization
5. IWAN Secure Connectivity
6. IWAN Management
7. Why Cisco IWAN?

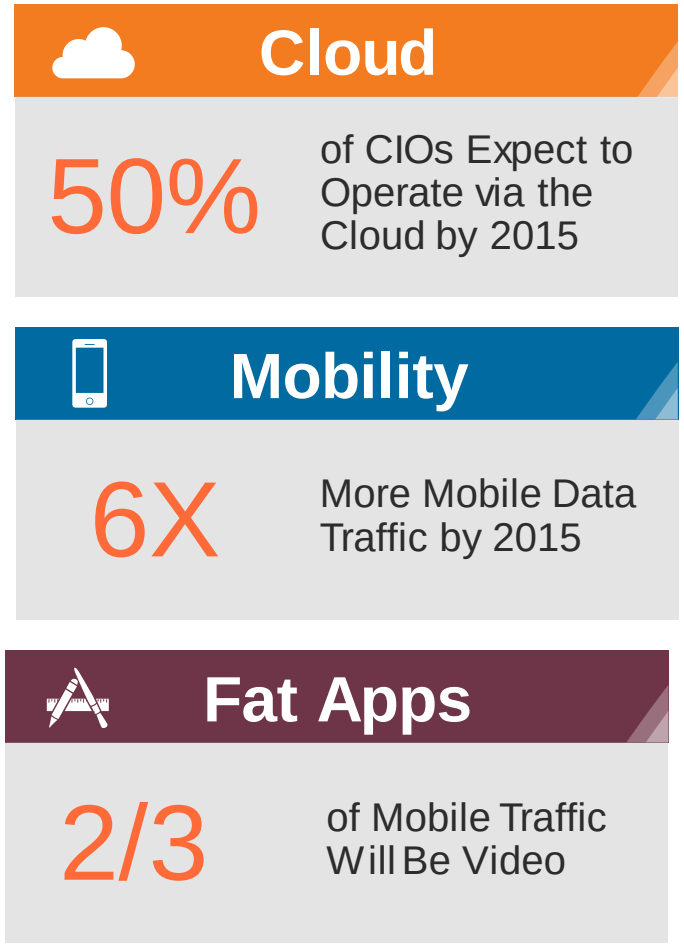
Cisco Connect
Seoul, Korea
April 1-2, 2015

1. IWAN Overview

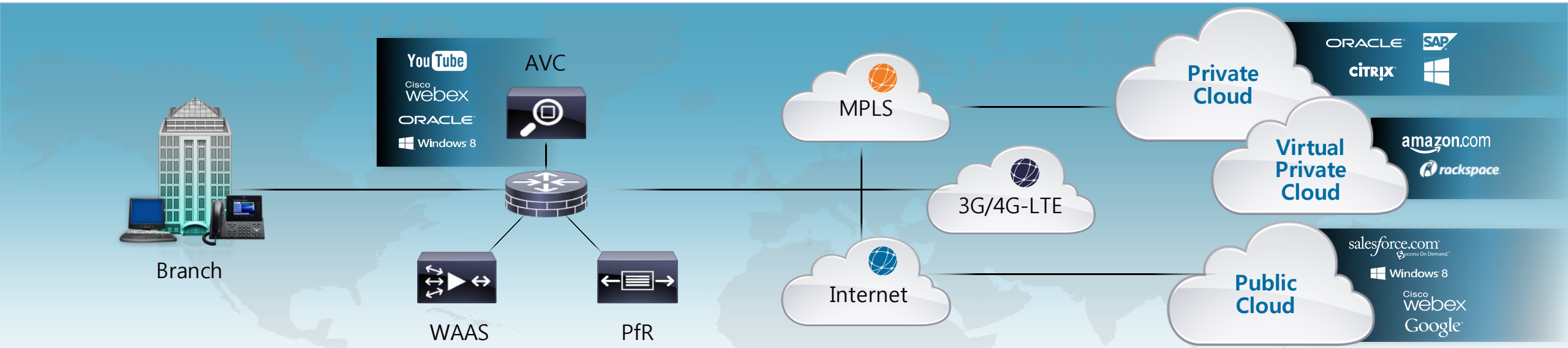
Enterprise WAN 환경의 변화

Cisco Connect

- WAN 대역폭의 요구 사항 증가!!
  - 클라우드, BYOD/IoE, 비디오로 인한 WAN bandwidth의 급격한 감소
- IT 예산 동결 또는 감소
  - 회선 및 대역폭의 비용이 WAN의 주요 고정 비용
- WAN 환경 변화의 주요 원인 요소
  - 낮은 비용의 전송 매체 – Internet, LTE, Carrier Ethernet,
  - 클라우드 기반의 어플리케이션 성능 모니터링 및 최적화
  - 보안 – 강력한 암호화 및 위협 방어 요구



Intelligent WAN 솔루션 구성 요소



APIC-EM을 통한 제어 및 관리의 자동화

Transport Independent

- 연속적인 운영 모델
- SP Migration의 단순화
- 모듈현 및 확장 용이한 디자인
- IPsec routing overlay 디자인

Intelligent Path Control

- 어플리케이션의 최적 경로를 위한 정책 기반의 동적 관리
- 대역폭 이용 극대화를 위한 로드밸런싱
- 이용률의 증가

Application Optimization

- 성능 모니터링을 위한 Application visibility
- 대역폭 최적화 및 애플리케이션 가속

Secure Connectivity

- 강력한 암호화 지원
- 지점의 Direct Internet Access를 위한 클라우드 기반의 보안 관리
- 지능적인 위협 방어

Cisco Connect
Seoul, Korea
April 1-2, 2015

2. Transport Independent Design

다양한 전송 매체를 통한 회선 구성

Cisco Connect

다양한 전송 매체 제공

WAN 구성의 단순화

- Carrier Service에 상관없는 multi-homing 제공
- 사업자와 연결의 단순화 제공을 위한 단일 Routing Control Plane

유연성

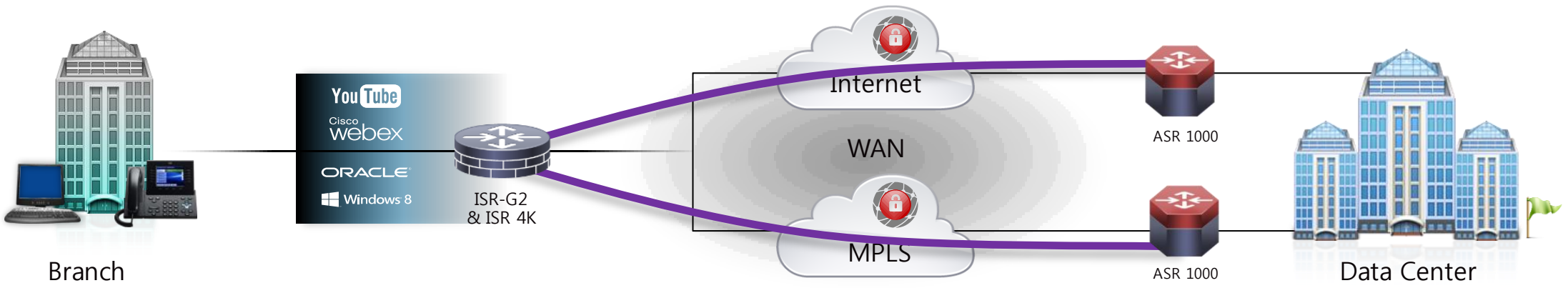
Dynamic Full-Meshed Connectivity

- 전송 media에 관계없이 구성 가능
- 자동화 된 site-to-site IPsec 터널
- 지점 확장을 위한 간편한 Hub configuration 제공

보안성의 극대화

검증된 높은 Security 제공

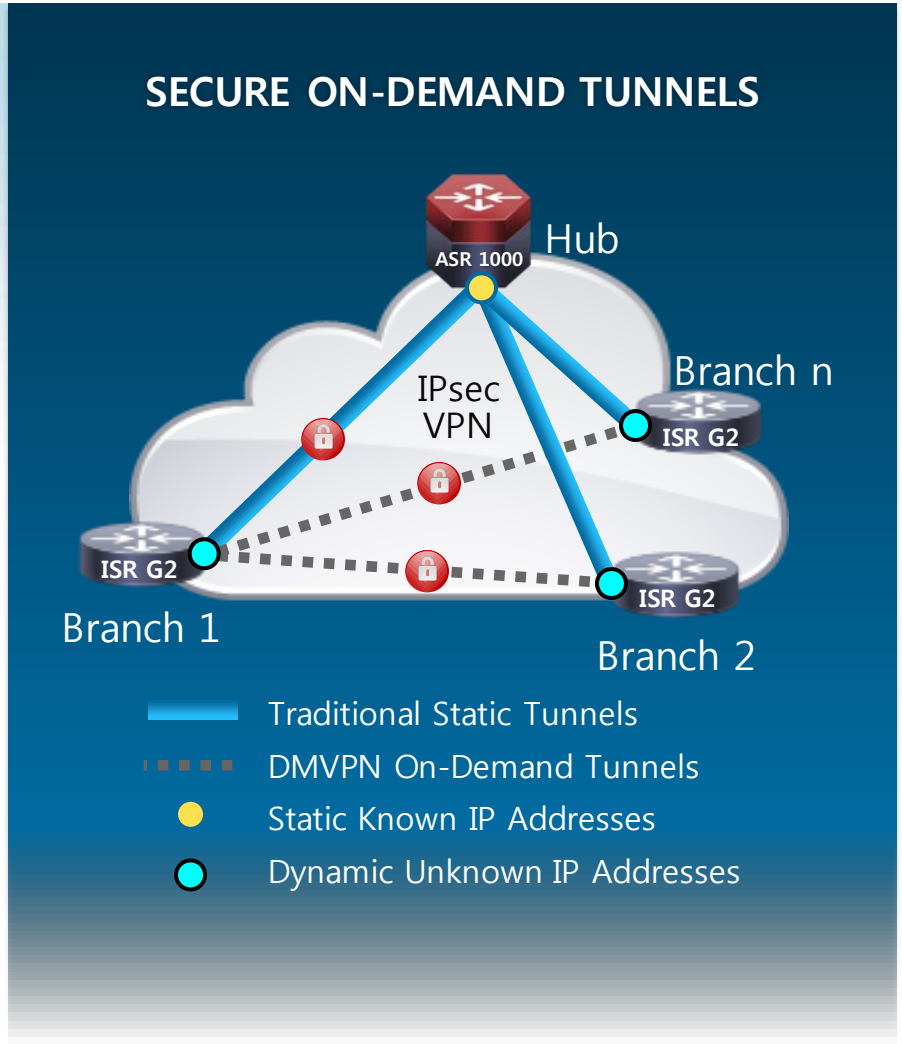
- 검증된 보안 기술 및 방화벽 서비스
- 하드웨어 기반의 고성능 cryptography 제공으로 높은 디자인 확장성 공급



Dynamic Multipoint VPN (DMVPN)

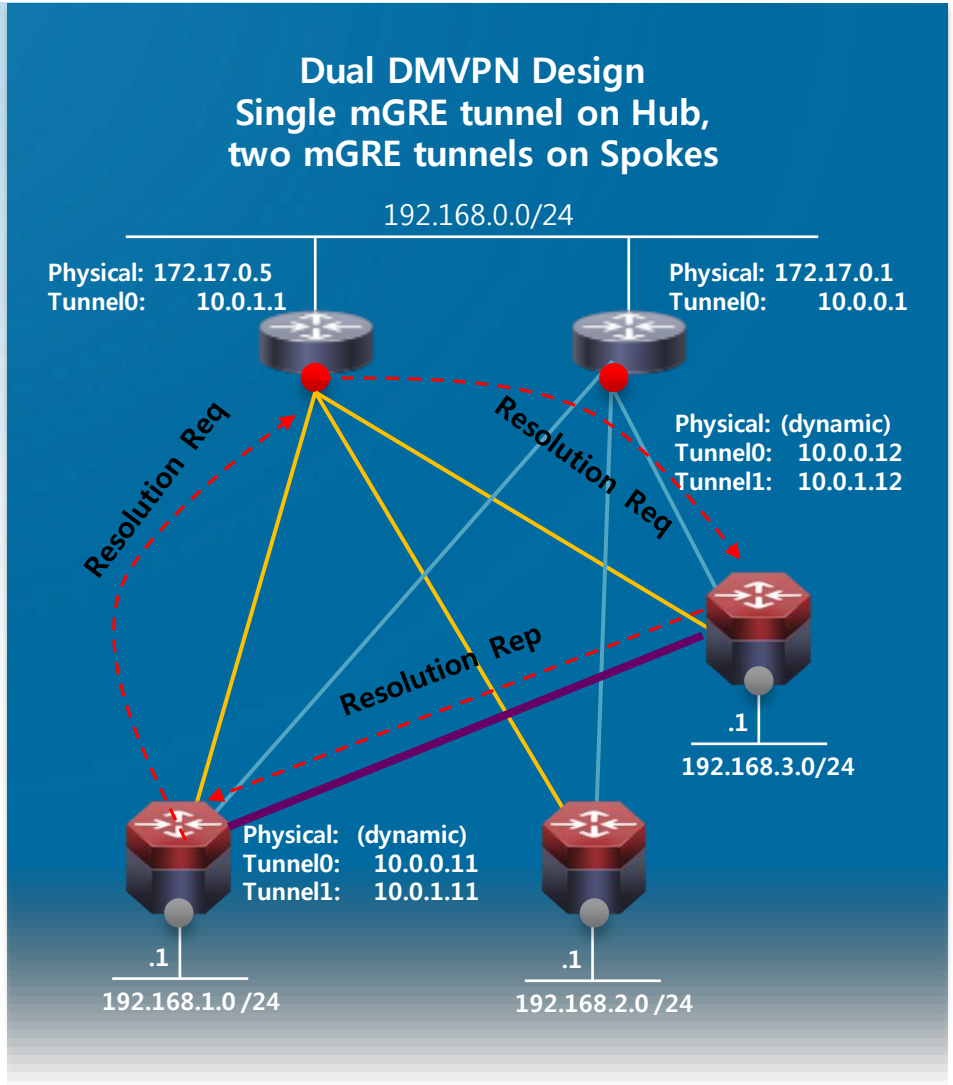
Cisco Connect

- **지점의 spoke site가 IPsec 터널을 이용하여 Hub Site에 등록**
- 각 지점 Site를 위한 IP Routing정보는 Prefix 정보를 교환
- 확장성을 위하여 BGP 또는 EIGRP Protocol 사용을 권고
- **Tunnel address로 WAN interface의 IP address를 사용하여 공급자 네트워크가 고객의 내부 IP prefix를 라우팅할 필요가 없음**
- DMVPN 터널을 통한 데이터 트래픽 전송
- 지점 간의 트래픽 전송 시, Hub site는 지점 간의 tunnel 생성을 제공
- **Hub와 Spoke 사이트 간의 Oversubscription 방지를 위하여 tunnel 별 QoS 지원**



DMVPN 동작 원리

- Spoke site에서 Hub site로 동적 GRE/IPsec tunnel을 생성하며, 각 spoke site가 NHRP server (Hub)의 클라이언트로 NBMA address를 등록
- Active-Active redundancy model (spoke당 두 개 이상의 Hub 지원)
- 모든 Hub장비는 Active로 동작하며 spoke장비와 라우팅 네이버 설립.
- Traffic 전송을 위해 라우팅 프로토콜 사용
- Spoke에서 다른 Spoke의 subnet으로 packet을 전달할 때, 도착지 spoke의 물리적(NBMA) 주소를 NHRP로 요청.
- Hub는 동일한 DMVPN 네트워크의 spoke site가 서로 통신할 수 있도록 이에 대한 정보를 관리하며, destination spoke의 요청을 중계하는 역활 제공
- 응답하는 spoke site는 초기 요청한 spoke로 dynamic GRE/Ipsec tunnel을 초기화 하고, NHRP reply를 전송. (이 경우, relay된 resolution request를 통해 peer의 NBMA address를 인지)
- mGRE interface를 통해서 동적 spoke-to-spoke tunnel을 생성
- 트래픽 전송이 중단되면 spoke-to-spoke tunnel 삭제



DMVPN 발전 방향

Cisco Connect

IWAN 1.0

IWAN 2.0

Phase 1

- **Hub-to-Spoke간의 연결 지원**
- Point-to-point GRE interface (Spoke), mGRE interface (Hub)
- Hub상의 Configuration 단순화
- CPE 상의 dynamic address (NAT) 지원
- Routing protocol 및 multicast지원
- Hub상의 routing summarization지원 (Spoke상에서 full routing 불필요)

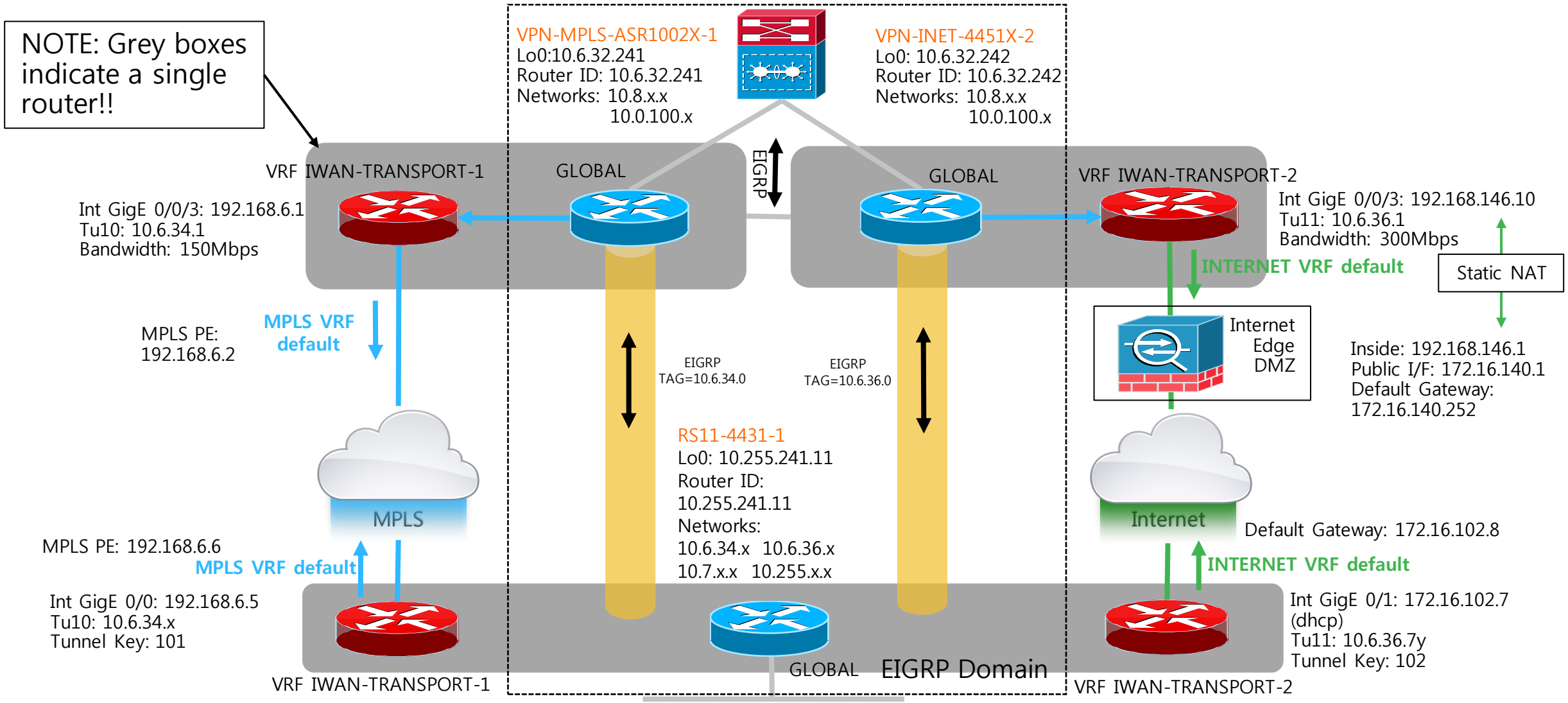
Phase 2

- **Spoke-to-Spoke VPN 연결 지원**
- mGRE interface (Spoke)
- Spoke-to-Spoke간의 direct data traffic 전송으로 Hub의 부하 감소
- Daisy chain 형태의 디자인
- Spoke 사이트의 full-routing table (no summarization)
- 개별 Spoke site에 의한 Spoke-to-Spoke tunnel 생성 trigger 기능
- 라우팅 프로토콜의 제한적인 확장성

Phase 3

- **높은 확장성 및 다양한 네트워크 디자인 제공**
- 계층적인 네트워크 디자인
- Spoke 사이트의 full routing table 불필요 (Summarization 지원)
- Hub site에 의한 Spoke-to-Spoke tunnel 생성 trigger 기능
- 라우팅 프로토콜 확장성의 제약 제거

Topology


NOTE: Grey boxes indicate a single router!!
VPN-MPLS-ASR1002X-1
Lo0:10.6.32.241
Router ID: 10.6.32.241
Networks: 10.8.x.x
10.0.100.x
VPN-INET-4451X-2
Lo0: 10.6.32.242
Router ID: 10.6.32.242
Networks: 10.8.x.x
10.0.100.x
EIGRP
VRF IWAN-TRANSPORT-1
GLOBAL
GLOBAL
VRF IWAN-TRANSPORT-2
Int GigE 0/0/3: 192.168.6.1
Tu10: 10.6.34.1
Bandwidth: 150Mbps
Int GigE 0/0/3: 192.168.146.10
Tu11: 10.6.36.1
Bandwidth: 300Mbps
INTERNET VRF default
Static NAT
MPLS PE:
192.168.6.2
MPLS VRF
default
Internet
Edge
DMZ
Inside: 192.168.146.1
Public I/F: 172.16.140.1
Default Gateway:
172.16.140.252
EIGRP
TAG=10.6.34.0
EIGRP
TAG=10.6.36.0
RS11-4431-1
Lo0: 10.255.241.11
Router ID:
10.255.241.11
Networks:
10.6.34.x 10.6.36.x
10.7.x.x 10.255.x.x
MPLS
Internet
Default Gateway: 172.16.102.8
MPLS PE: 192.168.6.6
MPLS VRF default
INTERNET VRF default
Int GigE 0/0: 192.168.6.5
Tu10: 10.6.34.x
Tunnel Key: 101
Int GigE 0/1: 172.16.102.7
(dhcp)
Tu11: 10.6.36.7y
Tunnel Key: 102
VRF IWAN-TRANSPORT-1
GLOBAL
EIGRP Domain
VRF IWAN-TRANSPORT-2

Hub 설정 – Interfaces & Routing

```
vrf definition IWAN-TRANSPORT-1
 address-family ipv4
 exit-address-family
```

MPLS 연결을 위한 Front-door VRF 설정

```
interface GigabitEthernet0/0/3
 description MPLS-TRANSPORT
 vrf forwarding IWAN-TRANSPORT-1
 ip address 192.168.6.1 255.255.255.0
```

MPLS Front-door VRF의 외부 인터페이스 설정

```
interface Tunnel10
 bandwidth 150000
 ip address 10.6.34.1 255.255.255.0
 no ip redirects
 ip mtu 1400

 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 600

 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0/3
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf IWAN-TRANSPORT-1
 tunnel protection ipsec profile DMVPN-PROFILE-1

ip route vrf IWAN-TRANSPORT-1 0.0.0.0 0.0.0.0 192.168.6.2
```

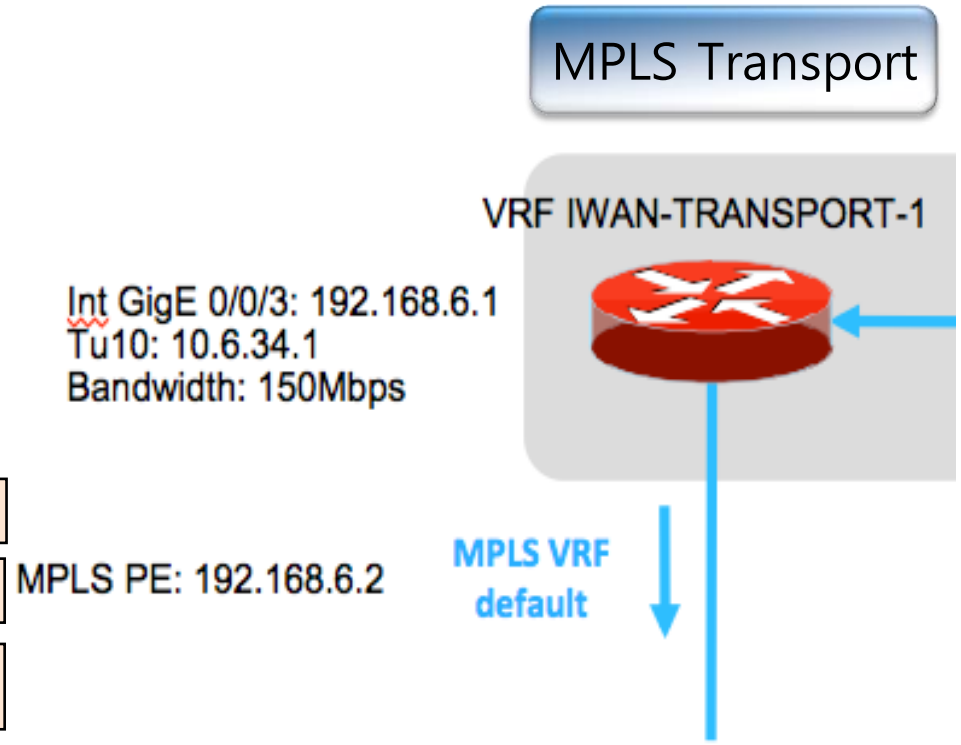
DMVPN 터널 예시

DMVPN Network ID 설정

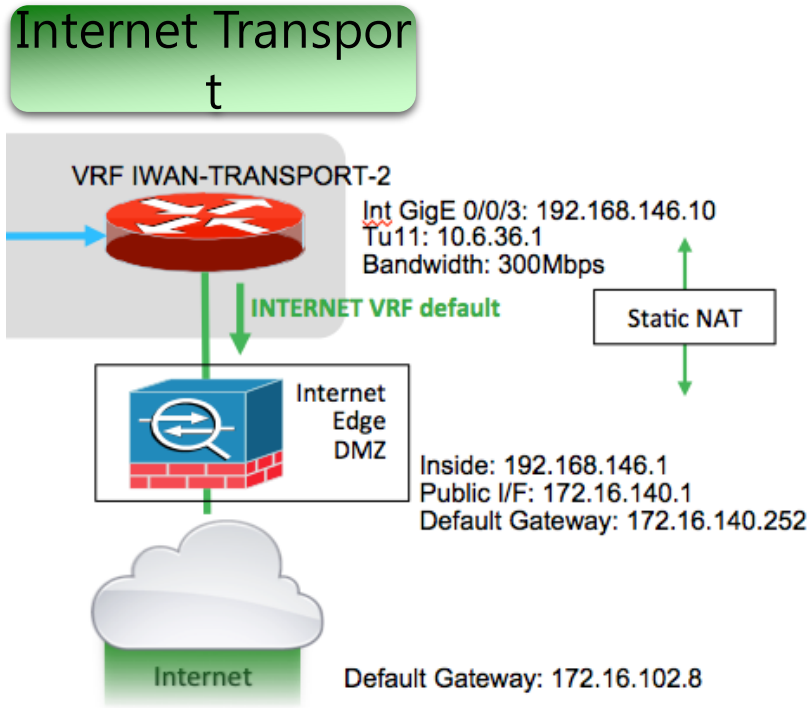
DMVPN Ph3 설정

물리적인 인터페이스 연동

Tunnel endpoint를 VRF로 지정



Hub 설정 – Interfaces & Routing



Internet Front-door VRF의 외부 인터페이스 설정

Internet DMVPN 터널을 위한 tunnel 인터페이스 설정

DMVPN Network ID 설정

Internet을 위한 default GW설정

```
Vrf definition IWAN-TRANSPORT-2
 address-family ipv4
 exit-address-family

interface GigabitEthernet0/0/3
 description INTERNET-TRANSPORT
 vrf forwarding IWAN-TRANSPORT-2
 ip address 192.168.146.10  255.255.255.0

interface Tunnel11
 bandwidth 300000
 ip address 10.6.36.1  255.255.255.0
 no ip redirects
 ip mtu 1400

 ip nhrp authentication cisco123 (suggest 321)
 ip nhrp map multicast dynamic
 ip nhrp network-id 102
 ip nhrp holdtime 600

 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0/3
 tunnel mode gre multipoint
 tunnel key 102
 tunnel vrf IWAN-TRANSPORT-2
 tunnel protection ipsec profile DMVPN-PROFILE-2
!
ip route vrf IWAN-TRANSPORT-2  0.0.0.0  0.0.0.0  192.168.146.1
```

DMVPN Crypto 설정

Hub 및 Branch Site

Cisco Connect

MPLS Transport

```
! <removed IKEv2 proposal, use smart defaults>
!
crypto ikev2 keyring DMVPN-KEYRING-1
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key c1sco123
!
crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-1
 match fvrf IWAN-TRANSPORT-1
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local DMVPN-KEYRING-1
!
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE-1
 set transform-set AES256/SHA/TRANSPORT
 set ikev2-profile FVRF-IKEv2-IWAN-TRANSPORT-1
```

```
crypto ikev2 dpd 40 5 on-demand
```

Spoke site의 인증 방식 설정 (Pre-shared key)

Front-door VRF와의 연동

모든 spoke site의 인증된 주소와 연동 허용

Crypto 및 transform set에 대한 설정

⚠ 지점에서만 DPD timers를 설정!!!

Internet Transport

```
! <removed IKEv2 proposal, will use smart defaults>
!
crypto ikev2 keyring DMVPN-KEYRING-2
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key c1sco123
!
crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-2
 match fvrf IWAN-TRANSPORT-2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local DMVPN-KEYRING-2

crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE-2
 set transform-set AES256/SHA/TRANSPORT
 set ikev2-profile FVRF-IKEv2-IWAN-TRASNPORT-2
```

```
crypto ikev2 dpd 40 5 on-demand
```

Spoke 설정 – Interfaces & Routing

```
vrf definition IWAN-TRANSPORT-1
 address-family ipv4
 exit-address-family
```

```
Interface GigabitEthernet0/0
 vrf forwarding IWAN-TRANSPORT-1
 ip address 192.168.6.5  255.255.255.0
```

MPLS Front-door VRF의 외부 인터페이스 설정

```
interface Tunnel10
 ip address 10.6.34.x  255.255.255.0
 no ip redirects
 ip mtu 1400
ip nhrp authentication cisco123
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.34.1  nbma 172.16.84.4  multicast priority 1
 ip nhrp nhs 10.0.34.2  nbma 172.16.92.2  multicast priority 2
 ip nhrp nhs cluster 0 max-connections 1
 ip nhrp registration  no-unique
 ip nhrp shortcut
 ip tcp adjust-mss  1360
 if-state nhrp
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 101
 tunnel vrf IWAN-TRANSPORT-1
 tunnel protection ipsec profile DMVPN-PROFILE-1
!
ip route vrf IWAN-TRANSPORT-1  0.0.0.0  0.0.0.0  192.168.6.6
```

DMVPN Tunnel 예시

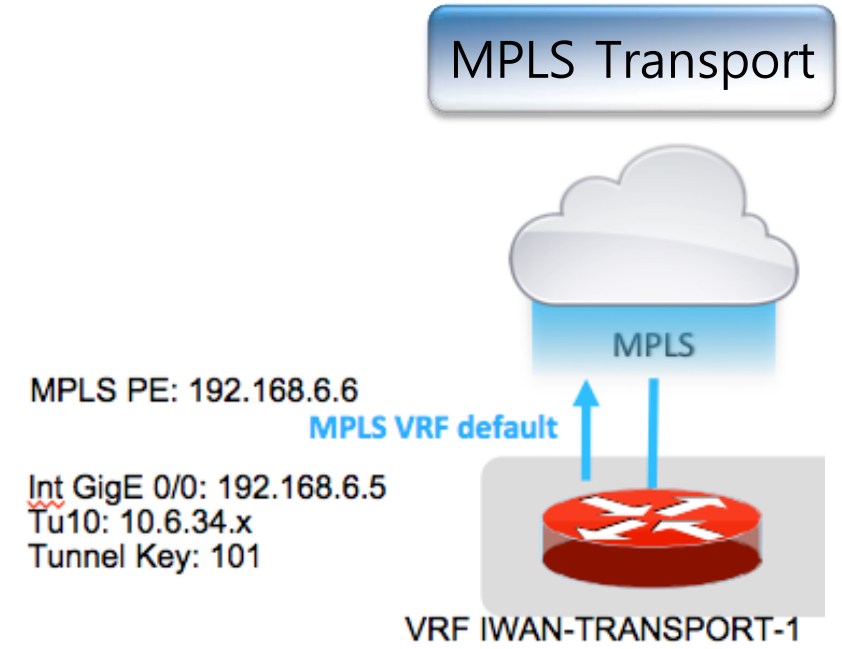
DMVPN Network ID설정

이중화를 위한 Backup DMVPN Hub 설정

NHS priority 1에 대한 우선 순위 설정

DMVPN Phase 3 설정

Front-door VRF에 대한 tunnel endpoint 설정



Spoke 설정 – Interfaces & Routing

```
Vrf definition IWAN-TRANSPORT-2
 address-family ipv4
 exit-address-family
```

```
Interface GigabitEthernet0/1
 vrf forwarding IWAN-TRANSPORT-2
 ip address 172.16.102.7  255.255.255.0
 ip access-group ACL-INET-PUBLIC in
```

Recommended:
ip address dhcp

```
interface Tunnel11
 ip address 10.6.36.y 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco123
 ip nhrp network-id 102
 ip nhrp holdtime 600
 ip nhrp nhs 10.6.36.1  nbma 172.16.140.1  multicast priority 1
 ip nhrp nhs 10.6.36.2  nbma 172.16.142.2  multicast priority 2
 ip nhrp nhs cluster 0 max-connections 1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 if-state nhrp
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 102
 tunnel vrf IWAN-TRANSPORT-2
 tunnel protection ipsec profile DMVPN-PROFILE-2
ip route vrf IWAN-TRANSPORT-2  0.0.0.0  0.0.0.0 172.16.102.8
```

Hub의 공인 아이피를 설정

DHCP 사용 시, 추가적인 Default gateway를 설정할 필요가 없음.(자동설정)

외부 공격에 대비한 protection:

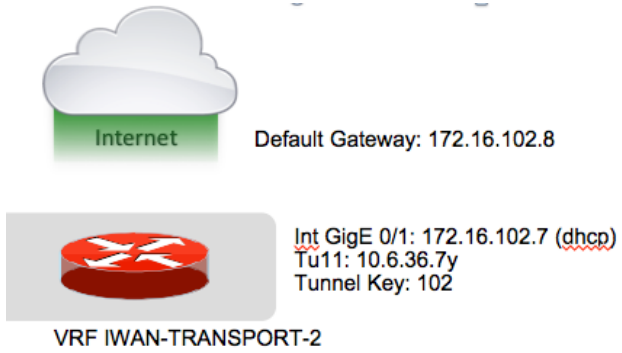
IPSec과 Key 프로토콜을 제외한 모든 트래픽 Block

```
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc

 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1

 permit tcp host 172.16.140.110  eq www any
```

IPsec 및 DHCP 에 대한 허용

추가적인 허용 룰:
- remote pings
- Ping replies
- traceroute replies
- remote traceroute

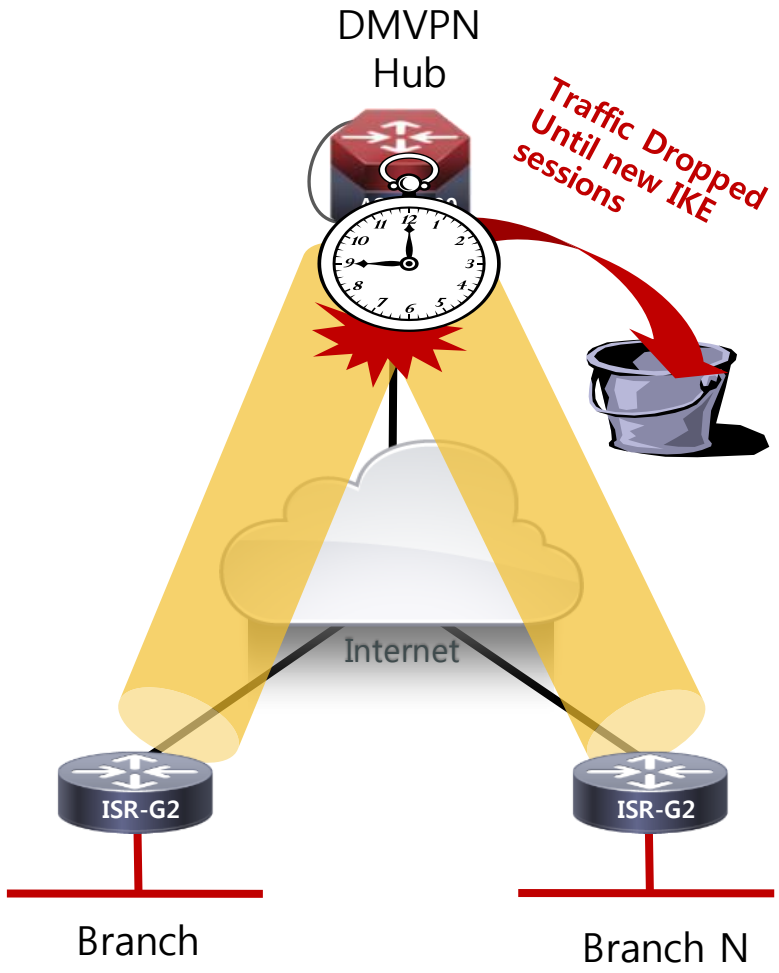
PKI 사용시 추가적인 80port 설정



Dead Peer Detection (DPD)

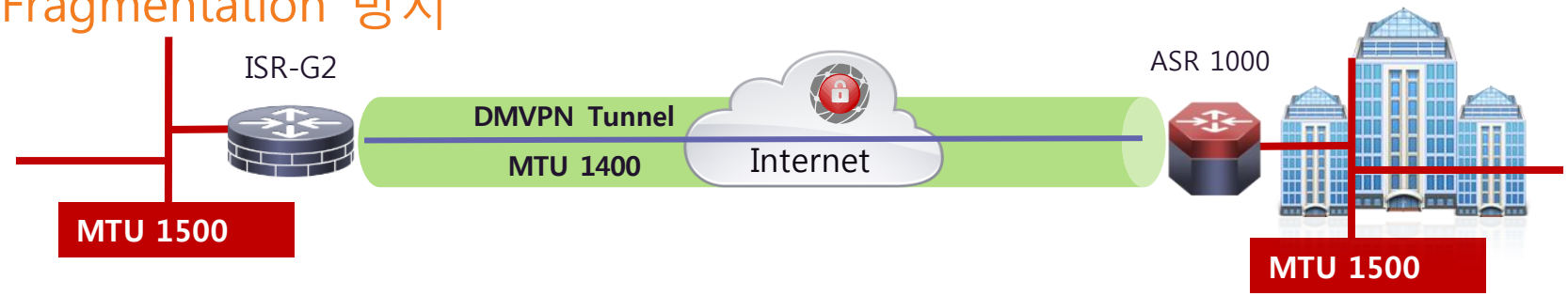
Informational RFC 3706

- Dead Peer Detection (DPD) unreachable IKE peer에 대한 감지.
- 각 라우터의 DPD 상태가 독립적으로 동작.
- DPD 미 사용 시, Spoke 라우터는 Hub에서 drop한 오래된 SPI session을 사용하여 계속적으로 트래픽 암호화를 시도
- Spoke 라우터의 re-converge를 위해 최대 60분의 시간이 필요
- Spoke 사이트에서 ISAKMP Keepalive를 사용
  - IKEv1/v2 keepalive/dpd 라우팅 프로토콜의 hold/dead timer보다 늦게 timeout되어야 하기 때문에, 라우팅 프로토콜의 hello 보다 커야 함.
  - crypto isakmp keepalive는 40초 기준으로 5번 retry 시도.
  - crypto ikev2 dpd는 40초 기준으로 5번 retry 시도 (On-demand)
- Peer의 수가 많은 Hub 라우터 상에서는 CPU의 overhead로 인하여 미 사용을 권고.



IWAN Best Practices

IPSec VPN의 Fragmentation 방지



Tunnel Setting	Minimum MTU	Recommended MTU
GRE/IPSec (Tunnel Mode)	1414 bytes	1400 bytes
GRE/IPSec (Transport Mode)	1434 bytes	1400 bytes

- IP fragmentation은 CPU/Memory에 대한 overhead를 발생 시키며, throughput의 저하를 발생
- 특정 Datagram의 fragmentation발생은 전체 IP datagram의 재 전송을 요구하는 원인이 됨.
- Crypto transform-set 설정 시, '***mode transport***'을 권고
  - NAT 설정 사용을 위해, 20Bytes의 여유 공간 필요
- MTU에 대한 이슈를 해결하기 위해서 모든 DMVPN tunnel에 대해서 아래와 같이 설정 필요.
  - ***ip mtu 1400***
  - ***ip tcp adjust-mss 1360***

IWAN Routing Protocol 설정

Cisco Connect

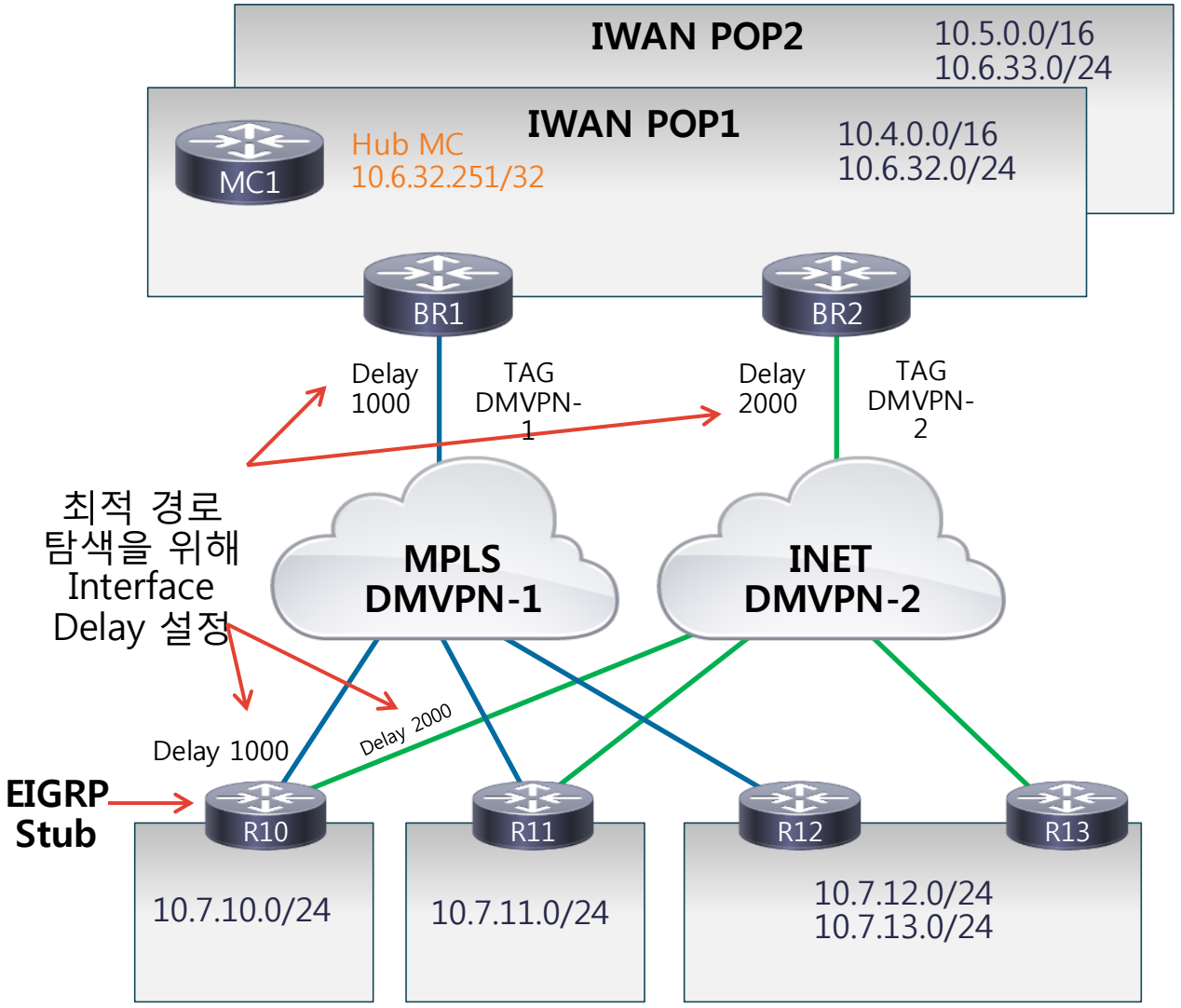
어떤 Routing protocol을 사용해야 할까?

- IWAN은 최적의 경로 관리 및 확장성을 위해서 BGP나 EIGRP protocol 사용을 권고
- 확장성:
  - BGP(Path Vector)와 EIGRP(Advanced Distance Vector)은 DMVPN을 통한 대형 Hub-and-Spoke 디자인 구성을 위해 최적의 확장성을 제공
  - OSPF(Link State)의 경우, 많은 network status 상태 업데이트와 네트워크 Area 분할이 필요.
- 지능적인 경로 관리:
  - PfR은 routing table(RIB)상에서 동작, 모든 routing protocol과 동작 가능.
    - 모든 WAN경로를 ECMP로 동작, 각 경로가 RIB에서 존재해야 함.
  - PfR은 best path와 secondary path를 결정하기 위해서 라우팅 프로토콜의 정보를 확인

IWAN Deployment - EIGRP

Principles

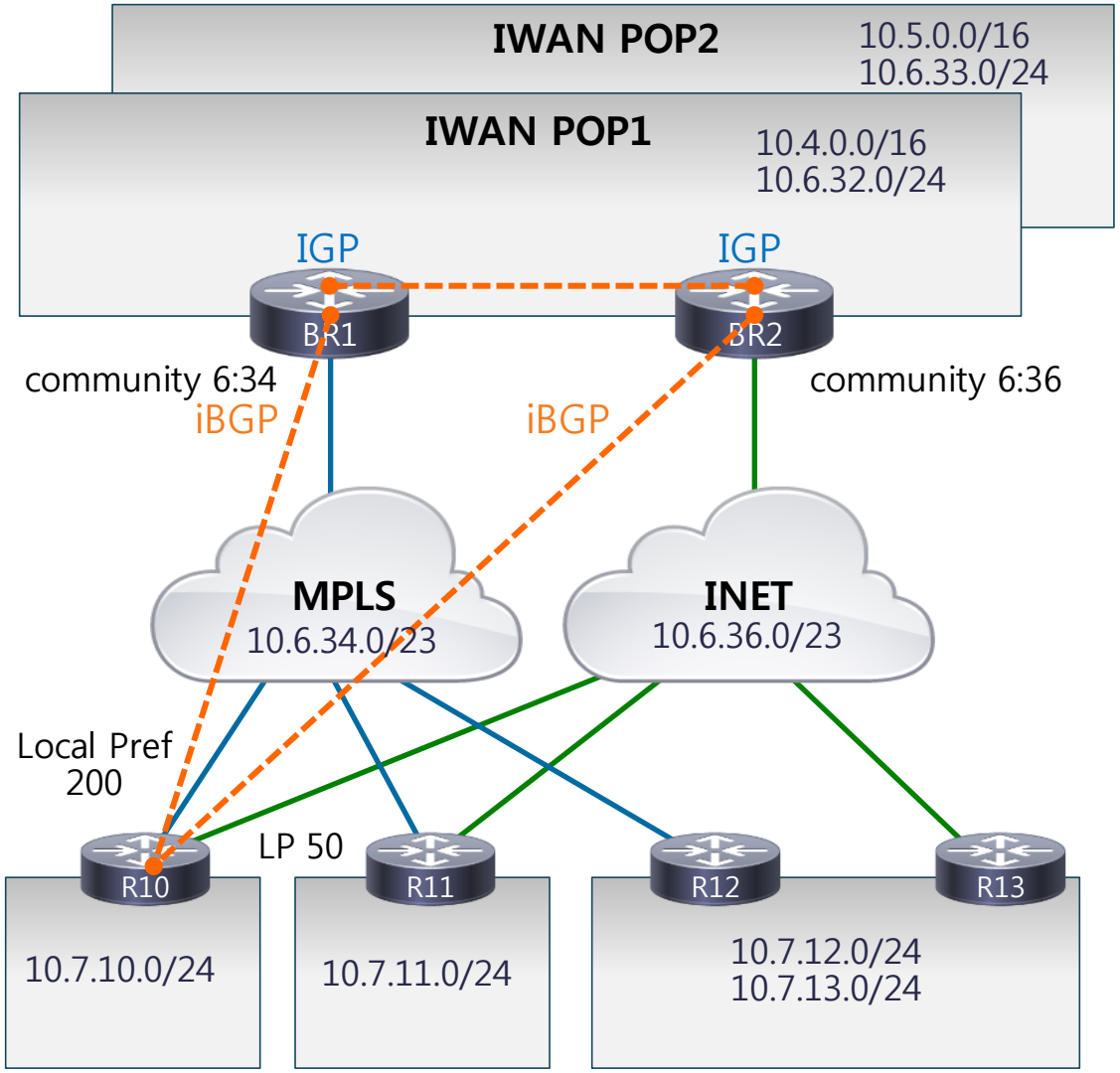
- Branch, WAN, POP/Hub site를 단일 EIGRP 프로세스로 구성
- WAN구간의 추가적인 Hello/Hold timers 조정
- Tunnel interface의 delay 값을 조정하여 WAN 회선에 대한 preference 설정
  - MPLS(primary) Internet(secondary)
- **Hub:**
  - DMVPN 구간 내의 Routing Loop 방지를 우해 Route Tag를 이용한 Filtering 설정
  - Branch prefix summary route for spoke-to-spoke tunnels
- **Spoke:**
  - 확장성을 위한 EIGRP Stub 설정



IWAN Deployment - BGP

Principles

- 단일 iBGP 라우팅 도메인 권고
- WAN구간의 추가적인 Hello/Hold timers 설정
- **Hub:**
  - Spoke 라우터를 위한 DMVPN Hub 라우터의 RR 설정
  - BGP의 dynamic peer feature 설정
  - Spoke 라우터로 전달되는 route의 Summarization
  - Site local prefix를 위한 Community값 설정
  - Local IGP의 경로를 BGP로 redistribute
- **Spokes:**
  - 각 DMVPN 망 내에서 redundant RR에 대해서 peer 설정
  - Community 값을 기반으로 local preference 설정을 위한 inbound route-map 설정
  - Local Preference를 통한 WAN 회선 선택

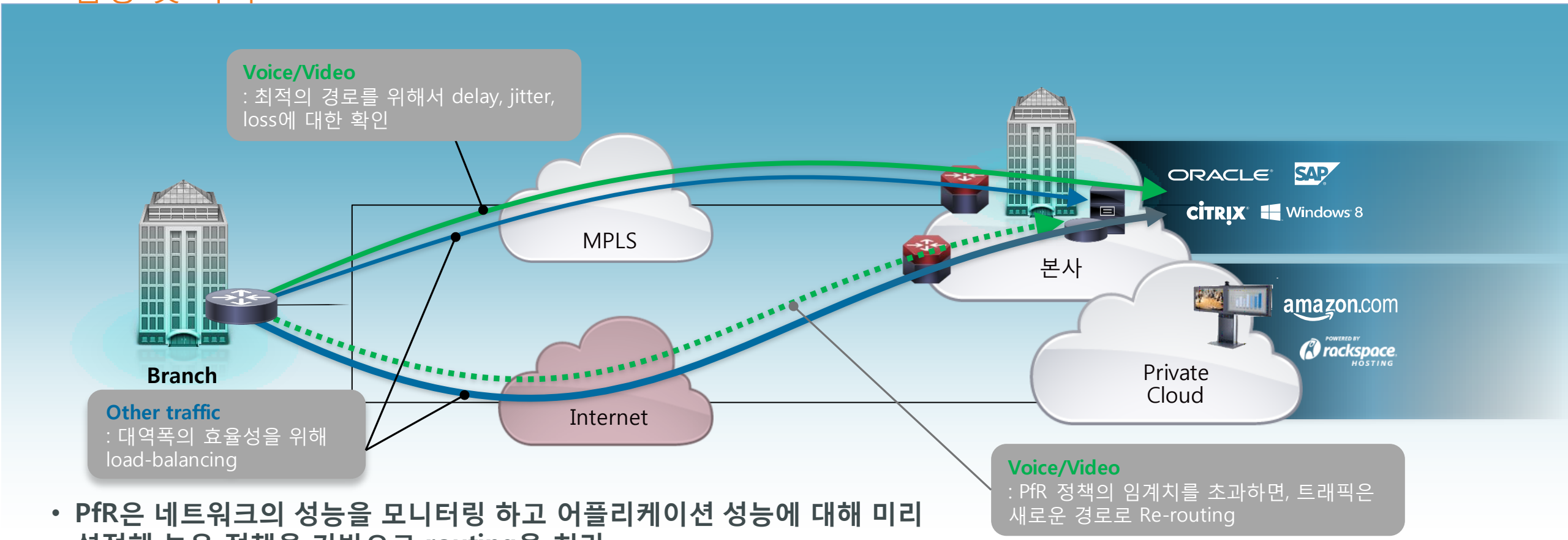


Cisco Connect
Seoul, Korea
April 1-2, 2015

3. Intelligent Path Control

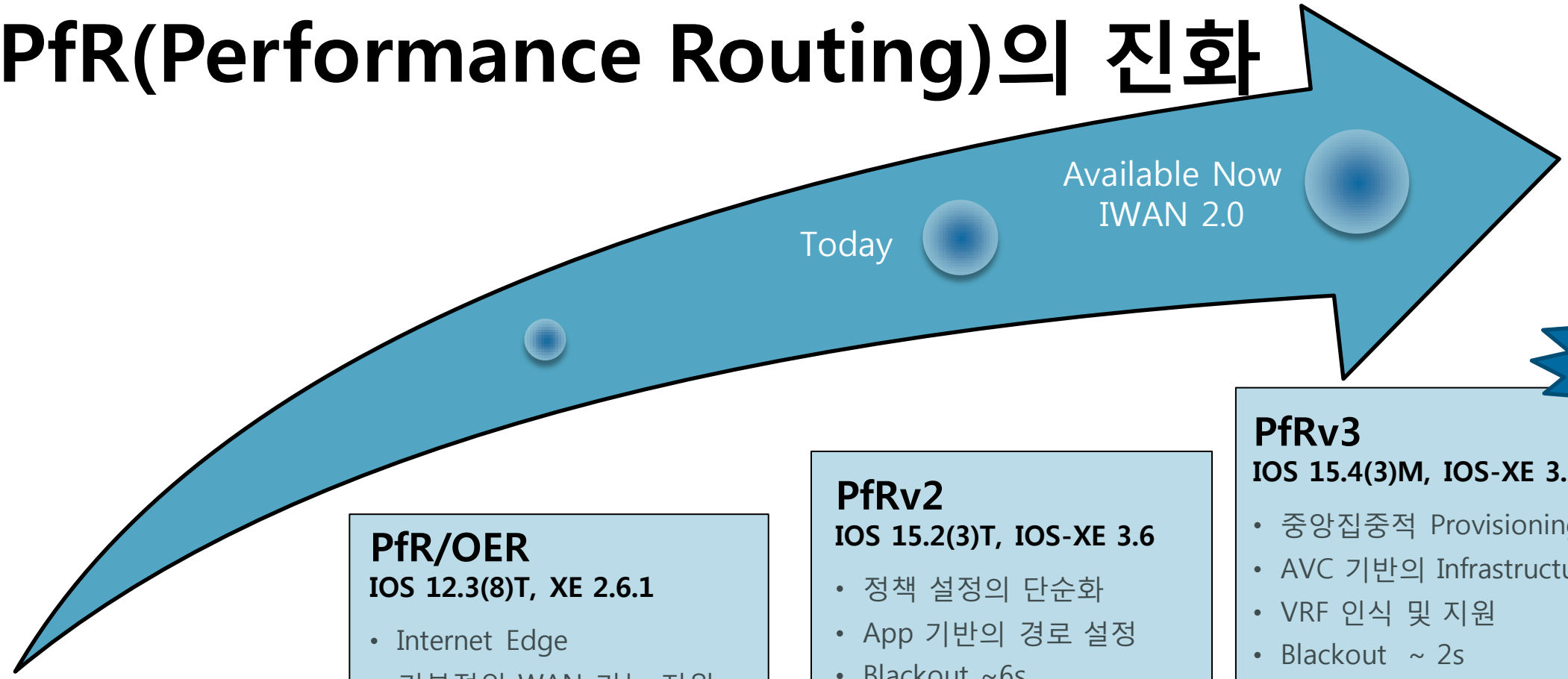
PfR을 이용한 지능적인 경로 관리

음성 및 비디오 Use-Case



- **PfR은 네트워크의 성능을 모니터링 하고 어플리케이션 성능에 대해 미리 설정해 놓은 정책을 기반으로 routing을 처리.**
- **PfR은 회선의 효율적인 사용을 위해 모든 회선을 이용하여, load-balancing을 구현**

PfR(Performance Routing)의 진화



New

PfR/OER
IOS 12.3(8)T, XE 2.6.1

- Internet Edge
- 기본적인 WAN 기능 지원
- Provisioning per site per policy
- 1000줄 이상의 configuration

PfRv2
IOS 15.2(3)T, IOS-XE 3.6

- 정책 설정의 단순화
- App 기반의 경로 설정
- Blackout ~6s
- Brownout ~9s
- **약 500개의 사이트 지원**
- 10줄 미만의 configuration

Internet Edge Support

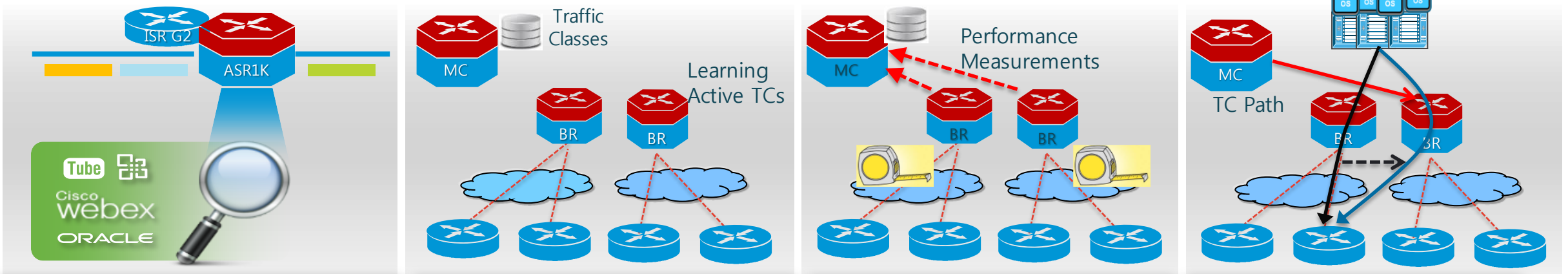
PfRv3
IOS 15.4(3)M, IOS-XE 3.13

- 중앙집중적 Provisioning
- AVC 기반의 Infrastructure
- VRF 인식 및 지원
- Blackout ~ 2s
- Brownout ~ 2s
- **약 2000개의 사이트 지원**
- Hub ONLY configuration

높은 확장성과 설정의 단순화

PfRv3 동작 원리

Cisco Connect



트래픽 정책에 대한 정의

- Hub MC에서 최적 경로에 대한 정책 정의
  - Load balancing
  - Path preference
  - Application metrics
- **DSCP기반의 정책**
- **Application 기반의 정책**

트래픽 패턴 학습

- BR(Border router)에 흐르는 트래픽 중, policy에 matching되는 트래픽에 대한 학습

통합 Performance Monitor

측정

- 측정된 TC(Traffic Class)의 성능을 MC로 리포팅

통합 Performance Monitor

경로 조정

- MC(Master Controller)가 설정된 policy조건에 맞게 BR(border router)의 경로를 직접 변경

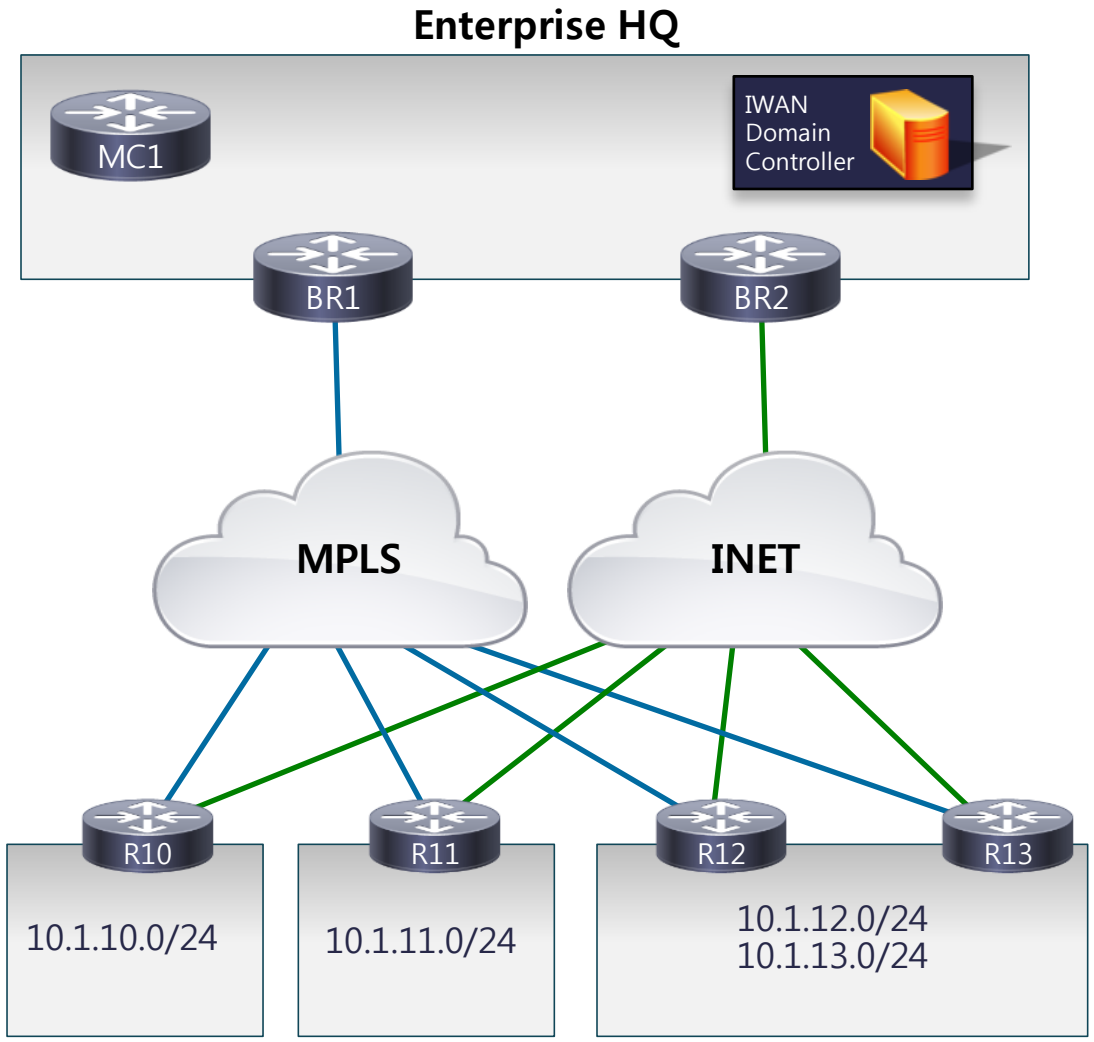
라우팅 경로에 대한 변경

Cisco Connect
Seoul, Korea
April 1-2, 2015

PfRv3 – Components

IWAN Domain (Concept)

- 동일한 정책의 세트를 공유하는 네트워크
- 각각의 모든 Site들은 Performance Routing의 구성요소를 운영
- 네트워크 내의 Domain Peering을 통해 제공하는 서비스 공유
- 중앙의 Domain Controller를 통해서 configuration을 관리



PfR 구성 요소

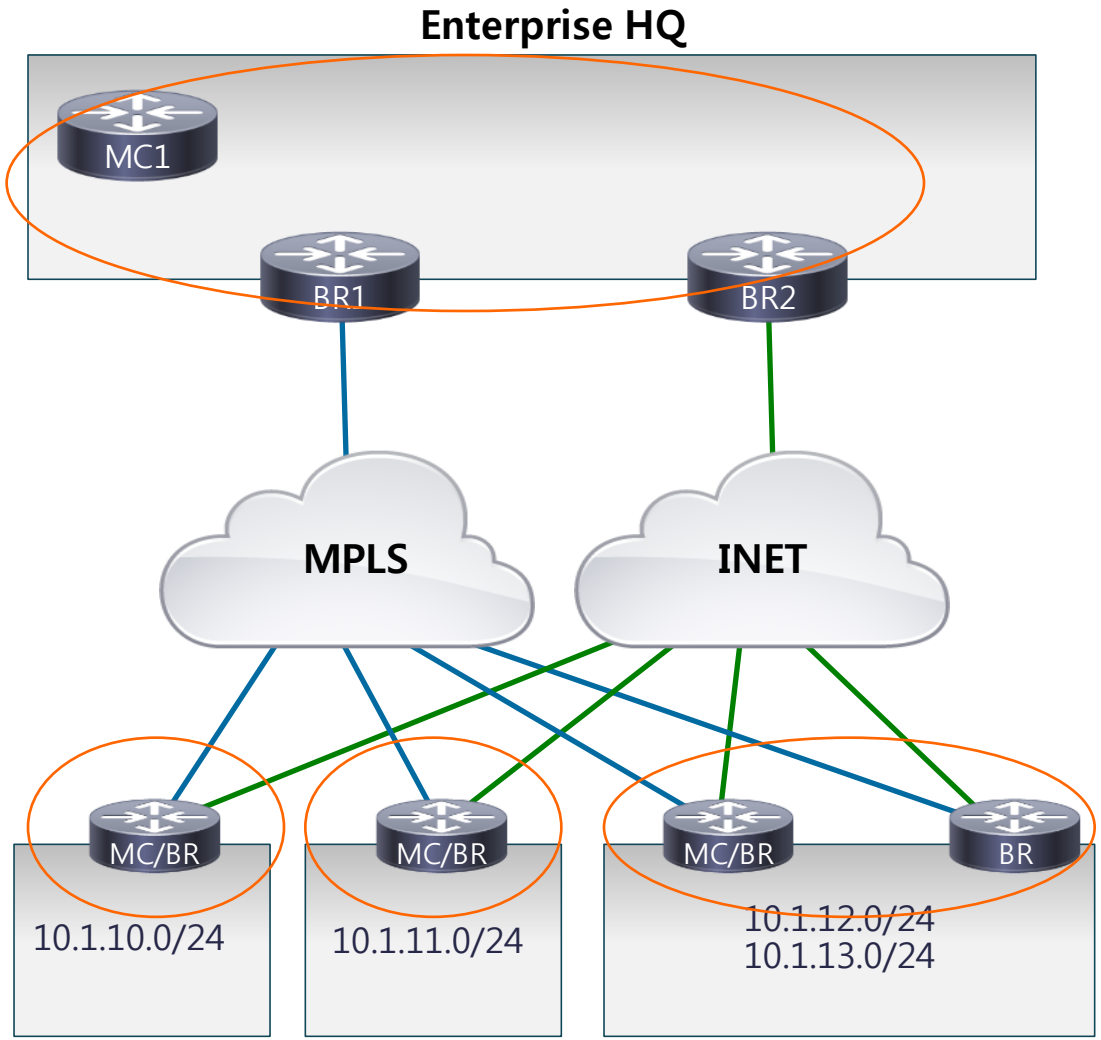
Cisco Connect

The Decision Maker: Master Controller (MC)

- 정책의 적용/확인/reporting
- Packet forwarding이나 inspection을 하지 않음
- BR과 함께 동작하거나 독립적으로 동작 가능
- VRF aware

The Forwarding Path: Border Router (BR)

- 전송 경로에 대한 network visibility (학습 및 측정)
- MC의 경로 결정에 대한 수행
- VRF aware

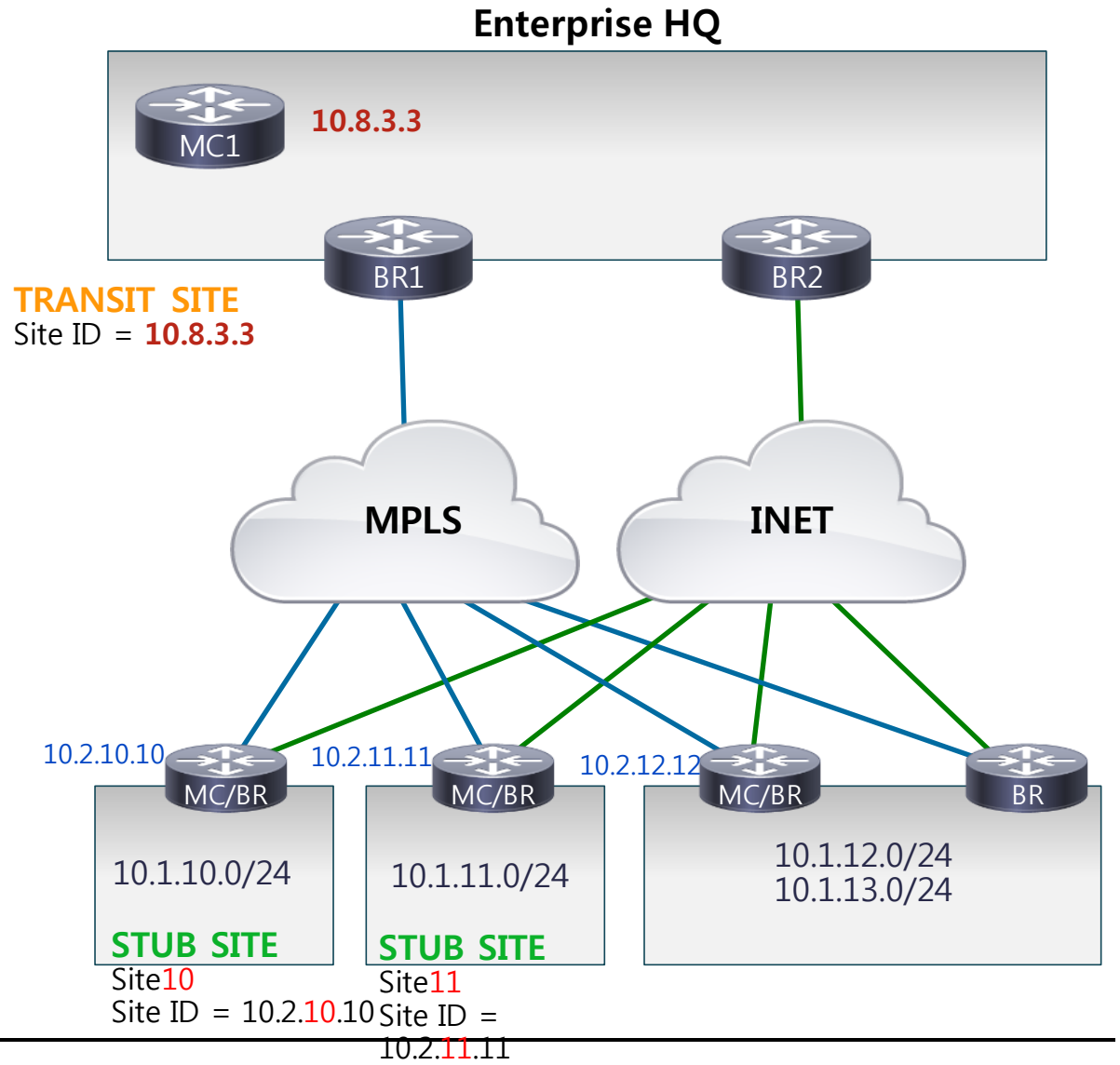


PfR Sites

Site Types

- Transit Sites – Enterprise POP 또는 HUB
- Branch Sites – Stub

- 내부의 Master Controller(MC)에 의해서 제어
- Site ID – MC의 Loopback address 사용
- 각 Site내에 하나 이상의 BR 존재 가능
- 각 Site내의 BR은 하나 이상의 Link 존재 가능



Transit Sites 및 Hub MC 설정

```
domain IWAN
 vrf default
  master hub
   source-interface Loopback0
   enterprise-prefix prefix-list ENTERPRISE_PREFIX
   site-prefixes prefix-list DC1_PREFIX
```

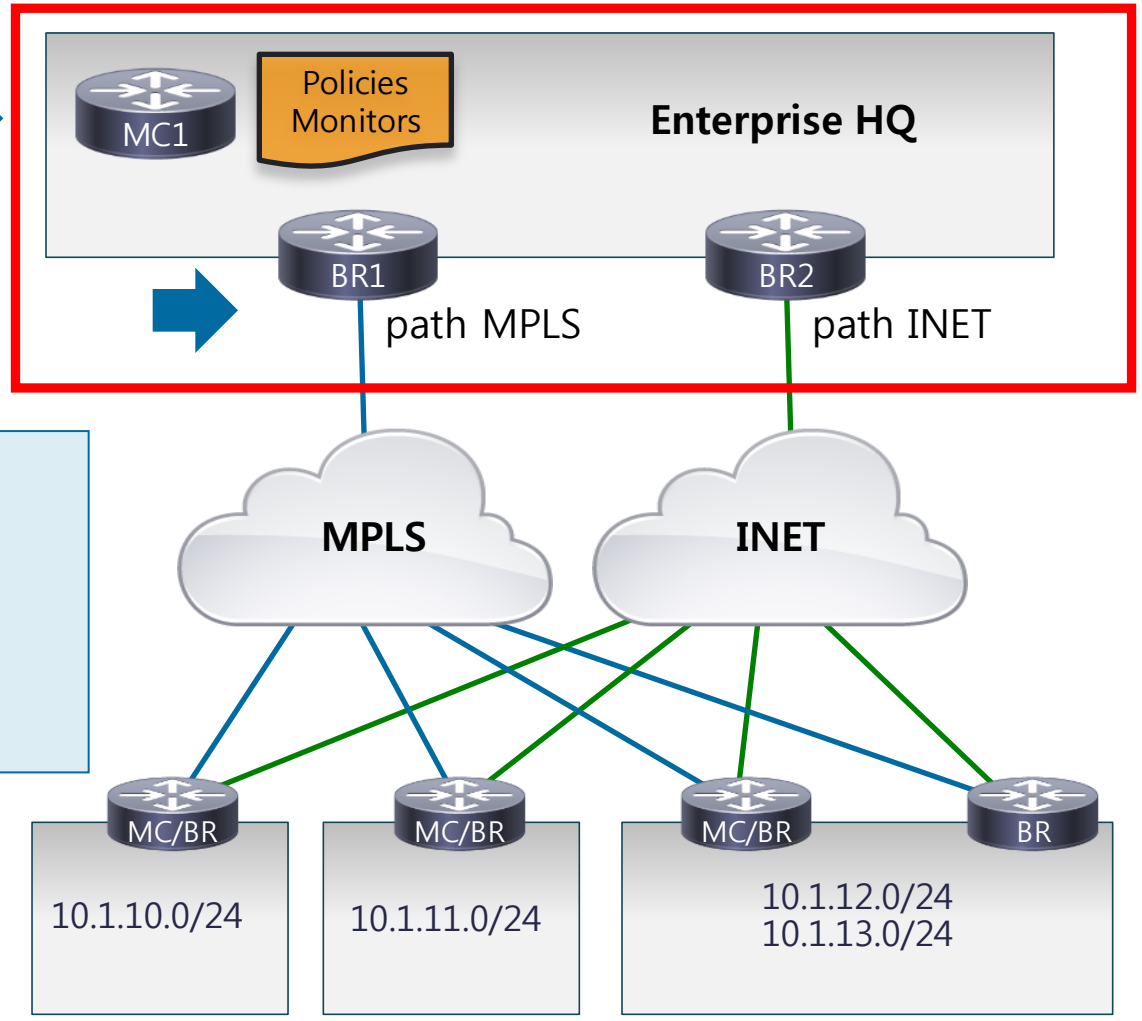
MC1

```
domain IWAN
 vrf default
   border
    master 10.8.3.3
    source-interface Loopback0
!
interface Tunnel100
 description -- Primary Path --
 domain IWAN path MPLS
```

BR1

```
domain IWAN
 vrf default
   border
    master 10.8.3.3
    source-interface Loopback0
!
interface Tunnel200
 description – Secondary Path --
 domain IWAN path INET
```

BR2



DSCP/App기반의 정책 설정 예시

Cisco Connect

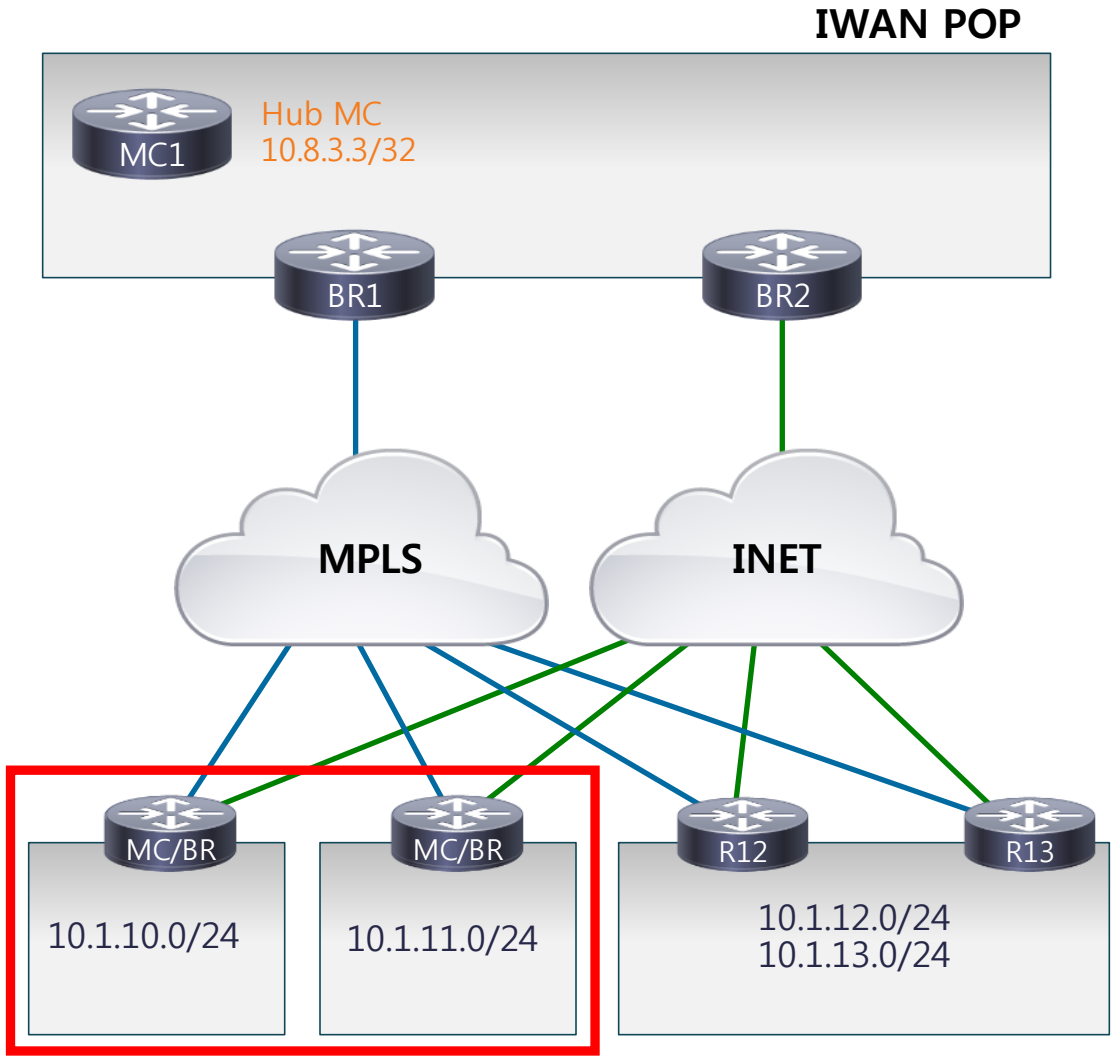
```
domain IWAN
 vrf default
  master hub
   load-balance
   class MEDIA sequence 10
    match application telepresence-media policy real-time-video
    match application ms-lync policy real-time-video
    path-preference MPLS fallback INET
   class VOICE sequence 20
    match dscp ef policy voice
    path-preference MPLS fallback INET
   class CRITICAL sequence 30
    match dscp af31 policy low-latency-data
```

- Policies:
  - DSCP 또는 Application 기반의 정책 설정 (NBAR2)
  - DSCP marking이 LAN interface (Ingress on BR) 상에서 NBAR2와 함께 설정 가능
  - Default Class에 matching되는 traffic은 load-balancing 제공

Branch site의 단일 라우터 구성

```
domain IWAN
 vrf default
  master branch
   source-interface Loopback0
   hub 10.8.3.3
  border
   master local
   source-interface Loopback0
```

R10 & R11



Branch site의 라우터 이중화 구성

Cisco Connect

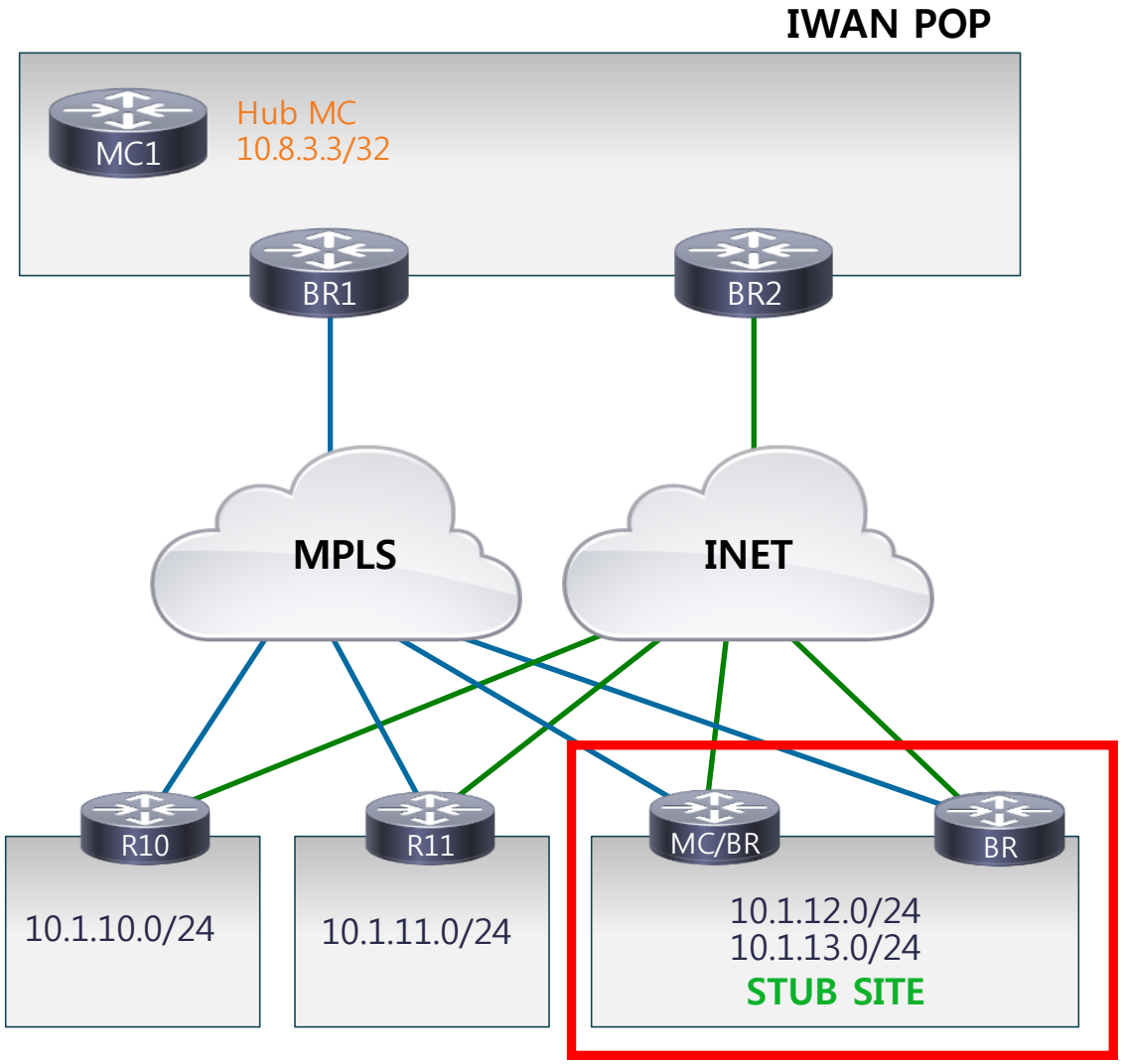
R12

```
domain IWAN
 vrf default
  master branch
   source-interface Loopback0
   hub 10.8.3.3
  border
   master local
   source-interface Loopback0
```

R13

```
domain IWAN
 vrf default
  border
   master 10.2.12.12
   source-interface Loopback0
```

- Stub Site로 구성
- **두 개의 BR 중에서 하나의 라우터는 MC로 구성**



PfRv3 – 각 라우터의 Role 정리

Cisco Connect

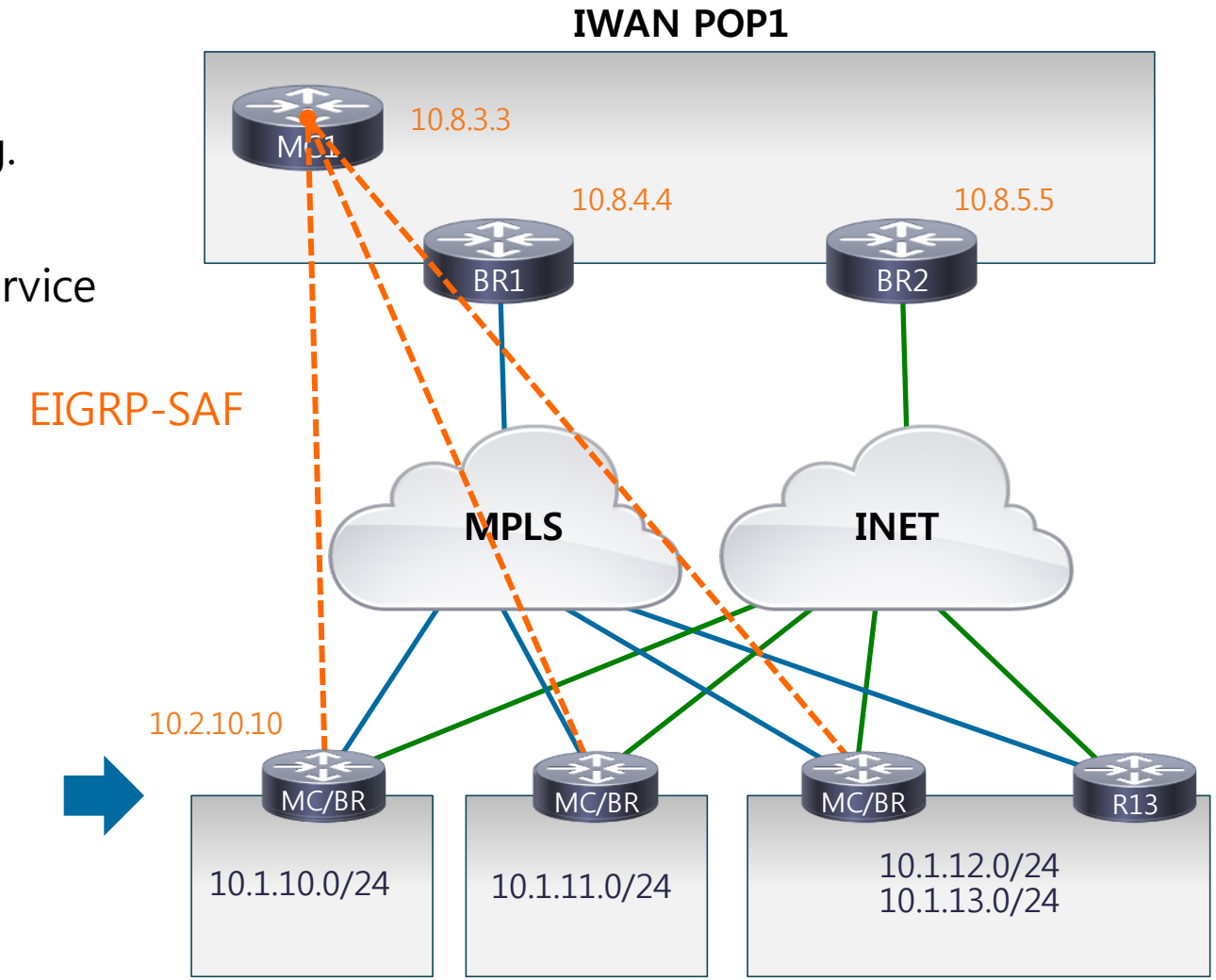
- **Hub의 Master Controller(MC)**: Hub MC는 데이터 센터 또는 HQ에서 구성되며, 모든 정책(policy)에 대한 설정 및 저장. 전체 Site의 Controller로 동작하며, 라우팅 최적 경로에 대한 결정.
- **Hub의 Border Router(BR)**: WAN interface가 있는 경계 라우터, PfRv3가 해당 WAN interface에서 설정됨. 동일한 장비 내에 여러 개의 WAN interface가 존재할 수 있으며, site 내에 여러 개의 BR이 존재 가능.
- **Branch의 Master Controller(MC)**: Policy Configuration이 불필요. Hub MC에서 정책이 다운로드되며 Branch 사이트 내에서 경로를 결정하는 MC로 동작. Configuration내에 Hub MC의 IP address를 포함.
- **Branch의 Border Router(BR)**: Policy Configuration이 불필요. 단지, PfRv3에 대한 설정만 enable. 장비의 WAN interface는 자동으로 감지.

Cisco Connect
Seoul, Korea
April 1-2, 2015

PfRv3 – Discovery

SAF Peering

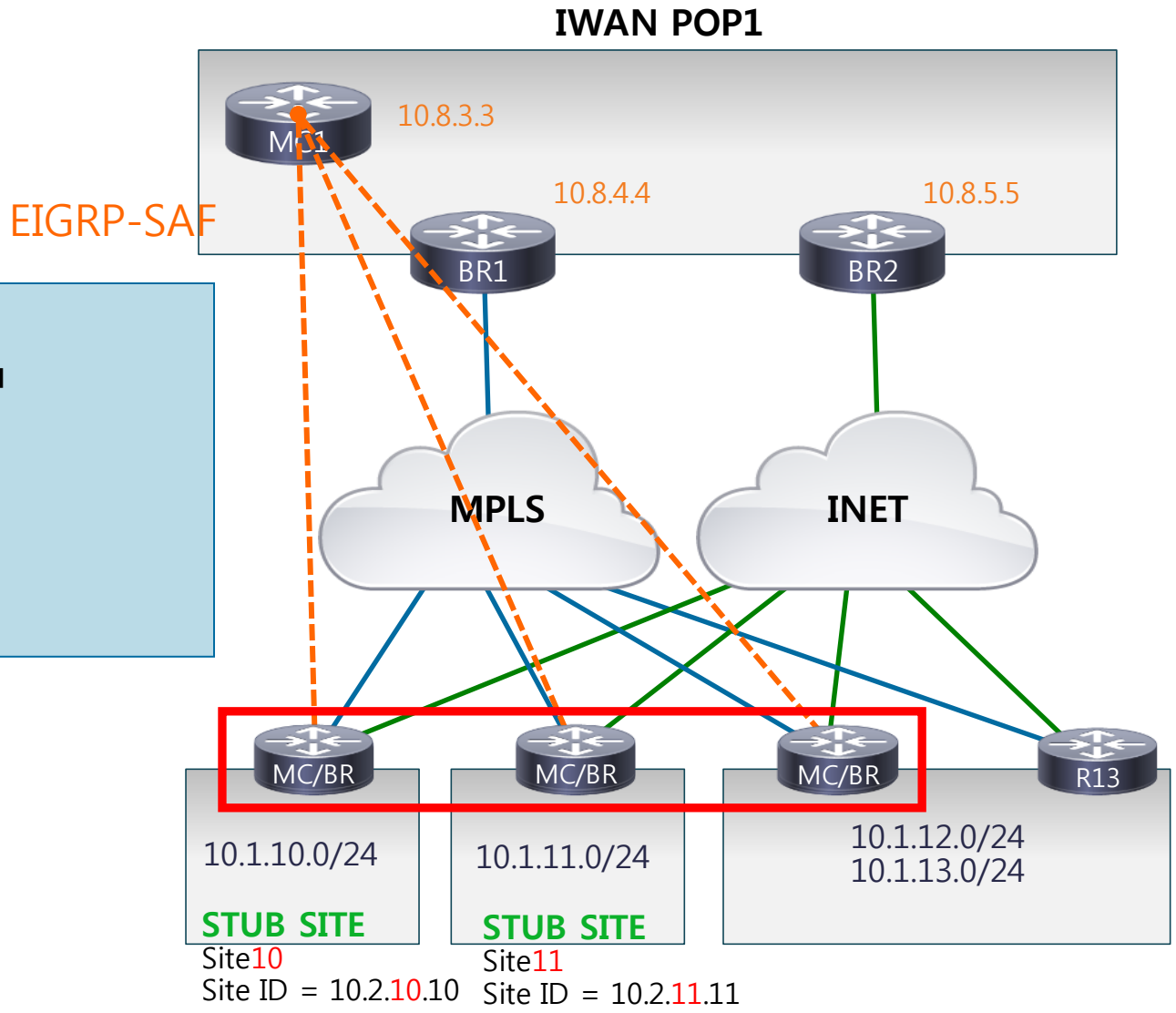
- Hub site의 MC는 들어오는 request를 listening.
- Branch sites의 MC는 Hub site의 MC로 SAF(Service Advertise Framework) peering을 설정
- Peering 시 다음과 같은 value 교환
  - Timers
  - 정책 및 모니터링에 대한 Configuration
  - Site Prefixes



SAF Peering

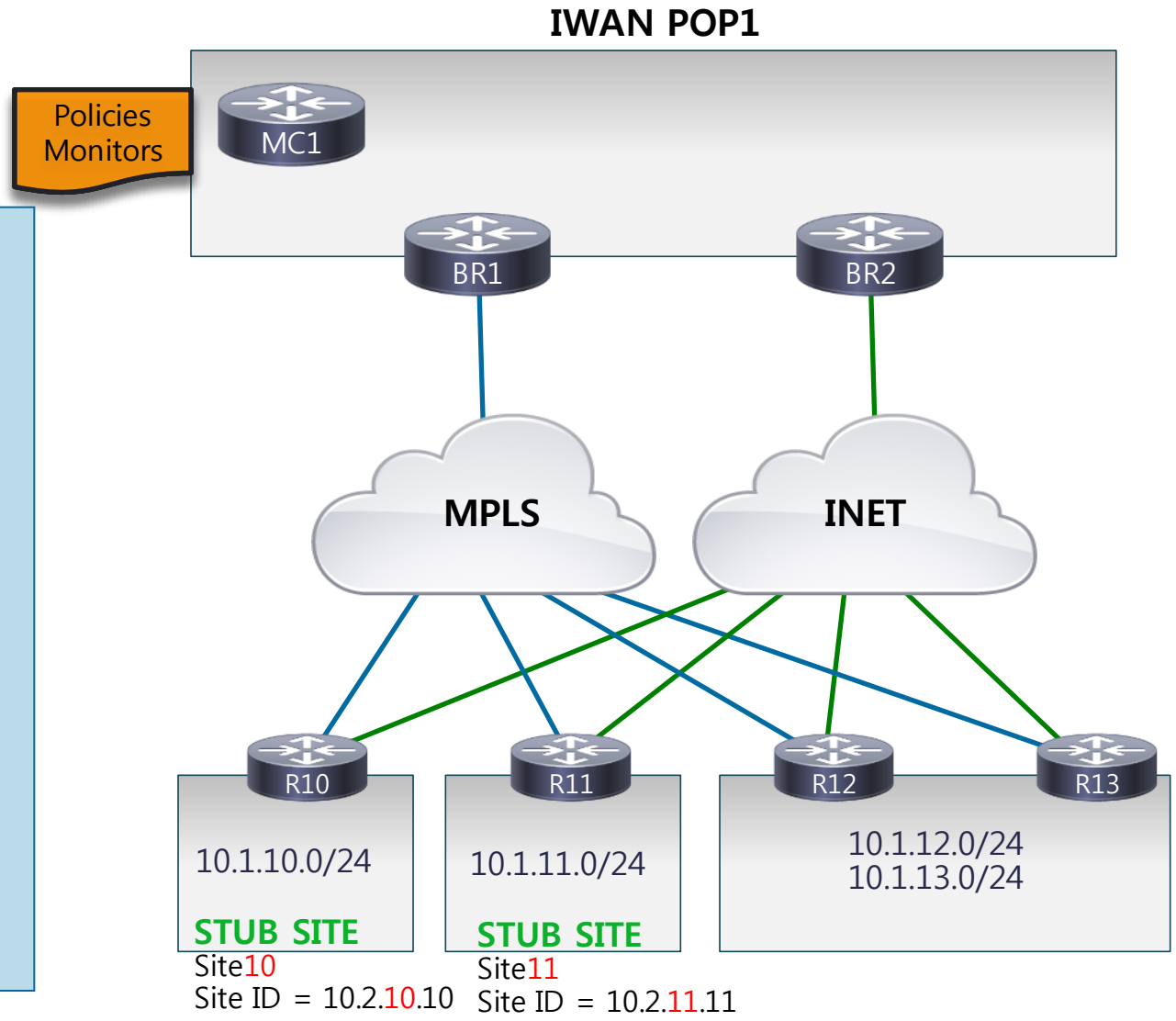
```
MC1#sh eigrp service-family ipv4 neighbors
EIGRP-SFv4 VR(#AUTOCFG#) Service-Family Neighbors for AS(59501)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
5   10.2.10.10              Lo0               513 01:17:12   65   390  0  39
4   10.2.11.11              Lo0               582 01:17:01   59   354  0  40
3   10.2.12.12              Lo0               510 01:17:04   61   366  0  78
2   10.8.4.4                Lo0               538 01:17:04    1   100  0  15
1   10.8.5.5                Lo0               562 01:17:05    4   100  0  18
0   10.9.3.3                Lo0               546 01:17:15    5   100  0  40
MC1#
```

Branch MC에 대한 검색 완료.
Peering 상태 UP



Branch Sites

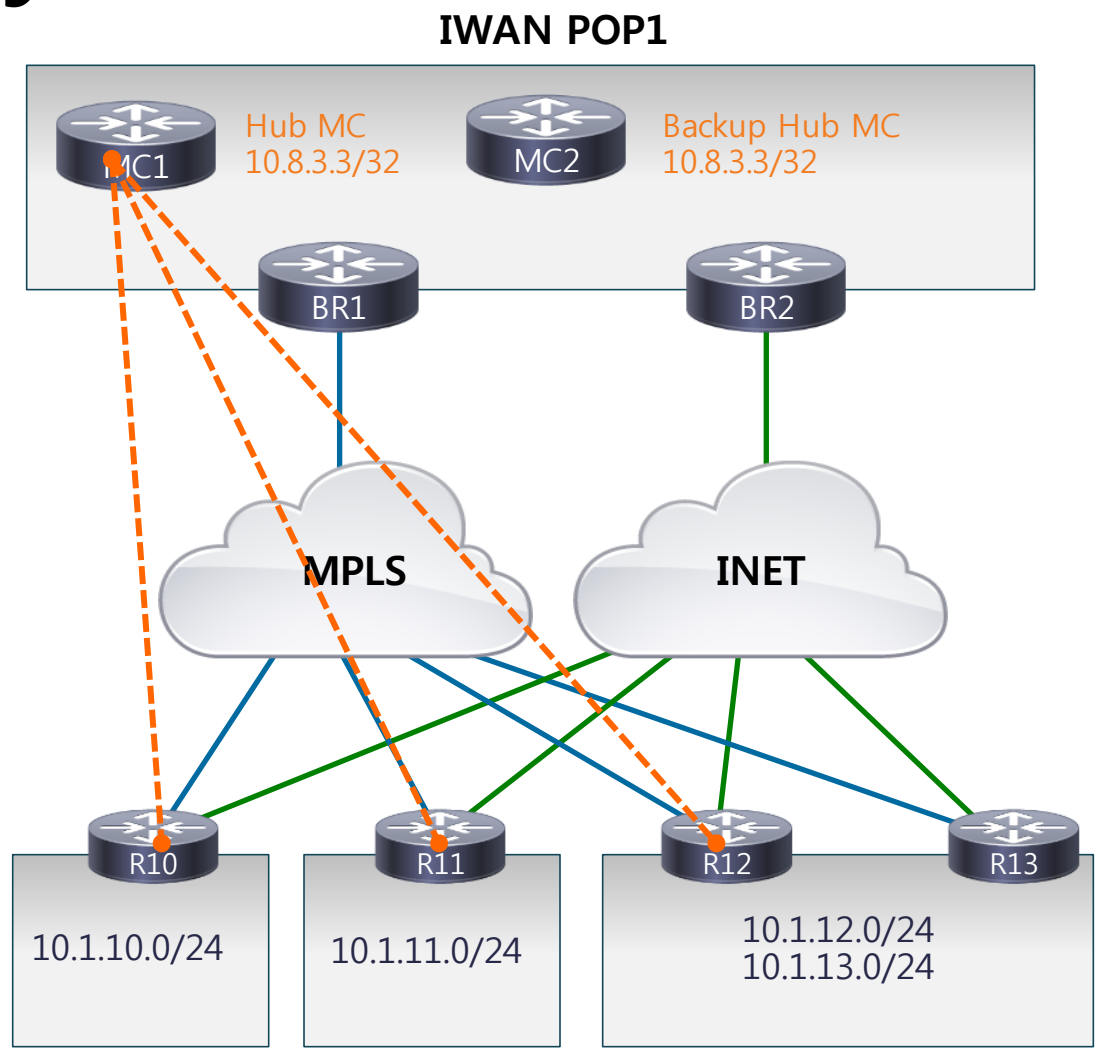
```
R10#sh domain one master policy
------------------------------------------------------------------

 class VOICE sequence 10
   path-preference MPLS fallback INET
   class type: Dscp Based
     match dscp ef policy custom
       priority 2 packet-loss-rate threshold 5.0 percent
       priority 1 one-way-delay threshold 150 msec
       priority 2 byte-loss-rate threshold 5.0 percent
       Number of Traffic classes using this policy: 3

 class VIDEO sequence 20
   path-preference MPLS fallback INET
   class type: Dscp Based
     match dscp af41 policy custom
       priority 2 packet-loss-rate threshold 5.0 percent
       priority 1 one-way-delay threshold 150 msec
       priority 2 byte-loss-rate threshold 5.0 percent
     match dscp cs4 policy custom
       priority 2 packet-loss-rate threshold 5.0 percent
       priority 1 one-way-delay threshold 150 msec
       priority 2 byte-loss-rate threshold 5.0 percent
```



MC 장비 이중화 구성 – Anycast IP

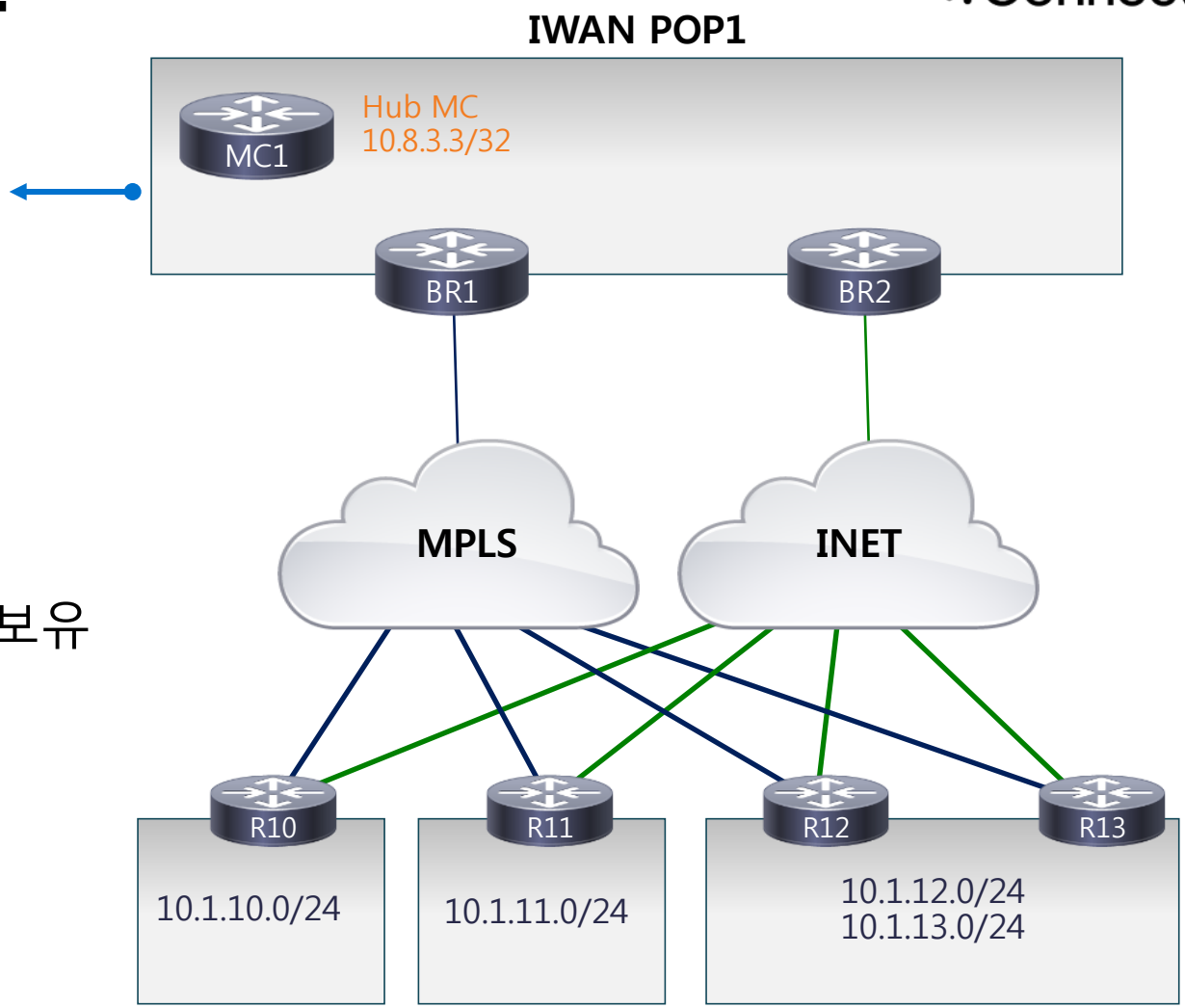
IWAN POP의 MC 구성 가이드

- MC 장비에서 fail이 발생할 경우??
  - 트래픽의 전송은 라우팅 정보를 기반으로 전송 (Packet drop이 발생하지 않음)
  - 지점의 MC 장비는 기존의 configuration 및 정책을 계속 유지
  - 트래픽의 optimization 기능 유지
- Hub site에서 추가적인 Backup MC 구성 필요
  - 추가적인 정책 및 configuration 변경이 불가
- Primary MC와 동일한 IP address 설정
- BR과 지점의 MC에 대한 Primary MC 연결 상태에 대한 확인은 라우팅 프로토콜을 사용
- Stateless redundancy
  - Backup MC는 traffic의 상태를 learning



Site Prefix 데이터베이스

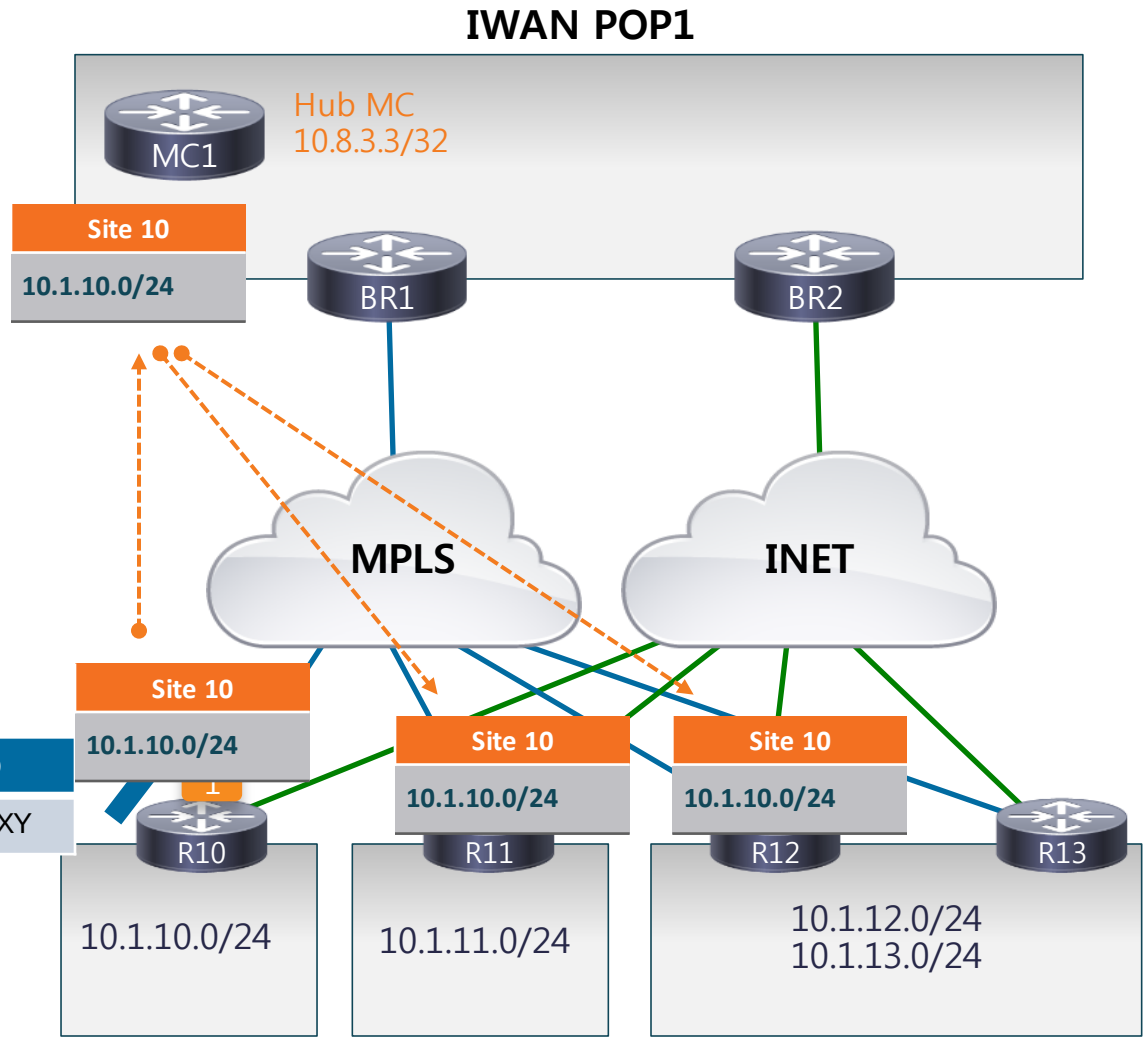
Site	Prefix List
Hub	10.8.0.0/16
R10	10.1.10.0/24
R11	10.1.11.0/24
R12	10.1.12.0/24
R12	10.1.13.0/24



- 도메인 내의 모든 MC는 Site Prefix database를 보유
- Site와 prefix 간의 mapping을 제공
- 2 options:
  - Static: 사용자가 직접 Prefix database 입력/관리
  - Automatic Learning: 자동 검색을 통한 learning

Site Prefix – 자동 학습 기능

- Performance monitor를 통한 Source Prefix 및 Mask 정보 수집
- Monitor interval: 30초
- BR라우터는 Local내의 MC로 정보 전달
- MC는 Peering을 맺고 있는 모든 peer로 수집된 정보를 전달



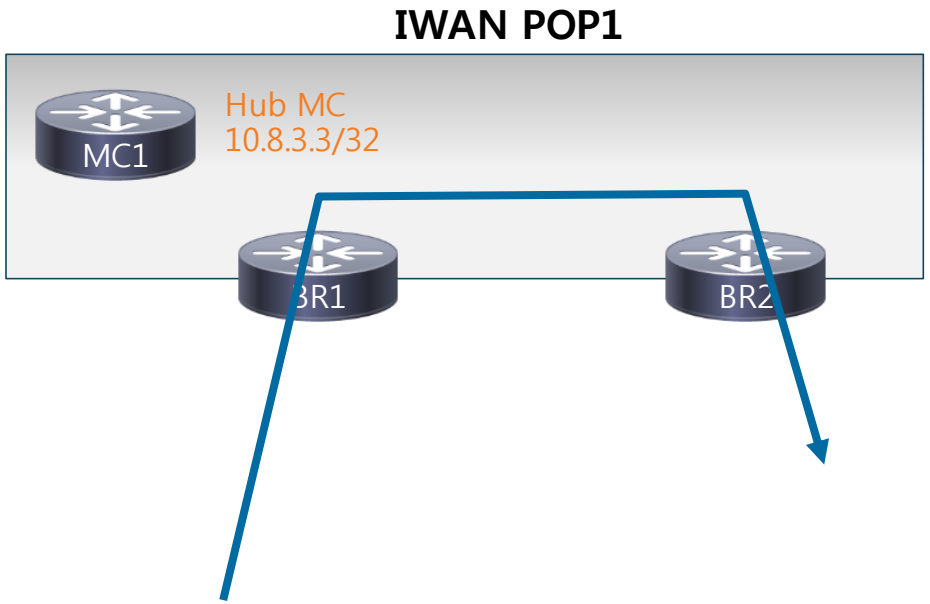
Source	Destination	DSCP	App
10.1.10.200	10.8.1.200	AF41	AppXY

R10 MC	Site-Pfx	Mask
	10.1.10.0	/24

Site Prefixes – 수동 설정

- 자동 검색/학습을 하지 않고 관리자를 통해서 직접 site prefix에 대한 정보를 설정
- 해당 configuration은 site가 transit site로 사용될 때 site내에서 사용
  - 예를 들어, Site A와 Site B로 Hub site를 통해서 트래픽을 전달할 때, 해당 hub site는 transit site로 동작.
  - **수동 설정을 통해서 site A의 prefix정보를 hub site의 prefix정보로 잘못 인식하는 것을 방지**

```
domain IWAN
 vrf default
  master hub
   source-interface Loopback0
   site-prefixes prefix-list DC1_PREFIX
!
ip prefix-list DC1_PREFIX seq 10 permit 10.8.0.0/16
!
```



Source	Destination	DSCP	App
10.1.10.200	10.1.11.200	AF41	AppXY

Cisco Connect
Seoul, Korea
April 1-2, 2015

PfRv3 – Monitoring

TC Bandwidth 수집

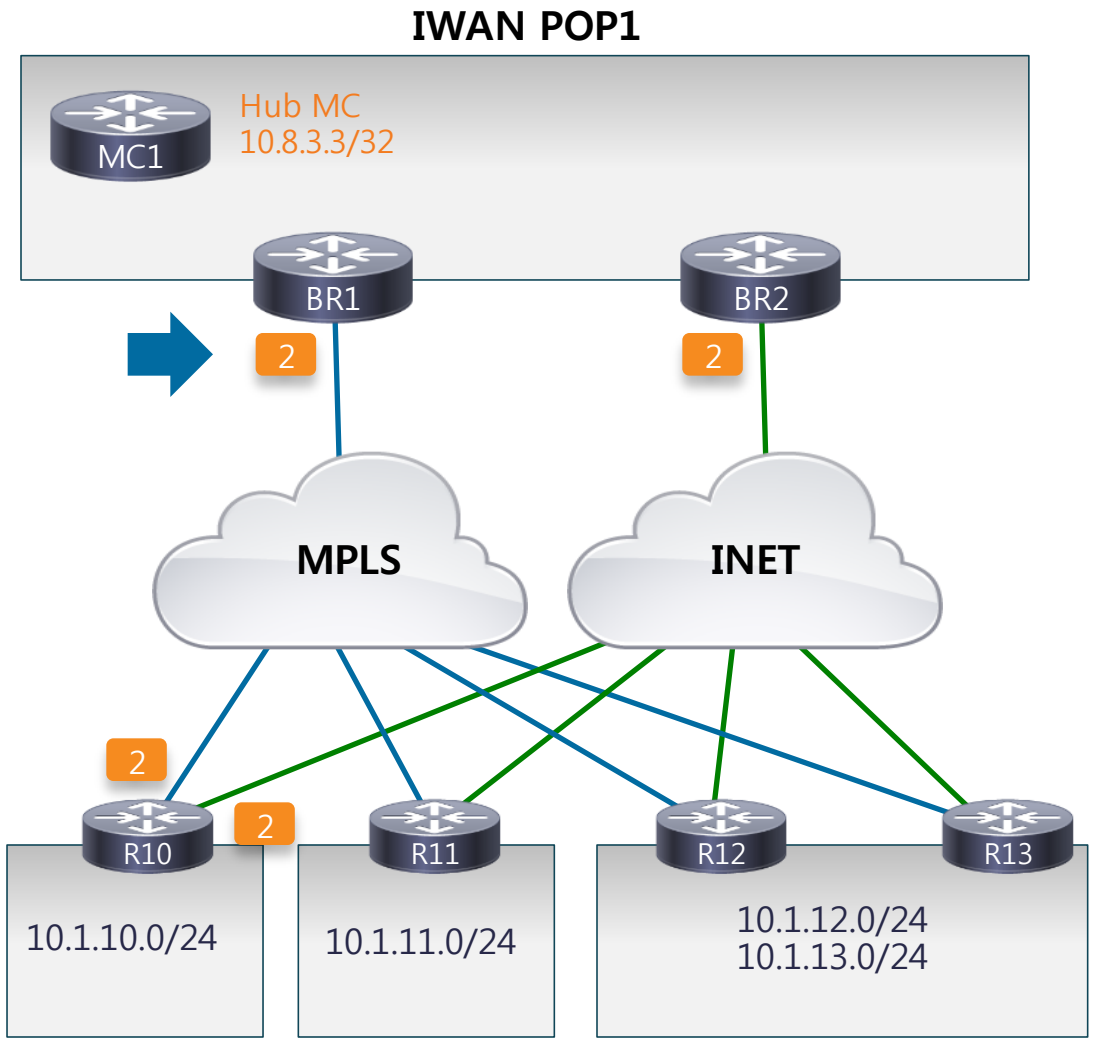
PMI: [Egress-Aggregate] - #2

Trigger NBAR: no/yes

Key Fields
- ipv4 destination prefix,
- ipv4 destination mask,
- pfr site destination prefix ipv4
- pfr site destination prefix mask ipv4
- [application id]
- ip dscp
- interface output

Non-Key Fields
- counter bytes long
- counter packet long
- timestamp absolute monitoring-interval start

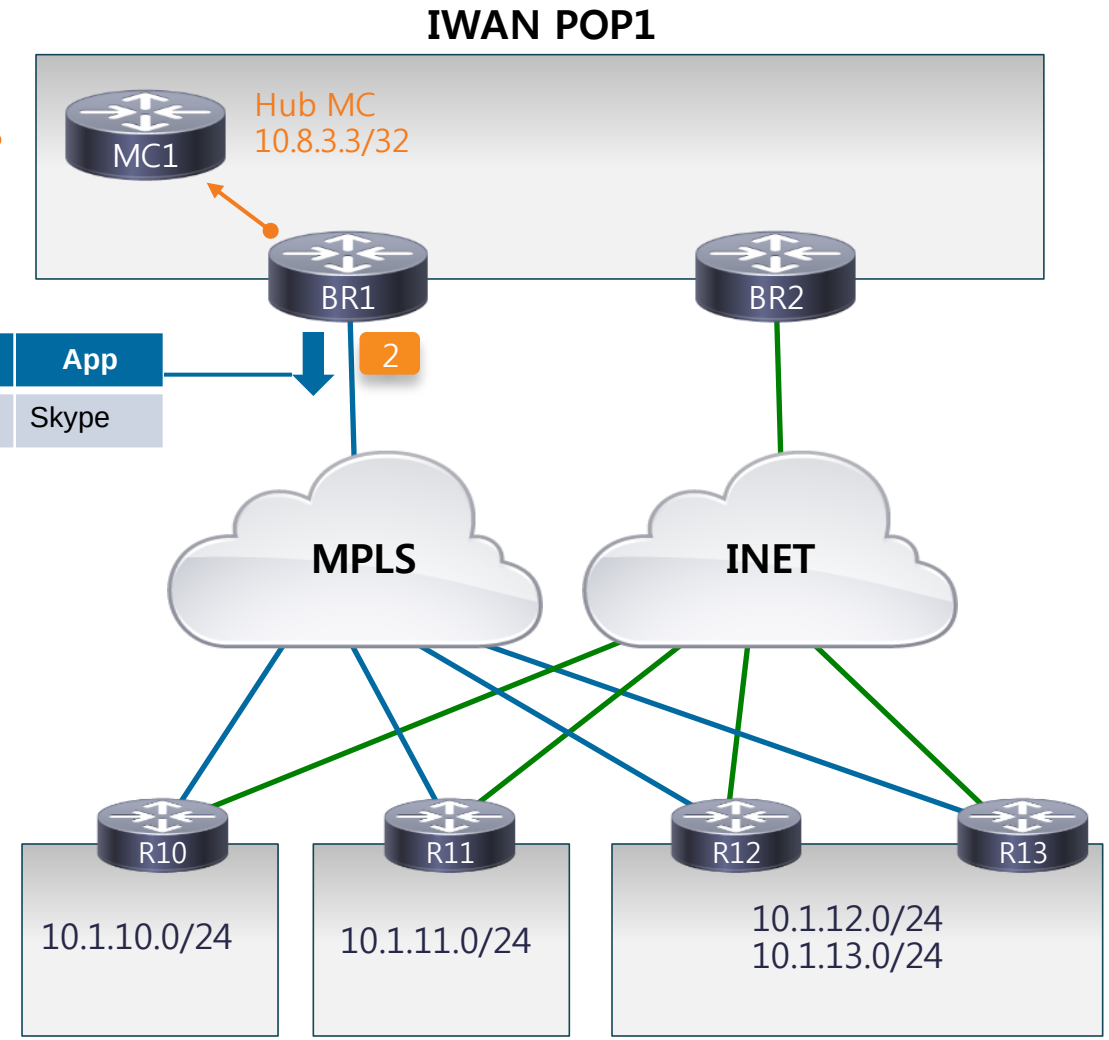
- Aggregate Bandwidth Per TC
- 대역폭은 egress방향으로 수집
- Using monitor #2
- Traffic class당 Bandwidth 수집



TC Bandwidth 수집

MC1	Dst-Site-Pfx	Dst-Site-id	App	DSCP	State	BW	BR	Exit
	10.1.10.0	10.2.10.10	Skype	AF41	CN	24	BR1	Tu10

Source	Destination	DSCP	App
10.8.1.200	10.1.10.200	AF41	Skype

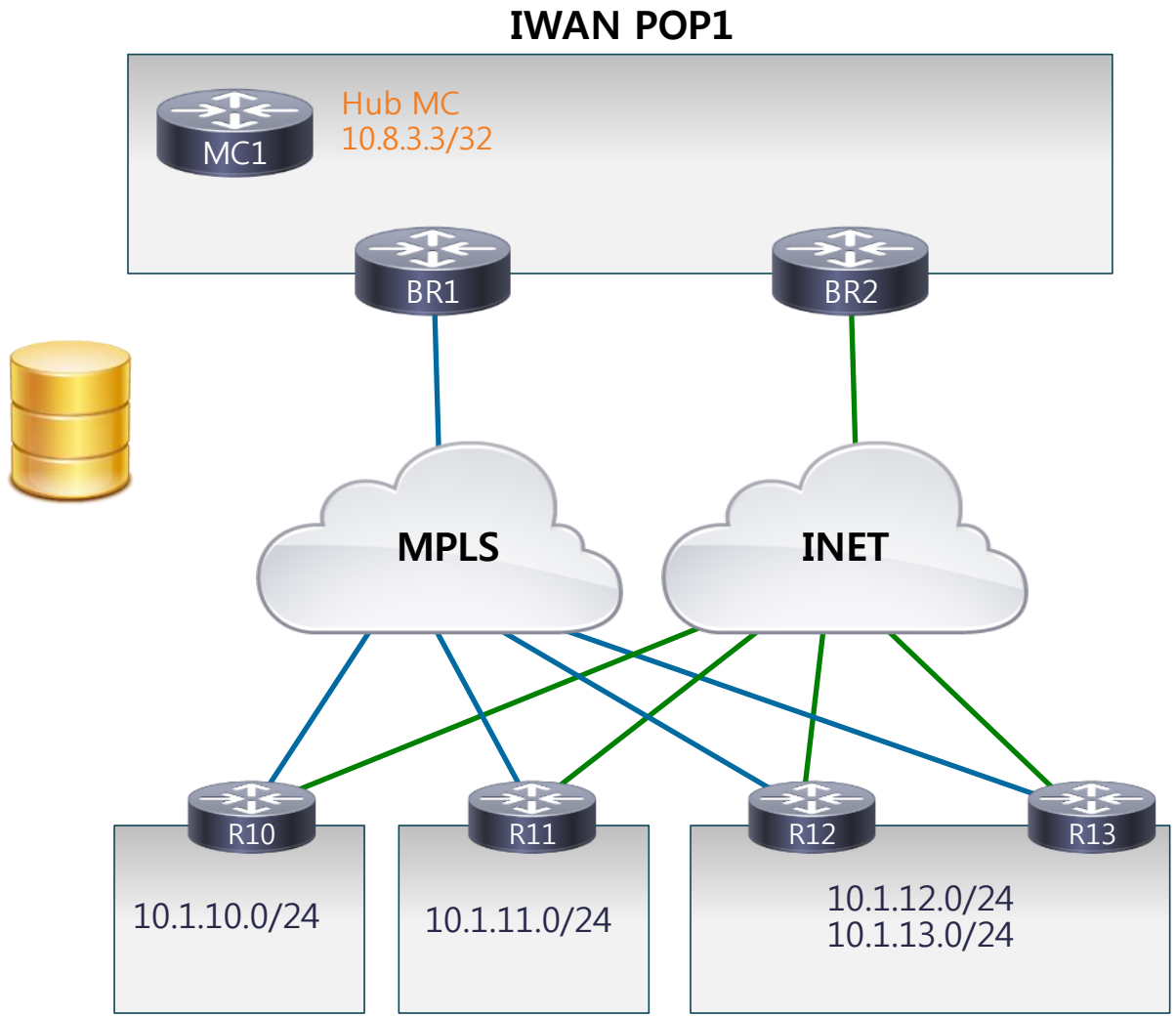


- 외부로 전송되는 트래픽
- 외부 인터페이스의 egress방향으로 Performance monitor에 의해 수집
- BR은 로컬의 MC로 reporting
- Destination Site ID와 mapping
- Monitor interval (30초)

Traffic Class 데이터베이스

Dst-Site-Pfx	Dst-Site-id	App	DSCP	State	BR	Exit
10.1.10.0	R10	Skype	AF41	CN		
10.1.10.0	R10	N/A	EF	CN		
10.1.10.0	R10	N/A	AF31	CN		
10.1.10.0	R10	N/A	0	CN		
10.1.11.0	R11	N/A	EF	CN		
10.1.11.0	R11	N/A	AF31	CN		
10.1.11.0	R11	N/A	0	CN		
10.1.12.0	R12	N/A	0	CN		

- 모든 site 내의 트래픽에 대해 동일 process로 동작
- 해당 데이터베이스는 대역폭, Destination Site, BR, 사용되는 외부경로에 대한 정보를 포함

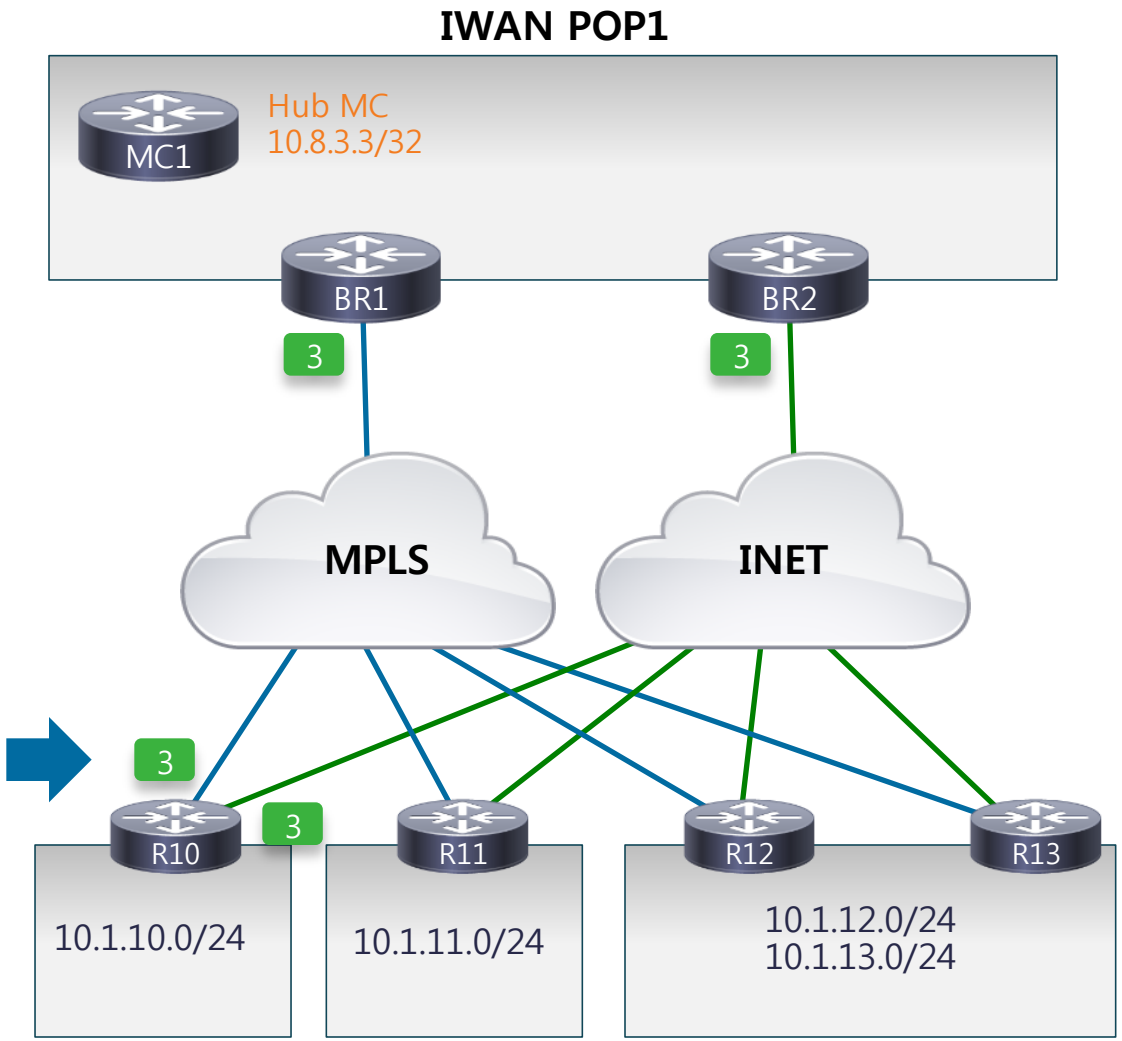


Ingress Performance Monitor

PMI [Ingress-per-DSCP] - #3

Key Fields
- pfr site source id ipv4
- pfr site destination id ipv4
- ip dscp
- Interface input
- policy performance-monitor classification hierarchy

Non-Key Fields
- transport packets lost rate
- transport bytes lost rate
- pfr one-way-delay
- network delay average
- transport rtp jitter inter arrival mean
- counter bytes long
- counter packets long
- timestamp absolute monitoring-interval start

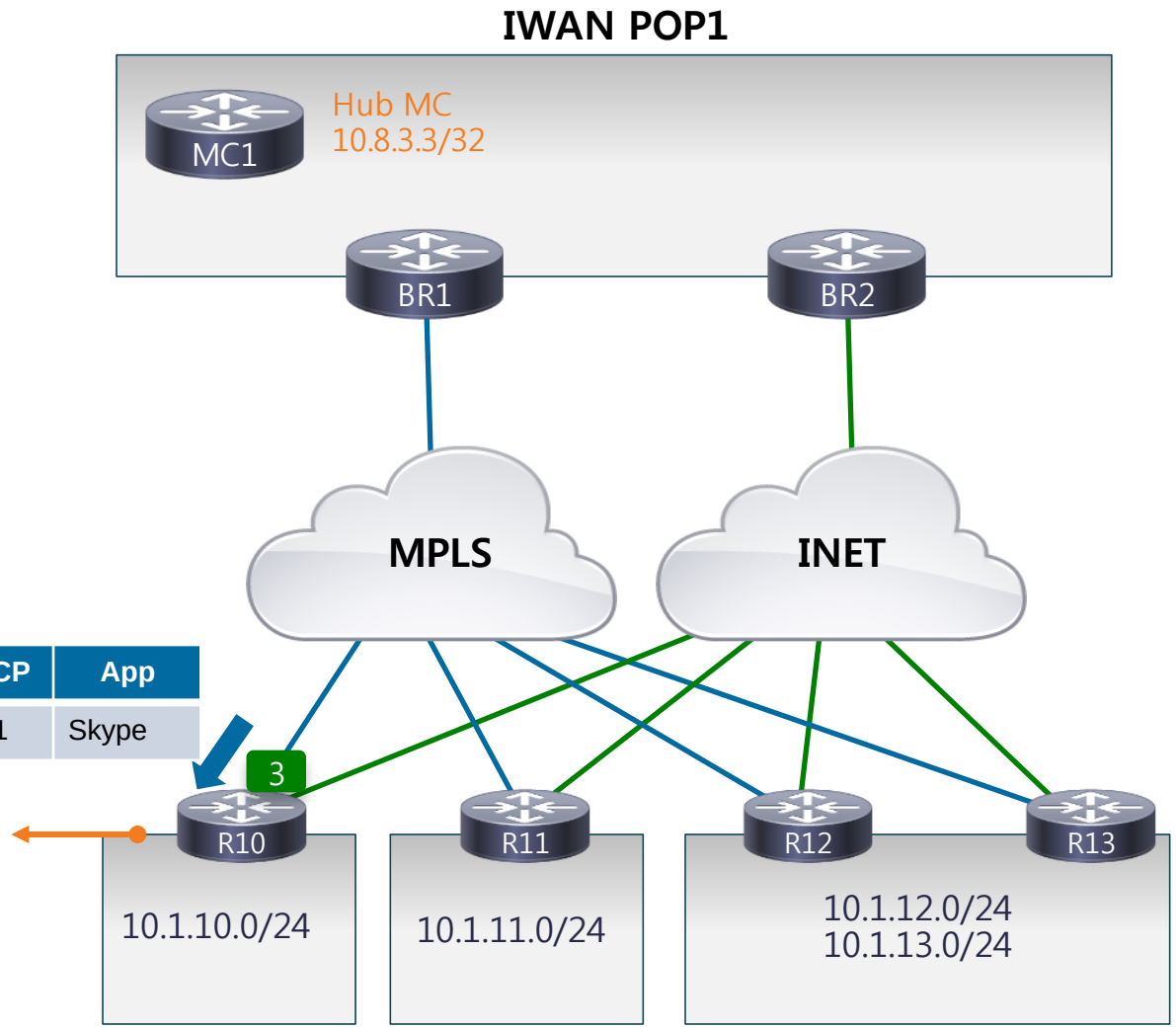


- Ingress 방향에 대한 성능 측정:
  - Actual Traffic
  - Smart Probes if no traffic
- DSCP 및 Site 별 performance metric을 측정

Destination Site – Ingress Traffic

Channel Performance

- Destination site에서 트래픽 플로우를 수집
- 성능 모니터가 Metric을 수집
- **Per Channel**
- 기본 Monitor interval은 30초



Source	Destination	DSCP	App
10.8.1.200	10.1.10.200	AF41	Skype

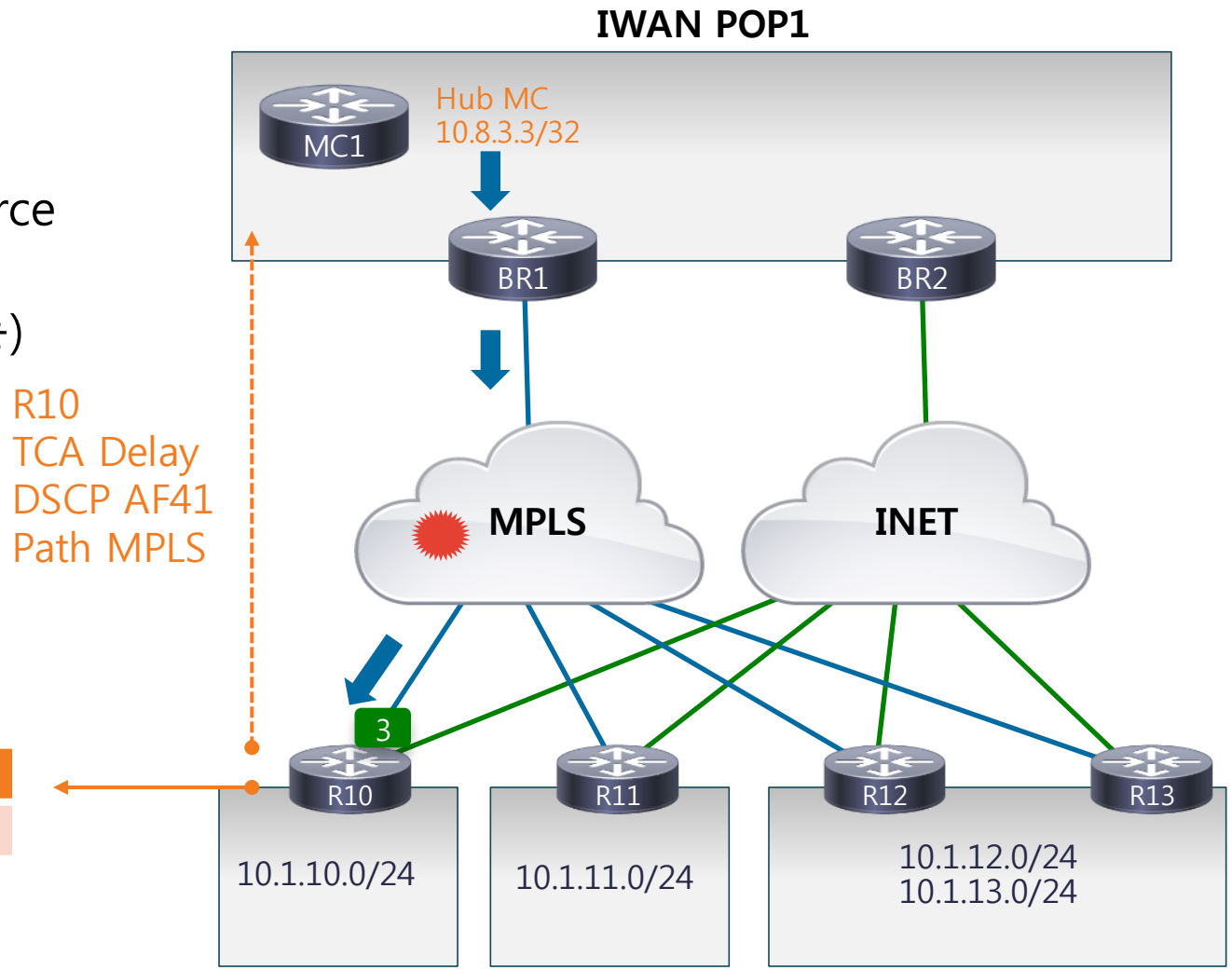
R10 MC	Channel	Dst-Site-id	Path	DSCP	BW	Delay	Jitter	Loss
	5	Hub	Tu1	AF41	24	51	2	1

Cisco Connect
Seoul, Korea
April 1-2, 2015

PfRv3 – Performance Violation

Performance Violation

- 특정 채널에서 violation이 발생했을 때, performance notification을 전달
  - BR의 Ingress monitor에서 생성하여, Source Site의 BR로 전달
  - 기본 monitoring interval (30초, 변경 가능)
  - 모든 external interface를 통해 전달

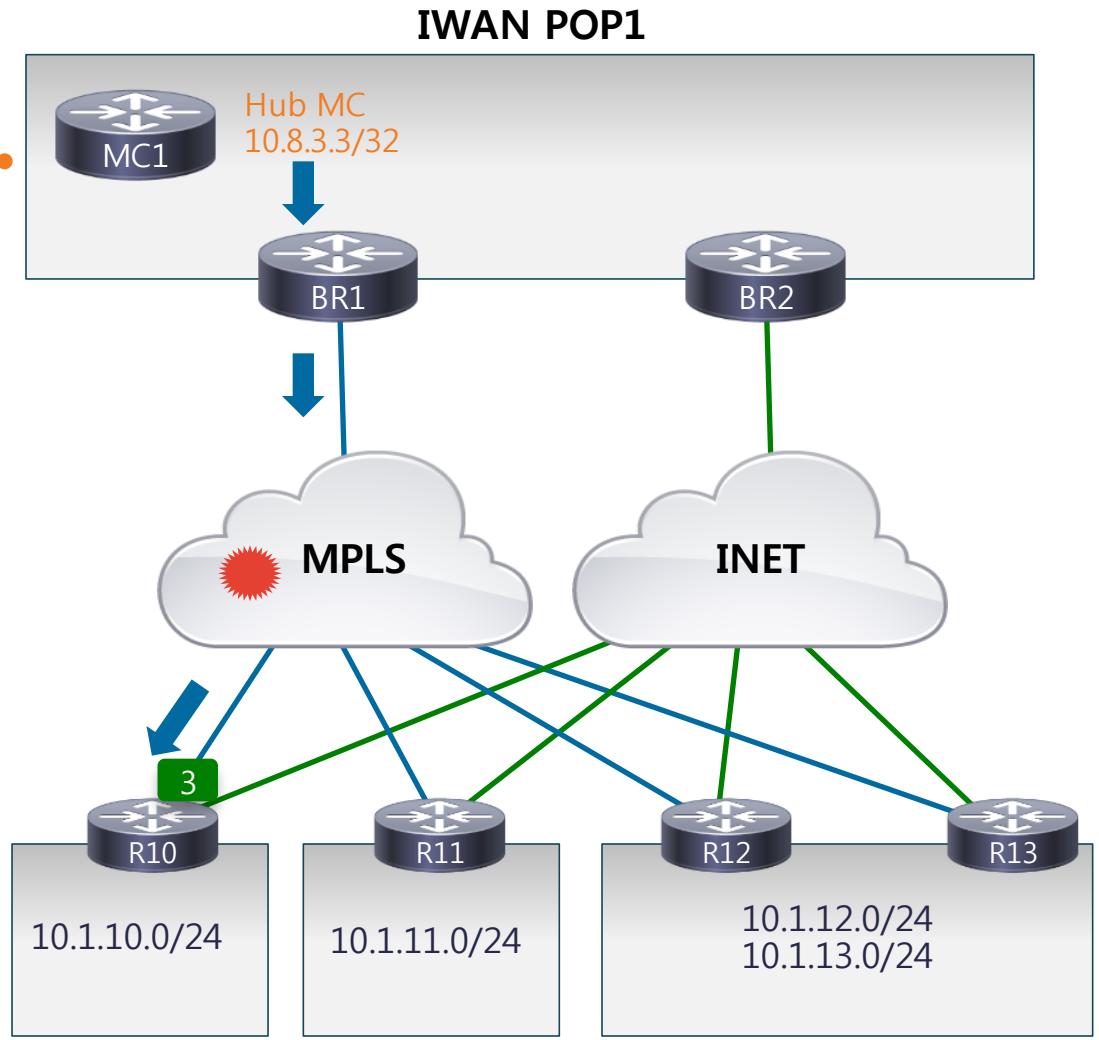


R10	Channel	Dst-Site-id	DSCP	Path	BW	Delay	Jitter	Loss
	5	Hub	AF41	Tu1	24	250	2	1

Performance Violation

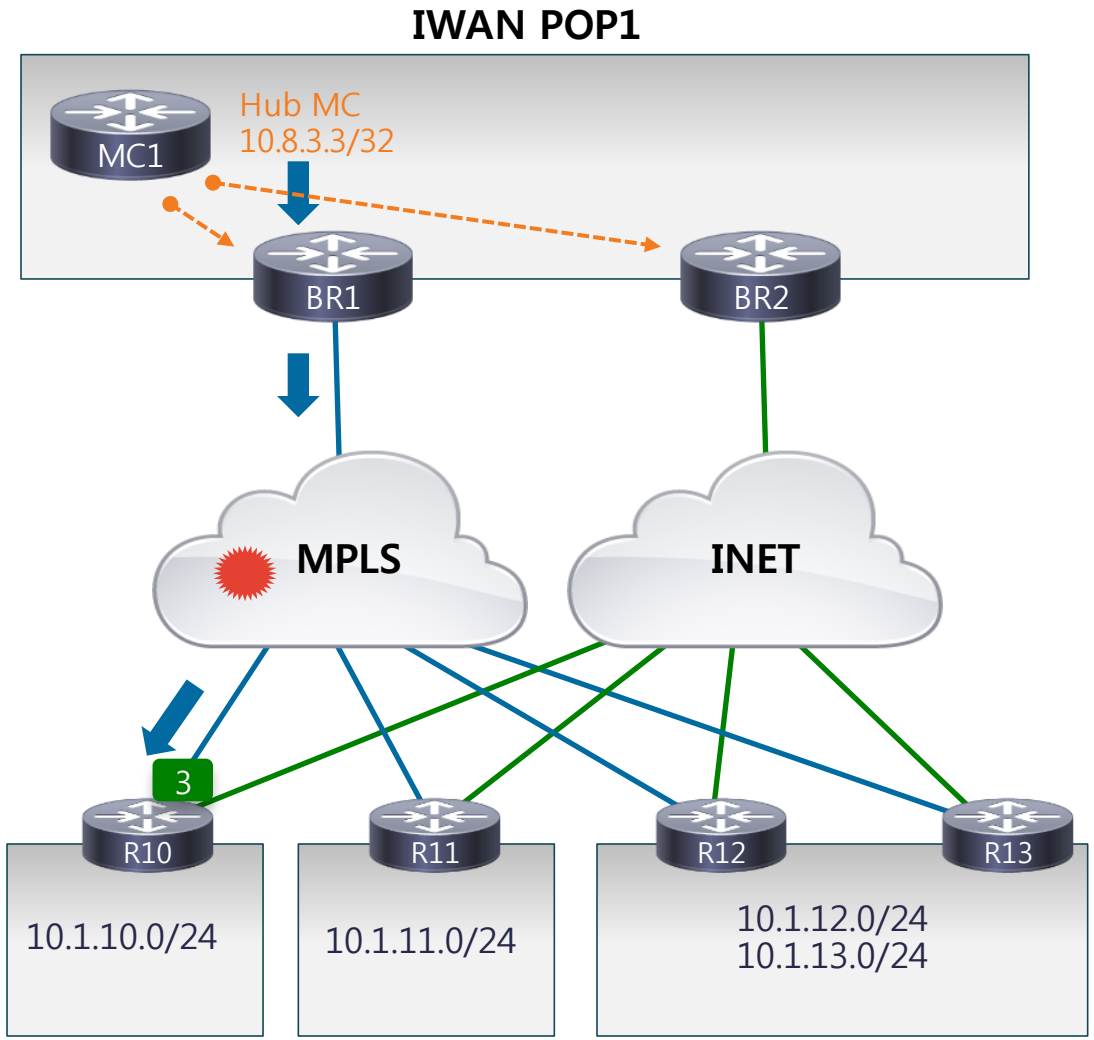
Dst-Site-Pfx	Dst-Site-id	App	DSCP	State	BR	Exit
10.1.10.0	R10	Skype	AF41	CN	BR1	Tu1
10.1.10.0	R10	N/A	AF41	CN	BR1	Tu1
10.1.10.0	R10	N/A	AF31	CN	BR1	Tu1
10.1.10.0	R10	N/A	0	CN	BR2	Tu2
10.1.11.0	R11	N/A	EF	CN	BR1	Tu1
10.1.11.0	R11	N/A	AF31	CN	BR1	Tu1
10.1.11.0	R11	N/A	0	CN	BR2	Tu2
10.1.12.0	R12	N/A	0	CN	BR2	Tu2

R10
TCA Delay
DSCP EF
Path MPLS



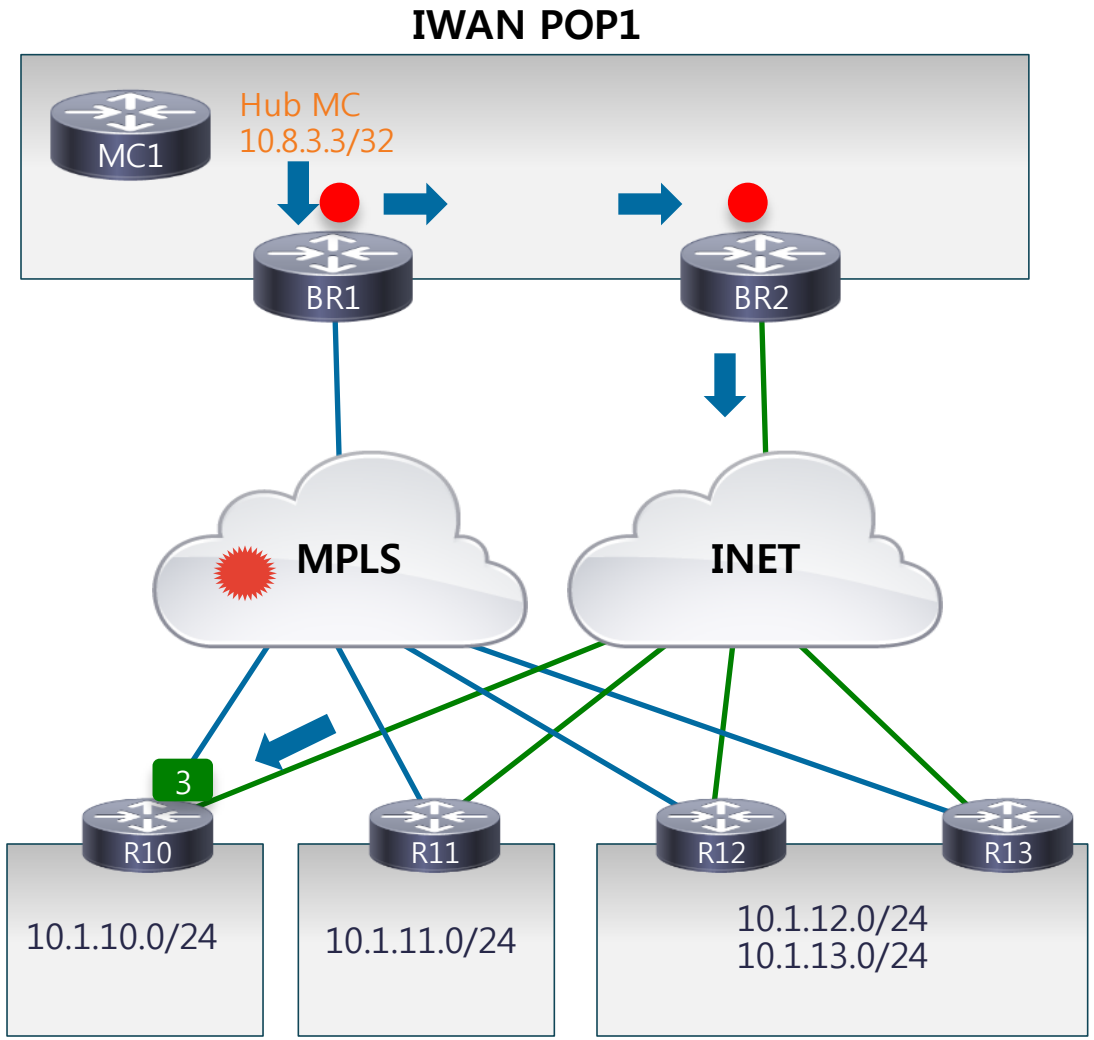
Rerouting을 위한 정책 적용 결정

- MC는 영향을 받은 TC(Traffic Class)에 대한 새로운 경로를 계산
- MC는 BR쪽으로 새로운 경로로 수정할 것을 전달



Reroute TC – 경로 변경

- 데이터 플레인 내의 forwarding변경
- 외부 interface를 제외한 모든 interface상에서 설정
- Lookup per packet - output-if/next hop retrieved
  - Packet Forwarded
  - If no entry – Uses FIB entry
- TC 플로우는 BR간의 자동 mGRE 터널을 통해 새로운 경로로 redirection
- 라우팅 테이블에 대한 변경을 없음

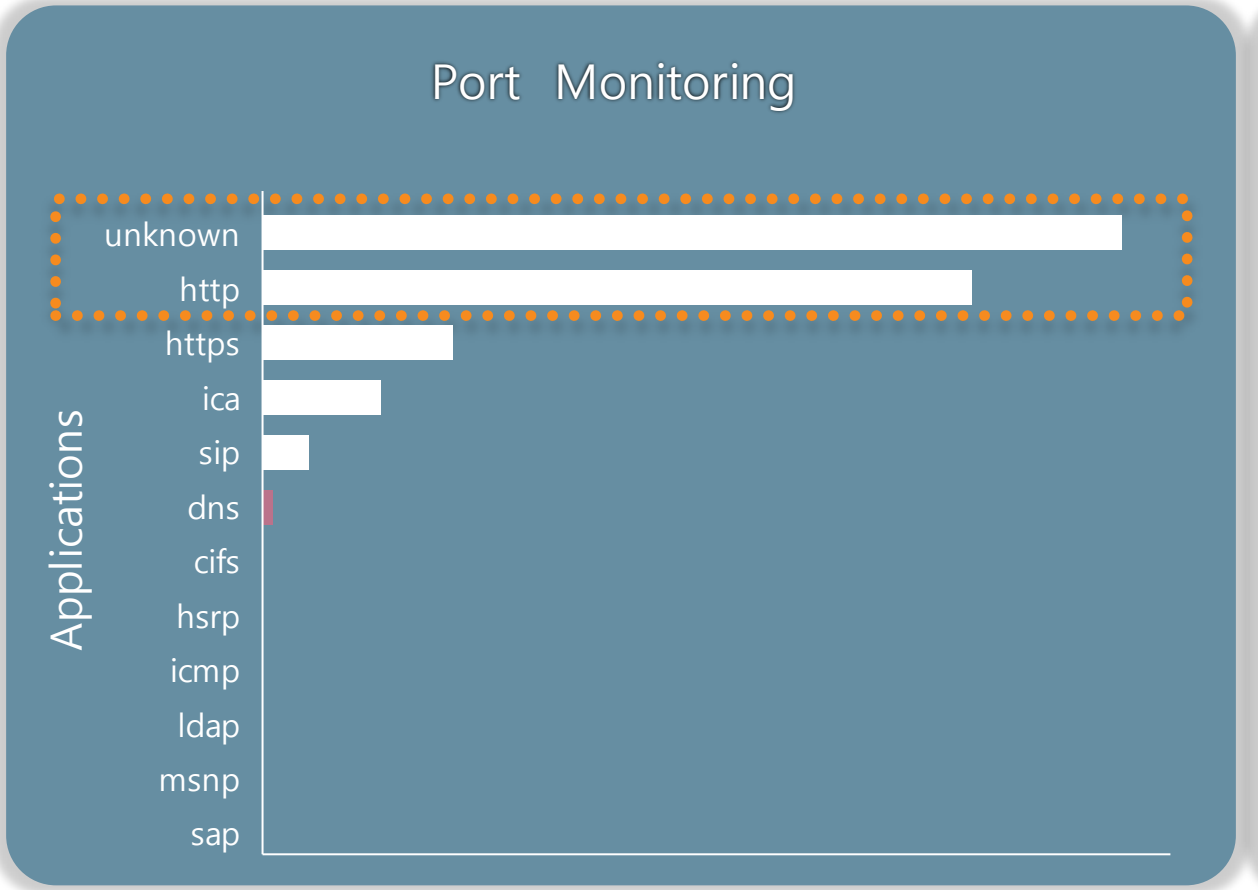


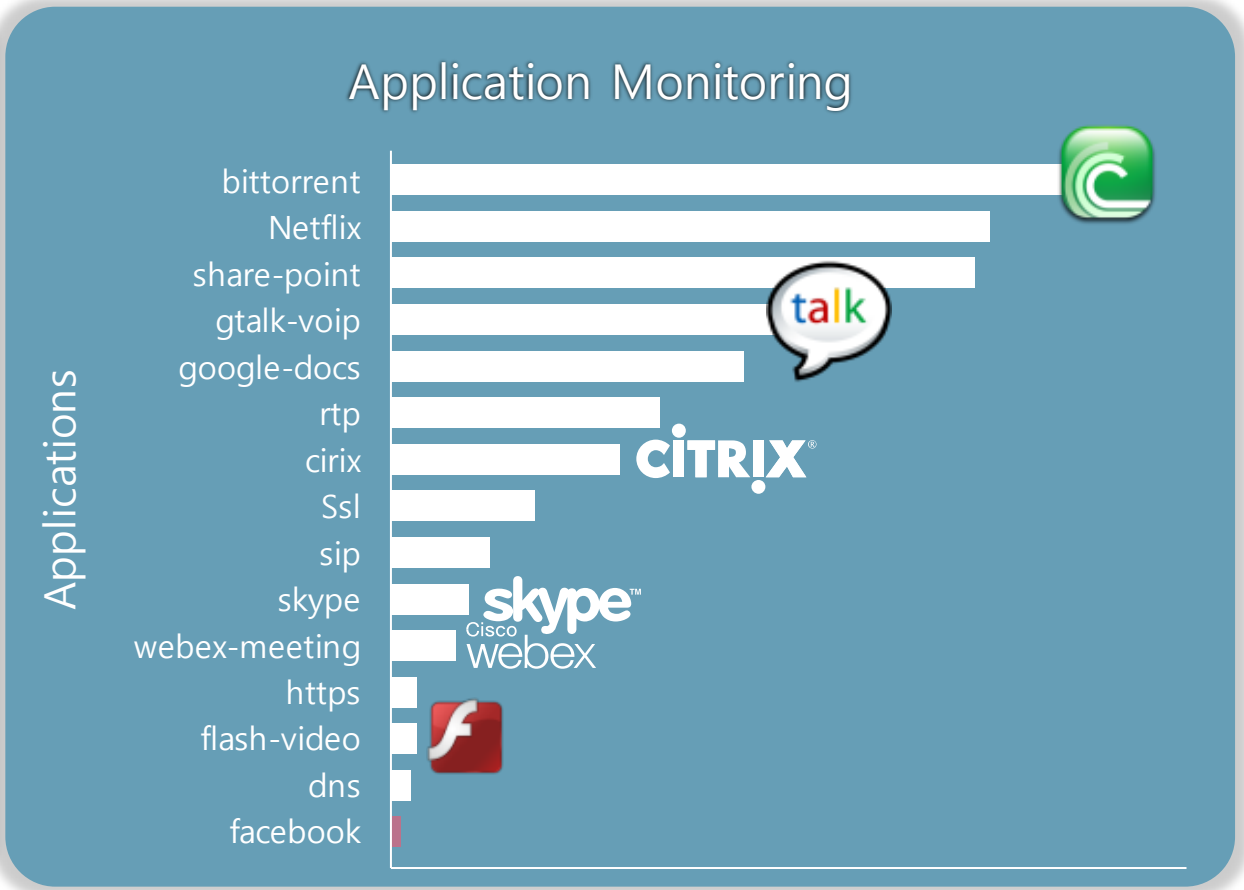
Cisco Connect
Seoul, Korea
April 1-2, 2015

4. Application Optimization

지금 네트워크의 모니터링은 잘 되십니까?

Cisco Connect





Cisco AVC with NBAR2 Provides Deep Packet Inspection at the Application Level

Application Visibility

통합 성능 모니터링 (Cisco AVC)

Cisco AVC

개별 Probe의 불필요

- Deep Packet Inspection 지원
- 음성/비디오/주요App/기타 트래픽에 대한 passive monitoring
- 추가적인 HW에 대한 불필요 (included in AX license)

스마트한 네트워크 확장 용량 계산

- 회선 대역폭에 대한 효율적인 사용
- 지점 별, 어플리케이션 별 리포팅 제공

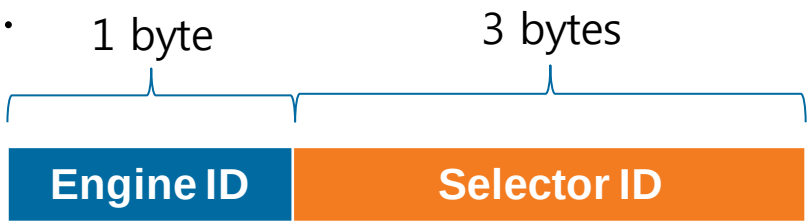
약 1000개 이상의 application 관리

- 복잡한 IP/포트 기반의 ACL 불필요
- 클라우드 기반의 Application을 인식하기 위한 HTTP flow분석 제공

60% of IT Professionals Cite Performance as Key Challenge for Cloud

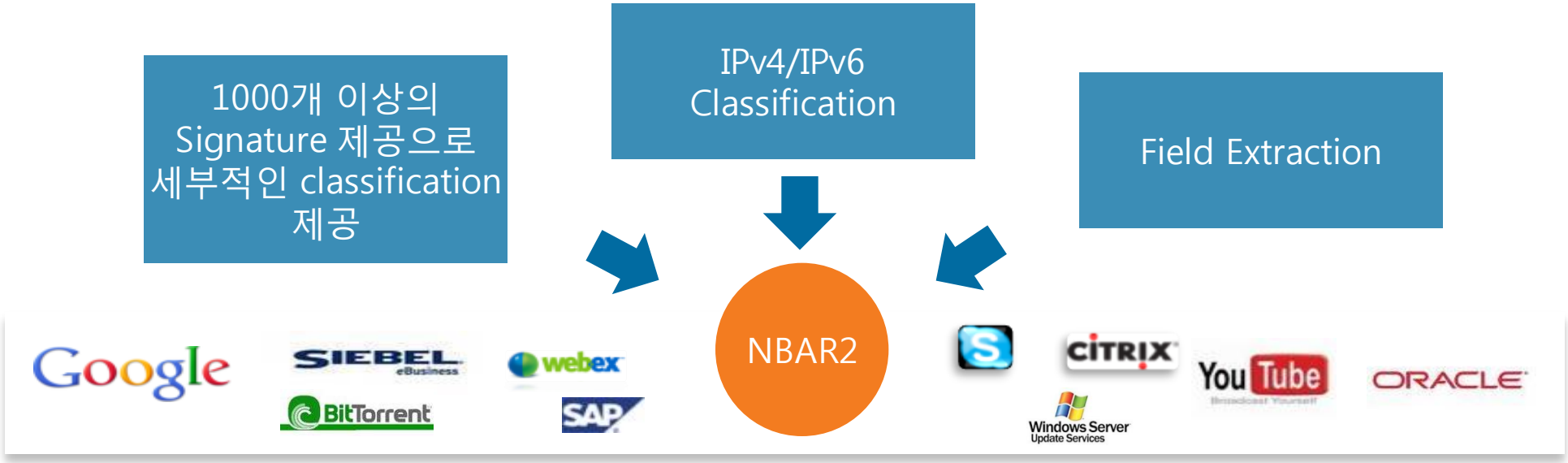
Global Application ID

- Global Application Id
  : 시스코 장비의 모든 DPI 엔진에서 사용되는 application 별 고유 ID.
  - IOS ISR, IOS-XE ASR1k, NAM module, IOS Firewall 지원
  - WAAS Express 지원 예정
- 독자적인 Cisco format으로 아래 표준을 기반으로 함.
  - On a L3 protocol (IANA protocol type)
  - On a L4 protocol (IANA well known ports)
  - On a L2 protocol (Ethertype)
  - On a L7 application/protocol: (NO IANA registry for L7)
- IETF의 표준화 진행
  - "Export of Application Information in IPFIX", RFC 6759



Deep Packet Inspection

Network Based (NBAR2)



- DPI 엔진을 통해서 부가적인 어플리케이션 분류 및 Field Extraction 제공
- 어플리케이션 관리의 단순화를 위한 categorization
- IOS에 대한 upgrade/reload 없이 Protocol Pack 추가 가능

어플리케이션 관리의 단순화

Cisco Connect

NBAR2 Attributes

- NBAR2 attribute를 통해 유사한 애플리케이션들을 그룹화하여 관리
- 어플리케이션 그룹에 대한 리포팅과 QoS classification 단순화를 위해 사용
- 각 어플리케이션 당 6개의 pre-defined attributes 제공 (사용자 지정 가능)

Category	동일 기능을 가진 애플리케이션의 첫 그룹 레벨
Sub-category	동일 기능을 가진 애플리케이션의 두 번째 그룹 레벨
Application-group	알려진 애플리케이션을 기반으로 한 그룹
P2P-technology?	Peer-to-Peer 애플리케이션 여부 표시
Encrypted?	애플리케이션의 암화화 여부 표시
Tunneled?	애플리케이션의 터널 사용 여부 표시

NBAR2 – 어플리케이션 속성

어플리케이션 속성 예제

```
R2#sh ip nbar protocol-attribute citrix
          Protocol Name :  citrix
               category :  business-and-productivity-tools
           sub-category :  terminal
       application-group :  other
         p2p-technology :  p2p-tech-no
                 tunnel :  tunnel-no
              encrypted :  encrypted-yes


R2#
```

Application name

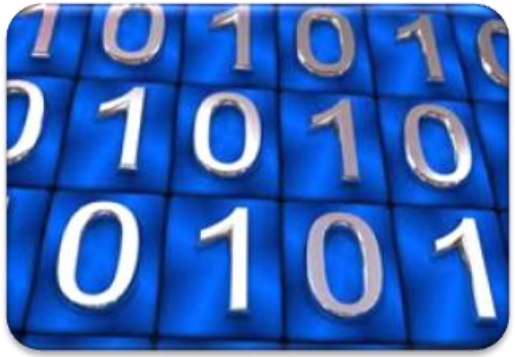
```
R2#show ip nbar protocol-attribute webex-meeting
          Protocol Name :  webex-meeting
               category :  voice-and-video
           sub-category :  voice-video-chat-collaboration
       application-group :  webex-group
         p2p-technology :  p2p-tech-no
                 tunnel :  tunnel-no
              encrypted :  encrypted-yes


R2#
```

Application name

Pre-defined Attributes

사용자 정의 NBAR2 Rule 생성

Customized Application



- **Port**
  - TCP or port
  - 16 static ports per application
  - Range of ports (최대 1000개)
- **IP and Port**
  - IOS-XE 3.12
  - IOS 15.4(3)M

- **Payload**
  - TCP/UDP payload의 첫 255bytes에 대한 검색
  - ASCII (16 characters)
  - Hex (4 bytes)
  - Decimal (1-4294967295)
  - Variable (4 bytes Hex)

- **HTTP**
  - URI regex
  - Host regex

URL 기반의 사용자 정의

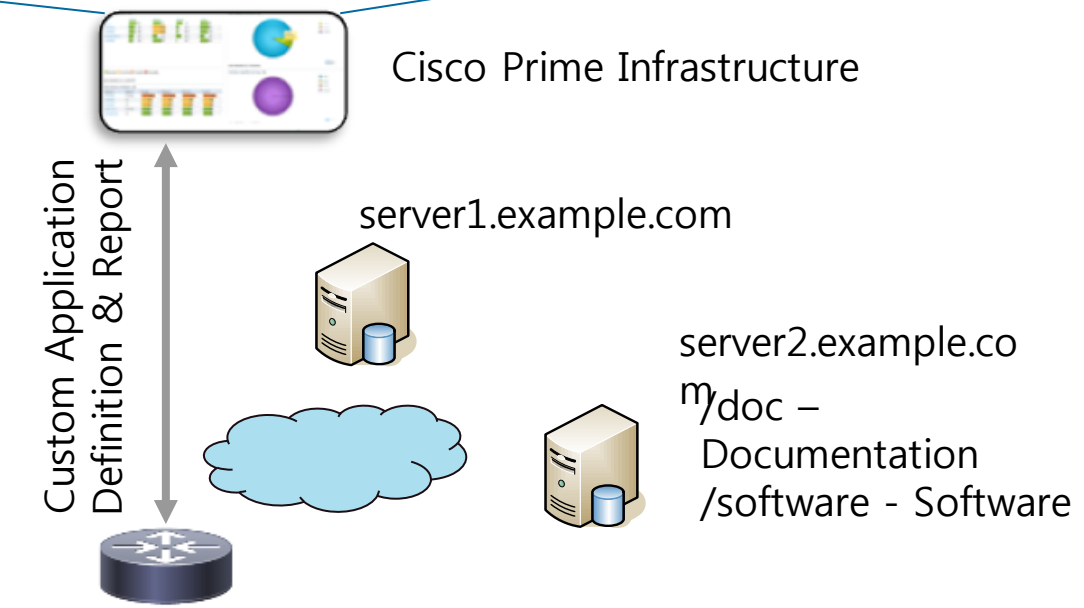
Customized Application

- 특정 HTTP URL 또는 host에 대한 matching

Custom Enterprise Application

Custom App	Server	URI	BW	Resp. Time
My Payroll	server1.example.com	-	2M	100ms
My Doc. Mgmt.	server2.example.com	/doc	1M	250ms
My Software Rep.	server2.example.com	/software	5M	30sec

```
ip nbar custom 001_payroll http host
server1.example.com id 60001

ip nbar custom 002_doc http url doc host
server2.example.com id 60002

ip nbar custom 003_soft http url software host
server2.example.com id 60003
```



IP 및 포트 기반의 사용자 정의

Cisco Connect

- IP subnet 또는 포트 범위로 matching 조건 생성

```
ip nbar custom 001_myapp transport tcp id 60001
 ip subnet 10.1.10.0 24
 port range 40000 41000
 direction any
```

- 사용자 어플리케이션 이름
- Custom App Selector ID

```
R82#sh flow exporter option application table | inc 60001
6:60001  001_myapp                User defined Protocol 001_myapp
R82#
```

개별 사용자 속성 : 최대 120개 지원

Cisco Connect

- 사용자는 ip nbar attribute-map 명령어를 통해서 사용자의 프로토콜에 대한 속성 profile을 생성하여 Custom Protocol을 사용
- ip nbar attribute-set 명령어를 통해서 사용자는 속성 profile을 Protocol과 mapping
- 생성된 개별 attribute는 Add/Edit/Delete가 가능.
- Attribute에 대한 수정은 profile과 protocol간 mapping에 영향을 주지 않음.

```
ip nbar attribute-map myapp-attrib
 attribute application-group ms-lync-group
 attribute category voice-and-video
 attribute encrypted encrypted-yes
!
ip nbar attribute-set 001_myapp myapp-attrib
```

```
R82#sh ip nbar protocol-attribute 001_myapp

          Protocol Name :  001_myapp
      application-group :  ms-lync-group
               category :  voice-and-video
              encrypted :  encrypted-yes
          p2p-technology :  p2p-tech-unassigned
           sub-category :  other
                 tunnel :  tunnel-unassigned
R82#
```

1. 트래픽 통계 기능

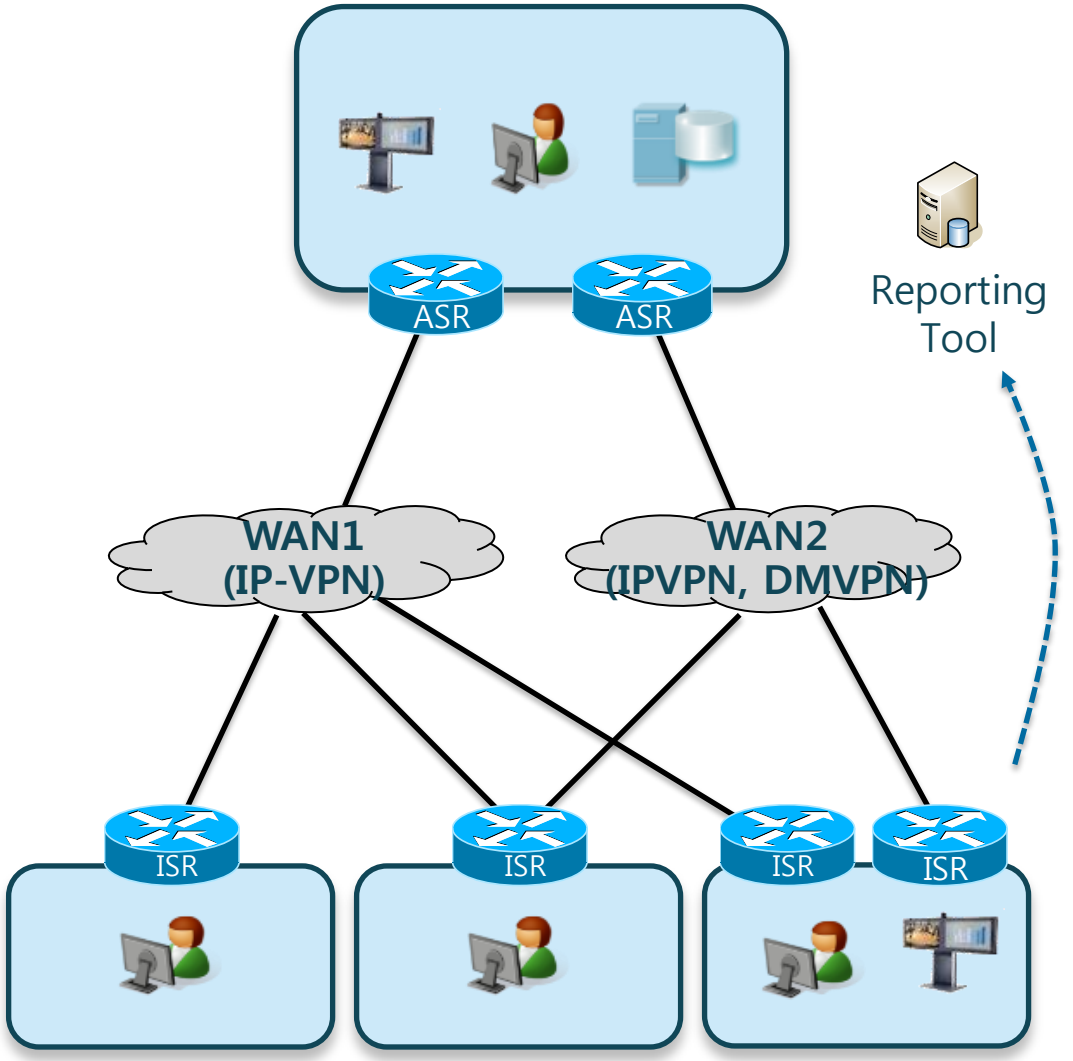
Cisco Connect

주요 특징

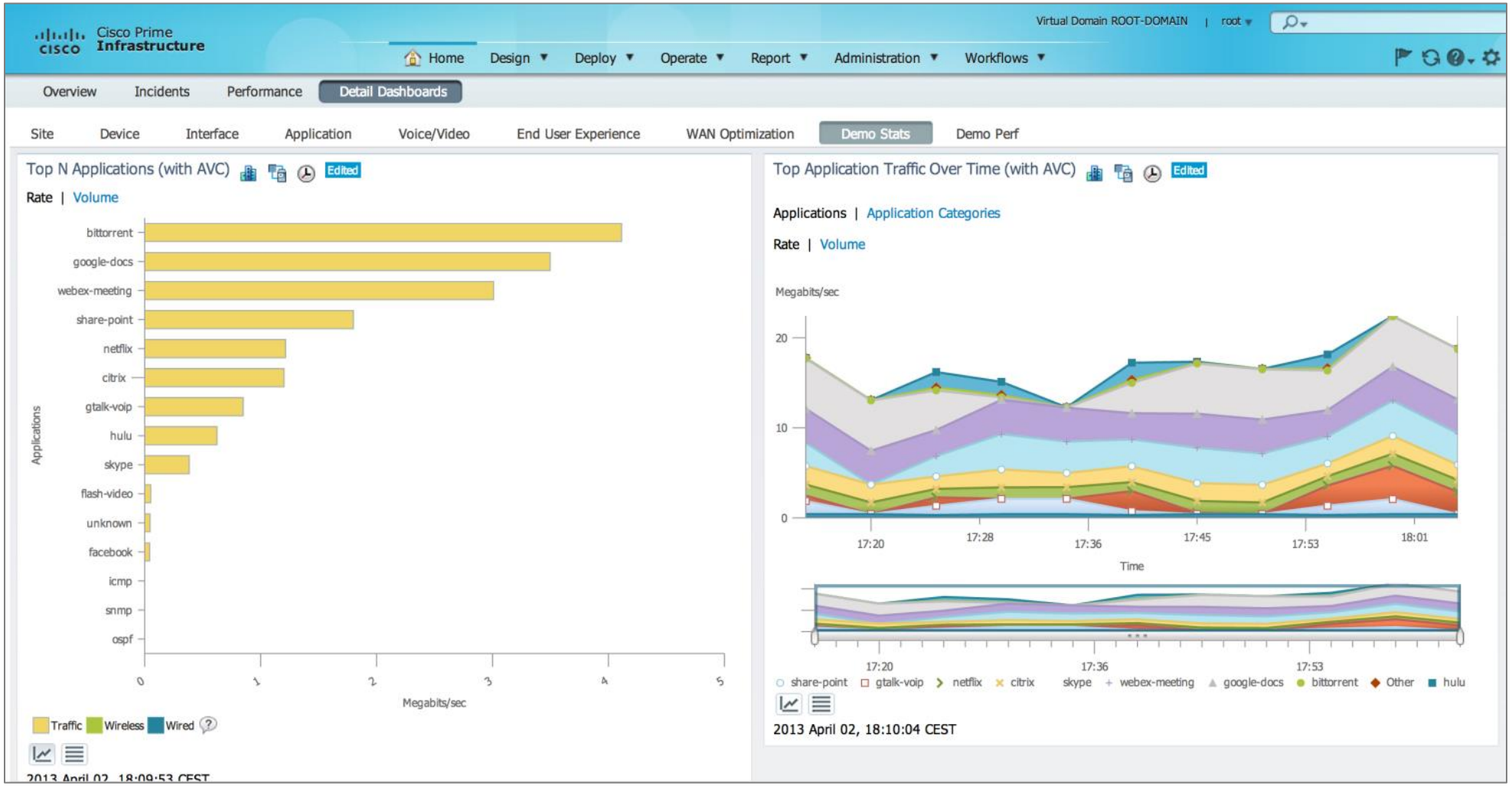
- Fields and flow record format을 이용
- NBAR2 통합
  - Examines data from Layers 3 thru 7
  - Layers 3 and 4 plus packet inspection
  - Stateful inspection
- IOS: FNF 또는 Unified Monitoring로 구현
- IOS-XE: FNF 또는 Unified Monitoring로 구현
- Export: NFv9 or IPFIX 사용

장점

- 어플리케이션 사용량에 대한 가시화
- L2에서 L7 Layer까지 Data monitoring
- 트래픽 통계를 통한 향후 용량 산정에 용이
- Top-N 어플리케이션에 대한 통계
- Top-N 클라이언트/서버에 대한 통계



Prime Infrastructure 예제



2. URL 수집 기능

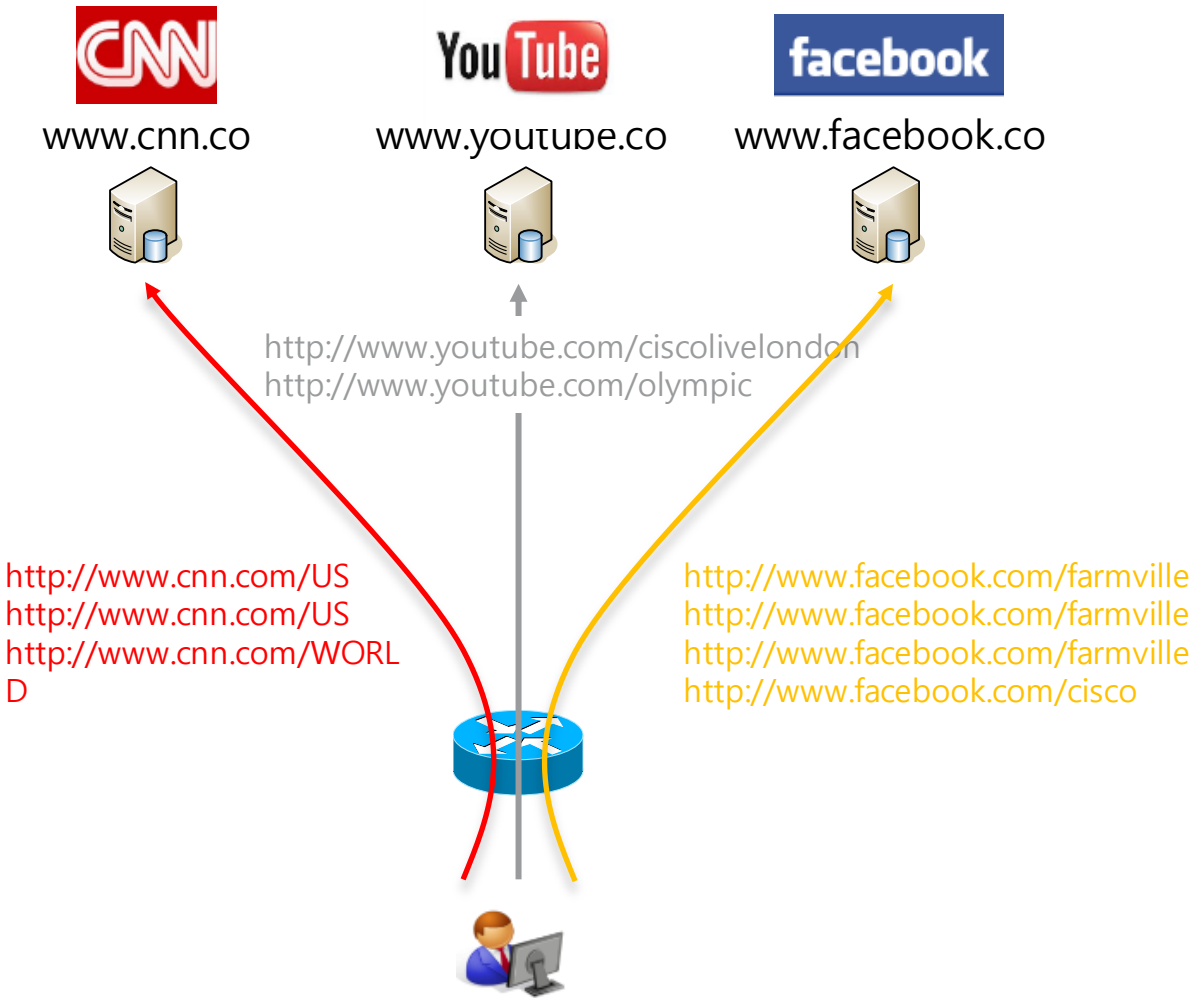
Cisco Connect

주요 특징

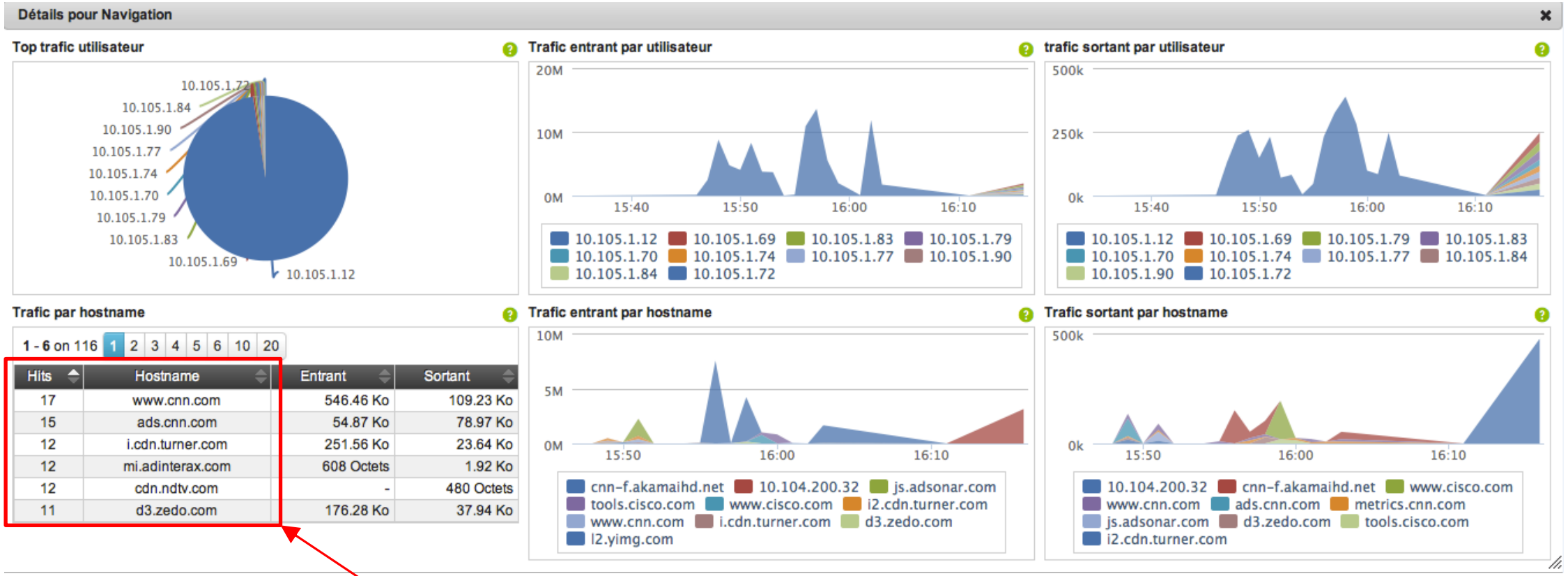
- 웹 브라우징에 대한 리포팅 공급
- 표준 IPFIX export 사용
- IOS: Unified Monitoring
- IOS-XE: Unified Monitoring

장점

- 탑 도메인에 대한 hit count 제공
- L2~L7 layer까지 데이터 모니터링
- 가장 많이 방문한 웹사이트에 대한 통계
- 지점 별 가장 많이 방문한 URL 통계
- 특정 도메인에 대한 Hit count 정보 제공



URL Hit Count Report 예제



각 URL 도메인 별 hit count matching

3. Application Response Time

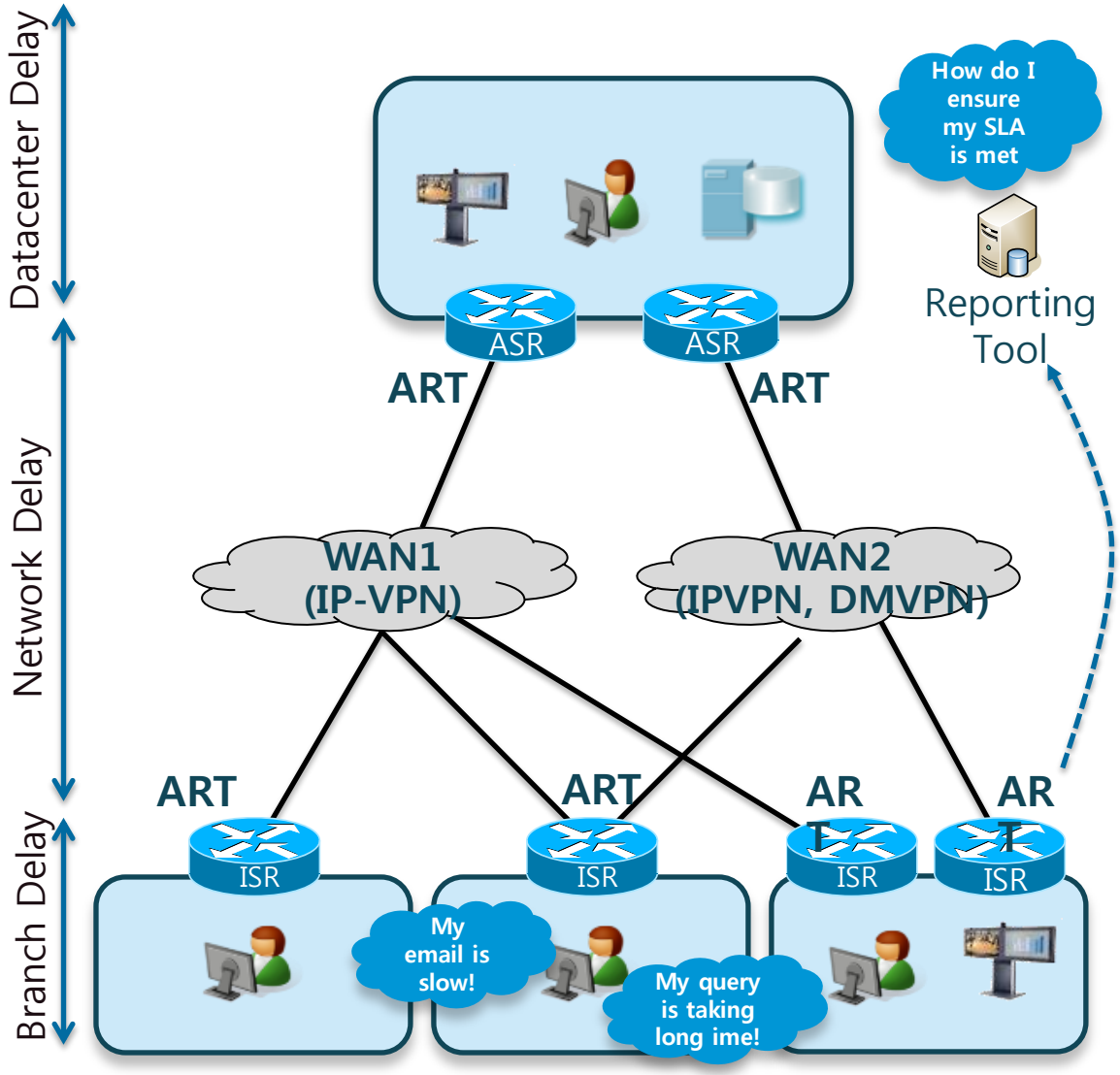
Cisco Connect

주요 특징

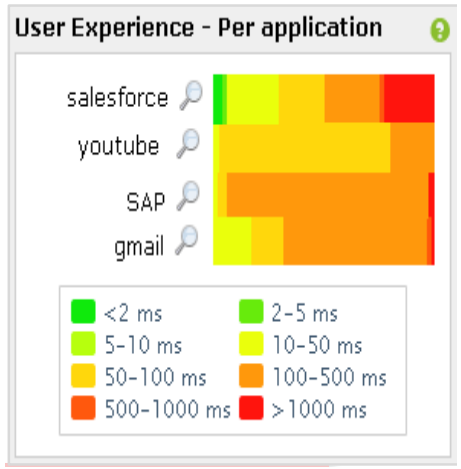
- 어플리케이션 응답 시간에 대한 Metrics
- NBAR2를 통해 Application ID 이용
- IOS: Unified Monitoring
- IOS-XE: Unified Monitoring
- Export: NFv9 and IPFIX export

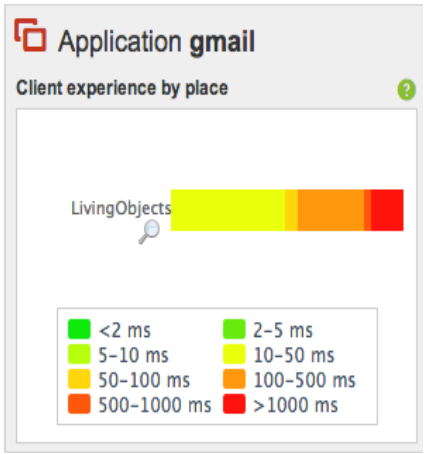
장점

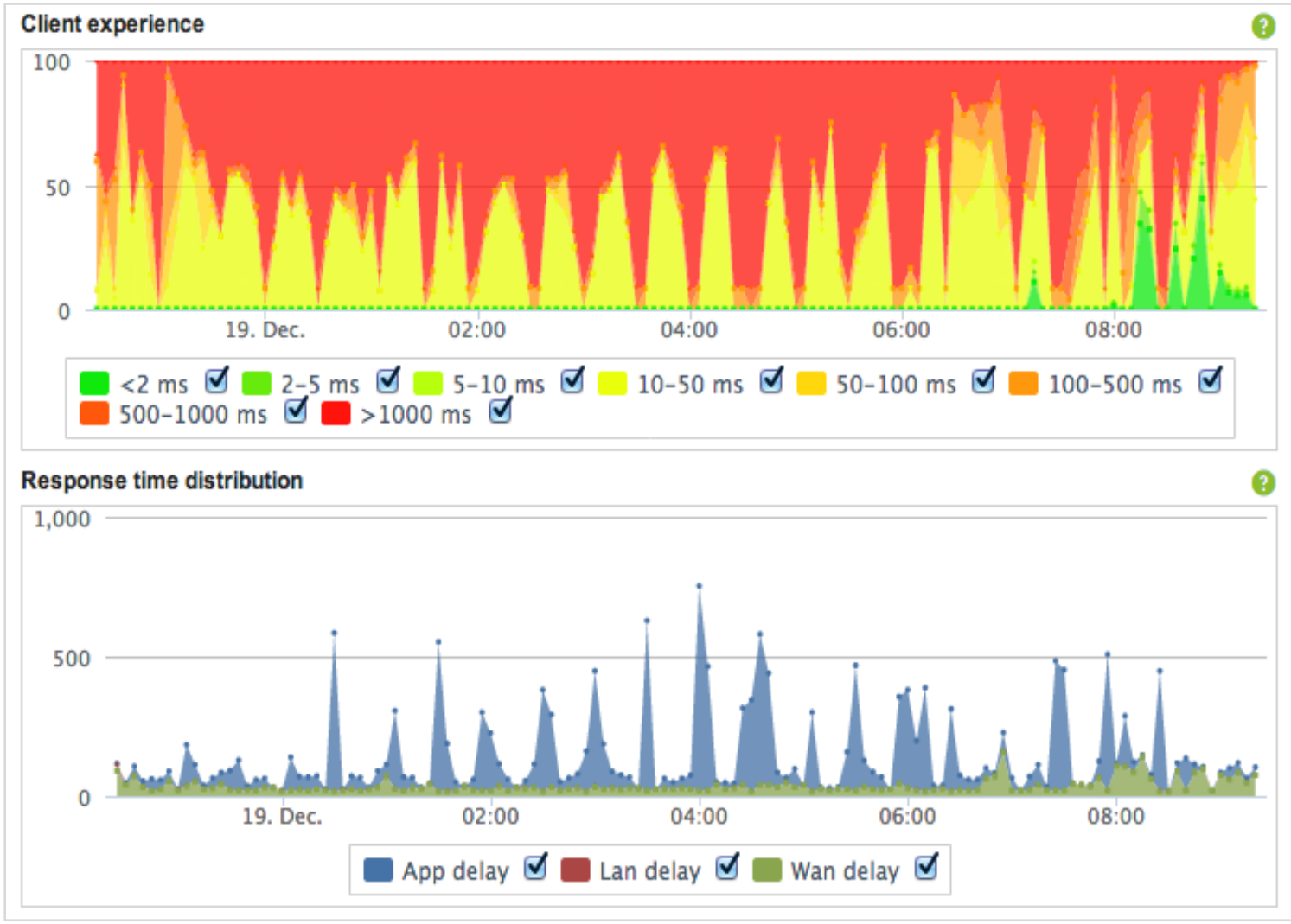
- 어플리케이션 사용 및 성능에 대한 가시화
- 사용자 경험에 대한 계측화
- 어플리케이션 성능에 대한 쉬운 장애 처리
- 어프리케이션에 대한 tracking service



ART 결과 리포트 예제


User Experience - Per application
salesforce
youtube
SAP
gmail
<2 ms
2-5 ms
5-10 ms
10-50 ms
50-100 ms
100-500 ms
500-1000 ms
>1000 ms


Application gmail
Client experience by place
LivingObjects
<2 ms
2-5 ms
5-10 ms
10-50 ms
50-100 ms
100-500 ms
500-1000 ms
>1000 ms


Client experience
100
50
0
19. Dec.
02:00
04:00
06:00
08:00
<2 ms
2-5 ms
5-10 ms
10-50 ms
50-100 ms
100-500 ms
500-1000 ms
>1000 ms
Response time distribution
1,000
500
0
19. Dec.
02:00
04:00
06:00
08:00
App delay
Lan delay
Wan delay

4. 미디어 모니터링

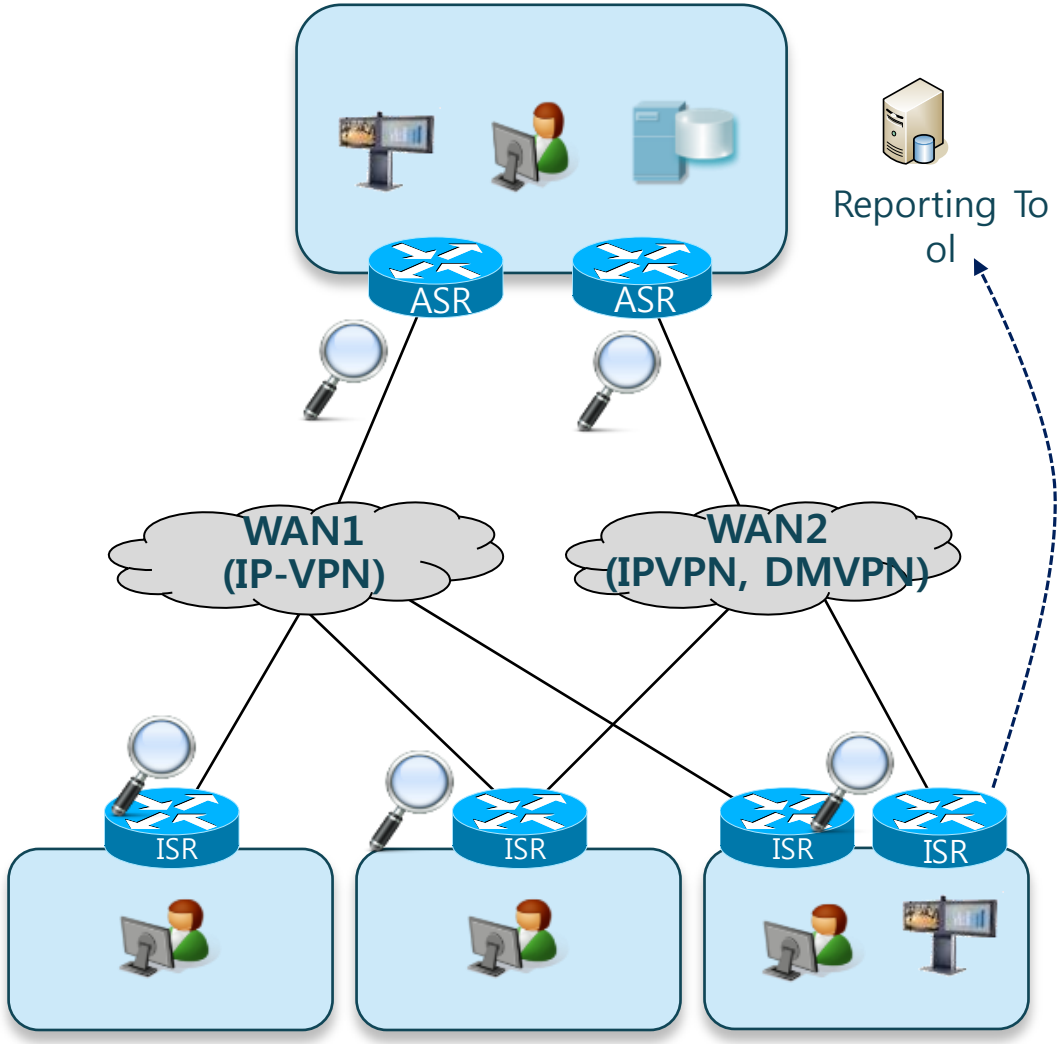
Cisco Connect

주요 기능

- 미디어 성능 매트릭에 대한 모니터링
- 애플리케이션 인식을 위한 NBAR2 연동
- 임계치 및 알람 설정
- IOS: Performance Monitoring or Unified Monitoring
- IOS-XE: Unified Monitoring
- Export: NFv9 or IPFIX export

장점

- 네트워크 상의 음성/비디오에 대한 real-time monitoring
- 빠르고 정확한 모니터링으로 쉬운 장애 처리
- 능동적인 장애처리 구현
- SLA에 대한 보장

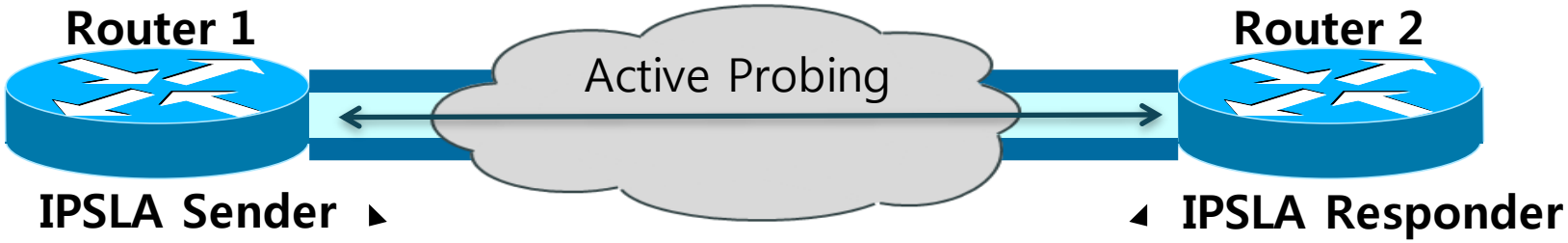


미디어 모니터링 – 성능 모니터링

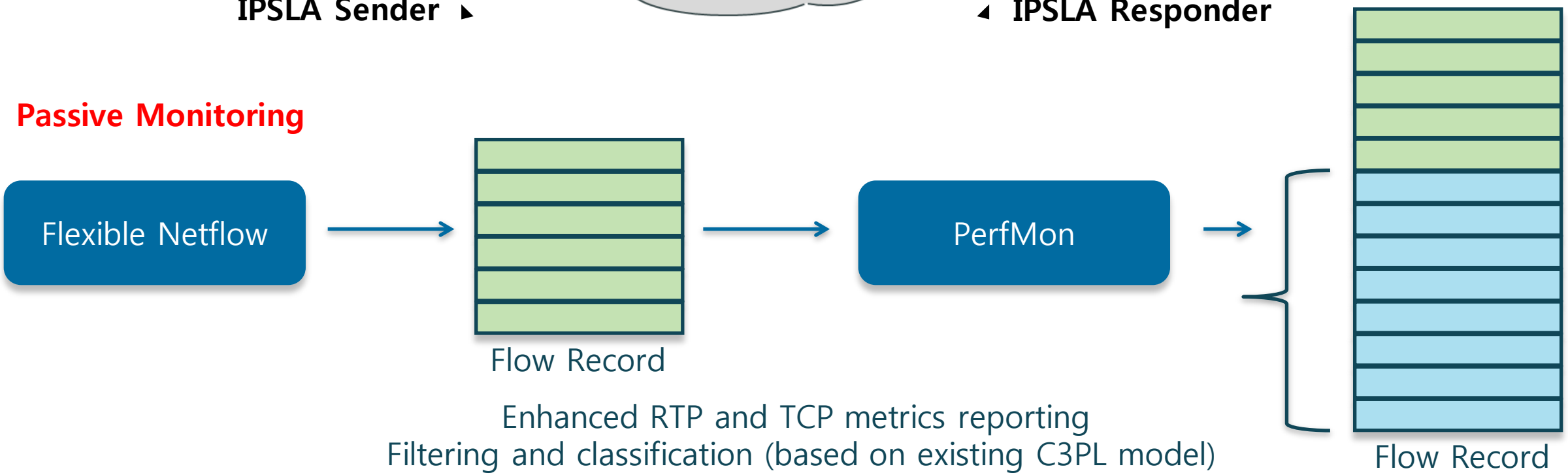
Cisco Connect

Active vs. Passive Monitoring

Active Monitoring



Passive Monitoring



Enhanced RTP and TCP metrics reporting
Filtering and classification (based on existing C3PL model)

WAAS + Akamai를 통한 WAN 최적화

Cisco Connect

Speed and Bandwidth Benefits on Top of the IWAN

어플리케이션의 가속과 대역폭에 대한 절감

- 90%이상의 HD Video의 최적화와 더 나은 사용자 경험 제공
- 동일 WAN 환경에서 Citrix 사용자의 체감 속도 약 70% 향상
- 연간 약 65% 대역폭 비용 절감 예상

편리한 구성 및 배포

- AX 라이센스를 통하여 현재 Branch 라우터와 연동 가능

높은 확장성

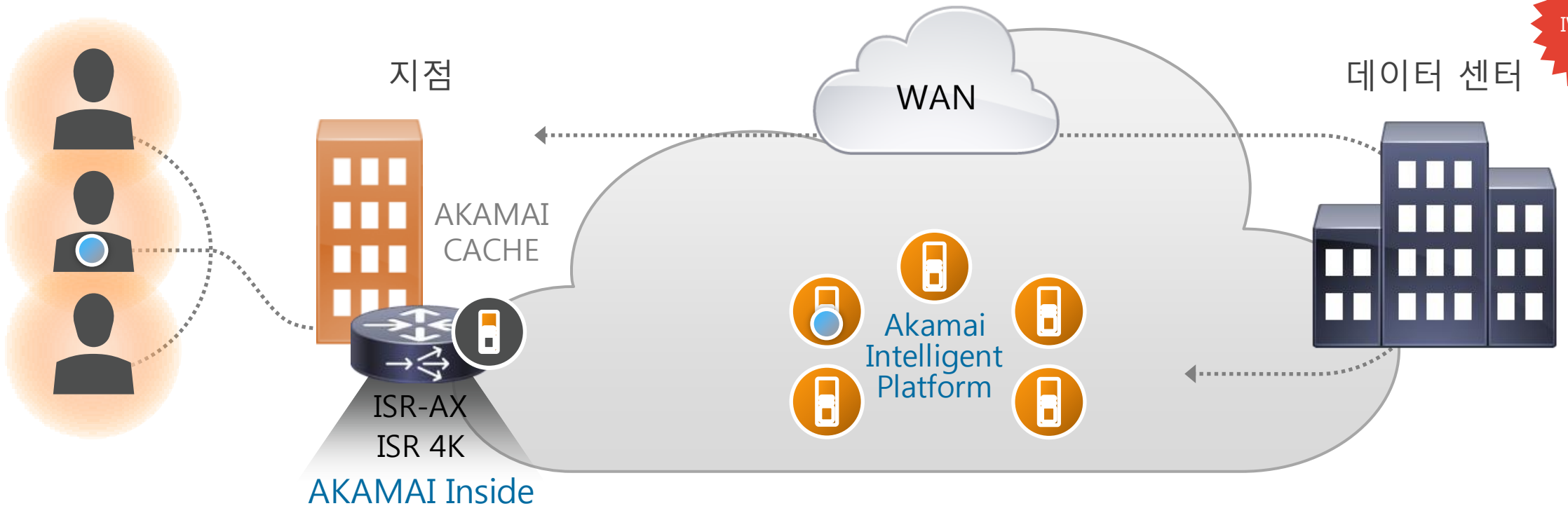
- AppNav Controller and WAVE pool is scalable
- Native HA capability

IWAN – 어플리케이션 최적화

Akamai Connect와 연동

Cisco Connect

IWAN 2.0



클라우드, WAN 회선, 장비 및 단말과 관계 없이 최적화된 사용자 경험 제공

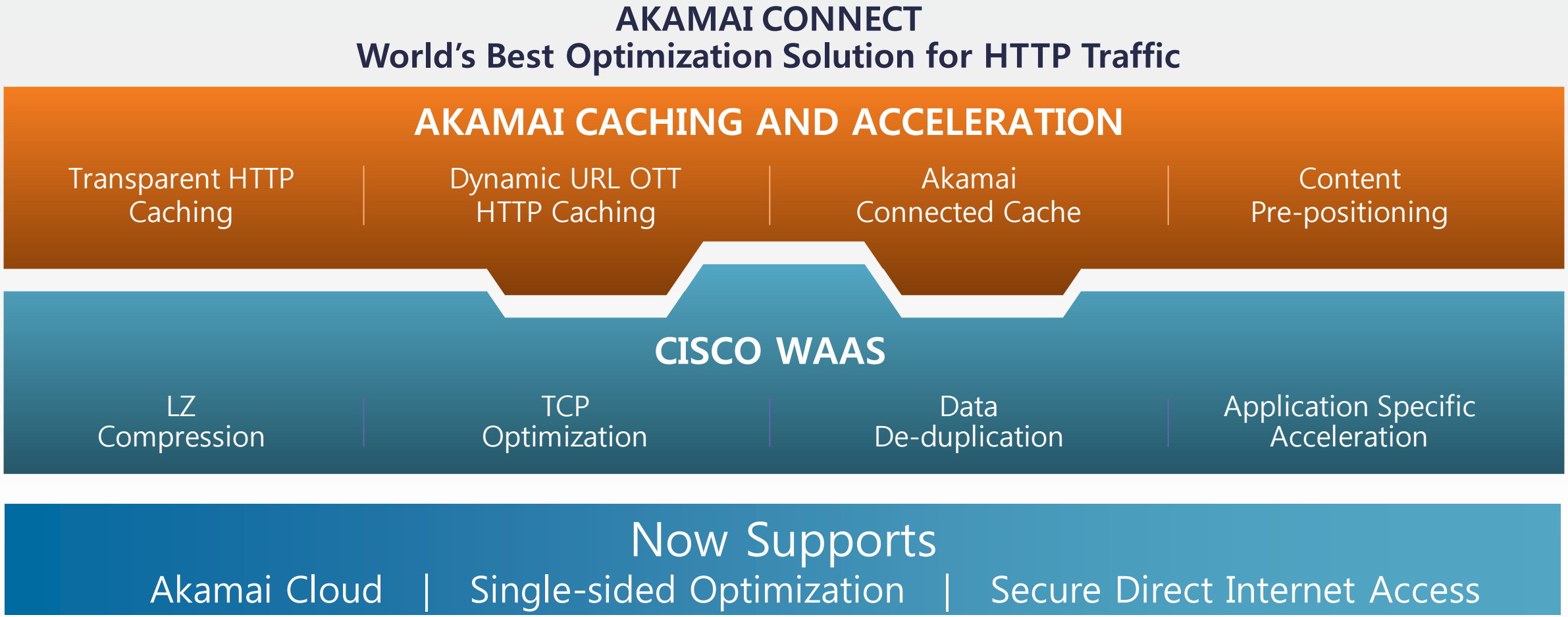
네트워크 구성과 상관없이 모든 HTTP 트래픽에 대한 캐싱 기능 제공

Prepositioning | Dynamic HTTP Caching (YouTube) | Any Transport

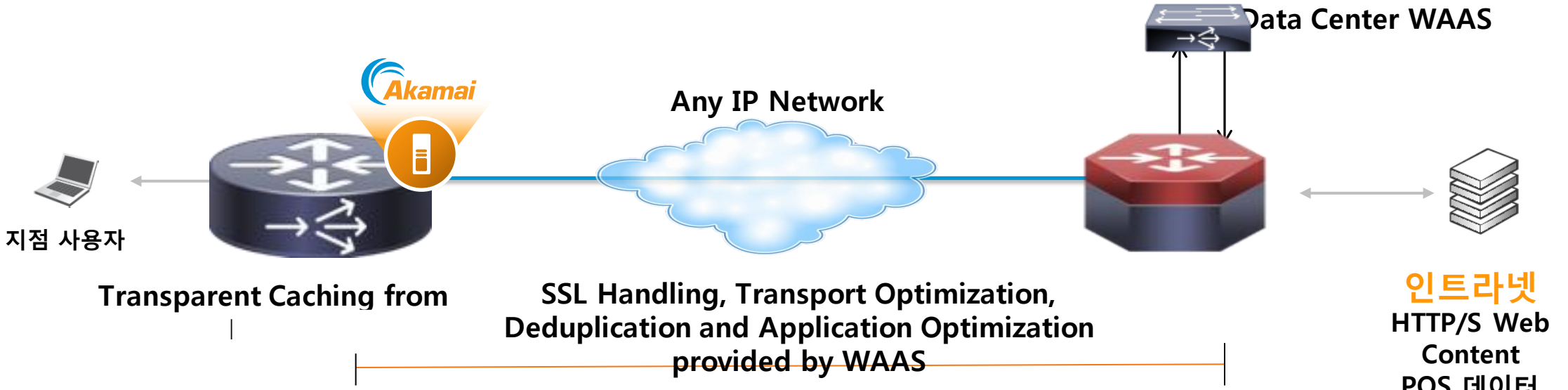
WAAS + AKAMAI

사용자 경험 증진을 위한 Edge Caching

Cisco Connect



Transparent Cache



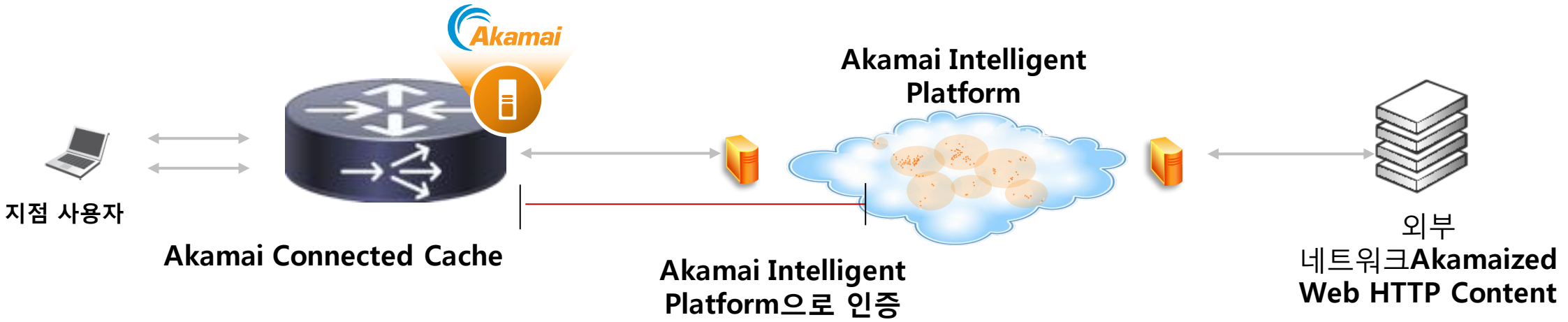
현 네트워크 상황:

- MPLS회선의 비싼 대역폭
- 사용자의 빠른 응답 속도 요구
- 다중 옴니채널 어플리케이션
- 다양한 미디어를 활요하는 비지니스 환경

아카마이 솔루션:

- 지점의 POS data에 대한 캐싱 제공
- Round Trip Time의 감소
- Latency 감소
- Network congestion 감소
- 컨텐츠에 대한 Pre-positioning

Akamai Connected Cache



현 네트워크 상황:

- 고객의 contents가 아카마이 플랫폼에 캐싱
- 환경 최적화 이후에도 최적의 환경에서도 문제점 미 해결
- 사용자는 지점에서 캐싱되어 있는 contents를 사용

아카마이 솔루션:

- 기존에 지점 내에 캐싱하지 못했던 contents에 대한 캐싱 지원
- 아카마이 플랫폼에서 제공하는 다양한 contents를 사용
- Akamai Intelligent Platform 내의 변경에 대해서는 자동으로 반영

Over-the-Top Caching

- 유투브 전문 채널
- 교육 비디오 컨텐츠
- 바이럴 비디오

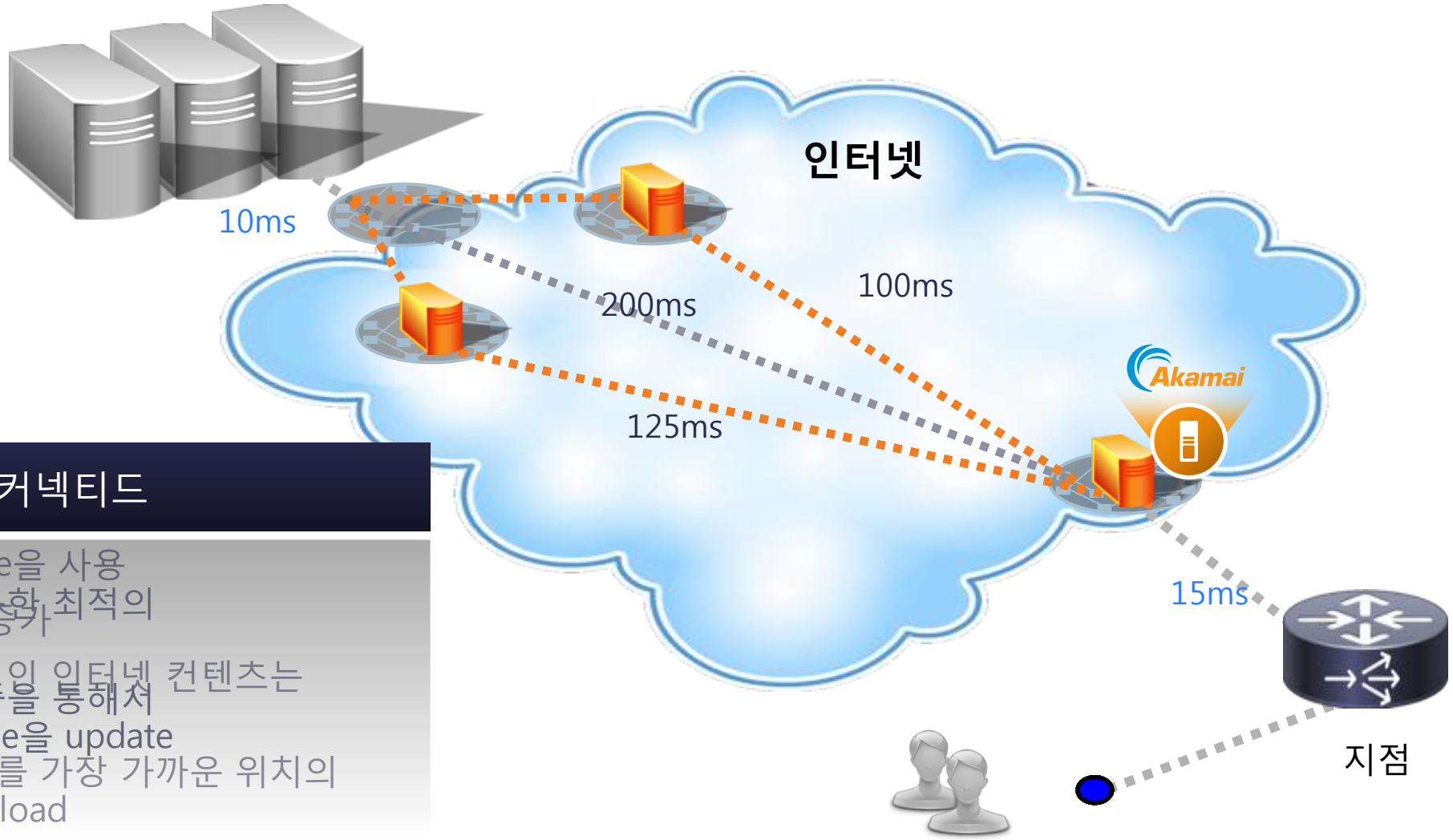
현 네트워크 상황:

- 비디오 트래픽의 높은 대역폭 점유
- Congestion의 증가
- YouTube채널에 대한 높은 사용률

아카마이 솔루션:

- 주요 비디오 컨텐츠에 대한 캐싱
- 대역폭 절감
- 지점 상에서 비지니스 유투브 채널 이용

Akamai Connected Cache 장점



Edge Caching — 아카마이 커넥티드

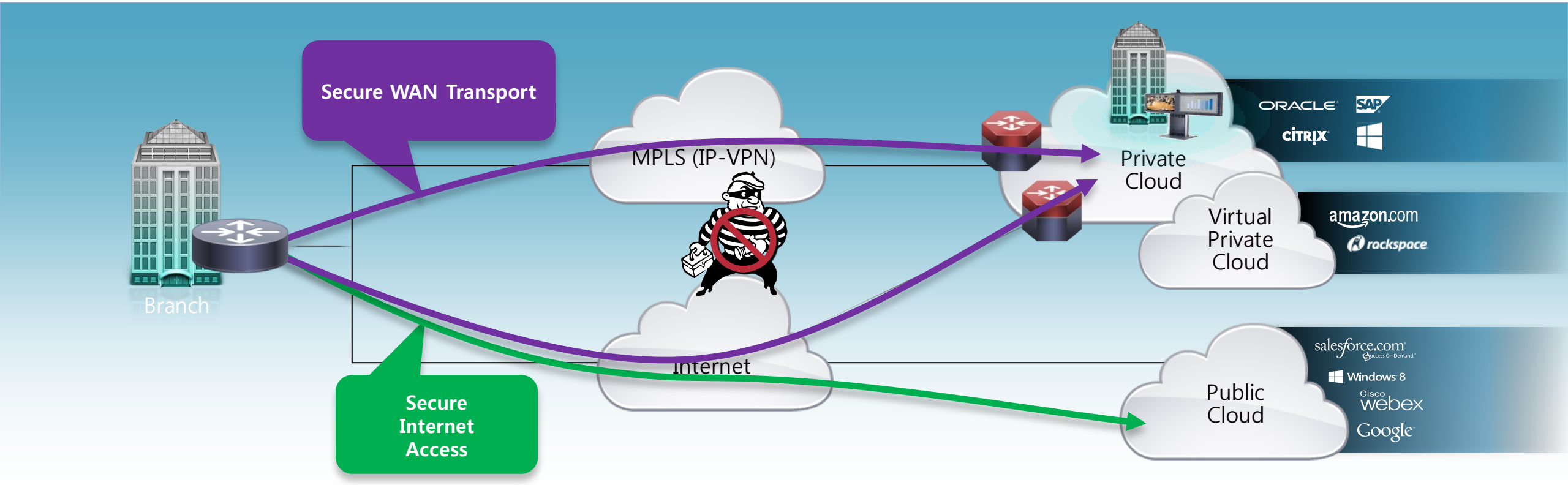
- 아카마이의 특정 caching rule을 사용
- 아카마이 전용 플랫폼을 이용한 최적의 caching 환경을 제공
- HTTP page loading 성능의 향상
- 클라우드 플랫폼 상의 일반적인 인터넷 컨텐츠는 캐시된 서버로 부터 응답
- 아카마이 서버에 대한 인증을 통해서 사용으로 최적의 Caching rule을 update
- 사용자가 이용하는 Contents를 가장 가까운 위치의 데이터센터 server에서 download

Cisco Connect
Seoul, Korea
April 1-2, 2015

5. IWAN Secure Connectivity

Secure Connectivity

네트워크 및 사용자 보안 강화



고려 사항

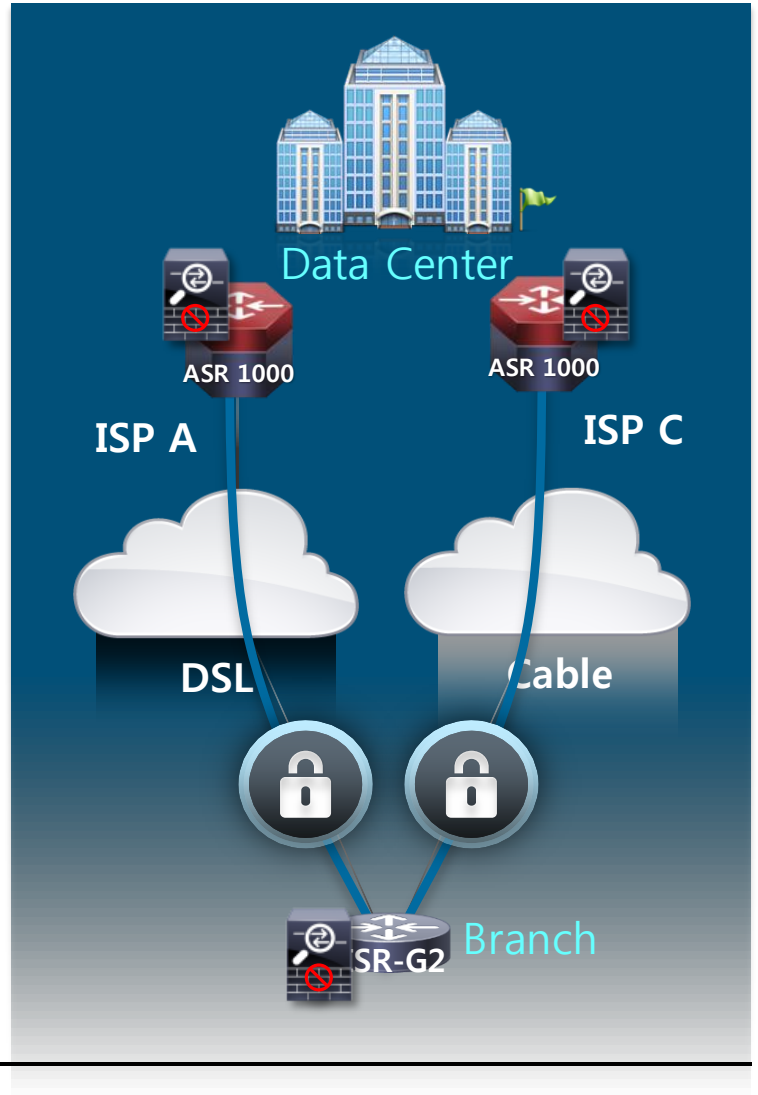
1. 사업자를 통해 전달되는 사용자 데이터에 대한 외부 위협 방어
2. 인터넷 서비스 및 공용 클라우드 서비스에 대한 사용자 액세스 보호

네트워크의 통합 위협 방어

Cisco Connect

IOS 기반의 방화벽

- Control the Perimeter:
  - 내부 및 외부 네트워크에 대한 보안 기능
  - Protocol anomaly detection 및 Stateful inspection 기능 지원
- 강화된 보안성:
  - 콜플로우에 대한 인식 (SIP, SCCP, H323)
  - DoS 공격에 대한 방어
- 가용성:
  - Split Tunnel 기능으로 Traffic에 대한 분산 및 다양한 디자인 제공
  - 내부 방화벽 기능
- 통합:
  - 추가적인 장비의 구성 없이 ISR에서 제공 (비용 절감)
  - 다양한 Cisco의 서비스와 연동: SRE, Scansafe, WaaS Express



Remote Site 보안 설정

IOS 기반의 방화벽 설정 (Inside to outside traffic)

```
zone security INSIDE
zone security OUTSIDE
```

1. 내/외부 Zone 설정

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp
 match protocol udp
 match protocol icmp
```

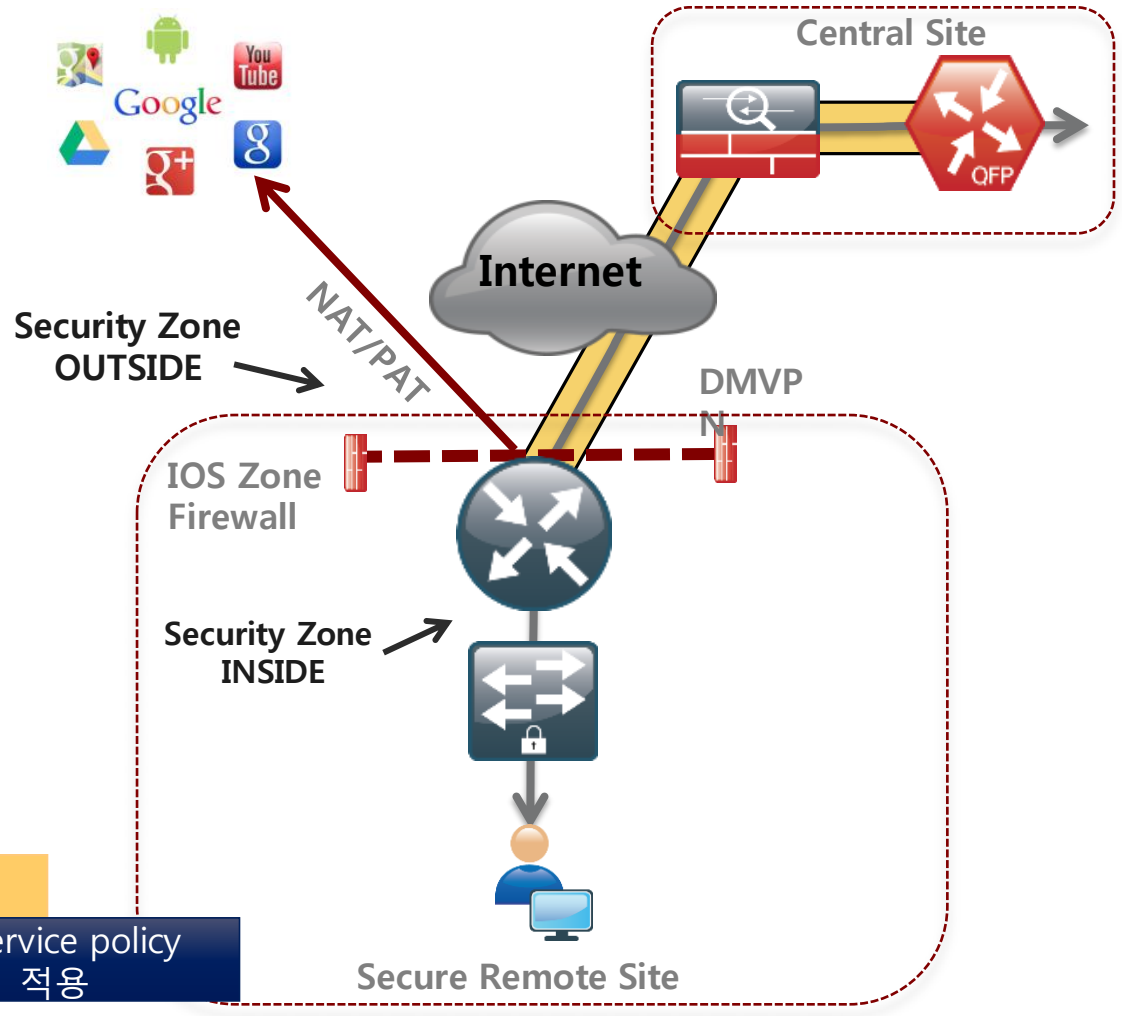
2. 외부로 전송되는 traffic에 대한 classification

```
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
 class type inspect INSIDE-TO-OUTSIDE-CLASS
  inspect
 class class-default
  drop
```

3. 분류된 traffic에 대한 policy mapping

```
zone-pair security IN_OUT source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
```

4. Service policy 적용



IOS 기반의 방화벽 – Interface rule 설정

DMVPN tunnel에 대한 inbound traffic 설정

```
ip access-list extended ACL-RTR-IN
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit icmp any any echo
 permit icmp any any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any gt 1023 ttl eq 1
```

1. ISAKMP/ESP/DHCP에 대한 inbound ACL permit 설정

```
ip access-list extended ESP-IN
 permit esp any any

ip access-list extended DHCP-IN
 permit udp any eq bootps any eq bootpc
```

```
class-map type inspect match-any INSPECT-ACL-IN-CLASS
 match access-group name ACL-RTR-IN

class-map type inspect match-any PASS-ACL-IN-CLASS
 match access-group name ESP-IN
 match access-group name DHCP-IN
```

2. ACL에 대한 Classification mapping

```
policy-map type inspect ACL-IN-POLICY
 class type inspect INSPECT-ACL-IN-CLASS
  inspect
 class type inspect PASS-ACL-IN-CLASS
   pass
 class class-default
   drop
```

3. Inbound Policy map 설정

IOS 기반의 방화벽 – Interface rule 설정

DMVPN tunnel에 대한 outbound traffic 설정

```
ip access-list extended ACL-RTR-OUT
permit udp any any eq non500-isakmp
permit udp any any eq isakmp
permit icmp any
```

1. ISAKMP/ESP/DHCP에 대한 outbound ACL permit 설정

```
ip access-list extended ESP-OUT
permit esp any any

ip access-list extended DHCP-OUT
permit udp any eq bootpc any eq bootps
```

```
class-map type inspect match-any INSPECT-ACL-OUT-CLASS
 match access-group name ACL-RTR-OUT

class-map type inspect match-any PASS-ACL-OUT-CLASS
 match access-group name ESP-OUT
 match access-group name DHCP-OUT

 policy-map type inspect ACL-OUT-POLICY
  class type inspect INSPECT-ACL-OUT-CLASS
   inspect
 class type inspect PASS-ACL-OUT-CLASS
   pass
 class class-default
  drop
```

2. ACL에 대한 Classification mapping

3. Outbound Policy map 설정

IOS 기반의 방화벽

Zone-pair 및 Zone member 설정

zone-pair security **TO-ROUTER** source **OUTSIDE** destination **self**
service-policy type inspect **ACL-IN-POLICY**

zone-pair security **FROM-ROUTER** source **self** destination **OUTSIDE**
service-policy type inspect **ACL-OUT-POLICY**

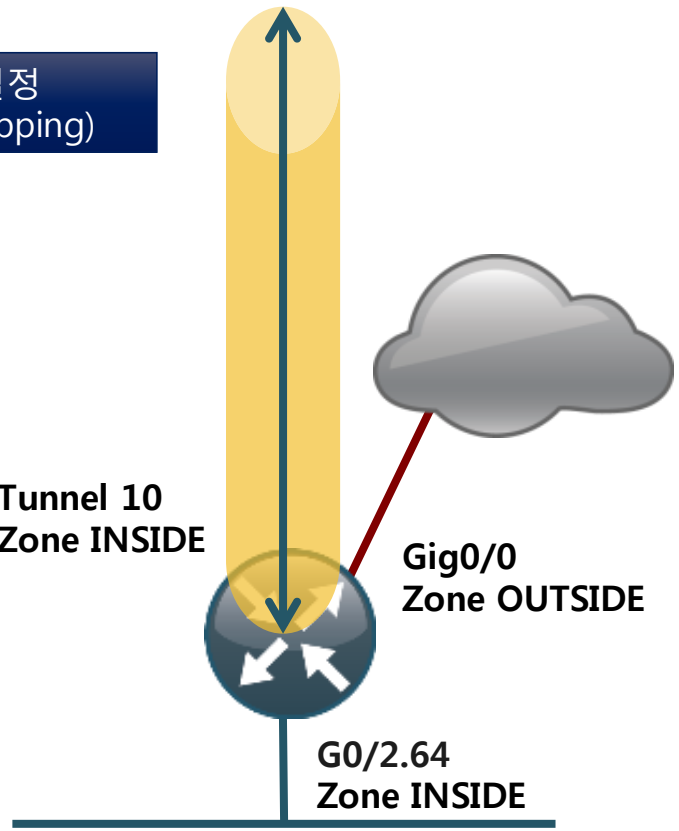
내/외부의 Zone-pair 설정
(생성한 Policy에 대한 mapping)

interface **GigabitEthernet0/0**
description **Internet Connection**
zone-member security **OUTSIDE**

Interface **GigabitEthernet0/2.64**
description **Wired Data**
zone-member security **INSIDE**

interface **Tunnel10**
description **DMVPN-1 tunnel interface**
zone-member security **INSIDE**

각 interface에 대한 zone-member 설정
1. Internal interface
2. External physical interface
3. DMVPN tunnel interface



Direct Internet Access

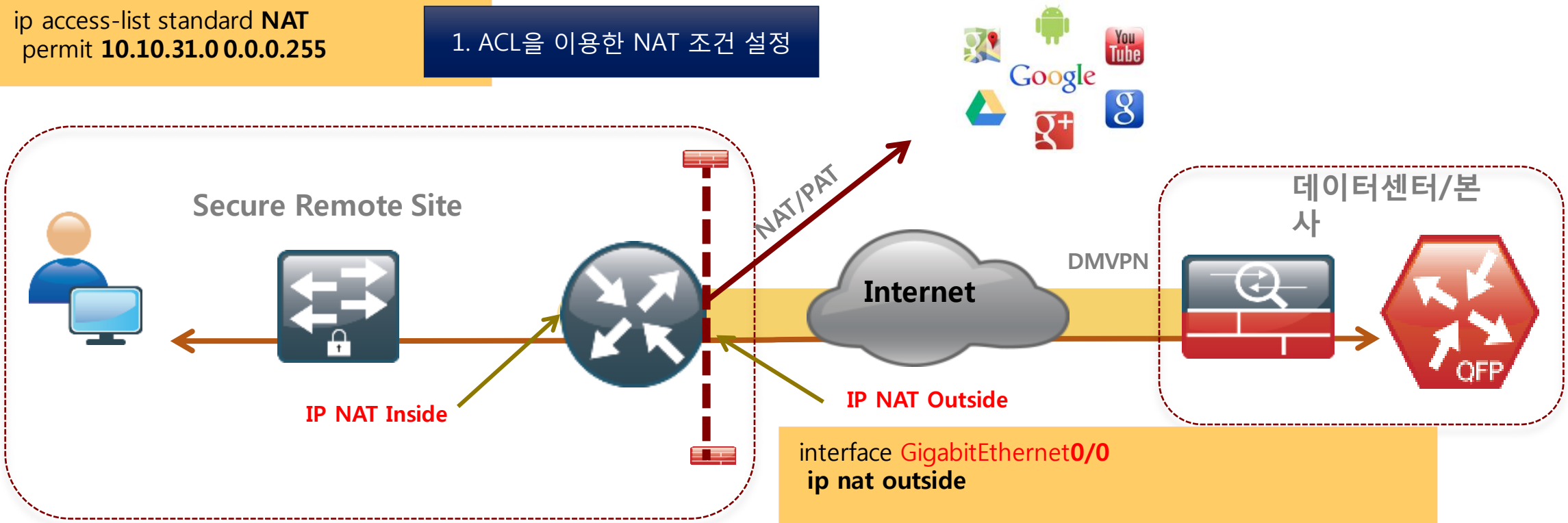
기본적인 NAT/PAT 설정

ip nat inside source list **NAT** interface GigabitEthernet**0/0** overload

2. NAT configuration

ip access-list standard **NAT**
permit **10.10.31.0 0.0.0.255**

1. ACL을 이용한 NAT 조건 설정



interface GigabitEthernet**0/0**
ip nat outside

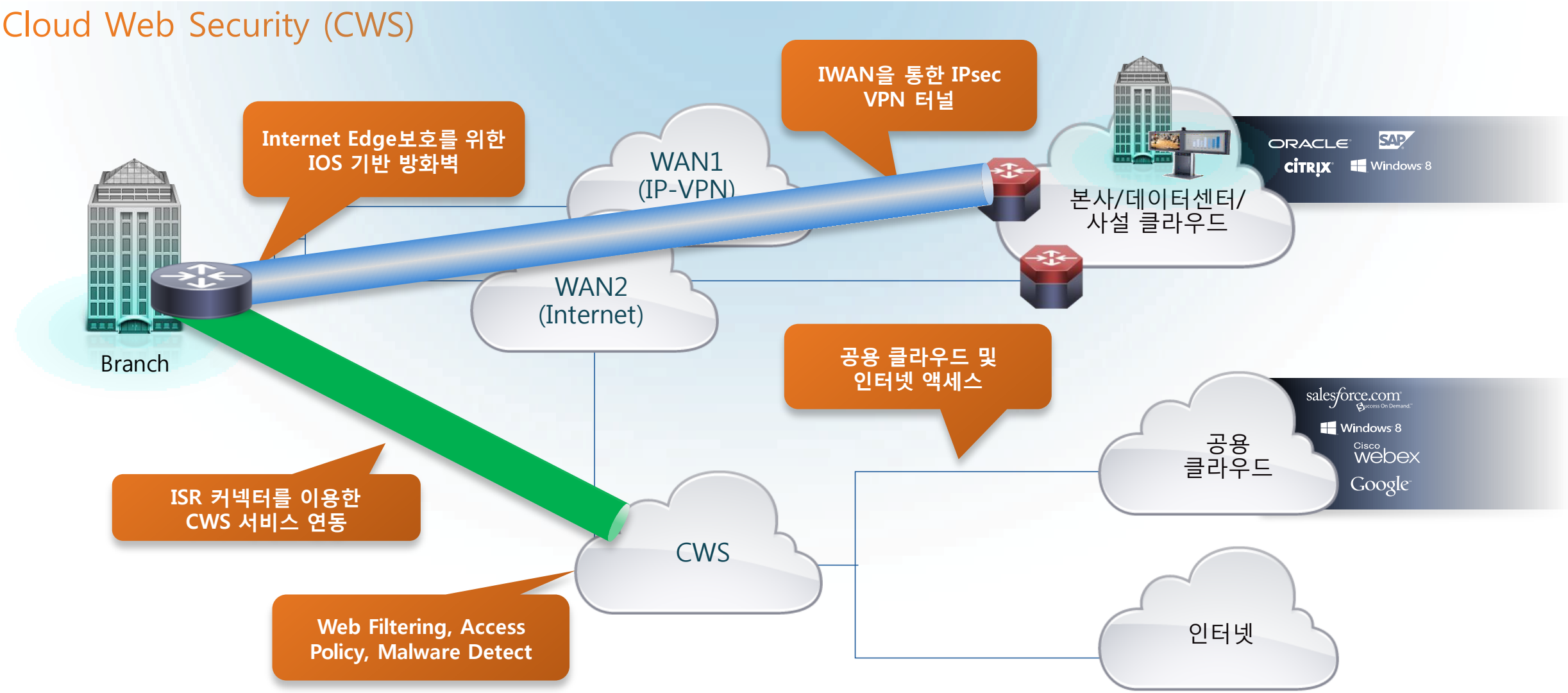
interface GigabitEthernet**0/2.64**
ip nat inside

3. Interface의 NAT IN/OUT 지정

Secure Internet Access

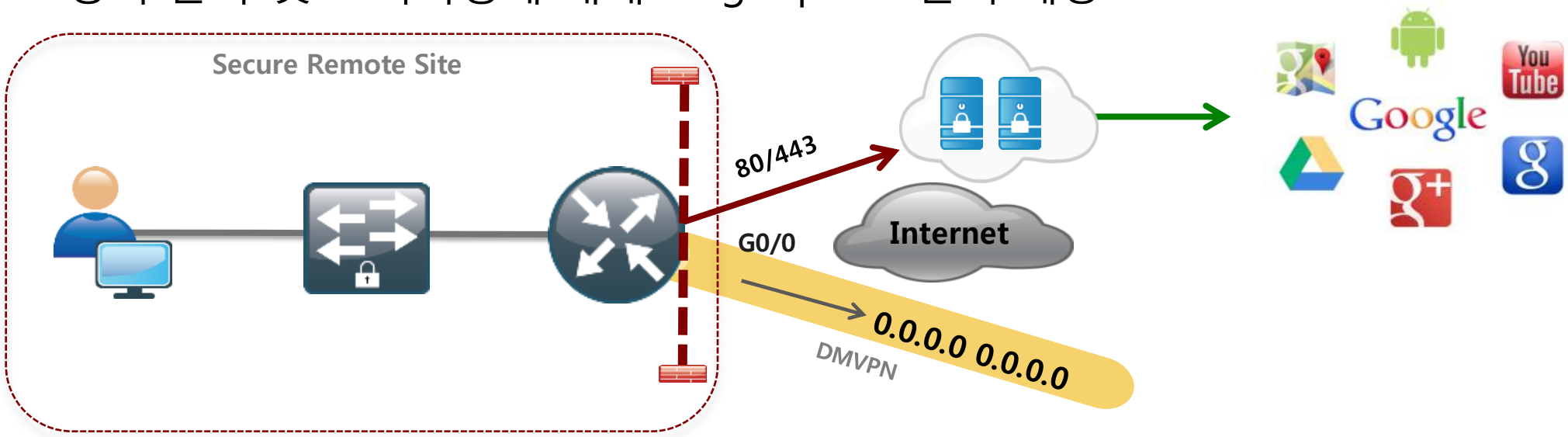
Cisco Connect

Cloud Web Security (CWS)



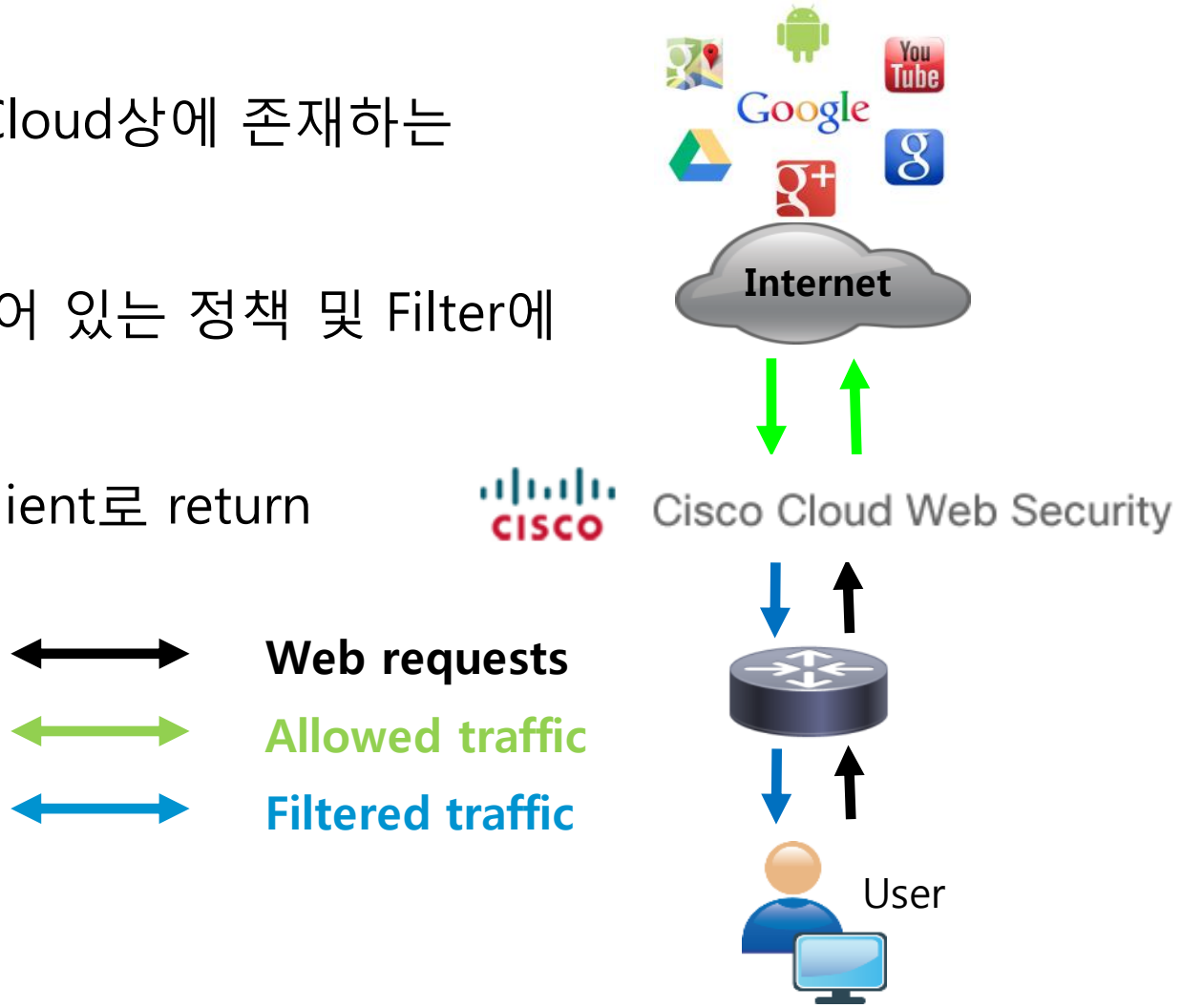
통합 CWS Connector

- 기본적으로 ISR G2 라우터 내에 내장.
  - IOS 15.4(1)T version부터 VRF에 대한 지원
- 지점 라우터 상에서 인터넷 트래픽에 대한 Redirection을 transparent forwarding
- Tower에 대한 Redundancy 제공
- 정책 관리 및 모니터링에 대해 Single point 관리 제공



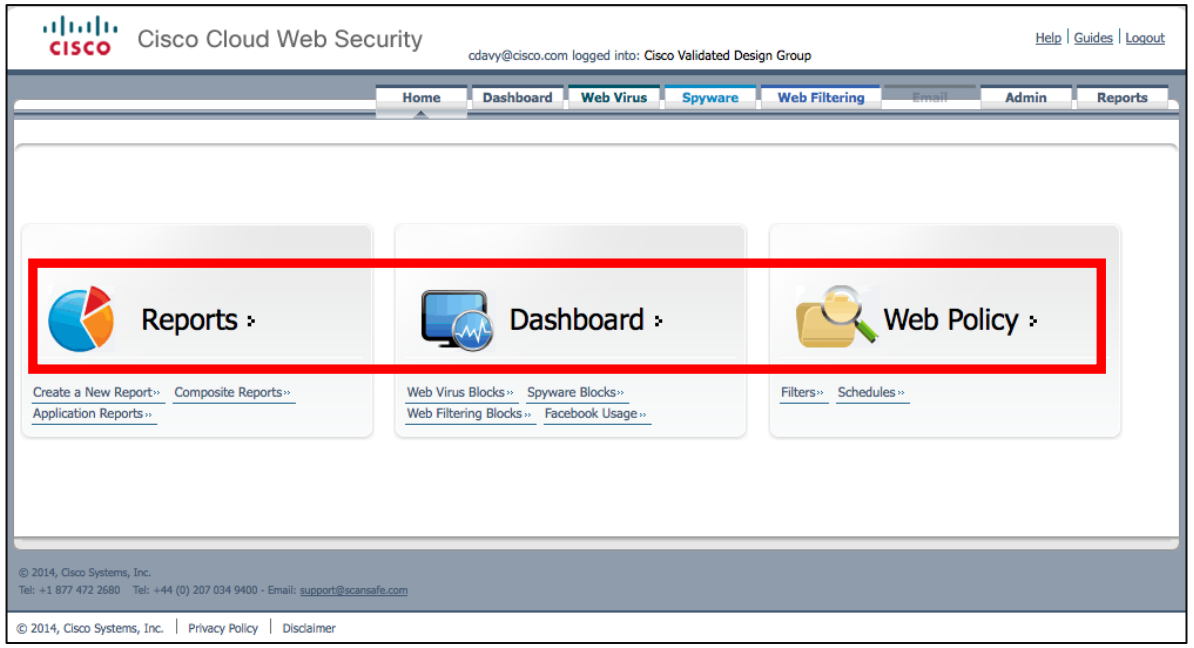
CWS를 통한 Data Flow

- HTTP/HTTPS 클라이언트의 요청은 Cloud상에 존재하는 CWS proxy로 redirection
- 해당 요청은 CWS proxy내에 설정되어 있는 정책 및 Filter에 checking
- 허용된 Request에 대해서 traffic을 client로 return



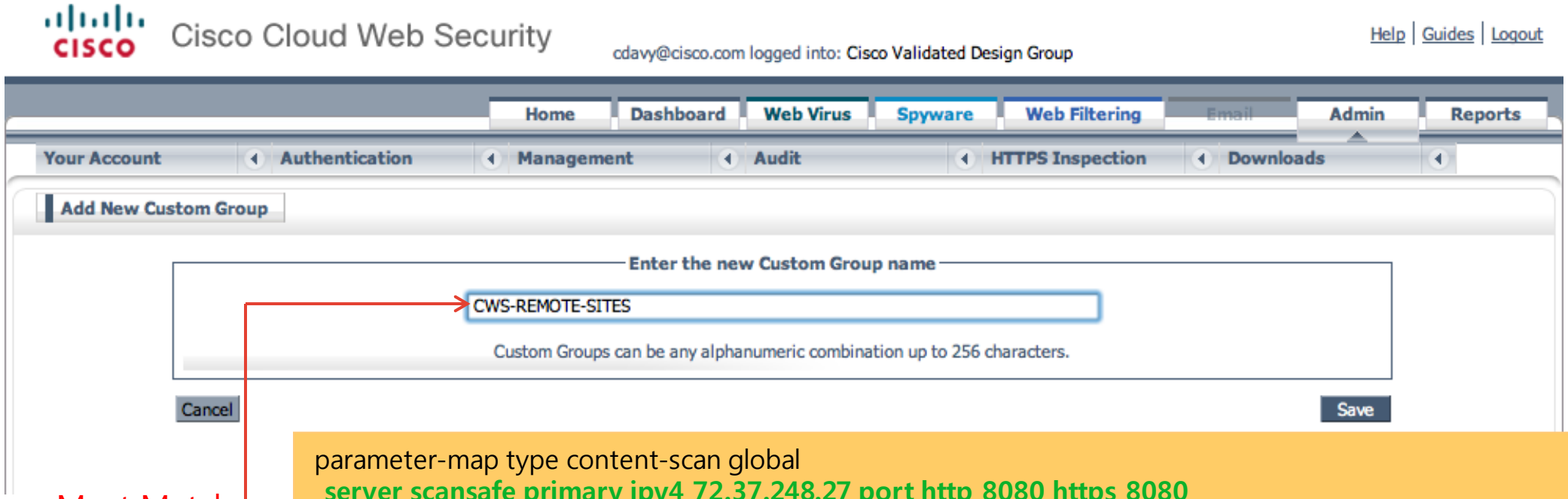
CWS의 중앙 집중적 관리 포털

Cisco ScanCenter Portal (https://scancenter.scansafe.com)



Cloud Web Security

Cisco ScanCenter Portal – 그룹 생성



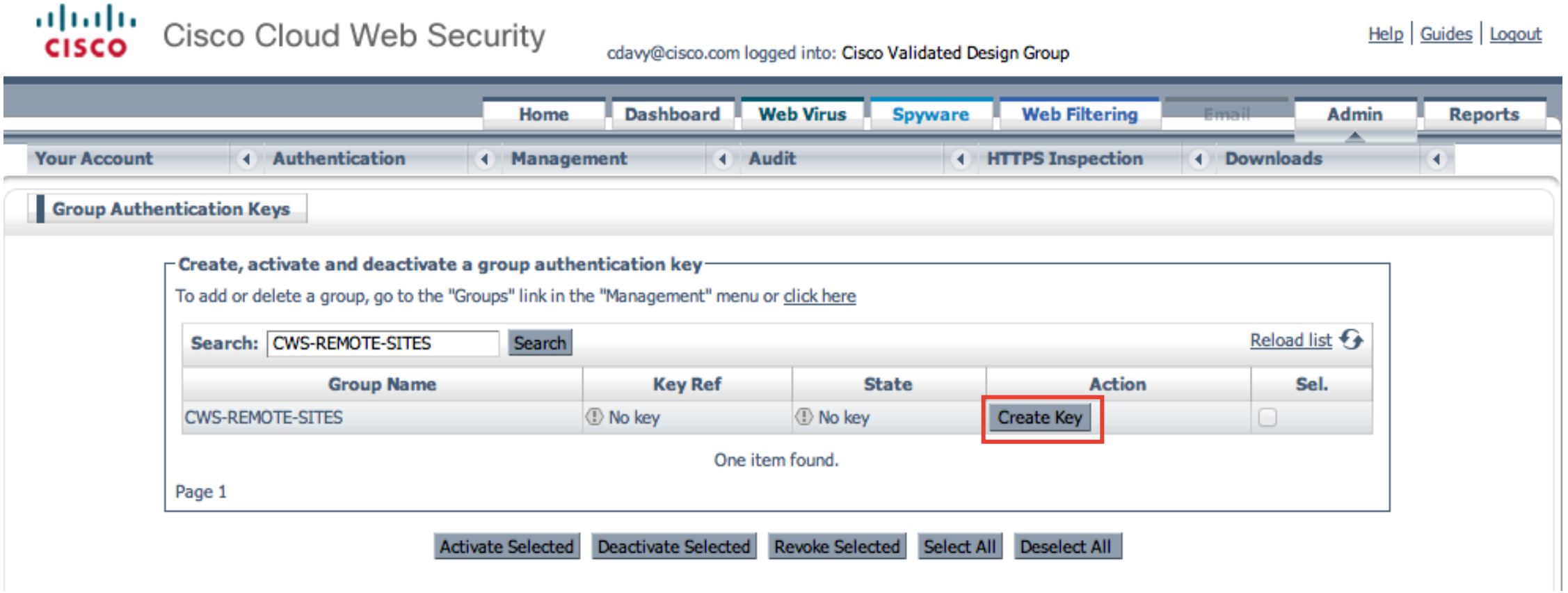
Must Match

```
parameter-map type content-scan global
 server scansafe primary ipv4 72.37.248.27 port http 8080 https 8080
 server scansafe secondary ipv4 69.174.58.187 port http 8080 https 8080
 license 0 893EECEED111C32D2A205A8204079043
 source interface GigabitEthernet0/0
 user-group CWS-REMOTE-SITES
 server scansafe on-failure block-all
```

Cloud Web Security

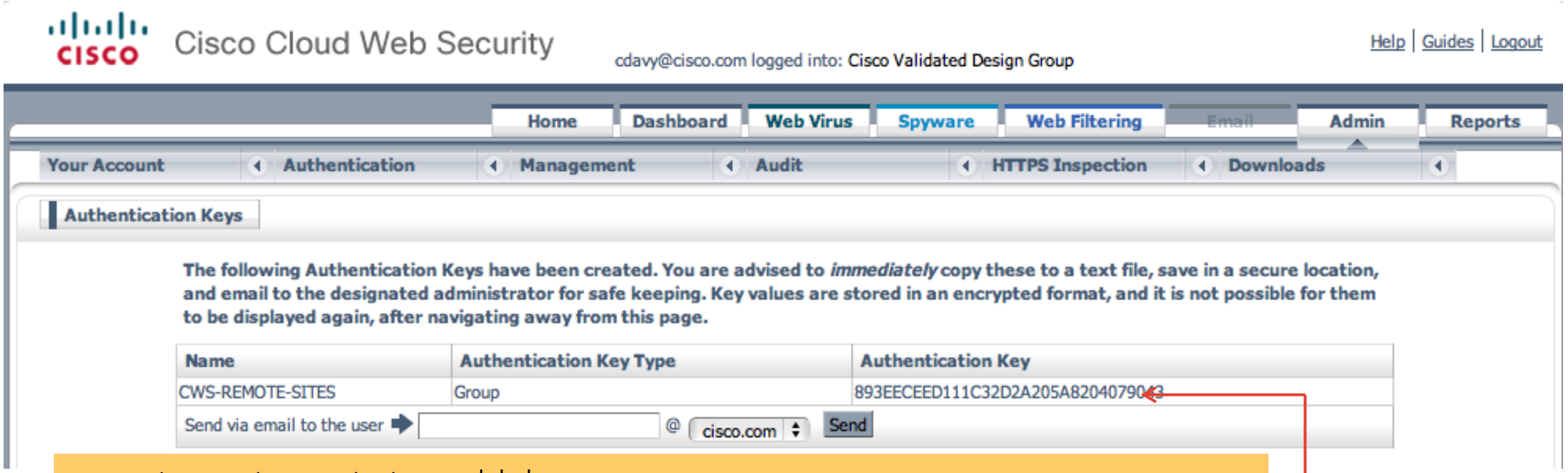
Cisco ScanCenter Portal – 그룹 키 생성

Cisco Connect



Cloud Web Security

Cisco ScanCenter Portal – 그룹 키 생성

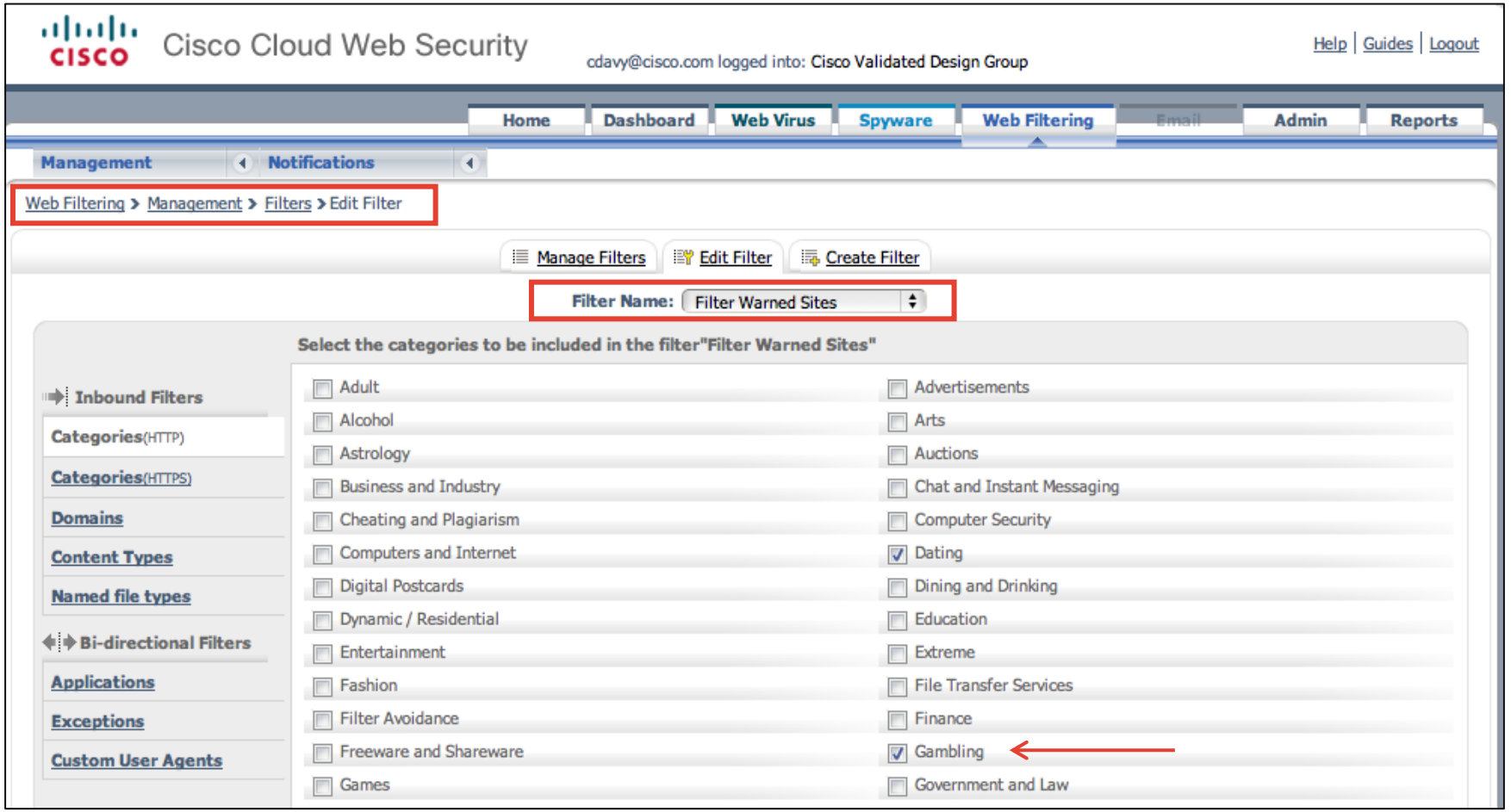



```
parameter-map type content-scan global
 server scansafe primary ipv4 72.37.248.27 port http 8080 https 8080
 server scansafe secondary ipv4 69.174.58.187 port http 8080 https 8080
 license 0 893EECEED111C32D2A205A8204079043
 source interface GigabitEthernet0/0
 user-group CWS-REMOTE-SITES
 server scansafe on-failure block-all
```

Must Match

Cloud Web Security

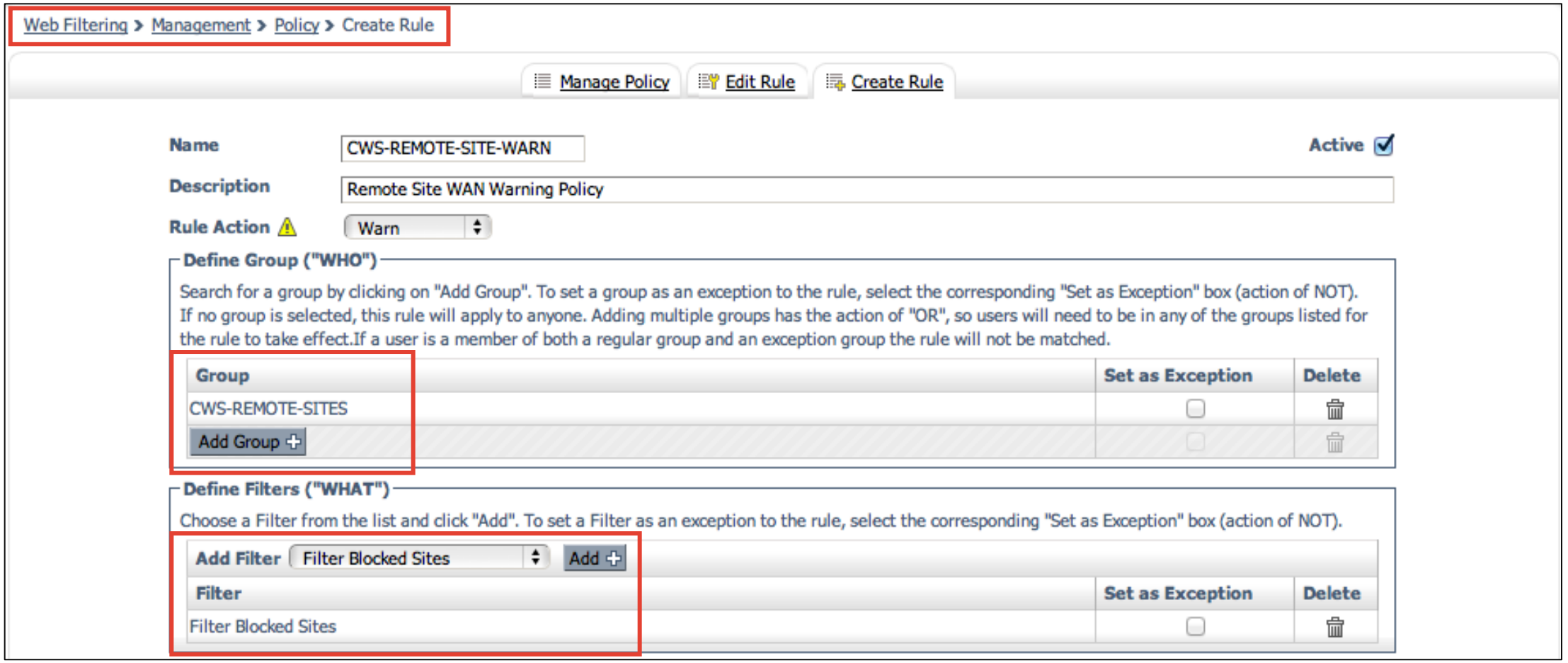
Cisco ScanCenter Portal – 필터 생성



Cloud Web Security

Cisco ScanCenter Portal – 정책 설정

Cisco Connect

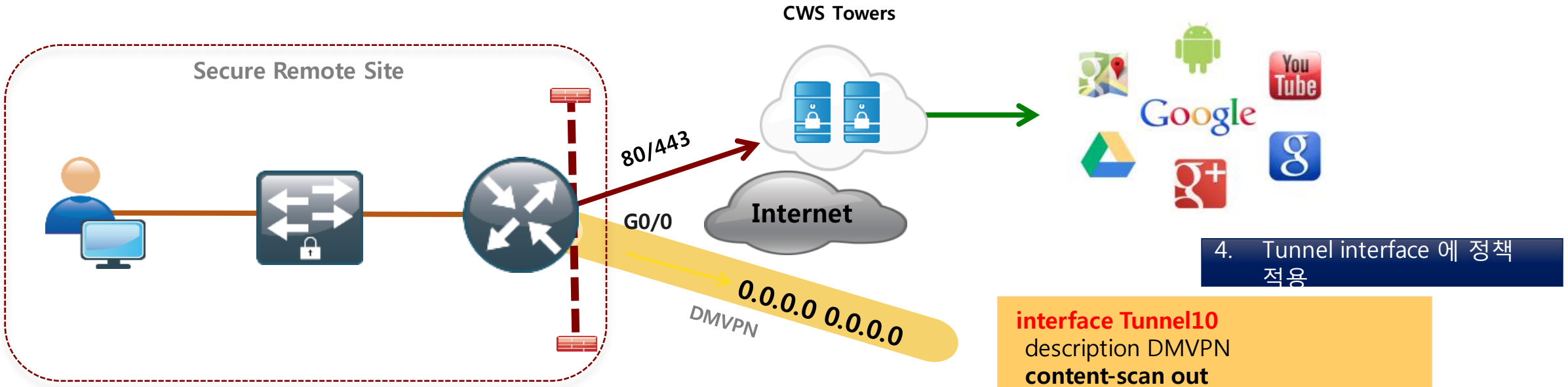


라우터 상의 CWS 설정

Direct Internet Access를 위한 CWS 기본 설정

```
parameter-map type content-scan global
 server scansafe primary ipv4 72.37.248.27 port http 8080 https 8080
 server scansafe secondary ipv4 69.174.58.187 port http 8080 https 8080
 license 7 04095B242A071A6A513B5133422D2F550B790170631074465233215204OF010502
 source interface GigabitEthernet0/0
 user-group CWS-REMOTE-SITES
 server scansafe on-failure block-all
```

1. ScanSafe server 지정
2. License 설정
3. 사용자 그룹 설정



4. Tunnel interface 에 정책 적용

```
interface Tunnel10
 description DMVPN
 content-scan out
```

CWS whitelist 설정

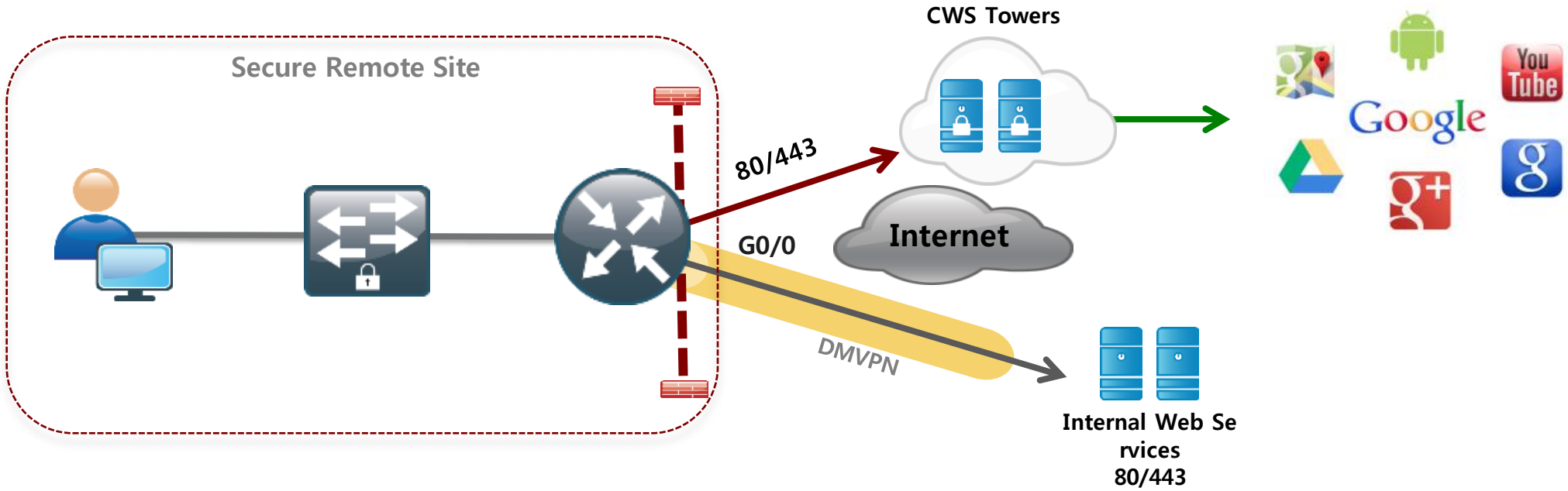
내부 웹 서비스를 위한 whitelist 설정

```
ip access-list extended CWS-EXCLUDE
 permit ip any 10.0.0.0 0.255.255.255
```

1. 내부 웹 서비스를 위한 ACL 조건 설정

```
content-scan whitelisting
 whitelist acl name CWS-EXCLUDE
```

2. 생성한 ACL을 Whitelist에 적용



Cisco Connect
Seoul, Korea
April 1-2, 2015

6. IWAN Management

Cisco IWAN 관리

Cisco Connect

구축 관리 및 Inventory 관리

Prime Infrastructure 2.2

End-to-End 배포 관리 및 Configuration 관리

- **Single-pane view of IWAN**
- IWAN 배포를 위한 workflow 제공
- Plug and Play 지원
- DMVPN, QoS, AVC 배포 및 모니터링
- PfR v3 지원
- 네트워크의 Health monitoring

어플리케이션 관리 및 가시성

LiveAction
Simplifying the Network

어플리케이션 인식 기반의 네트워크 성능 모니터링

- **Cisco AVC와 PfR의 통합**
- 어플리케이션 트래픽의 분석 및 모니터링
- End-to-end flow 가시화
- Flow 및 앱 기반의 장애처리
- 실 시간 모니터링

클라우드 기반의 관리

glue™ NETWORKS

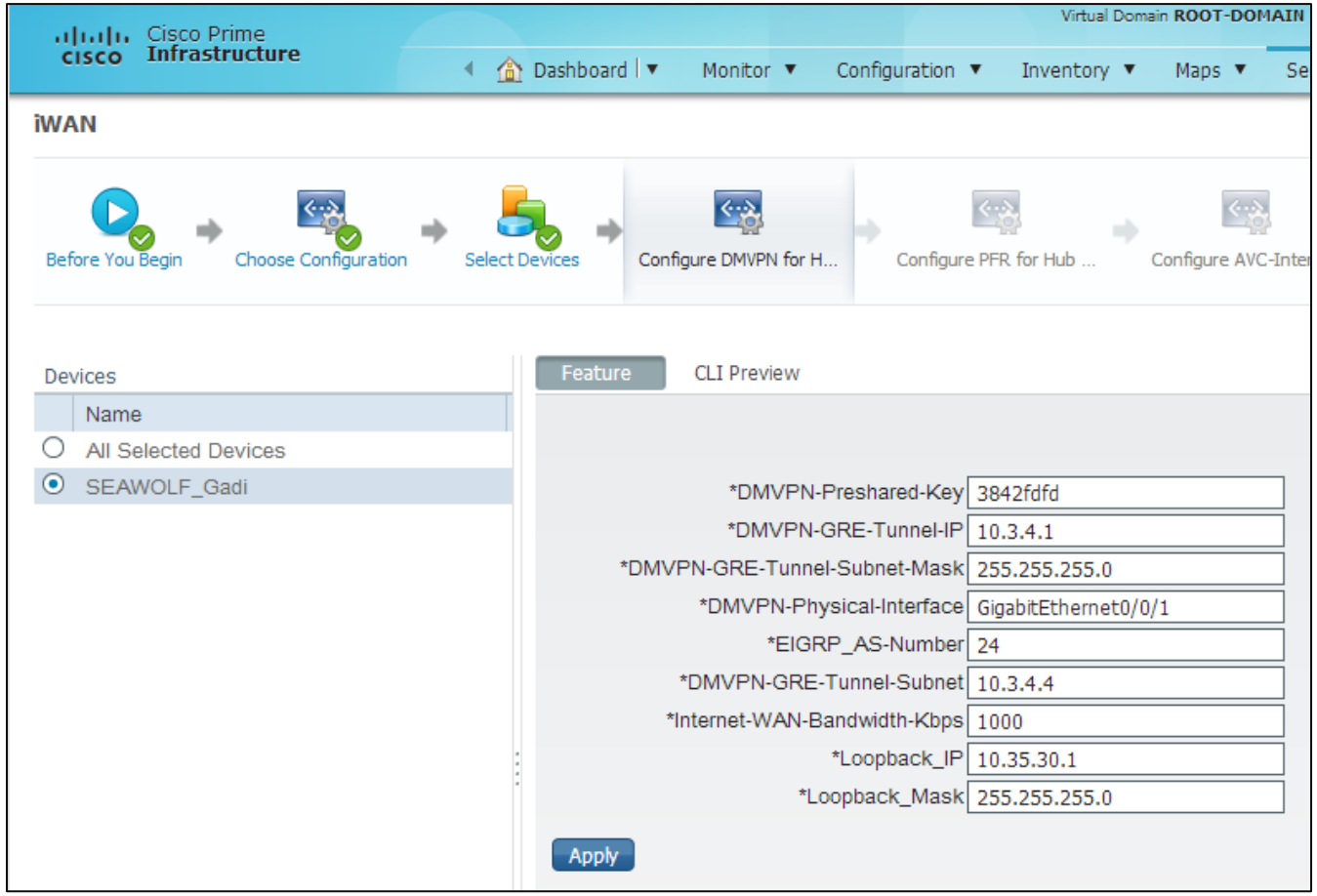
자동화 된 장비 배포 및 Lifecycle 관리

- **WAN 구축에 대한 수동적인 요소 제거**
- 자동화 된 WAN orchestration
- 중앙 집중적인 hybrid WAN 관리
- 빠른 Configuration 및 IOS 업그레이드
- OnePK 및 REST API 수용

Prime Infrastructure 2.2

Cisco Connect

- PnP 지원을 위한 IWAN workflow 마법사 제공
- 탬플릿 기반의 IWAN 설정
- PfRv3 도메인, MC/BR 설정
- AVC에 대한 원클릭 설정 지원
- QoS 설정 지원
- CVD 기반의 탬플릿 및 커스터마이징 제공
- AVC Readiness Assessment
- AVC, QoS, PfR 가시성 제공
- APIC EM 서비스와의 연동



Prime Infrastructure Plug-n-Play

Cisco Connect

PnP 1

USB 메모리를 이용한 Installation

- Installer connects LAN/WAN cables
- ISR은 USB메모리를 통해서 bootstrap을 로딩

PnP 2

Prime Plug-n-Play 어플리케이션

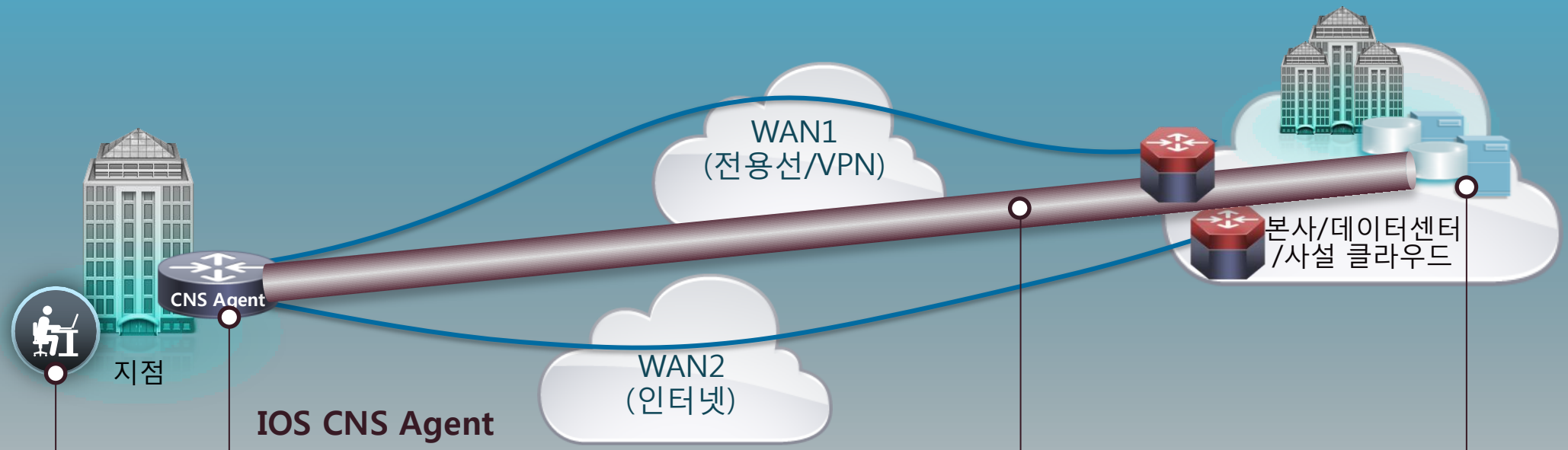
- Installer connects LAN/WAN cables + a USB console cable to a Laptop/iPhone/iPad
- PnP 어플리케이션이 라우터의 bootstrap을 로딩

PnP 3

Cisco Configuration Professional Express (ISR Device GUI)

- Installer connects LAN/WAN cables + a PC to a LAN port
- CCP Express 어플리케이션이 라우터의 bootstrap을 로딩

Prime Infrastructure Plug-n-Play



IOS CNS Agent

PnP 서버 접속을 위한 bootstrap configuration 사용

CNS Protocol

IOS 이미지 및 초기 configuration loading을 위한 Cisco PnP protocol

PnP Application

IOS장비의 부팅과 인증을 위한 설치 어플리케이션 (iPhone, iPad, Windows PC)

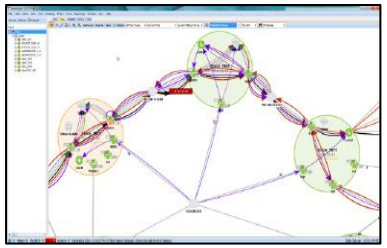
Prime Infrastructure Server

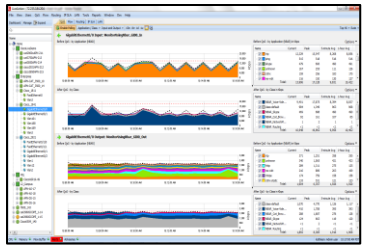
Deployment에 대한 관리/배포 정보를 포함 (images, configurations, and licenses)

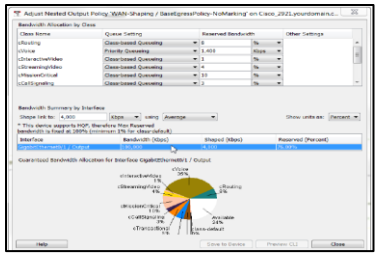
LiveAction

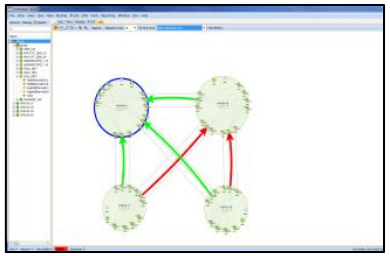
- 어플리케이션 인식 기반의 네트워크 성능 관리
- QoS 제어 어플리케이션
- 개별 어플리케이션에 대한 flow를 실 시간 모니터링
- 라우팅 및 IP SLA에 대한 직관적인 경로 제공
- QoS에 대한 상태 모니터링 및 설정 기능 제공

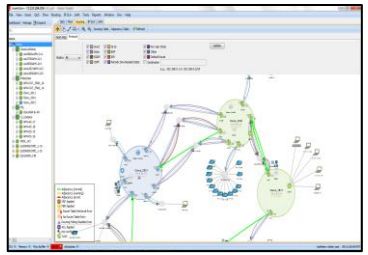
LiveAction 구성 요소

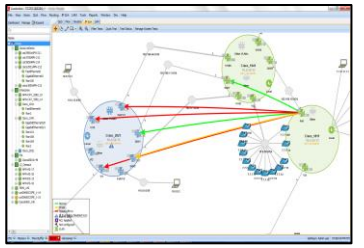

Flow


QoS Monitor


QoS Configure


LAN

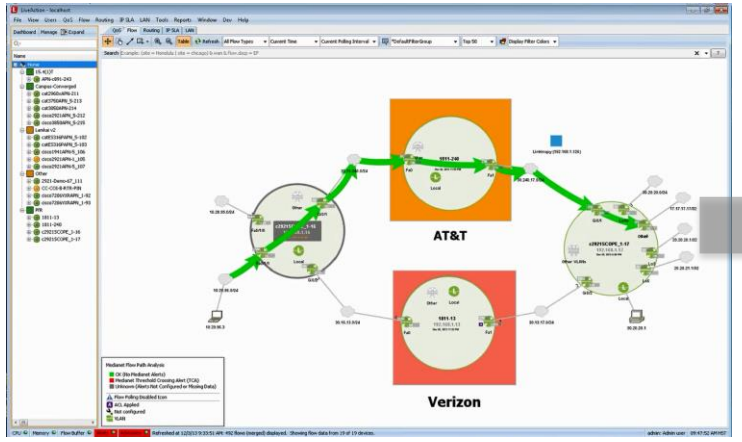

Routing


IP SLA

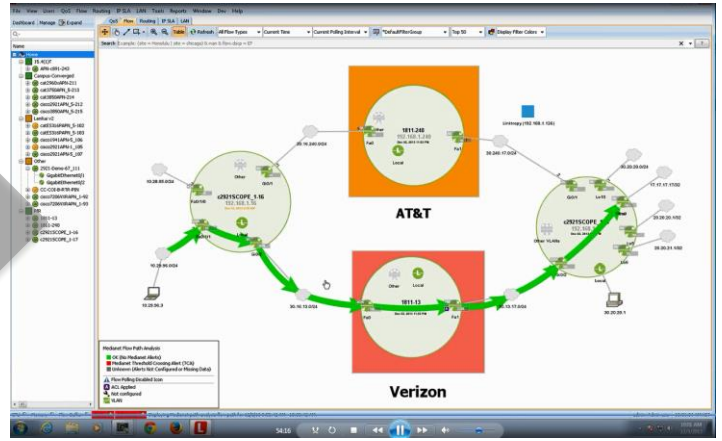
지능적 경로 관리

- PfR 경로에 대한 변경 시, 가시적인 모니터링 제공
- PfR 정책에 대한 이벤트 발생 시, 알람 및 리포팅
- 트래픽 클래스 및 어플리케이션 별, 리포팅 제공

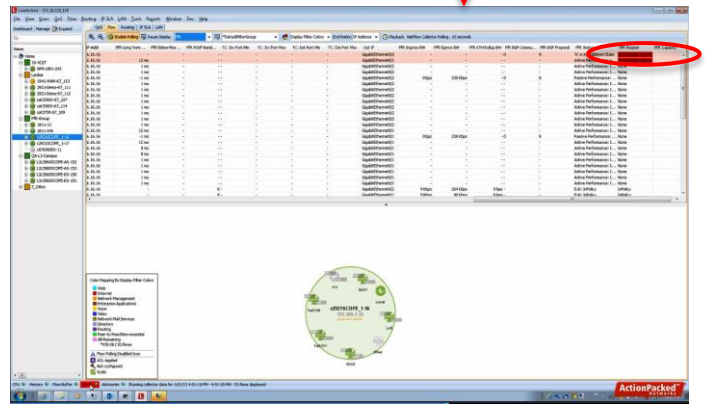
Before Brown-Out (Northern Path)



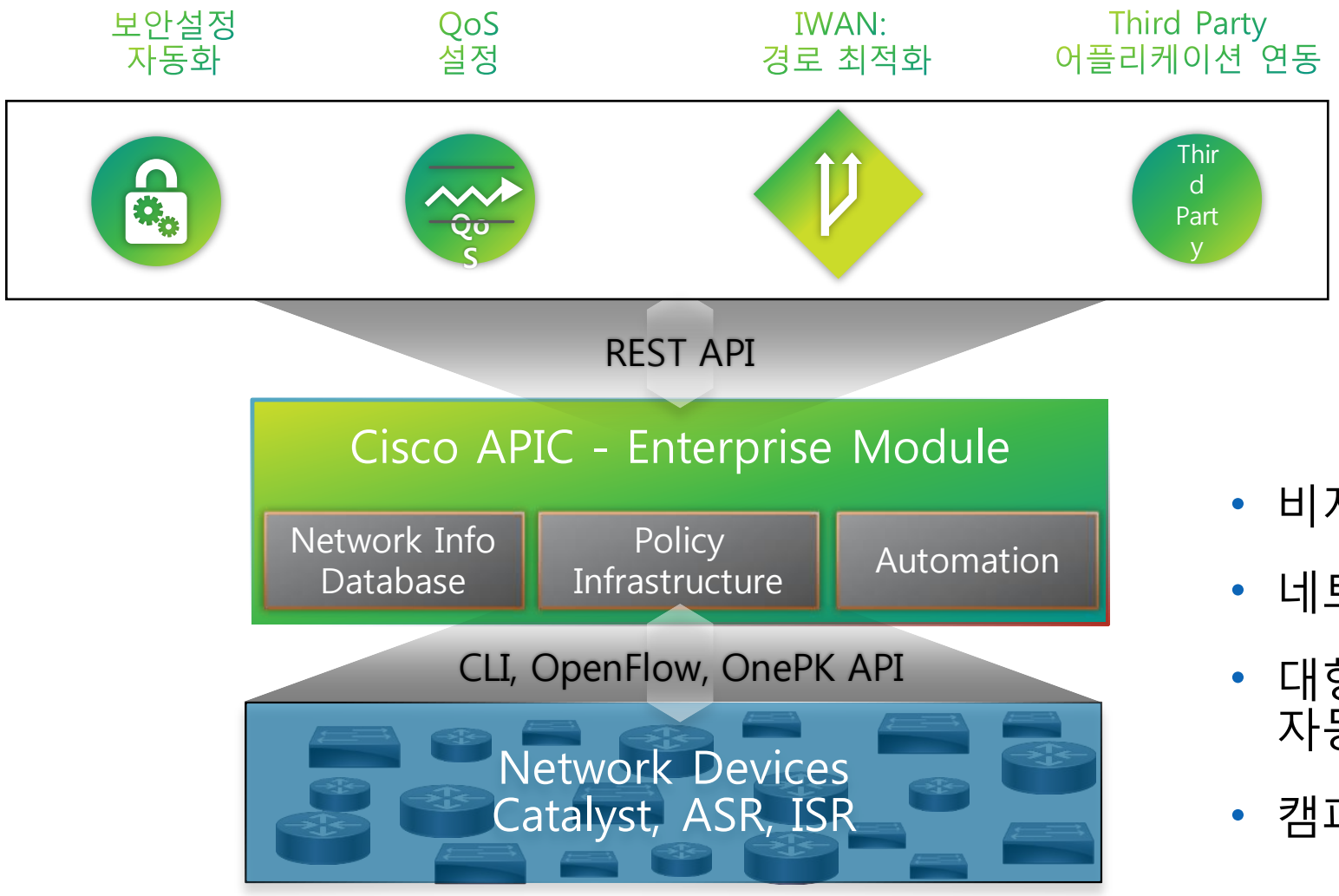
After Brown-Out (Southern Path)



Out-Of-Policy Threshold Crossing Alert



Cisco APIC - Enterprise Module



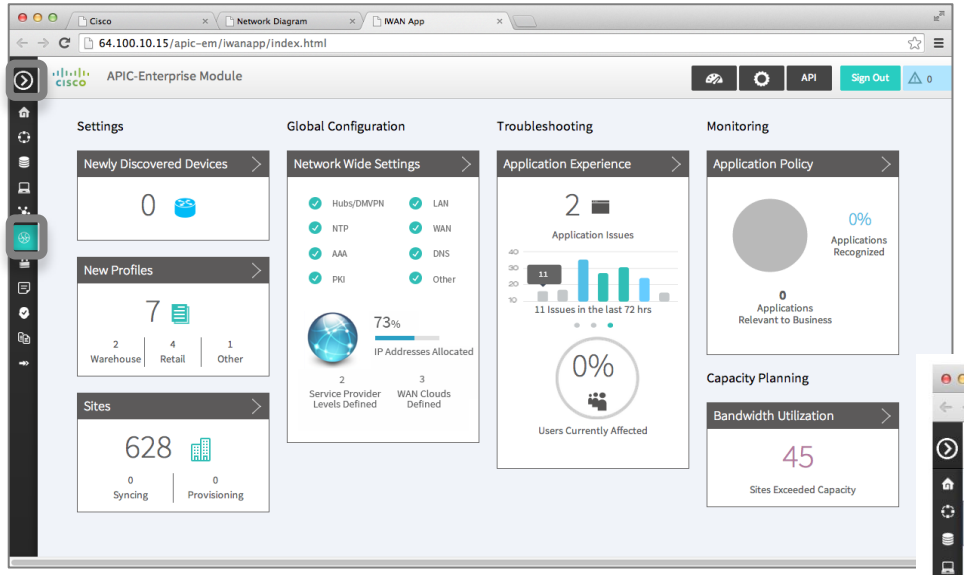
Cisco Prime

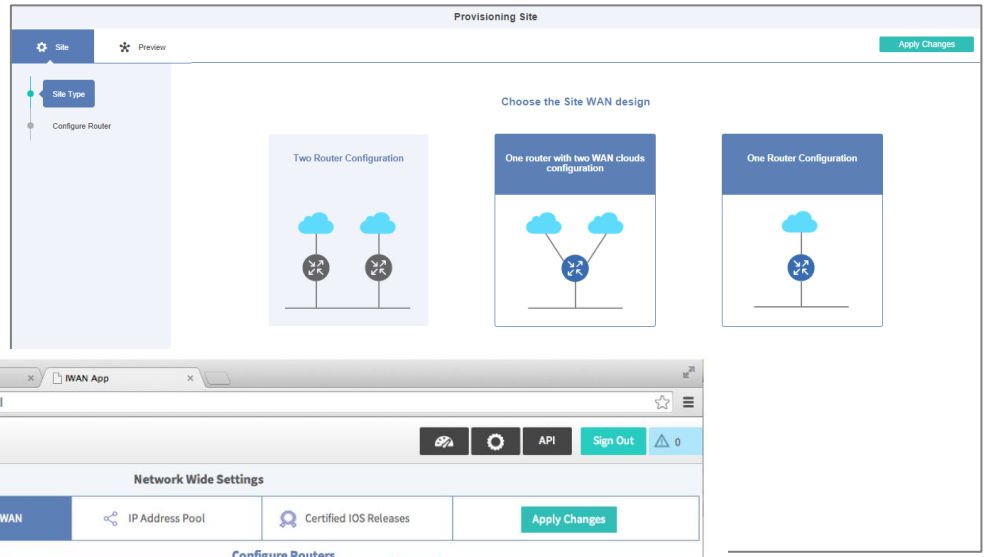
glue NETWORKS

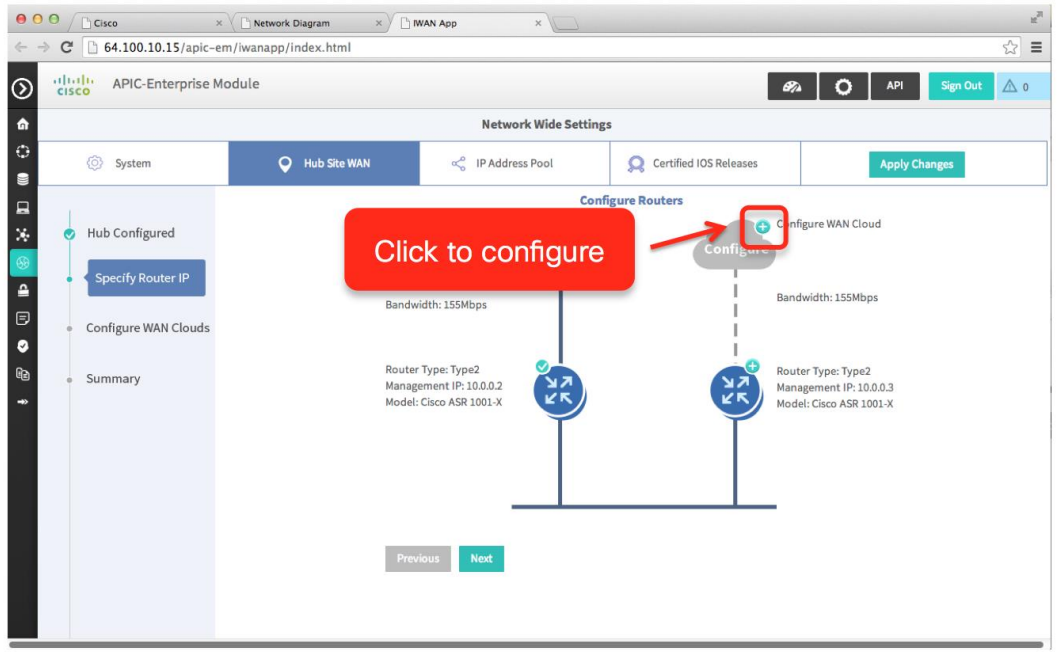
LiveAction

- 비지니스 환경 개선을 위한
- 네트워크의 지능화 및 전문화
- 대형 네트워크의 구축 및 배포의 자동화
- 캠퍼스 네트워크의 통합

Cisco APIC-EM 예제





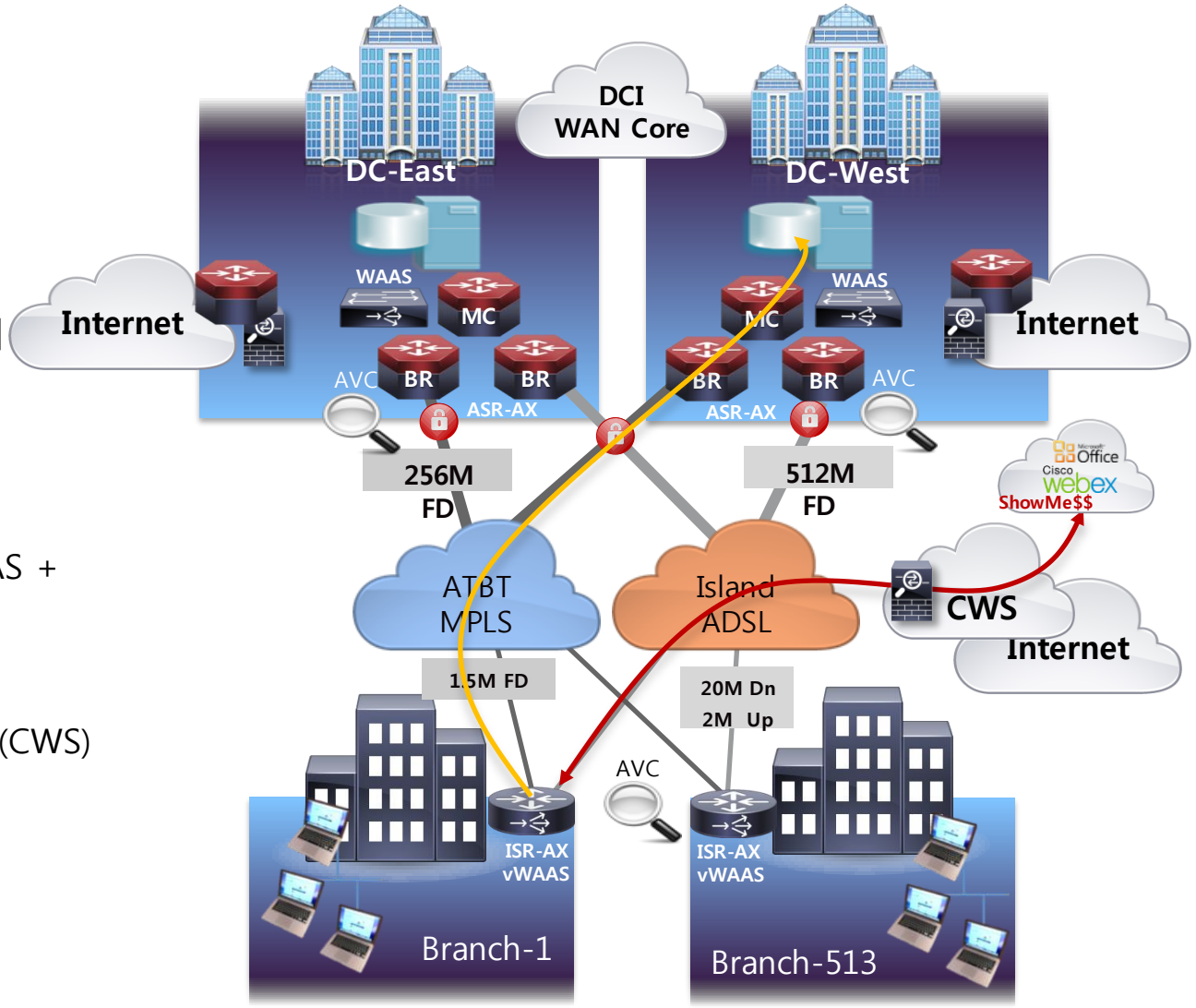


Cisco Connect
Seoul, Korea
April 1-2, 2015

7. Why Cisco IWAN?

Summary

- 다양하고 독립된 회선 사용
  - Hybrid MPLS + Internet 회선 사용
    높은 HA 제공 및 회선의 대역폭 사용률 제공
- 지능적인 경로 관리
  - 주요 어플리케이션 성능 보장을 위한 Performance Routing 지
  - 최적의 WAN 대역폭을 위한 Load-balancing 제공
- 어플리케이션 최적화
  - 지점의 어플리케이션 성능 모니터링을 위한 AVC
  - 어플리케이션 성능 향상과 대역폭 낭비를 방지하기 위한 WAAS + Akamai
- 보안이 강화된 회선 연결
  - 공용 클라우드 서비스 성능 향상을 위한 Cloud Web Security (CWS)
- IWAN 통합 관리
  - Prime, LiveAction, or GlueWare을 통한 다양한 관리 툴 제공
  - APIC-EM과 통합으로 SDN 솔루션 제공



IWAN의 비전 및 전략

Cisco Connect

지능적인 가상화 → 자동화 → 클라우드 서비스 통합 → 서비스 가상화 → SELF LEARNING NETWORKS

Predictive
Self Directed

vRouter, vService and App Orchestration

ACI 연동, Inter-Cloud 이동성 제공, 최적화, AMP

보안성, 단순성, 중앙집중적 정책 자동화

Secure VPN Overlay, 다양한 회선 사용, 대역폭의 효율성 증대, 애플리케이션의 SLA 보장

Thank You