유연한 확장성을 보장하는

금융권 스마트 가상 인트라넷 구축

차세대 SSL VPN 솔루션의 방향은?

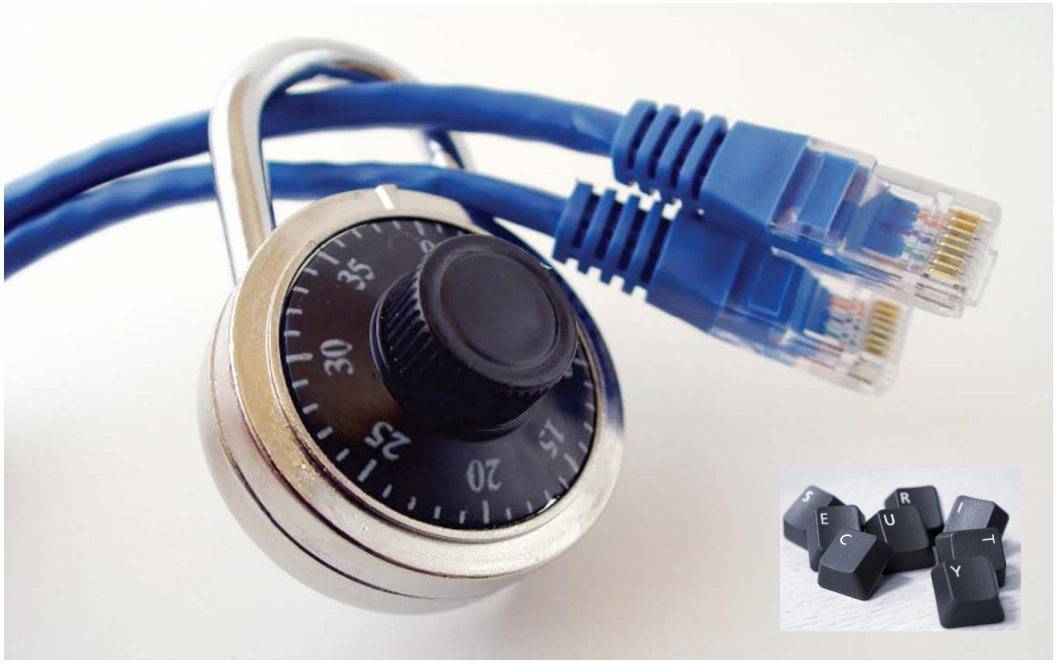
주니퍼 네트웍스

박달수 부장 (brianpark@juniper.net)

발표 순서

- SSL VPN 솔루션의 등장 그리고 기술의 발전
- Client 환경의 변화 (BYOD) 및 보안 위협 증가
- 차 세대 SSL VPN Solution 의 방향
- Juniper MAG Series 소개(신규 Platform)
- 차 세대 통합 모듈 Junos Pulse 소개

SSL VPN Solution의 등장 그리고 기술의 발전



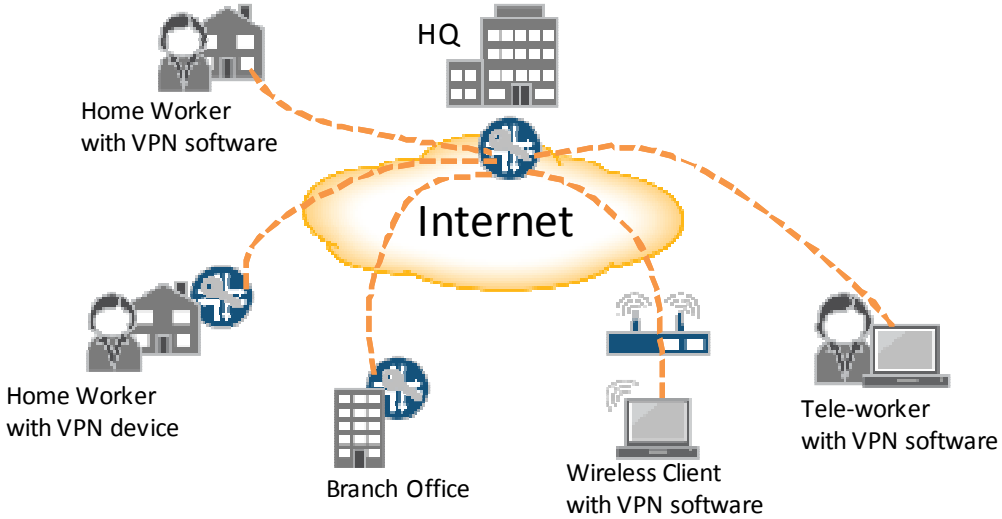
What's VPN (Virtual Private Network) ?

Internet 망을 통해 가상으로 사설망을 구축하여 고비용의 전용선을 대체하는 기술

IPSec VPN 은 인증/암호화/터널링 기술로 본사와 지점을 *Internet*을 통해 안전하게 연결

LAN to LAN (HQ – Remote office) 환경에서는 *IPSec VPN*이 가장 보편화된 기술

이동 사용자들은 *Software* 기반의 *IPSec VPN* 으로 본사 *Network*에 *Access* 가능



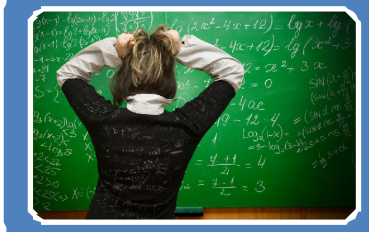
*IPSec VPN*의 한계 및 문제점

*IPSec VPN*은 *LAN to LAN* 환경에 최적화

- 본사와 지점간 IPSec VPN전용 장비를 통해 Tunneling 으로 구축 완료
- 사용자(Client) 입장에서 설정 변경 전혀 없음

원격 근무자(재택근무, 이동근무)를 위한 *VPN* 연결 방법 필요

- 원격 근무자 PC 에 IPSec Software를 설치하여 본사와 VPN 연결 가능
- IPSec Software 설치 후 설정 작업 필요 (사용자의 몫)



*Software Based IPSec VPN*의 문제점

- Software 배포 / 설치 / 설정 / 장애처리 관련된 업무 증가
- IPSec Protocol 특성상 인터넷 구간에서 잦은 장애 발생 (Firewall/ NAT / MTU 문제 등)

이동 근무자를 위한 최적의 *Solution*은?

SSL VPN solution 등장

- Software IPSec VPN 기술의 대안으로 SSL VPN 탄생
- Web기반의 Secure Socket Layer 기술을 응용한 VPN 솔루션으로서 Ubiquitous 컴퓨팅을 위한 필수 요소로 자리 매김

*SSL VPN*의 장점

- 사용자 관점에서 VPN 접속을 위해 필요한 것은 Only 인증(Login)뿐 !!
- 인터넷 환경 친화적인 SSL Protocol 사용으로 장애 확률 감소
- 사용자 편의성이 증대되고, 관리/운영비용의 감소
- Client / Group 별로 매우 세밀한 정책 수립 가능하여 보안성 증대 !
- 이동 근무자를 위한 최적의 Secure Access Solution !

1st Generation

*SSL VPN 1*세대 기술

- Web Browser 기반으로 완벽히 Clientless한 Secure Access Service 제공
- Simple 한 HTML로 짜여진 HTTP / HTTPS 기반의 Application 지원
- Proxy 방식에 의존한 SMB File Access 및 E-mail 에 대한 Secure Access 지원
- C/S 기반의 Application 미 지원으로 IPSec Software 를 완벽히 대체하지 못함

2nd Generation

*SSL VPN 2*세대 기술

- Application 지원 범위 확장을 위해 ActiveX 또는 Java- VM을 통해 Thin Client module을 사용자 Machine에 자동 설치하는 방식으로 변환
- Web Application 외에도 TCP 기반의 일반 C/S Application 지원
- NetBIOS protocol 및 Terminal Service 에 대한 지원
- Network Layer 에서의 Full Connectivity가 필요한 Application 지원 불가

3rd Generation

*SSL VPN 3*세대 기술 *(*성숙 단계*)*

- Network Layer에서 Full Connectivity를 제공하는 L3VPN 모듈을 통하여 모든 Application 에 대한 Accessibility 제공 함
- VDI 모듈을 탑재하여 인증된 사용자에게 가상 Desktop 환경 제공
- 다양한 Device 및 OS 환경에 대한 Support (Windows / Mac / Linux)

Client 환경의 변화 (BYOD) 및 보안 위협 증가

*Platform*의 다양성 & 지속적인 증가

Today's Mobile, Always on/Always connected LIFE

Proliferation of Devices

*Number of mobile devices sold worldwide expected to reach 1.9 billion in 2012**

Connected Socialization

Content Consumption

**Source: Gartner, Inc., Mobile Devices, Worldwide, 2008-2015, 4Q11 Update*

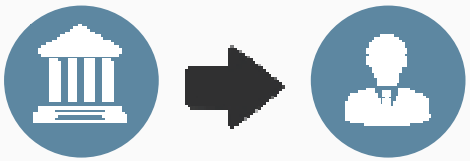
JUNIPER

보안위협의 증가

THE NEW SECURITY LANDSCAPE

Attacker

Attackers are using new indirect techniques to bypass perimeter security



Threats

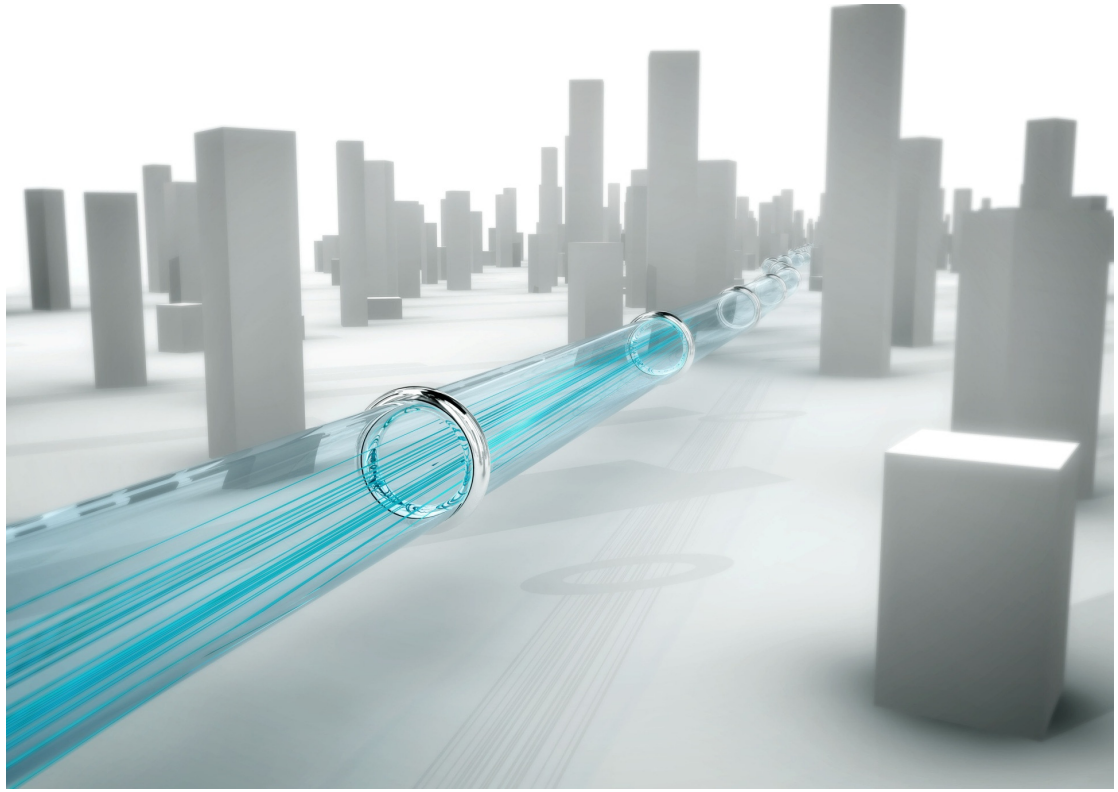
Attackers gain control of user devices

Target

Once inside, they go after sensitive data and intellectual property

새로운 환경에 대처하는

차세대 SSL VPN 솔루션의 방향은?



4th Generation

R U Ready?

4th Generation

Next Generation SSL VPN Solution…

- 다양한 Platform을 지원하며, 신규 Version Release시 즉각적인 Support
- 단일 Client Module에서 통합 기능을 제공 (L3 VPN / NAC / Application 가속 / Security 기능 등)
- 모바일 단말에서 개별 Application(업무용) 단위의 VPN Tunneling 지원
- 꾸준히 증가되는 사용자와 Traffic을 수용하기 위한 유연한 확장성 보장
- IPv6 으로의 Transition시에도 Network Full Connectivity를 제공
- Cloud 환경에 적합한 Virtual Appliance 형태의 Service 제공
- 미래의 새로운 Trend / Technique 탑재가 준비 되어있는 유연한 Platform

차세대 Secure Access 솔루션

Juniper MAG Series / Junos Pulse Client

Juniper만의 차세대 Secure Access 솔루션

MAG

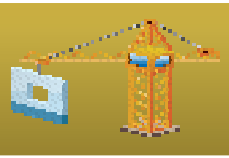
AppConnect

Junos Pulse

단일 Client , 단일 Gateway

고집적도 모듈형 설계

기능 전환 (Common License)



유연한 확장성

다양한 Platform 지원

New Technique Integration

Juniper MAG Series 제품 Lineup (Gateway Device)

MAG2600

- Appliance Type
- 1U Rack Size, ¼-width , 30W power consumption.
- 최대 100 SSL VPN users

MAG4610

- Appliance Type
- 1U Rack Size , ½-width
- 최대 1,000 SSL VPN users (or 5000 NAC users)

MAG6610

- **Chassis Type / Service module 2장 장착 가능**
- 1U Rack Size
- Optional management module
- 20,000 SSL VPN users or 30,000 NAC users

MAG6611

- **Chassis Type / Service module 4장 장착 가능**
- 2U Rack Size
- Optional management module.
- 40,000 SSL VPN users or 60,000 NAC users

MAG Chassis 구성 module

SM160
(Service module)

- MAG6610 / MAG6611 Chassis 에 장착
- 1,000 SSL VPN / 5,000 NAC users

SM160

SM360
(Service module)

- MAG6610 / MAG6611 Chassis 에 장착
- 10,000 SSL VPN / 15,000 NAC users

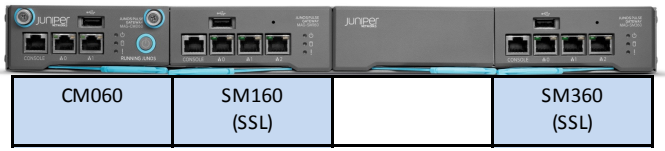
SM360

CM060
(Management Module)

- SM160 / SM360 Module 에 장착
- Chassis management 용도

CM060

MAG6610



CM060	SM160 (SSL)		SM360 (SSL)

✓ SSL VPN : 11,000 Users
✓ Chassis management

MAG6611

CM060	SM160 (UAC)		SM360 (SSL)
	SM360 (SSL)		SM360 (SSL)

✓ SSL VPN : 20,000 Users
✓ NAC : 5,000 Users
✓ Chassis management

Juniper MAG 6600 Series 특징

특징	설명
Single 클라이언트 모듈, Single 게이트웨이 장비	하나의 Chassis 에서 SSL VPN & NAC Gate 역할 수행 하나의 Client 모듈(Junos Pulse)로 SSL VPN & NAC Client
기능 스위칭	Service module 내에서 기능 변경 가능 (e.g., SSL VPN today, NAC tomorrow)
모듈 Type의 Design	고객사 요구사항에 따라 Chassis내에 서비스 모듈을 다양한 방식으로 Mix & Match
유연한 확장성	MAG6611 Chassis에서 최대 40,000 SSL VPN User 또는 60,000 NAC User 까지 확장 가능
Common access licenses	SSL VPN User 와 NAC User에게 동일한 License 적용
Third Party Integration	Application 가속 / Mobile Device Management (Riverbed / MobileIron / Airwatch / Samsung Knox)

License Server로 관리 시 장점

✓ 각 Member들은 License 서버에 Registration
✓ License Server에 각 Member별 정책 설정
(Reserved User / Max User)
✓ 평소에는 Reserved된 User License 수만큼 사용
✓ 동시 접속자가 Reserved User를 넘어설 경우
추가 License를 내려줌 (upto Max User)
✓ 동시 접속자가 평상 수준으로 복귀 시
추가 License 자동 반납

7,000 User Reserved
3,000 User available

✓ 구매한 User License는 License Server 에 일괄 등록

10,000 user 등록

Member-1

5,000 User Reserved

Member-2

100 User Reserved

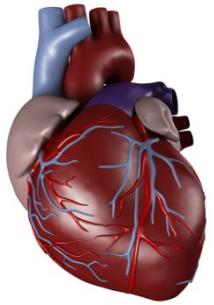
Member-3

400 User Reserved

Member-4

1,500 User Reserved

What is JUNOS PULSE ?



보안 접속 서비스 (L3 VPN)

Role-based, secure remote and mobile access to networks, clouds, and applications

Access Control 서비스 (NAC)

Standards-based, granular network access control

802.1X

JUNOS PULSE

모바일 보안 (Anti-Virus / Anti-Spam)

Comprehensive mobile device security, management and control

Third Party Integration

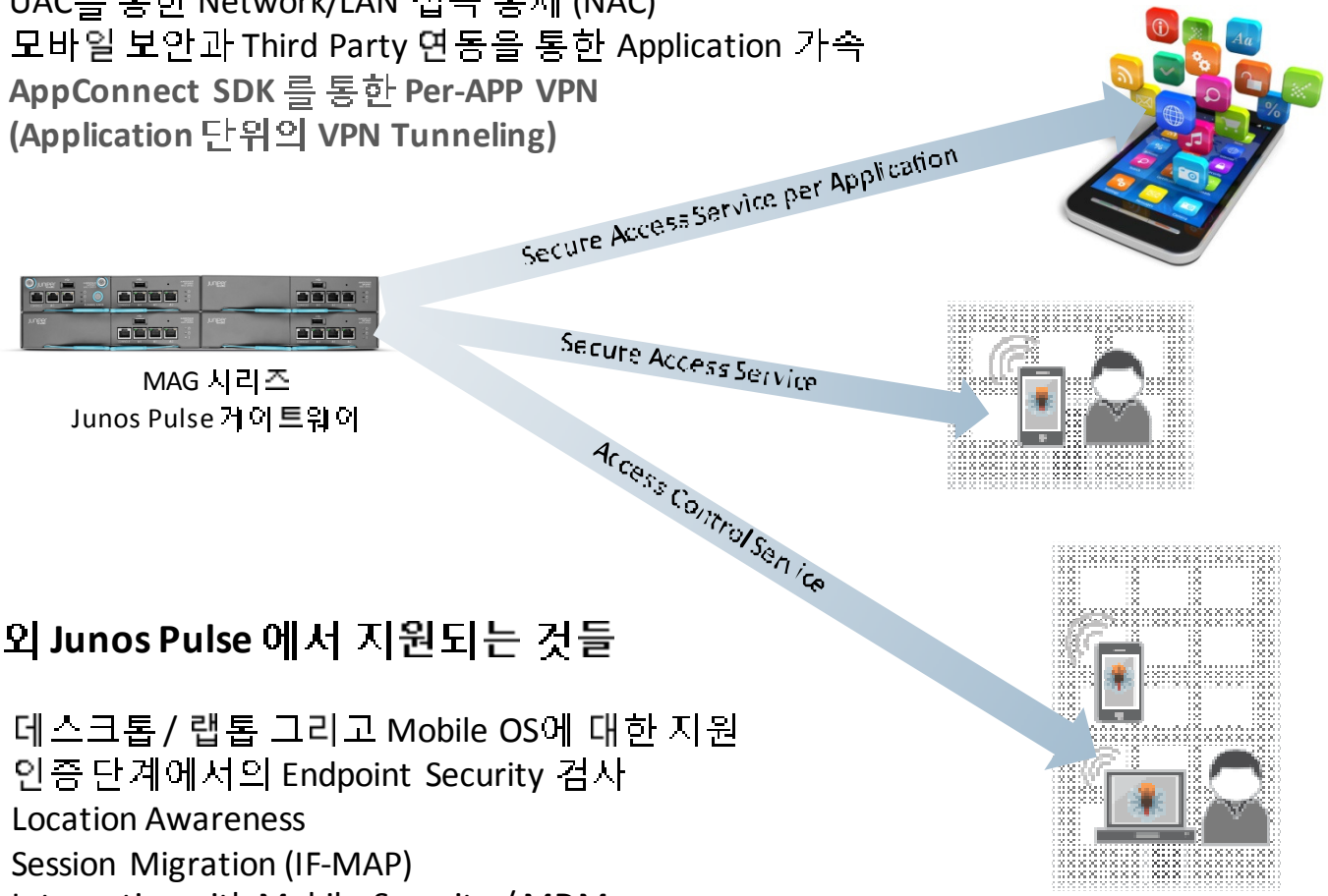
Application Acceleration
Mobile Device Management

✓ SSL VPN/NAC/Mobile Security 등의 기능을 통합한 Client Module
✓ Mobile / Desktop 의 다양한 Platform 을 지원 (iPhone, Android , Windows , Mac , Linux 등)
✓ MobileIron / Airwatch / Riverbed 와 Integration , Samsung Knox 지원

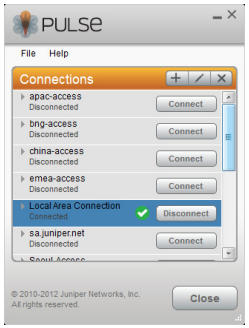
Junos Pulse 와 MAG를 통한 서비스

JUNOS Pulse Single Client 와 MAG Single gateway로 가능한 서비스

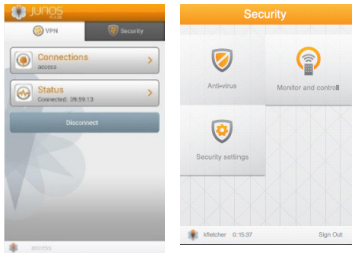
- SSL VPN 서비스를 통한 원격 보안 접속 (L3 VPN)
- UAC를 통한 Network/LAN 접속 통제 (NAC)
- 모바일 보안과 Third Party 연동을 통한 Application 가속
- **AppConnect SDK 를 통한 Per-APP VPN (Application 단위의 VPN Tunneling)**



MAG 시리즈
Junos Pulse 게이트웨이



Junos Pulse (on laptop/desktop)



Junos Pulse (on mobile device)

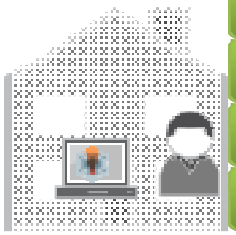
그 외 Junos Pulse 에서 지원되는 것들

- 데스크톱 / 랩톱 그리고 Mobile OS에 대한 지원
- 인증 단계에서의 Endpoint Security 검사
- Location Awareness
- Session Migration (IF-MAP)
- Integration with Mobile Security / MDM
- Integration with Application Acceleration

영업사원 김씨의 Junos Pulse 체험기

집
6 AM

1. 김씨가 집에서 일어나 E-mail 확인 차 PC를 켬
2. 김씨가 Remote 지역에 있다는 것을 Junos Pulse에서 감지
3. SSL VPN이 Access Type으로 선택됨
4. 사용자 인증
5. Junos Pulse로 SSL VPN Tunnel 연결
6. Application 가속 기능을 통한 빠른 연결



커피숍
10 AM

1. 김씨가 고객과의 미팅으로 "까페베네"로 이동 후 PC를 켬
2. PC가 Wi-Fi에 자동 연결
3. 김씨가 Remote 지역에 있다는 것을 Junos Pulse에서 감지
4. SSL VPN이 Access Type으로 선택됨
5. 기존 Session이 연결되어 있으므로 인증 필요 없음
6. Junos Pulse로 SSL VPN Tunnel 연결

영업사원 김씨의 Junos Pulse 체험기

사무실
1 PM

1. 김씨가 사무실로 이동 후 PC를 회사 무선 Network에 연결
2. Junos Pulse 에서 802.1X 인증이 필요한 것을 감지
3. NAC이 Access Type으로 선택
4. 인증 필요 없음 (Session 정보가 IF-MAP을 통해 migration 됨)
5. Junos Pulse로 회사 Network에 연결

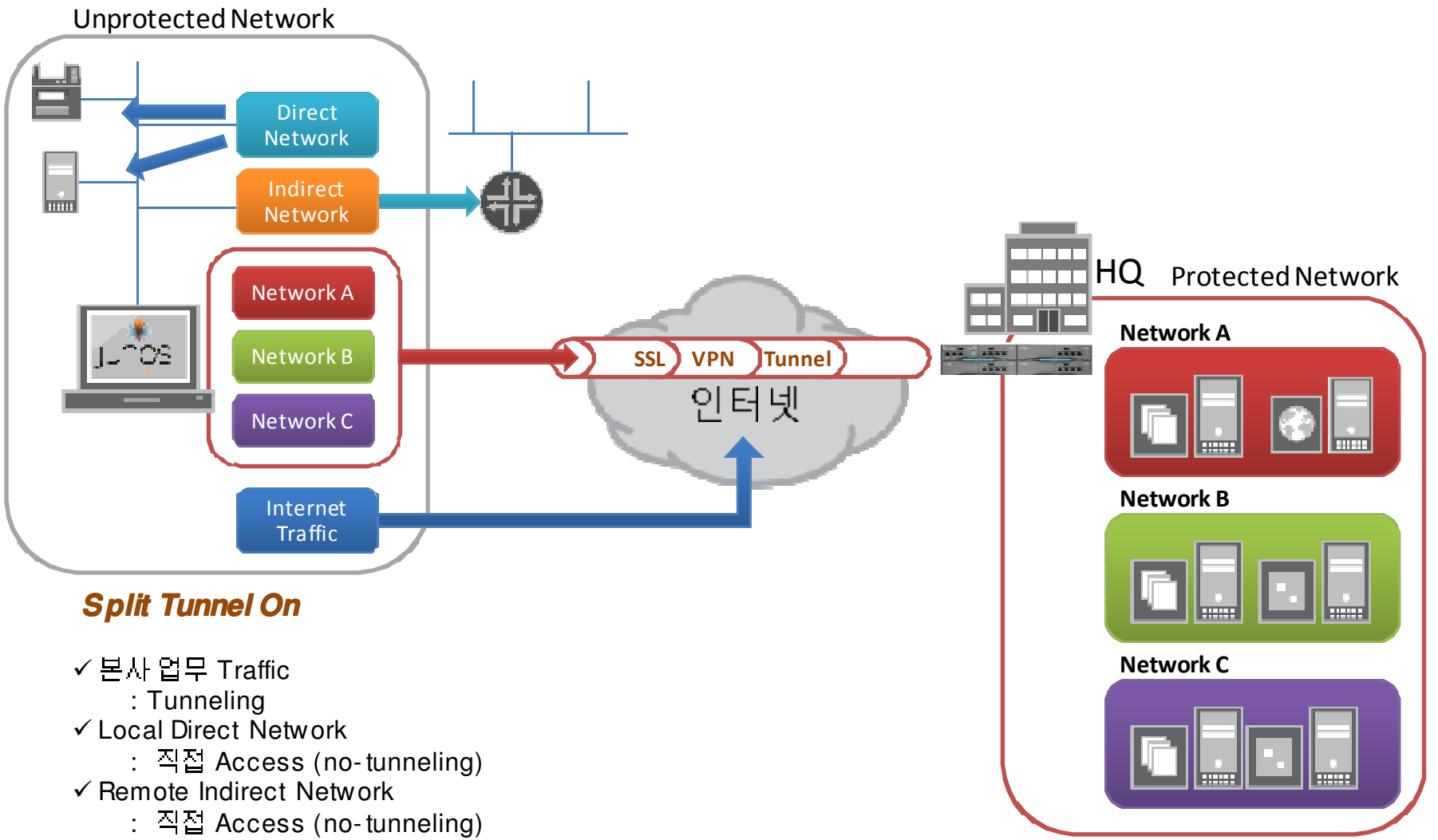
식당
7 PM

1. 김씨가 저녁식사 장소로 이동
2. 갑작스런 고객의 전화로 회사 ERP 시스템에 접속 필요
3. iPad 에서 ERP 앱 실행 (App Connect 로 Per-App VPN 개발)
4. ERP 앱 에서 사용자 인증
5. ERP 앱 과 MAG간 SSL VPN Tunnel 연결
6. iPad를 통해 회사 Email 과 ERP 시스템에 보안 접속 가능

업무 / 비업무 *Traffic* 의 논리적 분리

Split Tunnel mode	• 업무 Traffic 만 선별적으로 Secure Tunnel 로 처리 • 인터넷 등의 비업무 Traffic과 Local Network Traffic 은 직접 처리
Non-Split Tunnel mode	• Client의 모든 Traffic을 Secure Tunnel로 처리 (업무/비업무/인터넷/Local 포함)
Non-Split Tunnel + Local Access mode	• Local Network 프린터 / File Server등의 Local Network Access를 제외하고 모두 Secure Tunnel로 처리

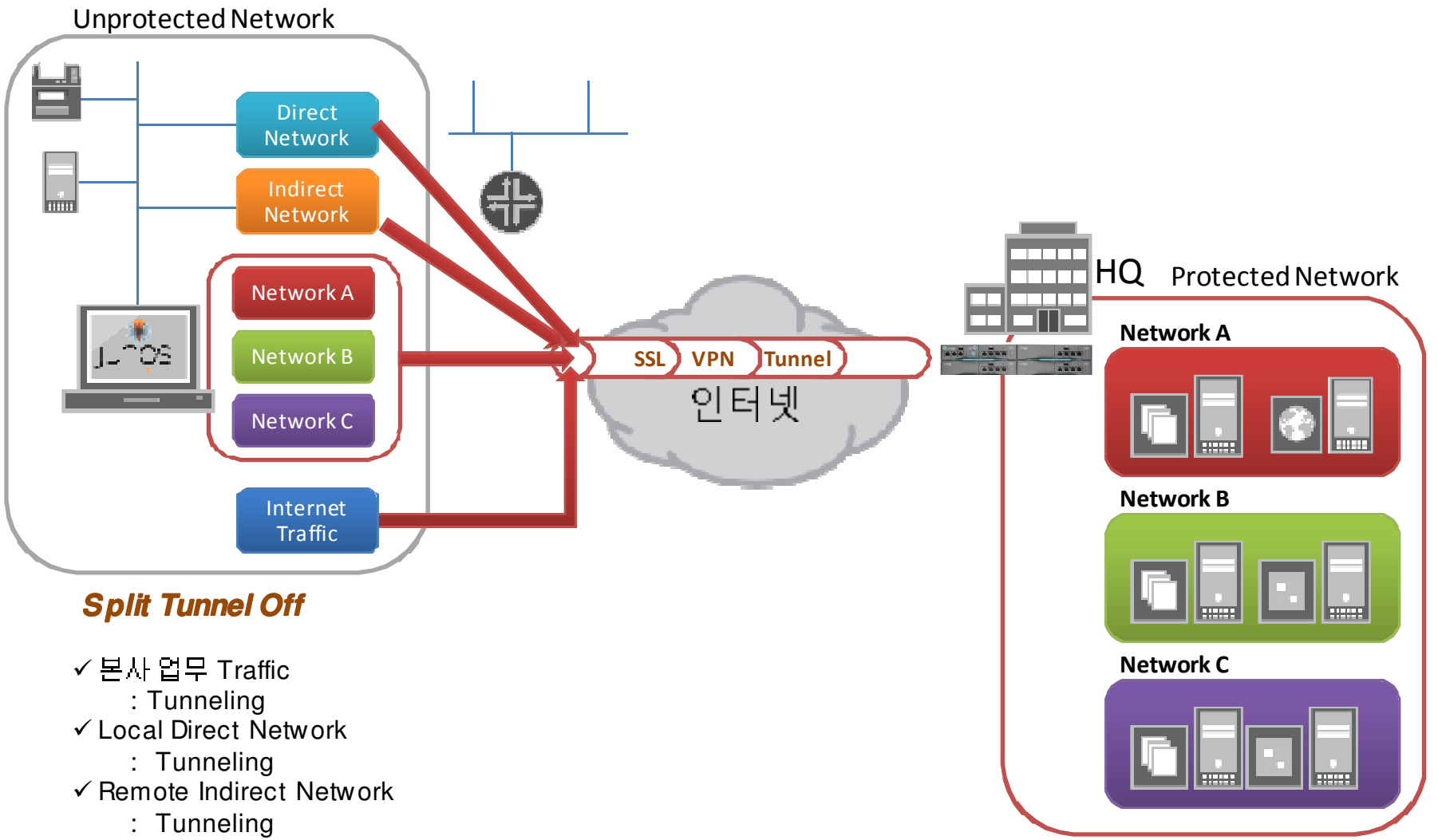
Split Tunnel mode



Split Tunnel On

- ✓ 본사 업무 Traffic
  : Tunneling
- ✓ Local Direct Network
  : 직접 Access (no-tunneling)
- ✓ Remote Indirect Network
  : 직접 Access (no-tunneling)
- ✓ Internet Traffic
  : 직접 Access (no-tunneling)

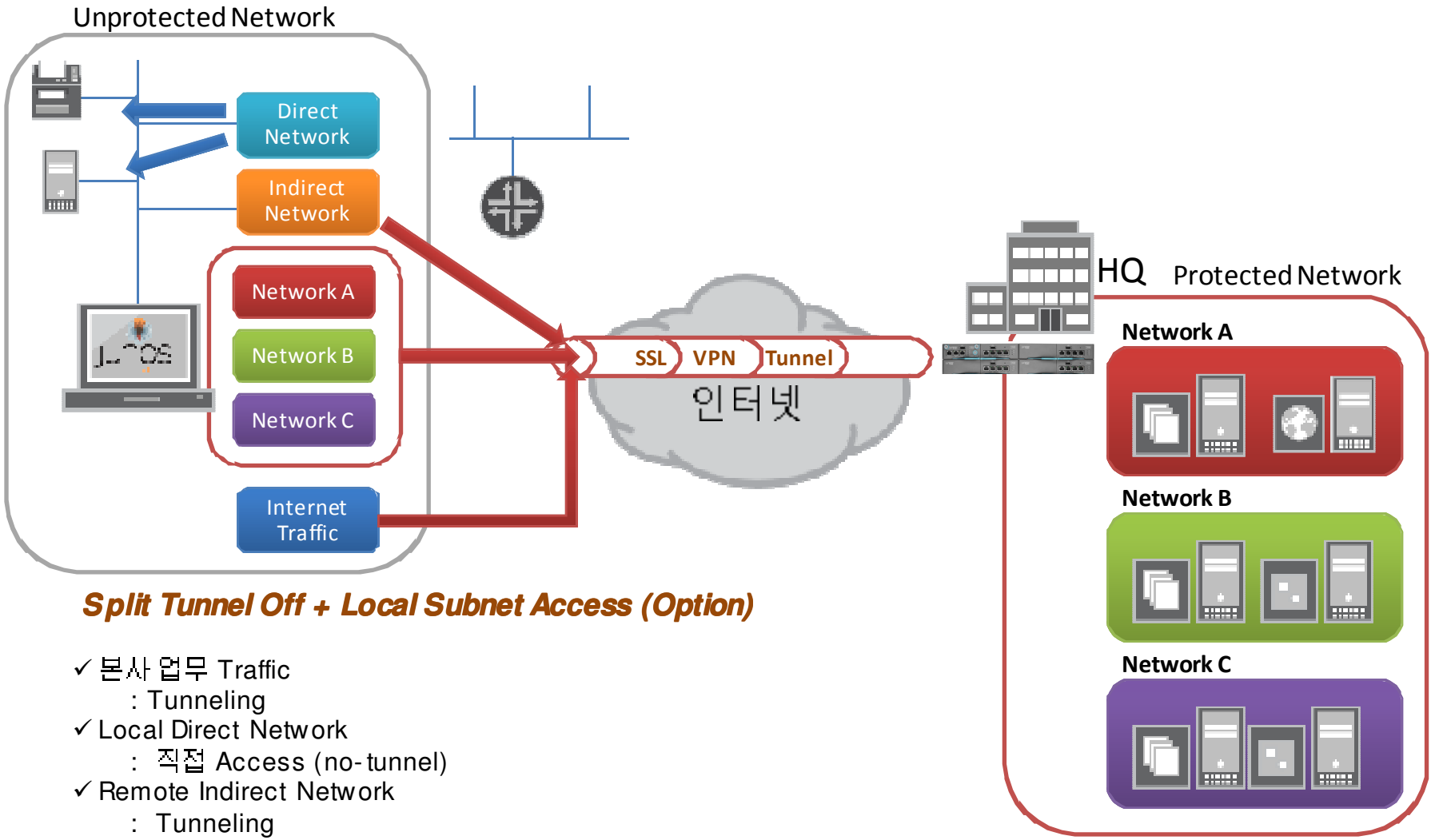
Non- Split Tunnel mode



Split Tunnel Off

- ✓ 본사 업무 Traffic
  : Tunneling
- ✓ Local Direct Network
  : Tunneling
- ✓ Remote Indirect Network
  : Tunneling
- ✓ Internet Traffic
  : Tunneling

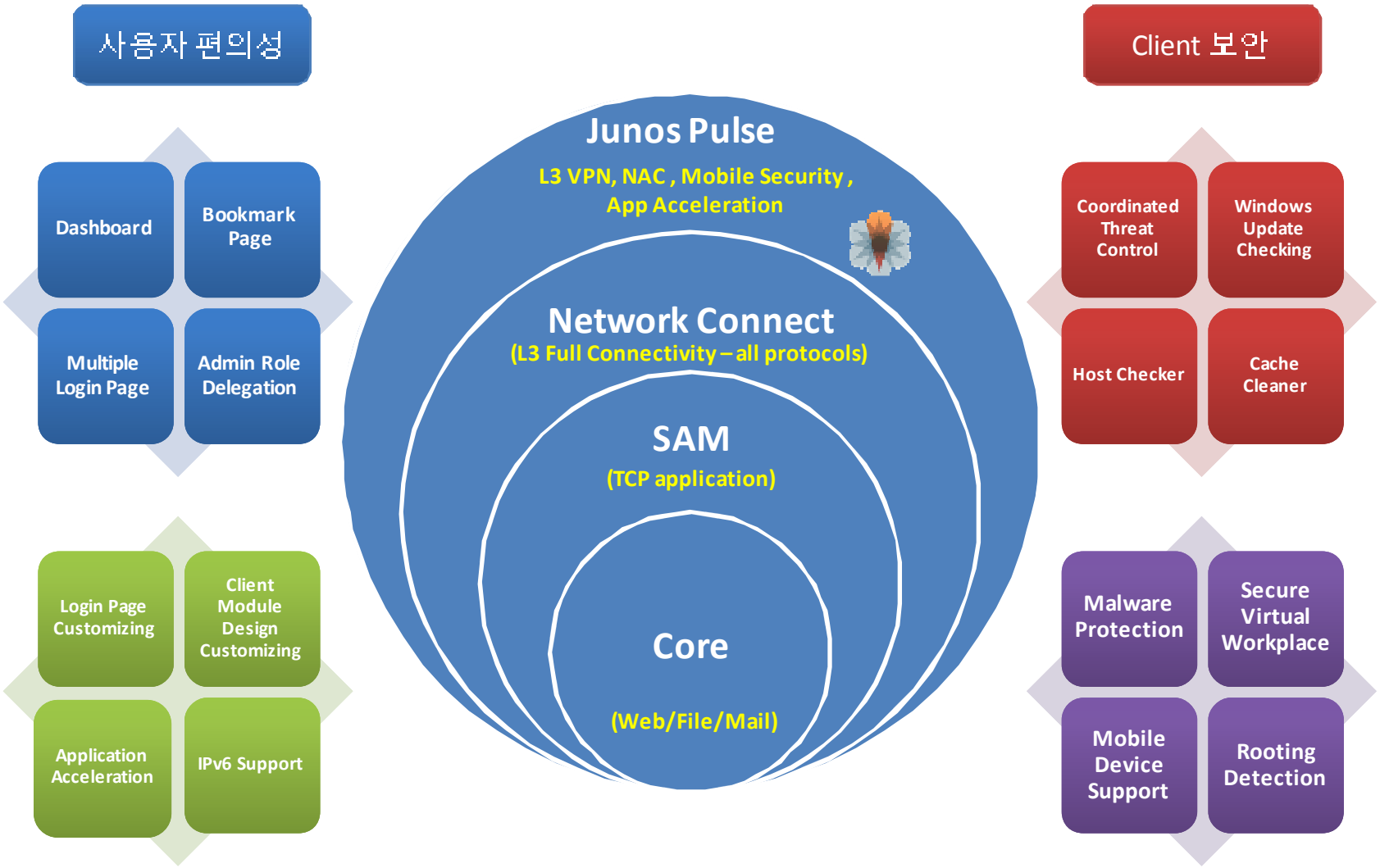
Non- Split Tunnel mode
(Local Subnet Access - Optional)



Split Tunnel Off + Local Subnet Access (Option)

- ✓ 본사 업무 Traffic
  : Tunneling
- ✓ Local Direct Network
  : 직접 Access (no-tunnel)
- ✓ Remote Indirect Network
  : Tunneling
- ✓ Internet Traffic
  : Tunneling

Juniper SSL VPN 적용 기술



Benefit of Juniper SSL VPN Solution

SSL VPN 1세대부터 시장을 Lead하며 지속적인 기술개발을 통하여 새로운 환경에 적합하고 가장 안정적인 서비스를 제공

기존 SA Series 에서 MAG Series로 진화하여 4세대 SSL VPN Solution을 제공

업계 최고인 Juniper Security Product Line Up과의 연계를 통한 최상의 보안 Solution 제공

10년 이상 시장점유율 1위를 지속하고 있으며 업계최고의 Reference 를 보유

THANK YOU

JUNOS PULSE

JUNIPER NETWORKS