Gigamon®

지능적인 네트워크 트래픽 모니터링을 통한 비즈니스 효율성 확보와

클라우드 네트워크 트래픽 모니터링 방안

싸이버텍홀딩스 보안사업부 황정길 부장

목차

1. 제조사 소개

1.1 기가몬(Gigamon) - 제조사

- 2004년도 설립 및 Visibility Fabric 솔루션 개발
- 2006년부터 흑자 전환
- 매년 50% 이상의 성장률
- 40개국 이상에서, 8,000 이상의 장비 운용 레퍼런스 보유
- 포춘지 100대 기업중 75개 고객 보유
- 글로벌 선두기업으로 성장
- 미국에서 개발 및 생산
- 2013년 NYSE 상장(IPO)
- 2015년 한국 지사 설립

1. 제조사 소개

1.2 제조사 소개 – 기술 파트너 (50여개 이상의 글로벌 벤더와 기술 협력)

Check Point SOFTWARE TECHNOLOGIES LTD.

"…our joint customers will benefit from some of the most advanced security technology available."

IMPERVA

"Even the best security appliance will fail to deliver if it does not get the right traffic,…"

splunk>

"…Gigamon's high performance security delivery platform is the right match…"

DAMBALLA

"…a robust and systematic framework to deliver pervasive network visibility to security appliances…"

riverbed

"…critical manageability and control to traffic and flow visibility."

FireEye

"…To be effective, a security appliance needs to be able to access the right network traffic…"

FORTINET

"…a security delivery platform addresses the real need for pervasive, high fidelity visibility…"

Lancope

"…Together, Lancope and Gigamon enable customers to solve today's tough security challenges."

SOURCEfire

"…much needed operational efficiency to the task of ensuring pervasive visibility for security tools."

LIGHTCYBER

"…allows joint customers to leverage Gigamon's Security Delivery Platform to effectively extend and access the critical data flows …"

LogRhythm

"…efficient access to traffic flows and high fidelity meta-data from anywhere in the network…"

niara

"…significantly increasing the efficiency and effectiveness of [business] security teams…"

paloalto NETWORKS

"…GigaSECURE Security Delivery Platform sheds light on insider initiated threats, it can provide complementary visibility to the network traffic that Palo Alto Networks sees… "

RSA SECURITY™

"… access to high fidelity network traffic is a vital step in the implementation of advanced protections…"

CISCO DEVELOPER Registered

"…Gigamon's Security Delivery Platform will allow Savvius's products to continue to provide the insight our customers depend on..."

1. 제조사 소개

1.3 가트너 리포트

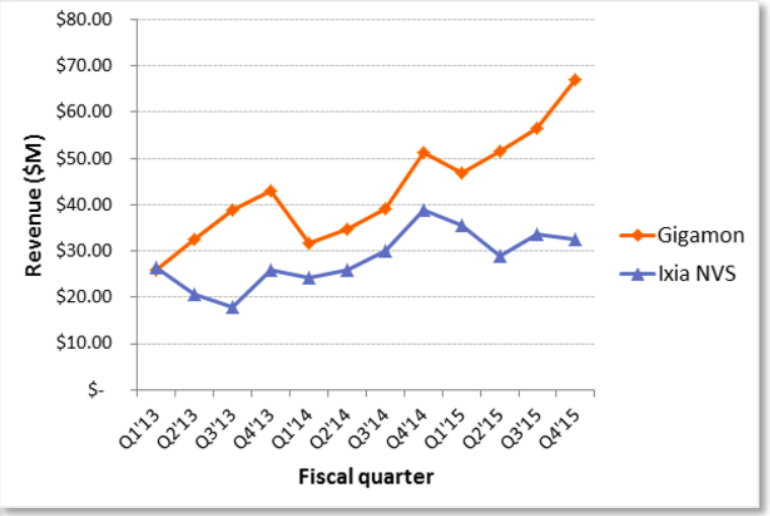
On January 19, 2016, Gartner published its *Market Guide for Network Packet Brokers* (NPB), naming Gigamon as the market share leader in the NPB market. Gartner estimates the size of the market for the NPB space was $591 million for 2015. Based on Gigamon's actual revenues of $222 million in 2015, that places Gigamon firmly in the #1 position at 37.6% market share.

Below is an excerpt from this market guide:

"Gigamon is representative of pure-play, fully featured NPB vendors. Based on available data points, Gigamon is the market share leader in the NPB market delivering Layer 2 through Layer 7 NPB visibility, filtering and correlation via its GigaSMART platform. Its solutions scale up to 100G environments and are available in a number of different form factors, both physical and virtual. GigaVUE-FM is the company's consolidated management interface of physical and virtual components.

Gigamon's solutions are well-suited to large enterprises, government organizations and service providers looking for a fully featured NPB."

In fact, based on available public data for the two largest market players (Gigamon and Ixia Network Visibility Systems [NVS]), Gigamon has consistently grown market share over the last three years, as shown by the chart below:



2016년 1월 19일 Network Packet Broker(NPB) 시장에서 가트너 선정 **마켓 리더 벤더**로 발표

기가몬은 Network Packet Broker **전문 벤더**로서 L2 ~ L7 레이어의 모든 패킷에 대한 **지능적인 필터링 기능**을 제공하며 최대 100G 환경까지 **유연한 확장성** 제공 및 물리적인 환경 및 가상화 환경에서도 네트워크 트래픽 모니터링이 가능함. 또한 GigaVUE-FM을 통해 **물리적인 환경/가상화 환경에 대한 통합 모니터링 기능**을 제공함.

2. 네트워크 가시성 확보 솔루션의 필요성

2.1 모니터링의 중요성

"**볼 수 없는 것**은 **측정**할 수 없으며,
측정할 수 없는 것은 **관리**할 수 없다."

You cannot manage what you cannot see!

2. 네트워크 가시성 확보 솔루션의 필요성

2.2 어플리케이션 모니터링과 트러블슈팅의 이슈

90% 문제를 해결하는데 90%의 시간은 문제를 발견하는데 사용한다.

75% 문제의 75%는 운영 부서가 아니라 현업 사용자에 의해 발견된다.

You cannot manage what you cannot see!

2. 네트워크 가시성 확보 솔루션의 필요성

2.3 보안 이슈 – 지능형지속위협(APT) 등

97% 63개국 1200 기업을 대상으로 실 조사 결과 테스트 기간 중 97% 기업이 공격을 받았고, 그 중 75% 기업이 공격에 노출되었음. [1)]

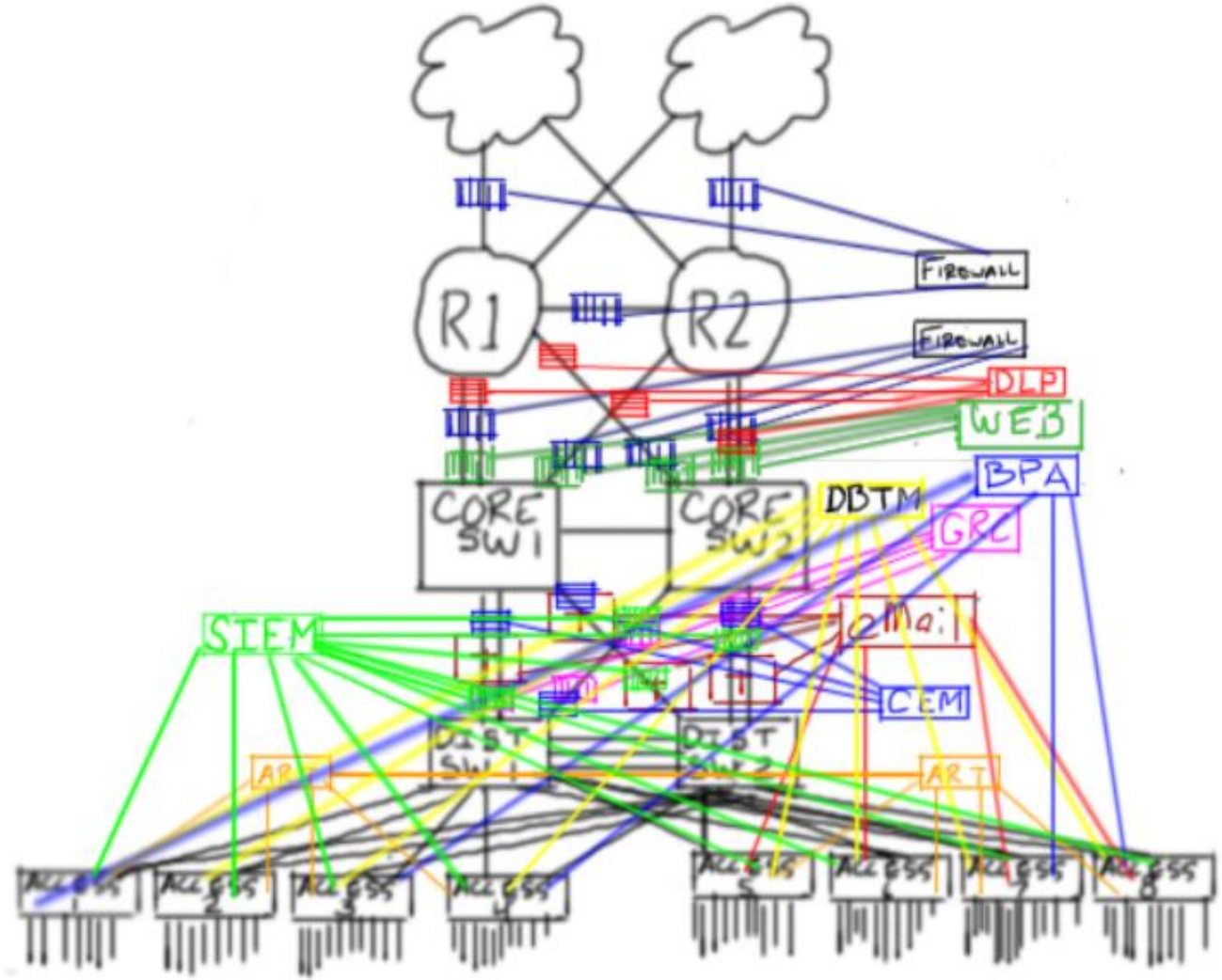
134 Days **최초 공격 후 발견하기까지 걸린 평균 시간.** [2)]

You cannot secure what you cannot see!

- 1)FireEye. 2015. Maginot revisited: More Real-World Results from Real-World Tests. https://www2.fireeye.com/WEB-2015RPTMaginotRevisited.html
  2) Trustwave. 2014. Global Security Report. https://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf

2. 네트워크 가시성 확보 솔루션의 필요성

2.4 모니터링 인프라의 복잡성



복잡성
네트워크가 확장되면서
모니터링 솔루션 구성이 점차 복잡

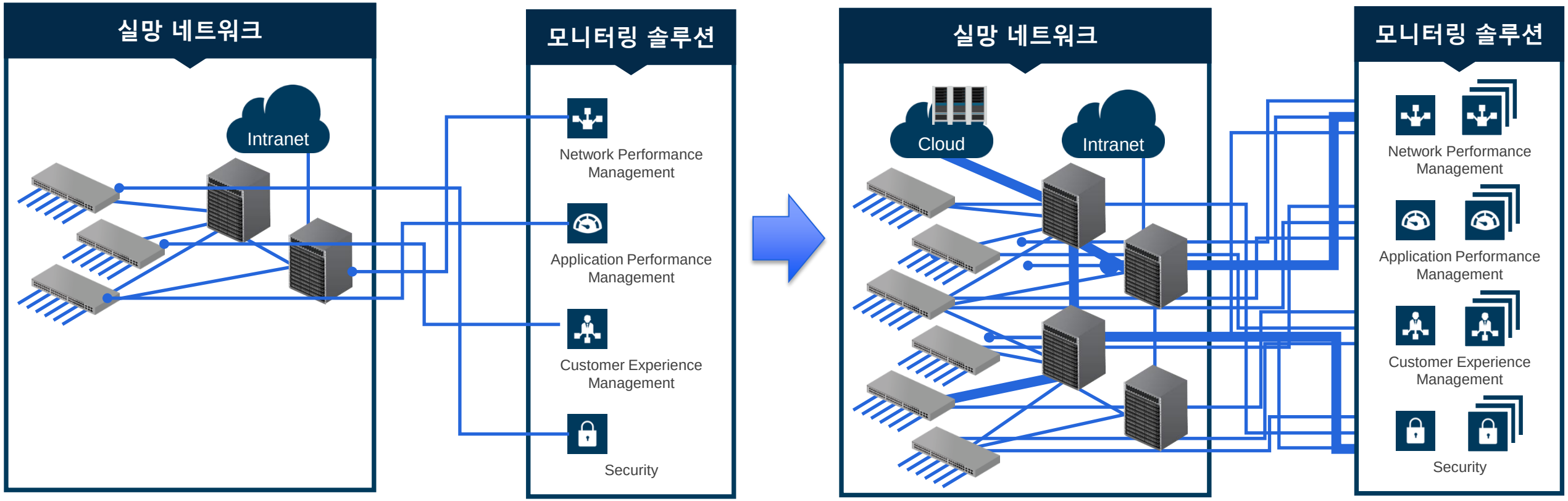
개별관리
네트워크 모니터링 및 분석 솔루션들이 팀 단위/부서 단위로 구축되고
개별로 관리되어 중복투자 발생

누락구간
Span 또는 Mirror 포트 구성 제약으로 인해
네트워크 전 구간의 모니터링 불가

운용의 비효율
모니터링 솔루션의 중복 투자로
CAPEX/OPEX 증가로 인한 비용증가

2. 네트워크 가시성 확보 솔루션의 필요성

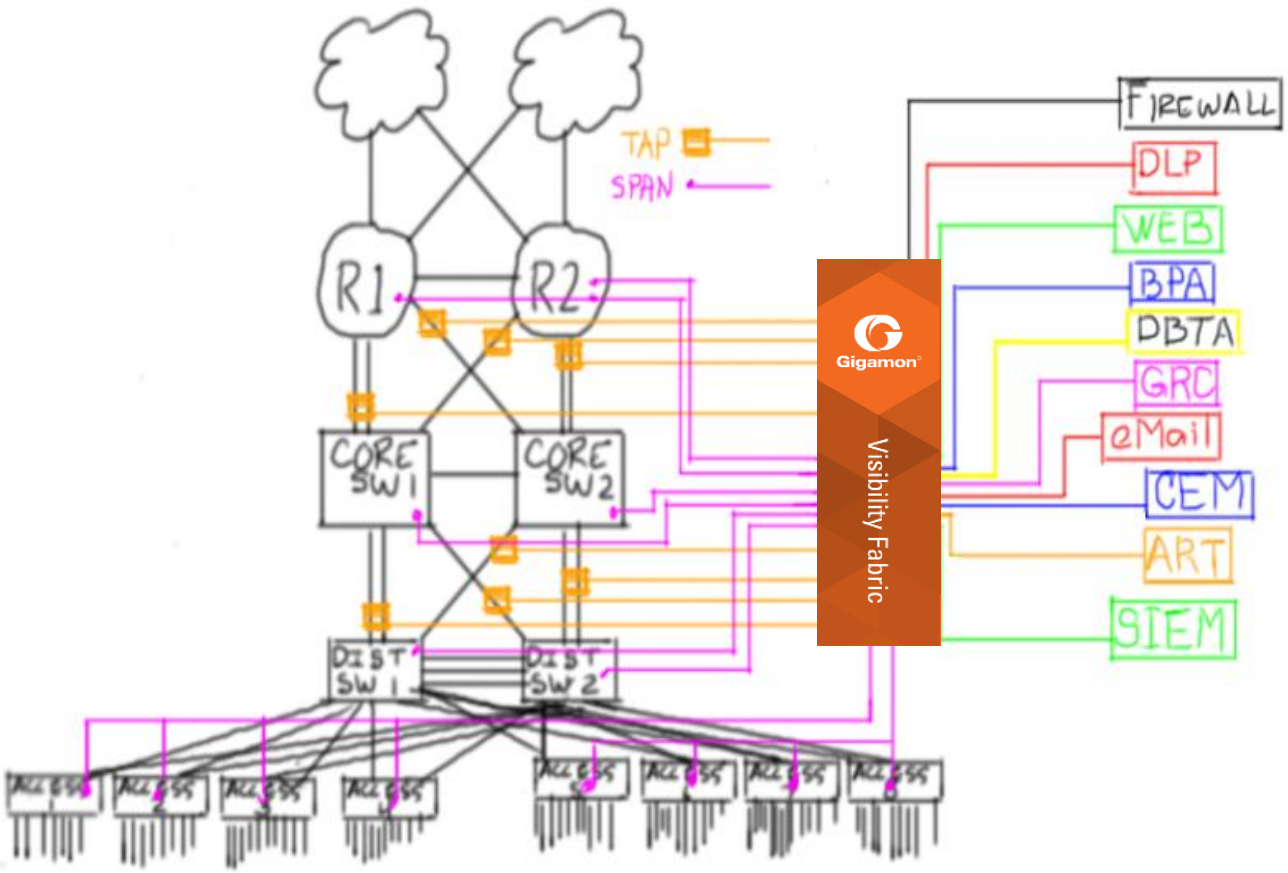
2.5 모니터링 인프라의 복잡성



- ✓ 솔루션 도입 비용 증가
- ✓ 모니터링 인프라 확장성 부족
- ✓ 네트워크 복잡성 증가

2. 네트워크 가시성 확보 솔루션의 필요성

2.6 지능형 네트워크 트래픽 모니터링 솔루션 도입 시 개선사항



트래픽 수집

주요 네트워크 구간에 대해 누락 없는 트래픽 모니터링

통합콘솔

Gigamon 장비에서 모니터링 트래픽에 대한 통합 관리 기능 제공

서비스

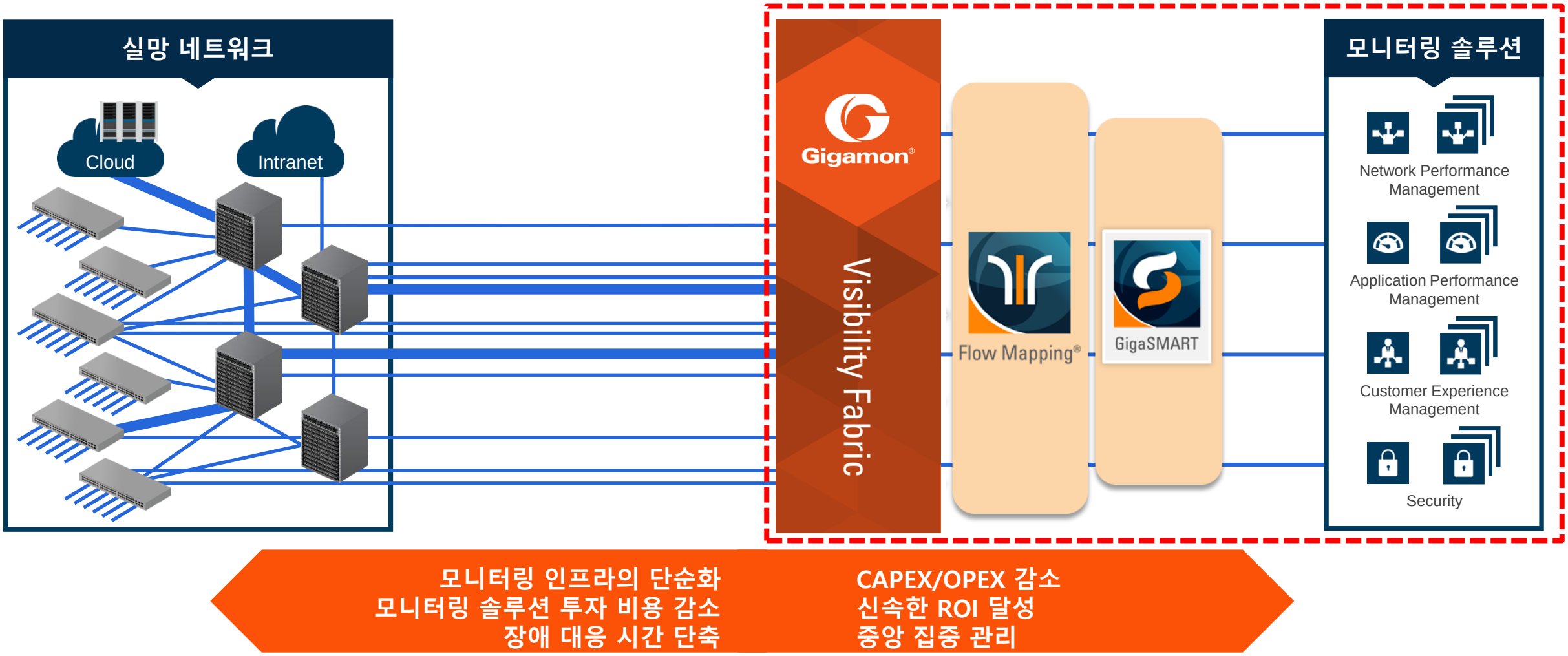
모든 설정의 변경작업등은 Out-Of-Band 구간에서 수행되므로 기존 네트워크에 영향 전무

운용의 효율성

혁신적인 트래픽 필터링 기능은 모니터링 툴의 특성에 맞게 최적화된 트래픽 전송

2. 네트워크 가시성 확보 솔루션의 필요성

2.7 지능형 네트워크 트래픽 모니터링 솔루션 도입 시 개선사항

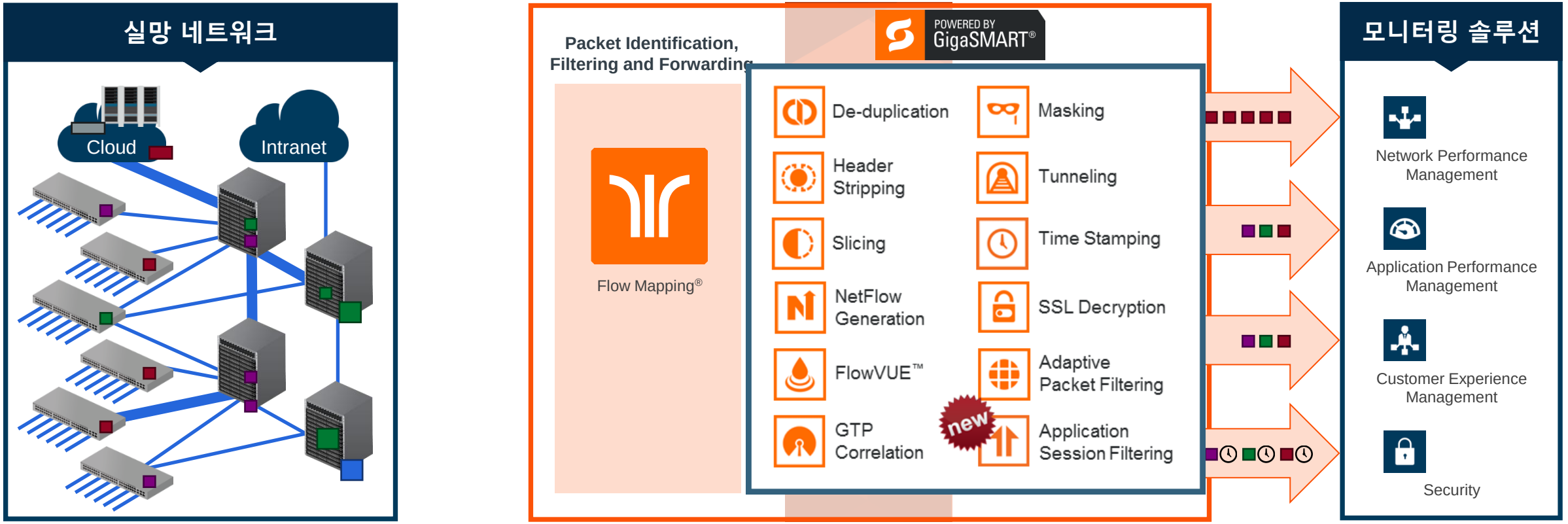


모니터링 인프라의 단순화
모니터링 솔루션 투자 비용 감소
장애 대응 시간 단축

CAPEX/OPEX 감소
신속한 ROI 달성
중앙 집중 관리

2. 네트워크 가시성 확보 솔루션의 필요성

2.8 기대효과 - 혁신적인 트래픽 필터링 기능을 통한 CAPEX/OPEX 감소로 **비즈니스 효율성 확보**



모니터링 인프라의 단순화
모니터링 솔루션 투자 비용 감소
장애 대응 시간 단축

CAPEX/OPEX 감소
신속한 ROI 달성
중앙 집중 관리

3. 지능적인 트래픽 필터링 기능 소개

3.1 GigaSMART® – Traffic Intelligence

License	Description	개선 효과
Packet Slicing	▪ Large Packet의 사이즈를 잘라서 모니터링 장비로 전달	▪ 모니터링 장비 부하 감소/모니터링 장비 스토리지 사용량 감소
Masking	• 패킷 내부의 개인정보(카드)를 마스킹 처리해서 모니터링 솔루션으로 전달	• 모니터링 솔루션에 대한 개인정보 관련 업무 부하 감소
Source Port Labeling	• 기가몬에 유입된 모니터링 트래픽 개별 패킷에 기가몬 포트 정보를 추가하여 모니터링 장비에 전달	• 모니터링 구간 별 Latency 측정이 가능함에 따라 트러블슈팅 용이
De-duplication	• 다중 구간에서 수집된 트래픽에 대해 동일 패킷 중복 제거	▪ 모니터링 장비 부하 감소/모니터링 장비 스토리지 사용량 감소
Header Stripping	• VLAN Tagging/VXLAN,MPLS와 같은 환경에서 수집된 패킷에 대해 불필요한 부분 제거	• 모니터링 솔루션 연동 호환성 증가
Tunneling	• 본사와 지사간 암호화된 터널링을 통해 지사 트래픽을 본사 장비로 안전하게 패킷 전송	• 지사/지점에 대한 모니터링 본사 통합 관리

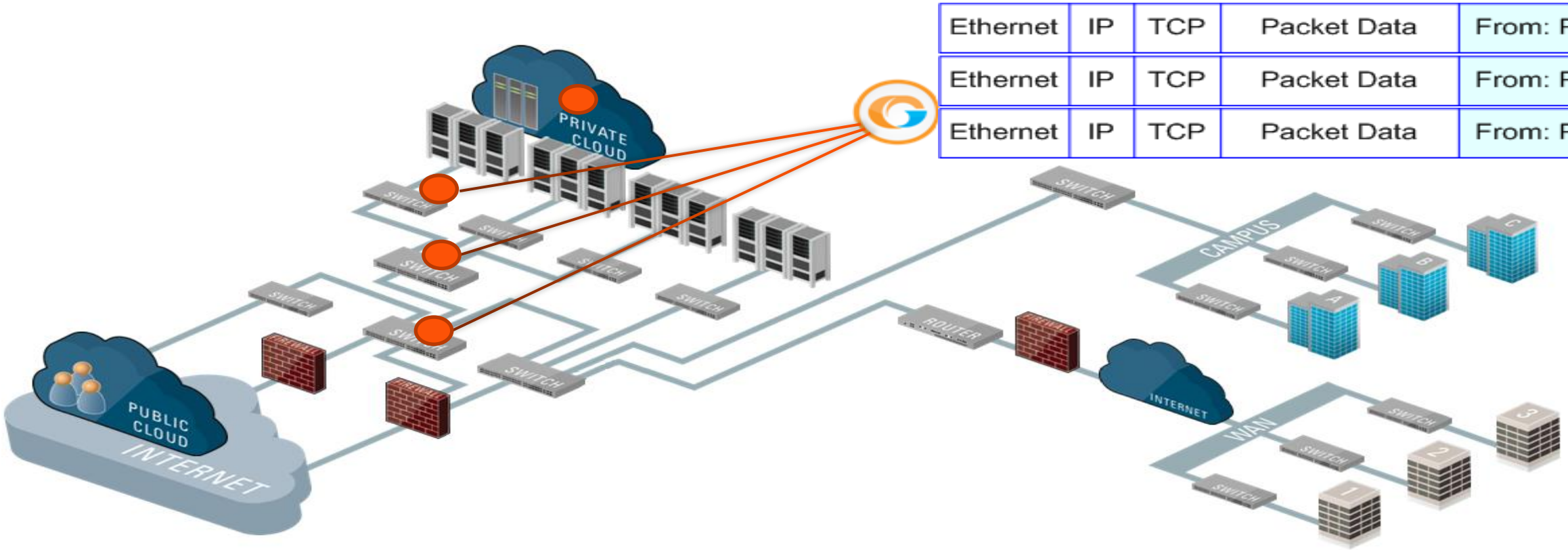
3. 지능적인 트래픽 필터링 기능 소개

3.1 GigaSMART® – Traffic Intelligence

License	Description	기대 효과
Adaptive Packet Filtering / Application Session Filtering	▪ VXLAN, VN-Tag, and VGRE 기반의 패킷 필터링 ▪ 패킷 내부의 데이터 중 특정 패턴 기반으로 패킷 필터링 ▪ Application Session Filtering은 특정 패턴 기반으로 매칭되는 세션 전체를 필터링하여 모니터링 장비로 전달	▪ 모니터링 장비 부하 감소/모니터링 장비 스토리지 사용량 감소
SSL Decryption	▪ 암호화된 SSL 트래픽을 평문으로 복호화 하여 모니터링 솔루션으로 전달	• 암호화된 트래픽에 대한 모니터링 가시성 확보
NetFlow Generation	▪ 기가몬으로 유입된 모니터링 트래픽에 대해 100% Netflow 트래픽을 생성하여 모니터링 솔루션으로 전달	• 누락 없는 Netflow 트래픽 생성으로 향후 포렌직/감사 수행 시
FlowVUE	▪ IP/User/Session 기반으로 샘플링 하여 다수의 모니터링 솔루션으로 트래픽을 분산 전달	▪ CEM(Customer Experience Management) 모니터링 솔루션의 효율적인 운영 가능
GTP Filtering and Correlation	▪ 통신사에서 가입자 기반으로 트래픽 필터링	• 모니터링 솔루션 운용 효율성 증가
Time Stamping	• 기가몬에 유입된 모니터링 트래픽 개별 패킷에 Time Stamp를 추가하여 모니터링 장비에 전달	• 패킷 지연 이슈에 대한 트러블슈팅 용이

3. 지능적인 트래픽 필터링 기능 소개

3.2 GigaSMART® – Source Port Labeling



- 패킷이 유입된 포트 라벨링을 통해 패킷 처리가 지연된 구간 확인 트러블슈팅에 활용

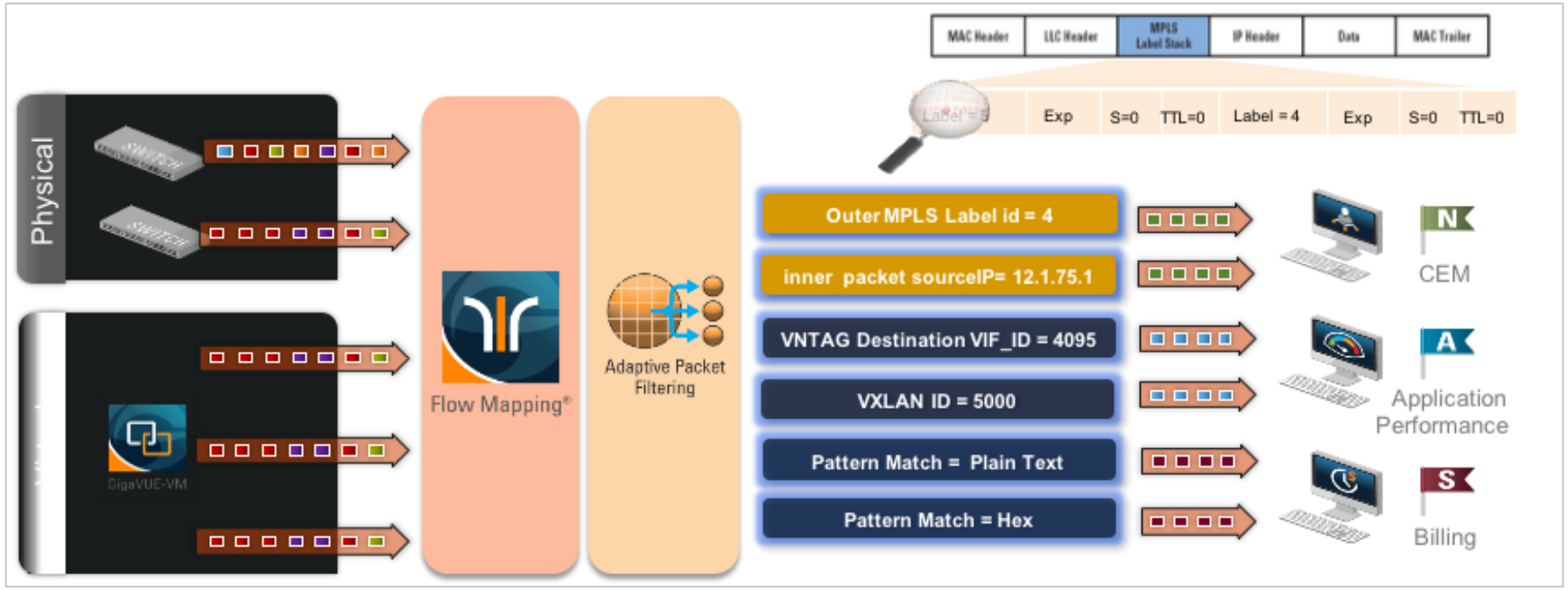
3. 지능적인 트래픽 필터링 기능 소개

3.3 GigaSMART® – De Duplication

- 분석/모니터링 장비의 정확성을 위하여 중복 패킷 제거를 통한 모니터링 장비 운용 효율성 증가

3. 지능적인 트래픽 필터링 기능 소개

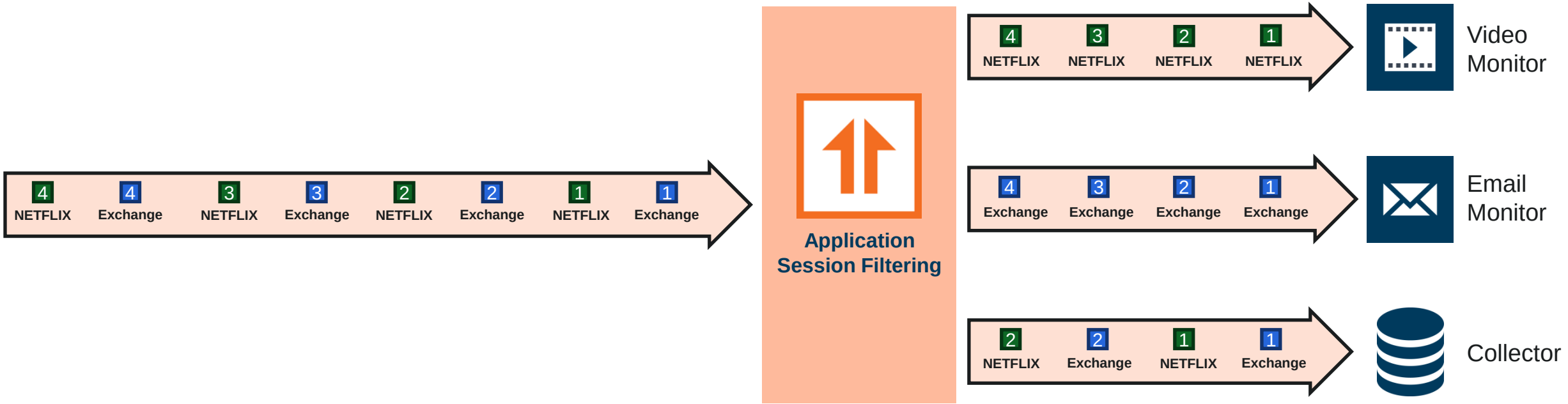
3.4 GigaSMART® – Application packet filtering



- MPLS/VLAN ID 및 패킷 내부의 컨텐츠 기반으로 트래픽을 필터링하여 모니터링 장비로 전달

3. 지능적인 트래픽 필터링 기능 소개

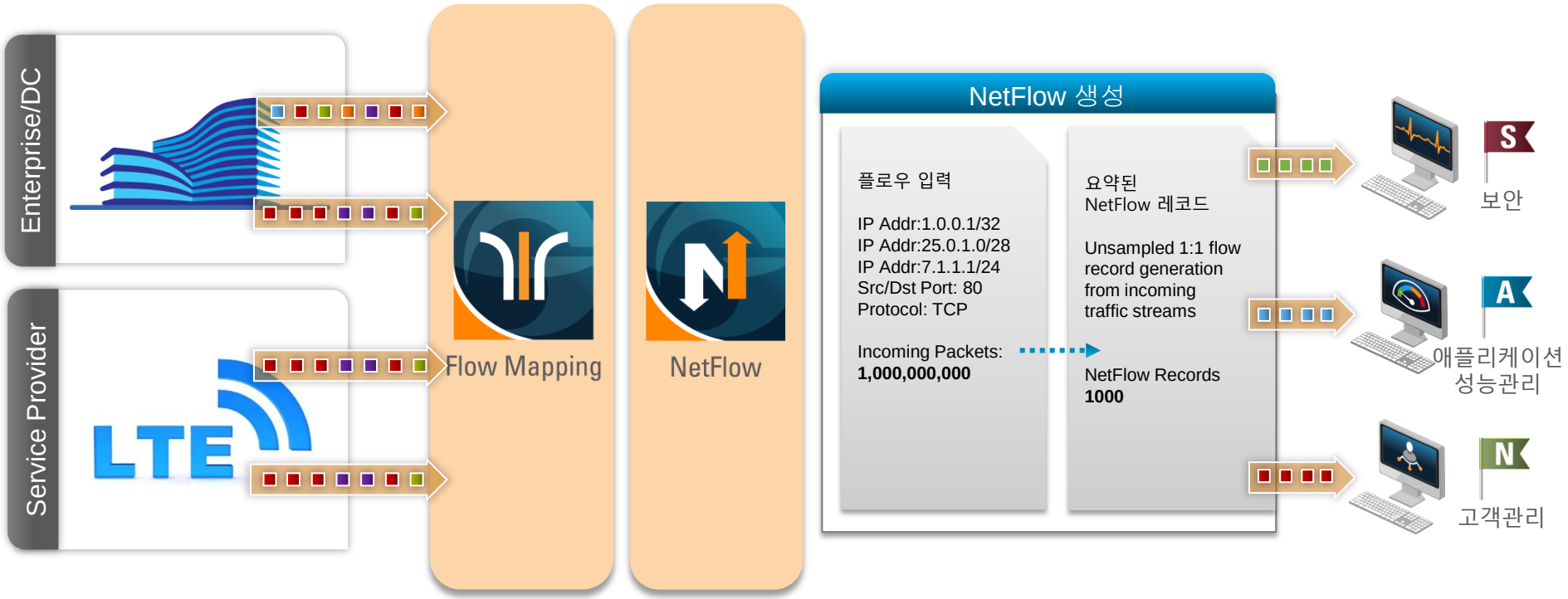
3.5 GigaSMART® – Application Session Filtering



- 패킷 단위가 아닌 세션 기반으로 트래픽을 필터링하여 모니터링 솔루션으로 트래픽 전달
- 이를 통해 제한된 모니터링/분석 도구를 효율적으로 사용할 수 있는 경제성을 제공

3. 지능적인 트래픽 필터링 기능 소개

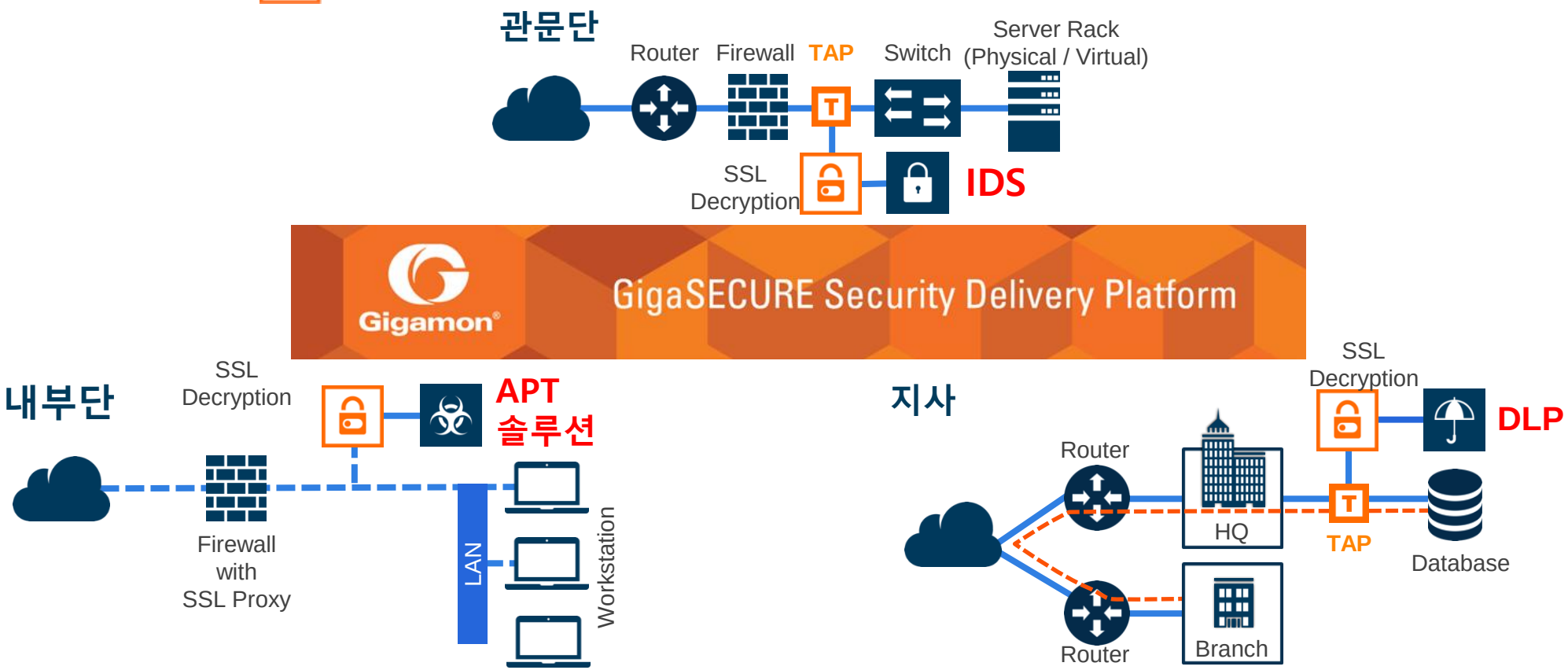
3.6 GigaSMART® – NetFlow Generation



- 모니터링 트래픽에 대한 전수 Netflow 생성 지원. 동시에 최대 6개의 수집 서버로 Netflow 전송 지원(지원 버전 : Netflow V5, V9 및 IPFIX)
- Out of box 형태로 구성되어 성능 저하에 따른 서비스 지연 이슈 없음

3. 지능적인 트래픽 필터링 기능 소개

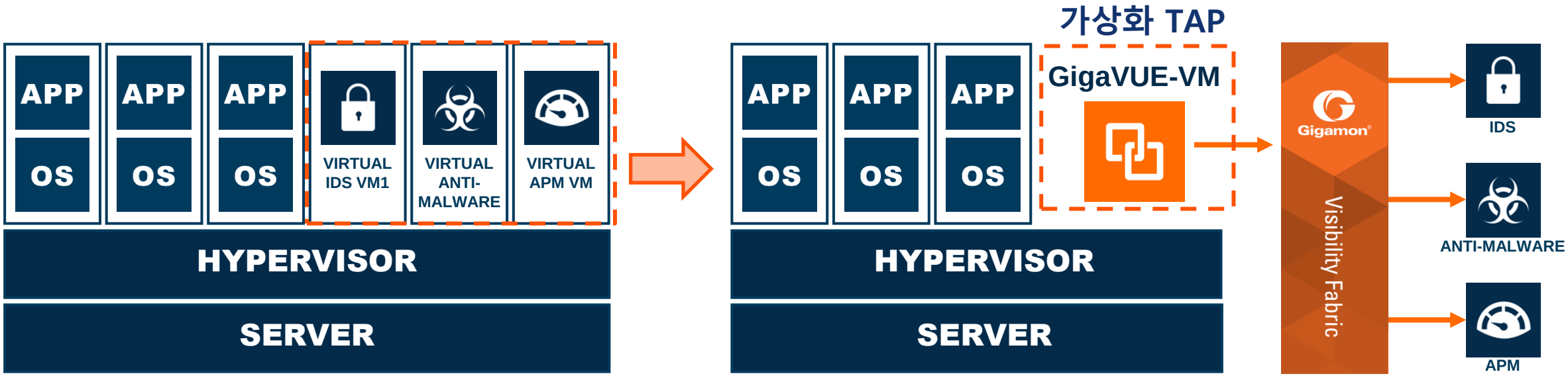
3.7 GigaSMART® – SSL Decryption



- SSL 암호화 트래픽을 평문으로 복호화 하여 모니터링 솔루션으로 전달
- Out Of Box 형태로 구성되어 있어 성능 저하에 따른 서비스 지연 이슈 없음

4. 클라우드 네트워크 모니터링 방안

4.1 클라우드 가상화를 위한 가시성 확보 - 필요성



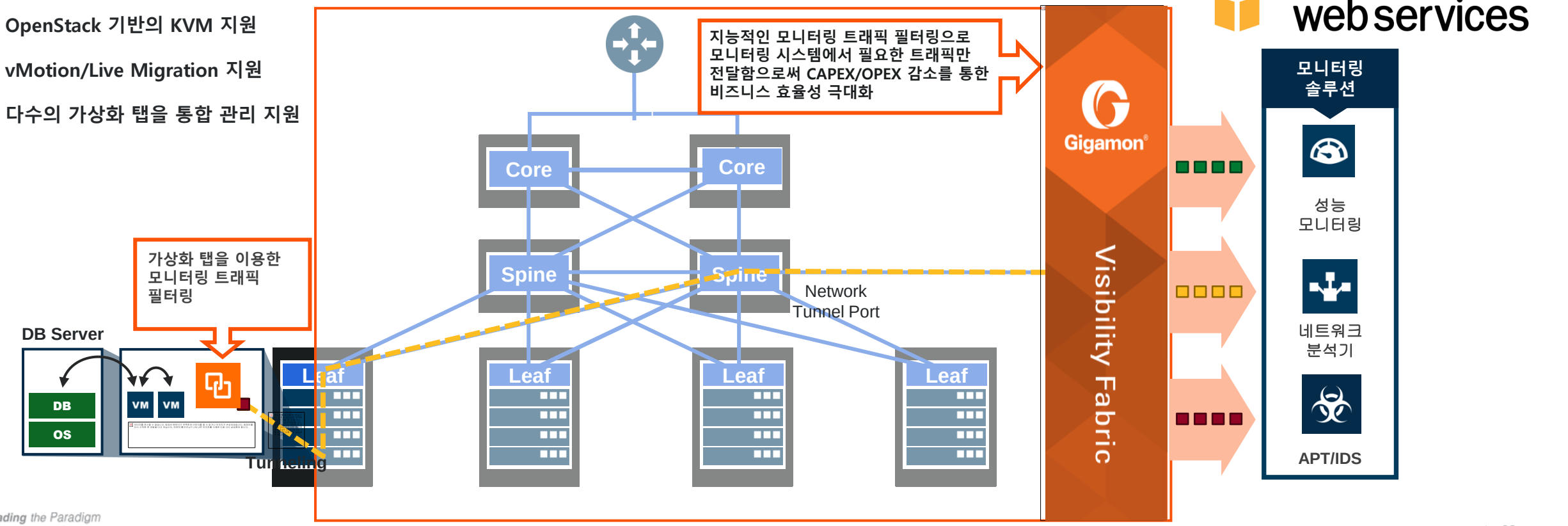
- ✓ 가상화 환경에서 보안의 중요성이 점차 강조
- ✓ 가상화를 통한 미션 크리티컬 호스트 증가
- ✓ 보안 및 어플리케이션 성능 분석을 위해 VM간 트래픽에 대한 모니터링 필요성 증가
- ✓ 가상화 인스턴스를 생성하는 것이 전체 성능에 영향
- ✓ VM 마이그레이션 후 자동화된 모니터링 방안 필요

4. 클라우드 네트워크 모니터링 방안

4.2 클라우드 가상화를 위한 네트워크 가시성 확보 아키텍처

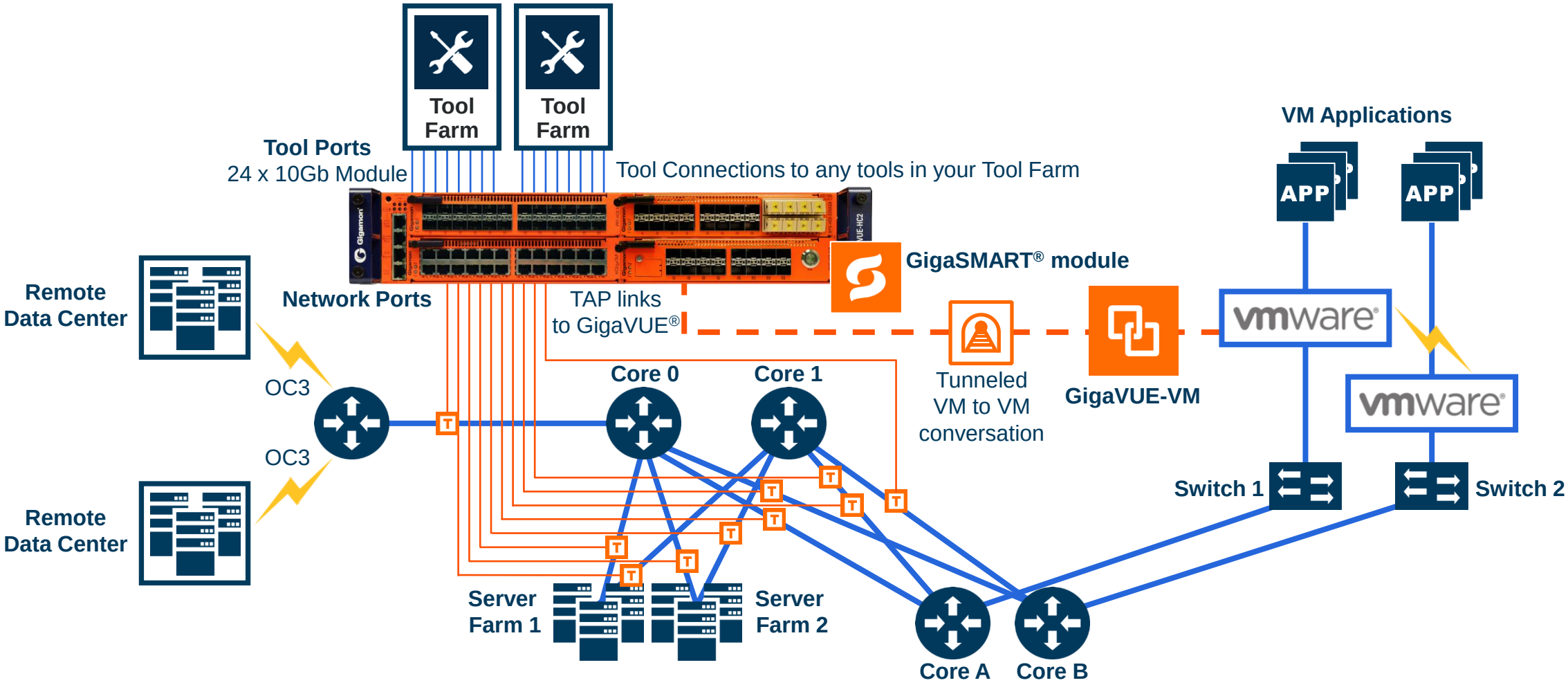
- 가상화 TAP(Virtual Tap)을 통하여 호스트 어플리케이션 간의 트래픽 분석
- Vmware 기반의 SDDC(ESX/NSX-V) 지원
- OpenStack 기반의 KVM 지원
- vMotion/Live Migration 지원
- 다수의 가상화 탭을 통합 관리 지원

- 가상화 트래픽을 터널링을 통해 분석 장비로 전달



5. 운영 사례

5.1 미 연방 정부 – 물리/가상 네트워크 전사 네트워크 트래픽 모니터링



5. 운영 사례

5.2 글로벌 상거래 기업 – 다중 100G 트래픽에 대한 어플리케이션 레벨 트래픽 필터링

요구사항

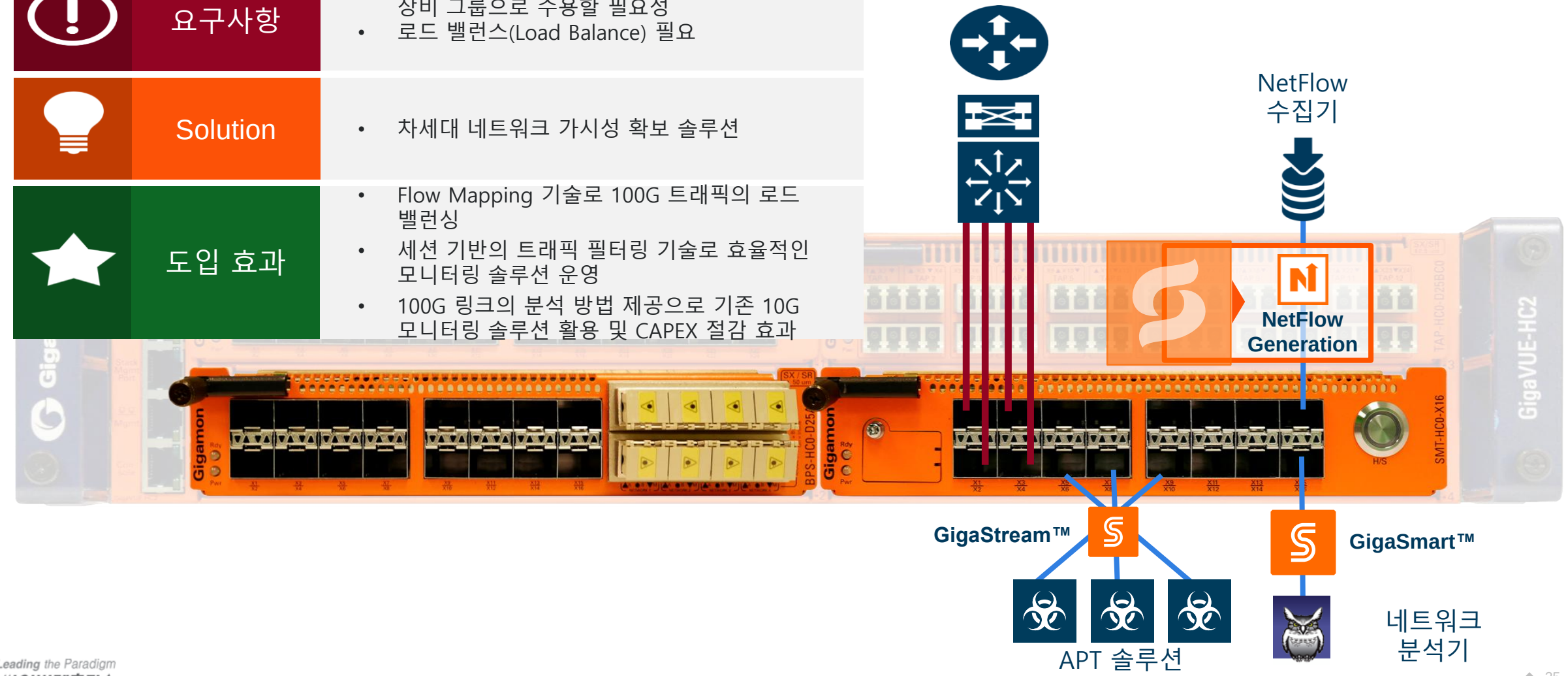
- 다수의 100G 링크의 트래픽을 10G 링크의 분석 장비 그룹으로 수용할 필요성
- 로드 밸런스(Load Balance) 필요

Solution

- 차세대 네트워크 가시성 확보 솔루션

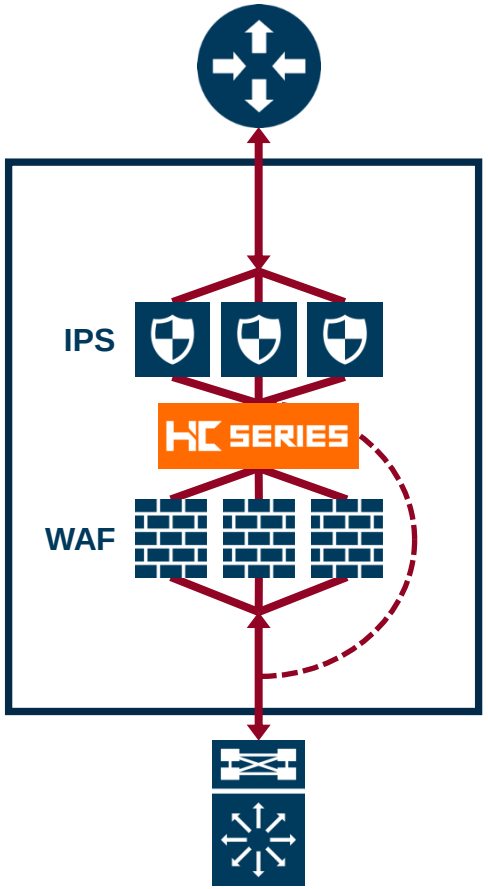
도입 효과

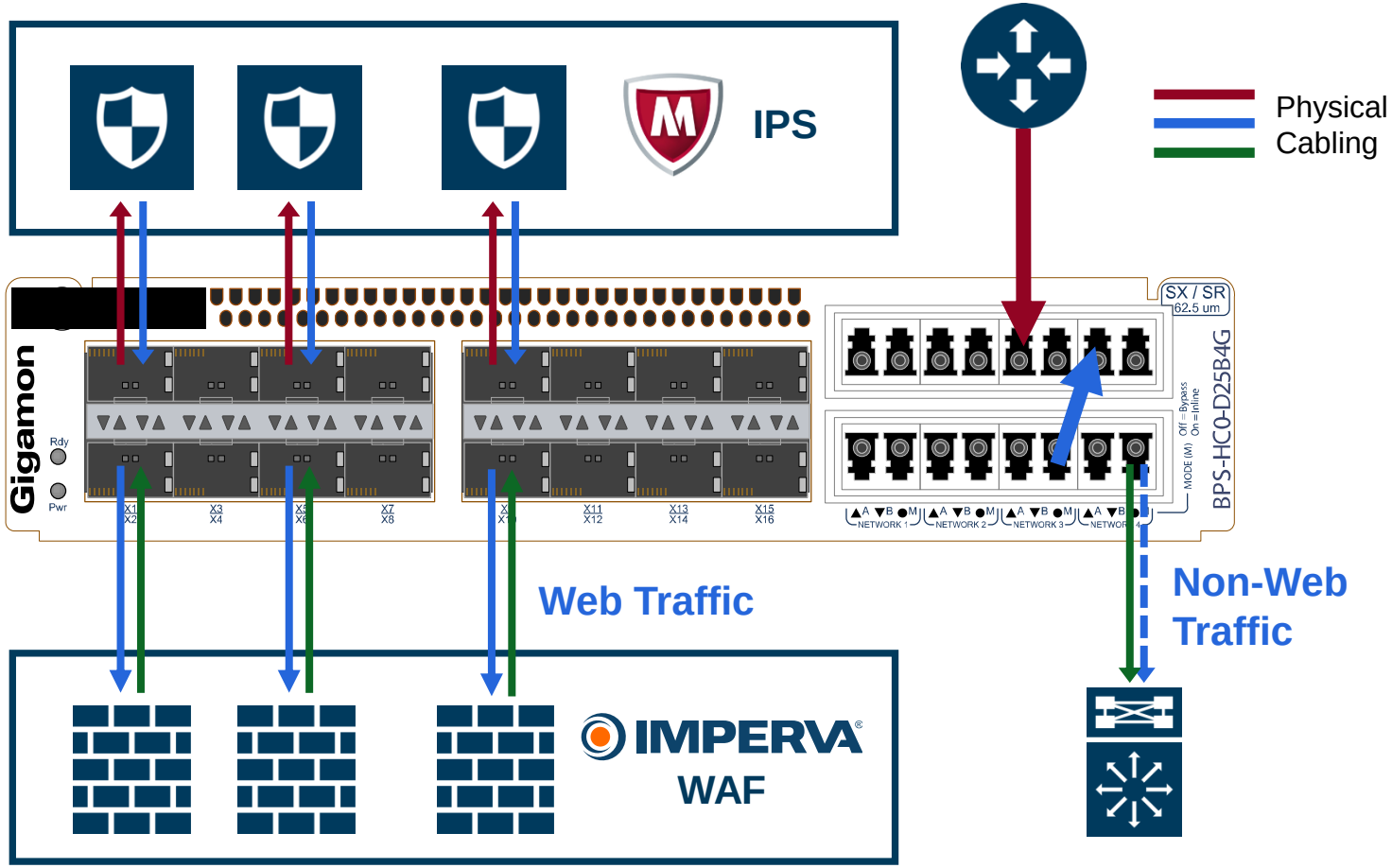
- Flow Mapping 기술로 100G 트래픽의 로드 밸런싱
- 세션 기반의 트래픽 필터링 기술로 효율적인 모니터링 솔루션 운영
- 100G 링크의 분석 방법 제공으로 기존 10G 모니터링 솔루션 활용 및 CAPEX 절감 효과



5. 운영 사례

5.3 IPS, WAF 로드밸런싱 및 트래픽 필터링 적용 사례

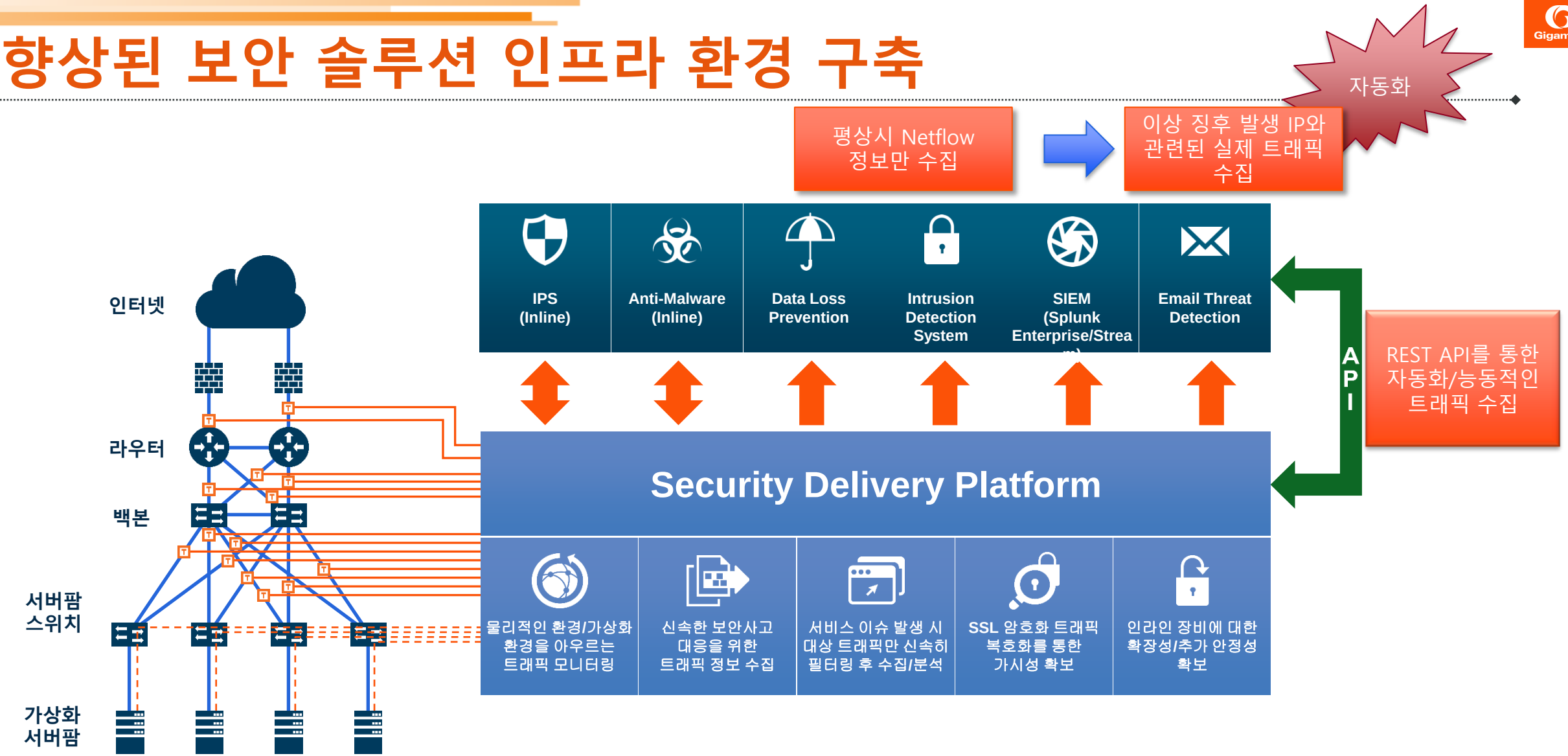




추가 투자 비용 없는 보안 신속대응팀 운영

해외에서 사건.사고가 발생했을 때 신속히 현장에 파견되어 우리 국민을 보호하는데 필요한 조치를 빠르게 추진하는 외교부의 최정예 조직

향상된 보안 솔루션 인프라 환경 구축



You can manage what you can see!

대내외 환경 변화에 따른 지속 가능한 보안인프라 운영

- ✓ 예산절감을 통한 비즈니스 효율성 확보
- ✓ 신속한 장애 대응으로 고객 서비스 품질 개선
- ✓ 보안 인프라 환경 개선으로 운용 효율 개선
- ✓ 3rd Party 보안 장비와의 연동으로 능동적인 보안 침해 대응

Gigamon®

감사합니다!