Gigamon®

지능적인 네트워크 트래픽 모니터링과 보안 인프라 관리 플랫폼을 통한

비즈니스 효율성 확보 솔루션

기가몬 Visibility Fabric ™

목차

1. 보안 관리 전달 플랫폼 소개

1. 보안 관리 전달 플랫폼 소개

1.1 모니터링의 중요성

인문 경영학의 아버지

오스트리아 출생의 미국인으로, 작가이자 경영 컨설턴트, 교수였다.

스스로는 자신을 "사회생태학자 (social ecologist)"라고 불렀다.

20세기와 그 다음 세기의 기업 경영에 큰 영향을 준 인물로, 30권도 넘는 경영서적을 저술하였다. 새로운 지식경영의 패러다임을 연 선구자. 그러므로 경영학 공부를 하
다보면 정말 지겹게 만나게 되는 사람이기도 하다. 저술하지 않은 분야가 없다.(...)[4]
민영화와 마케팅에 대한 화두를 던진건 매우 유명하다. 애초에 **마케팅이란 단어를 창시한 사람이다.** 뿐만 아니라 1959년에는 **지식 노동자**라는 단어를 만들었다.

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

You cannot manage what you cannot see!

1. 보안 관리 전달 플랫폼 소개

1.1 모니터링의 중요성

보안 이슈 - 지능형지속위협(APT) 공격 등

134 Days

최초 공격 후 발견하기까지 걸린
평균 시간*

97%

63개국 1200 기업을 대상으로 실 조사 결과
테스트 기간 중 97% 기업이 공격을 받았고, 그
중 75% 기업이 공격에 노출되었음 **

어플리케이션 모니터링/관리/트러블슈팅

90%

문제를 해결하는데 90%의 시간은 문제를
발견하는데 사용 됨. ***

75%

문제의 75%는 IT 부서가 아니라 엔드 유저에
의해 발견 됨.***

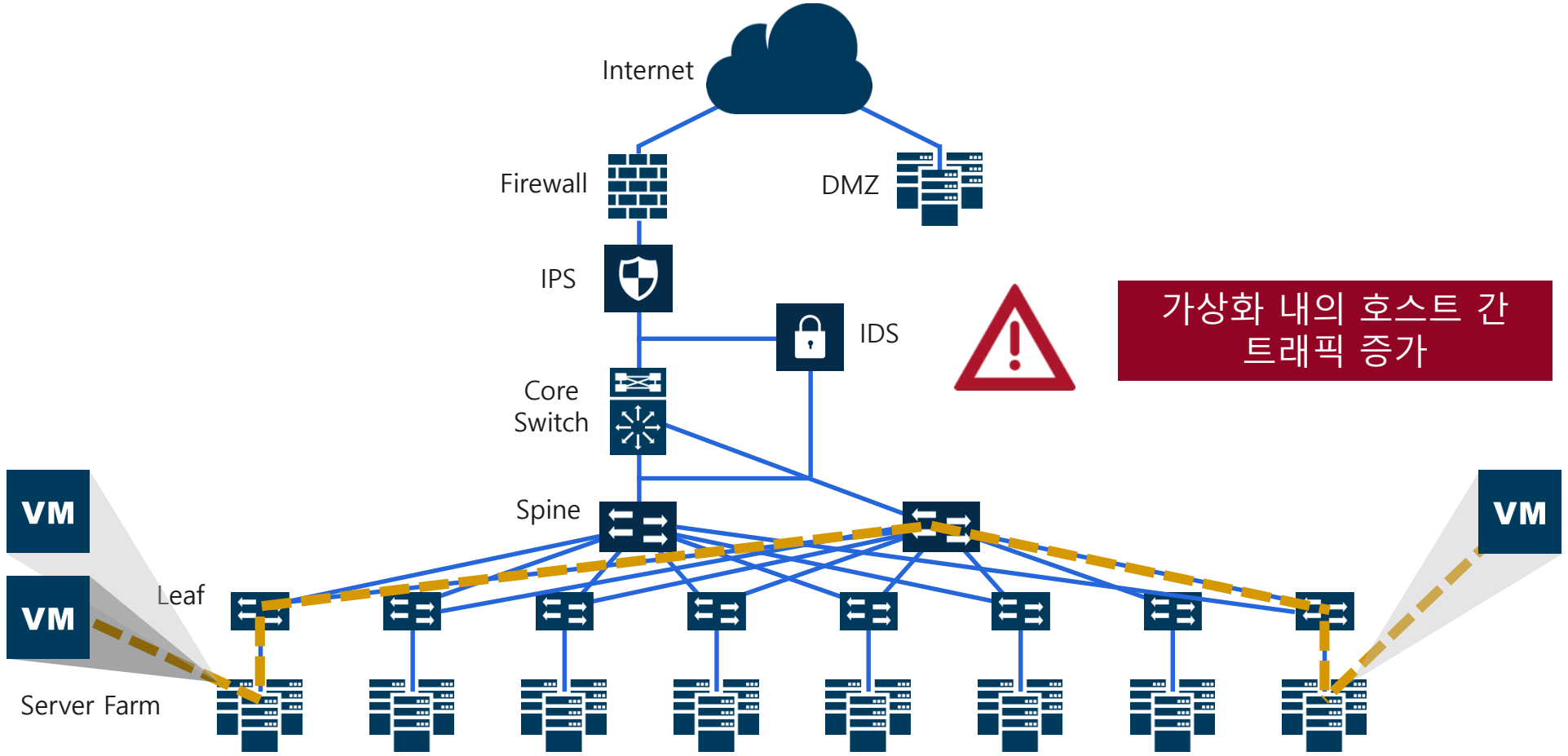
You cannot secure/manage what you cannot see!

Sources: *Trustwave 2014 global security report **FireEye: Maginot revisited, ***2013 ZK Research, A division of Kerravala Consulting

1. 보안 관리 전달 플랫폼 소개

1.2 보안 관련 이슈 사항 - 트래픽 패턴의 변화

- 최근 많은 기업들이 전산자원의 **효율적인 배분** 및 **비용 절감**을 위해 **가상화 솔루션을 도입**하면서 가상화 **서버 간 트래픽**에 대한 **보안 위협 모니터링**의 필요성이 **높아지고 있습니다.**



1. 보안 관리 전달 플랫폼 소개

1.2 보안 관련 이슈 사항 – 너무나 많은 데이터량

1. 보안 관리 전달 플랫폼 소개

1.2 보안 관련 이슈 사항 – 점점 어려워지는 실시간 위협 방지

너무 짧은 시간

- 판단을 위한 너무 짧은 시간 (67.2 ns at 10Gb)
- 미인지 위협에 대한, 결정을 하기 위한 충분하지 않은 시간, 지식 및 상황정보(Context)

너무 많은 Bad Guys

- 악성코드 (malware)에 대한 광범위한 유통 생태계
- 지능적 장비 및 손쉬운 도구 임대
- 전방, 후방의 지원 인프라

사이버 위협의 대중화!

1. 보안 관리 전달 플랫폼 소개

1.2 보안 관련 이슈 사항 – 암호화 트래픽(SSL)의 증가

SSL 트래픽 (현재) : 기업 트래픽의 25%-35% [1]

보안 및 성능관리 툴은 SSL 트래픽의 미 인식 하거나, 복호화 시 과부화가 발생

Large (2048b) ciphers 는 현재 SSL 구조의 **81%** 성능 감소를 유발 [1]

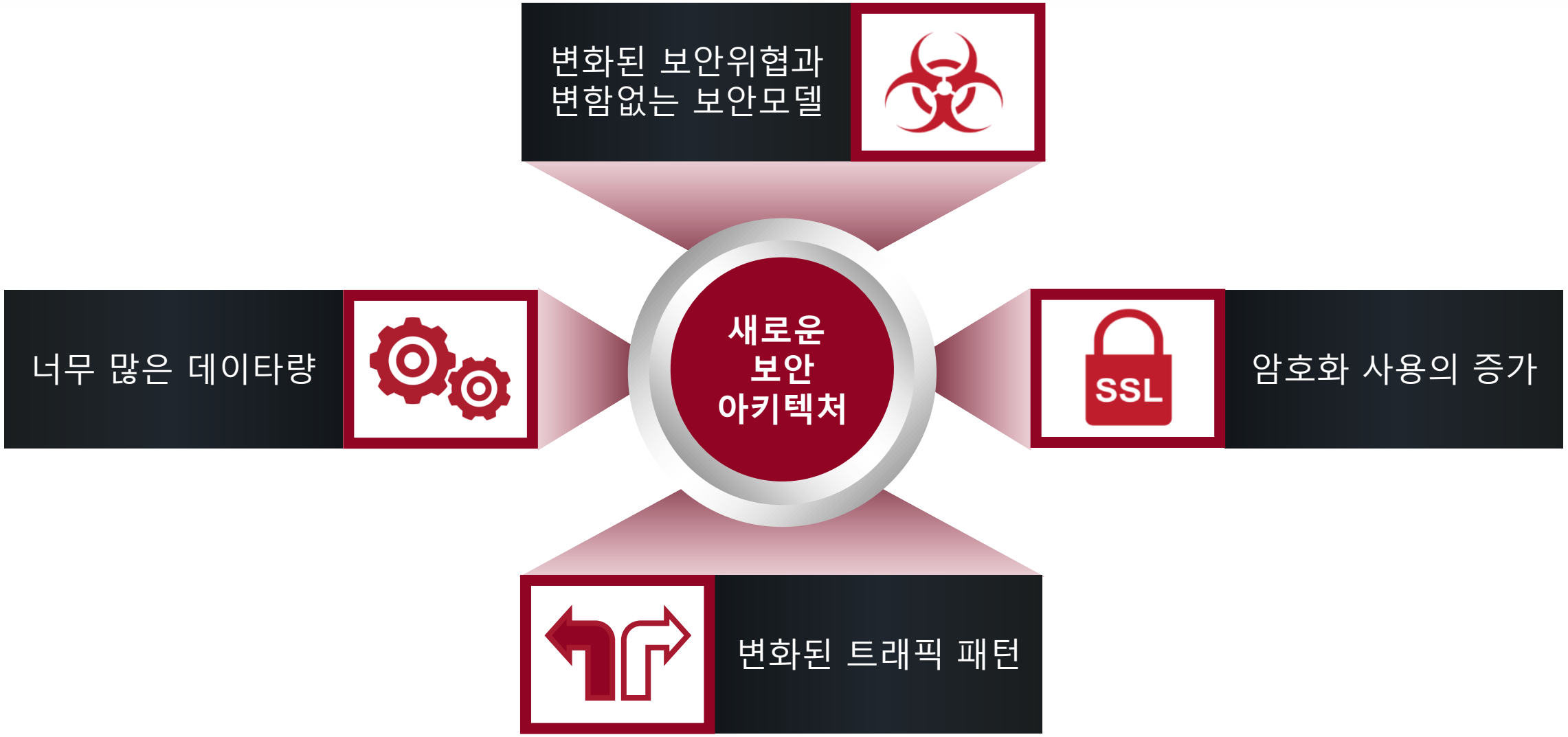
2017년, 네트워크 공격의 50% 이상이 보안통제를 우회하기 위해 암호화된 트래픽을 이용할 것으로 예측 (vs. 5% today)[2]

늘어나는 암호화된 트래픽에 대응 할 보안 및 위험 관리 방법?

[1] NSS Labs
[2] Gartner

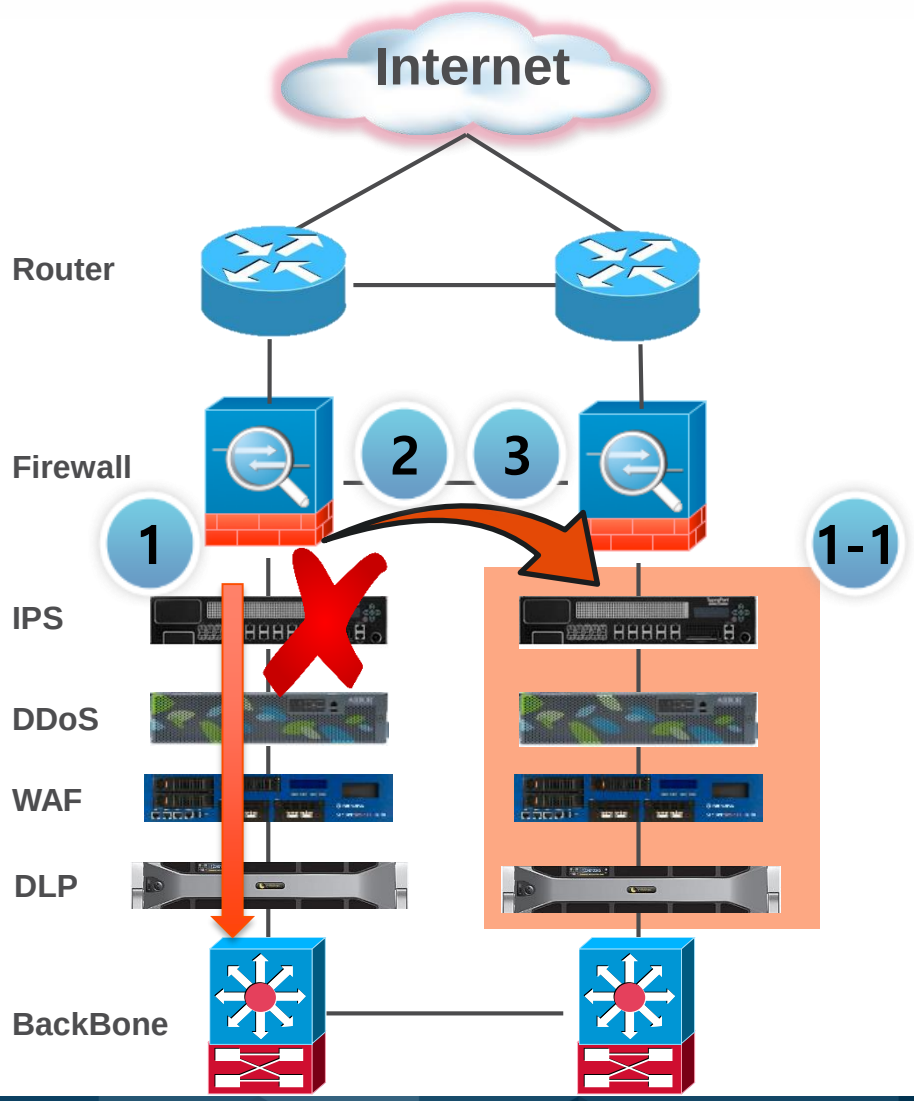
1. 보안 관리 전달 플랫폼 소개

1.3 보안 아키텍처의 재고



2. 보안 관리 전달 플랫폼 소개

2.4 인라인 보안장비 인프라 구성



1 장비운영 비효율성

- 관문단 인라인 장비에 **불필요**한 트래픽 유입에 따른 장비 **도입 비용 증가**

1-1 장비운영 비효율성

- 평상 시 Standby 회선의 인라인 장비 **유휴상태**

2 서비스 안정성

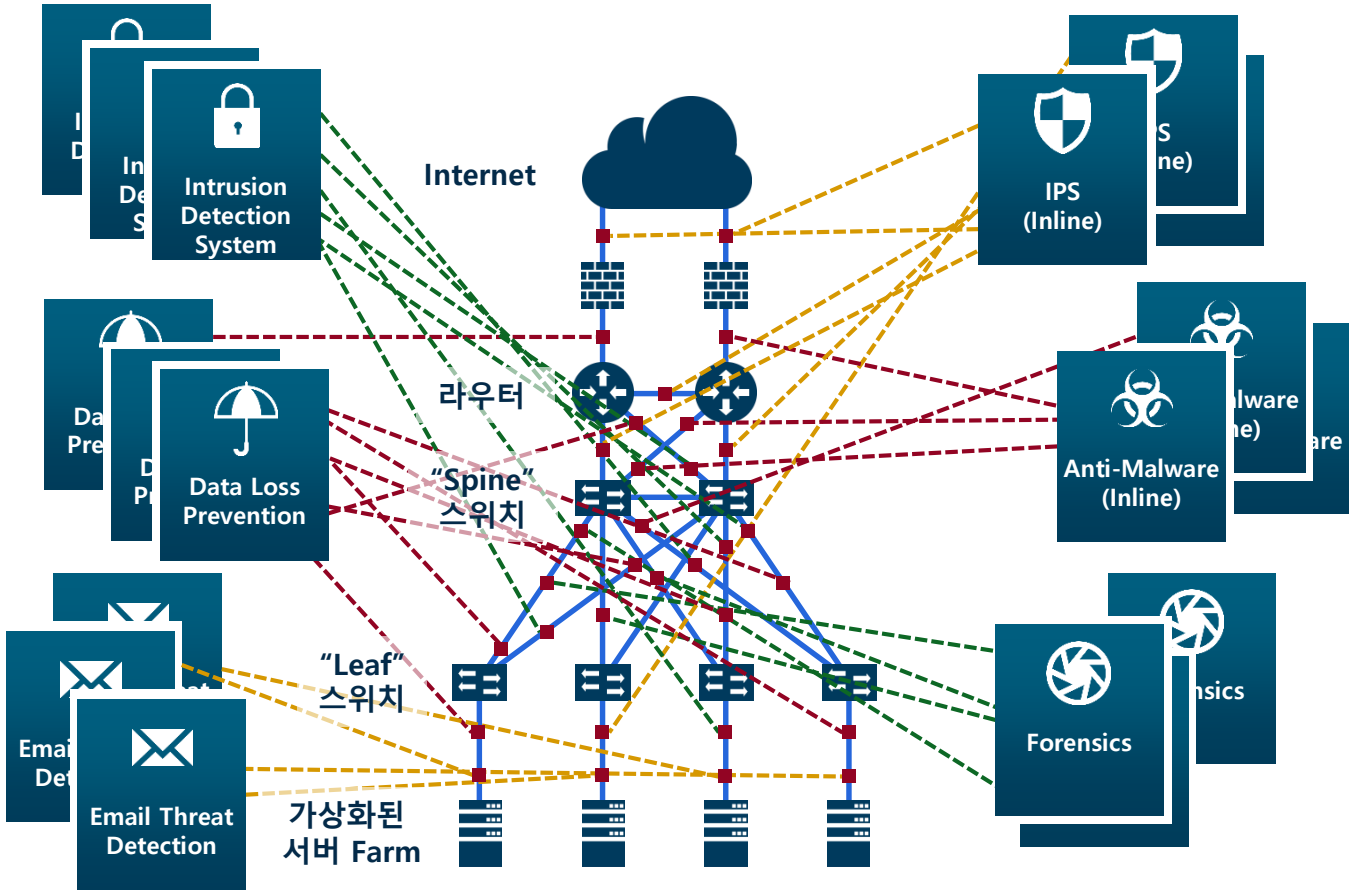
- Active 회선 인라인 **장비 장애** 시 회선 Fail over로 인한 **서비스 장애** 발생
- 인라인 장비 Hang시 서비스 장애 발생

3 유지보수

- 인라인 장비 **작업** 시 회선 **Fail over 발생**

1. 보안 관리 전달 플랫폼 소개

1.5 모니터링 인프라의 복잡성 : 너무 많은 모니터링 구간



복잡성 네트워크가 확장되면서 모니터링 솔루션 구성이 점차 복잡

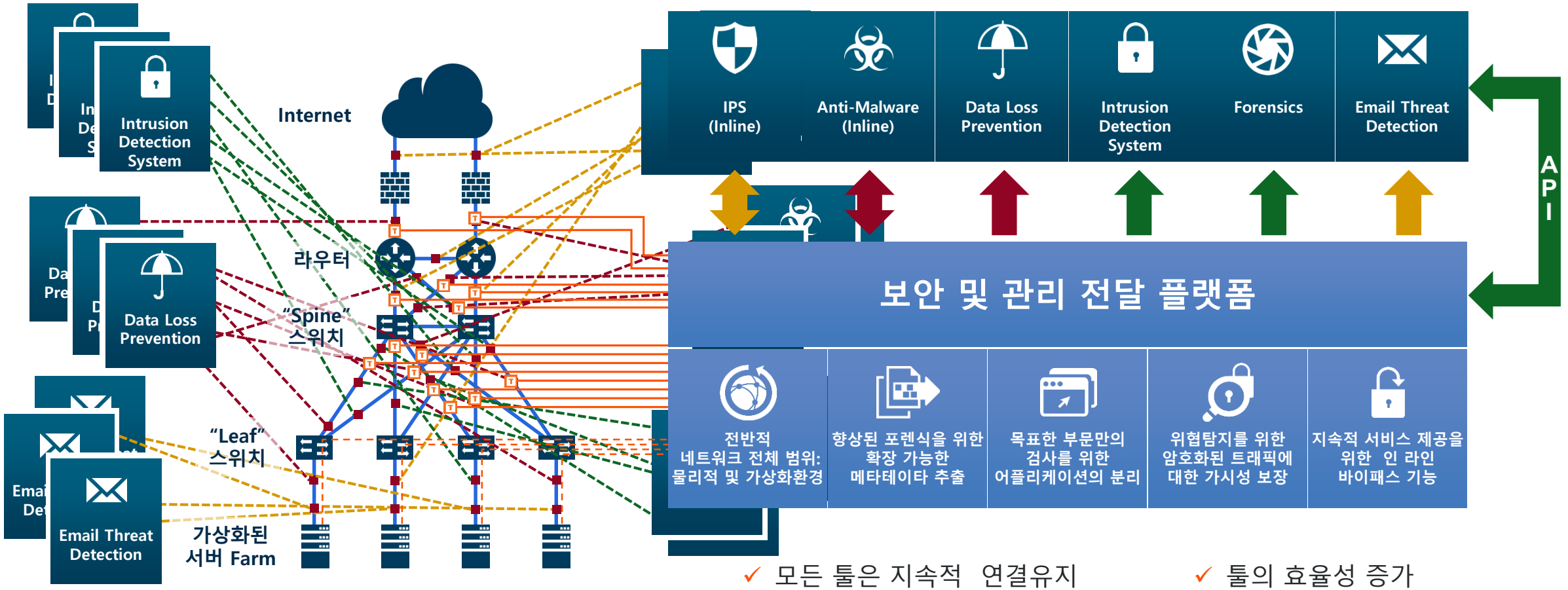
개별관리 네트워크 모니터링 및 분석 솔루션들이 팀 단위/부서 단위로 구축되고 개별로 관리되어 중복투자 발생

사각지대 Span 또는 Mirror 포트 구성 제약으로 인해 네트워크 전 구간의 모니터링 불가, 사각지대 발생

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

1. 보안 관리 전달 플랫폼 소개

1.6 보안 관리 전달 플랫폼: “SEE EVERYTHING”

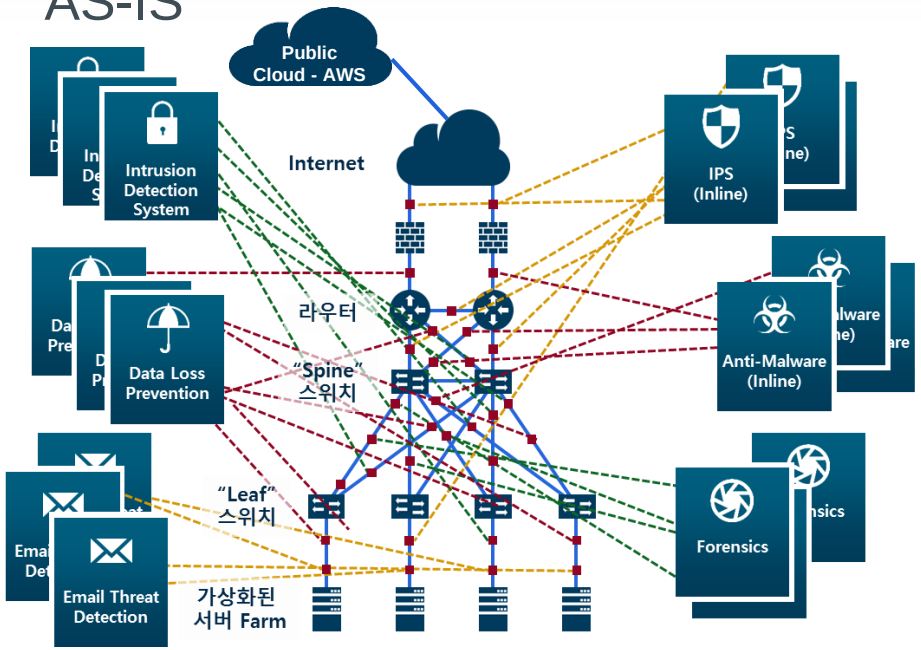


- ✓ 모든 툴은 지속적 연결유지
- ✓ 적은 수의 네트워크 접속 포인트
- ✓ 툴의 효율성 증가
- ✓ OPEX 비용 감소

1. 보안 관리 전달 플랫폼 소개

1.6 보안 관리 전달 플랫폼: “SEE EVERYTHING”

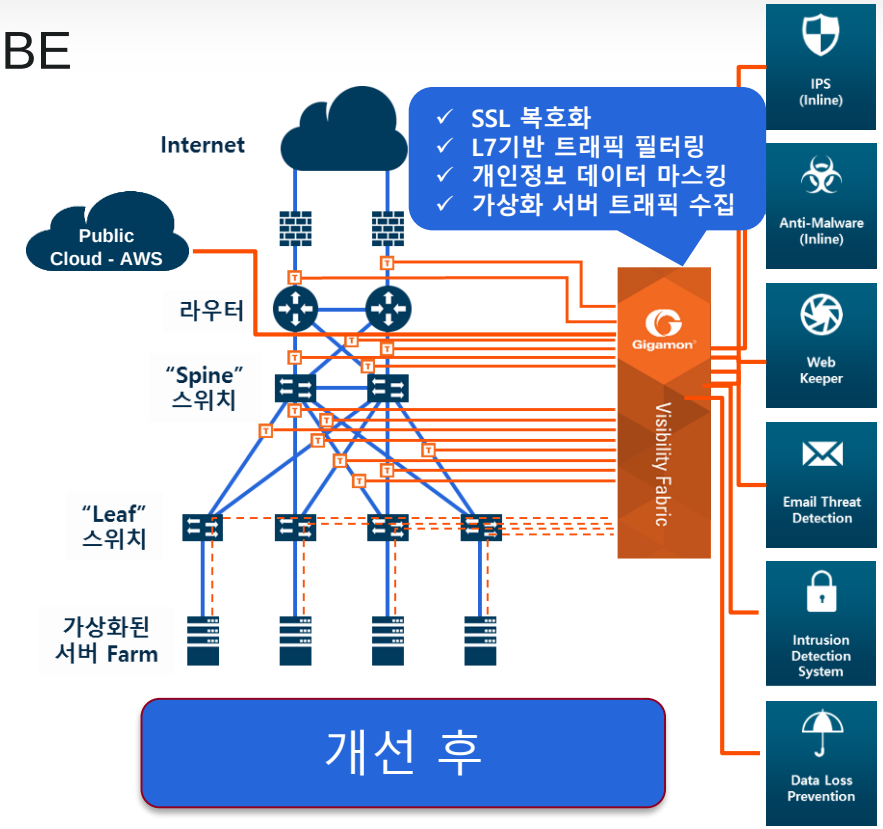
AS-IS



개선 전

개별 관리	팀별 필요성에 따른 개별 도입으로 전사 측면의 장비 운영 효율성 저하
투자비용 증가	네트워크 증설/고도화에 따른 지속적인 보안 모니터링 장비의 도입 필요
효율적인 장비 운영 불가	각 보안 장비들로 불필요한 트래픽이 같이 유입됨에 따라 효율적인 장비 운영 불가

TO-BE

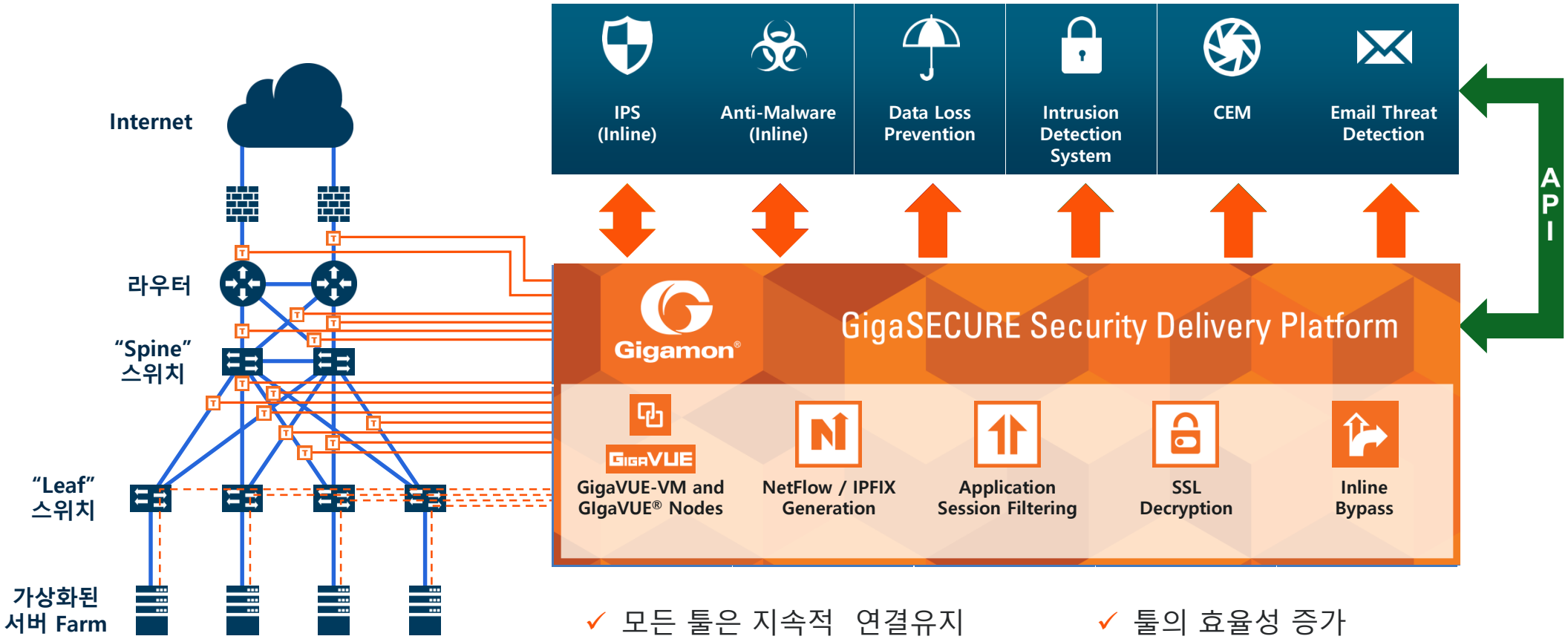


개선 후

통합 관리	모니터링 트래픽에 대한 전사적인 통합 관리
투자비용 감소	부서별 중복 도입 방지를 통한 투자비용(CAPEX) 억제
장비 운영 효율성 극대화	각 보안장비 별로 필요한 트래픽만 전달

1. 보안 관리 전달 플랫폼 소개

1.7 VISIBILITY FABRIC™ 구조



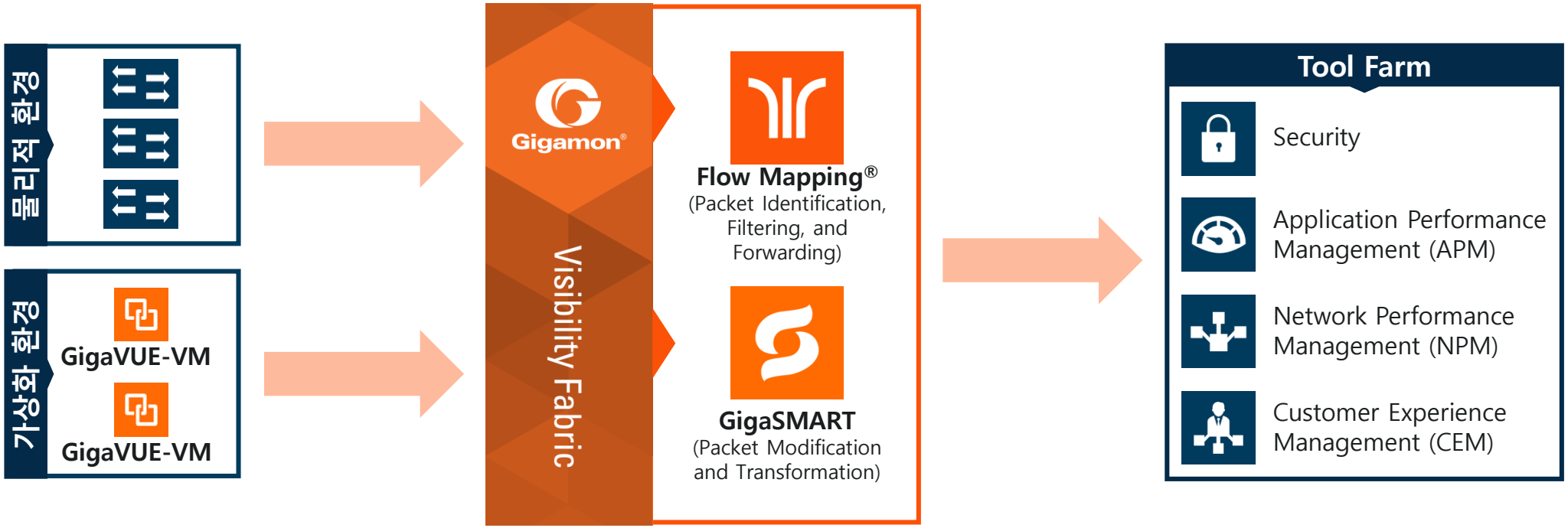
- ✓ 모든 툴은 지속적 연결유지
- ✓ 적은 수의 네트워크 접속 포인트
- ✓ 툴의 효율성 증가
- ✓ OPEX 비용 감소

1. 보안 관리 전달 플랫폼 소개

1.7 VISIBILITY FABRIC™ 구조

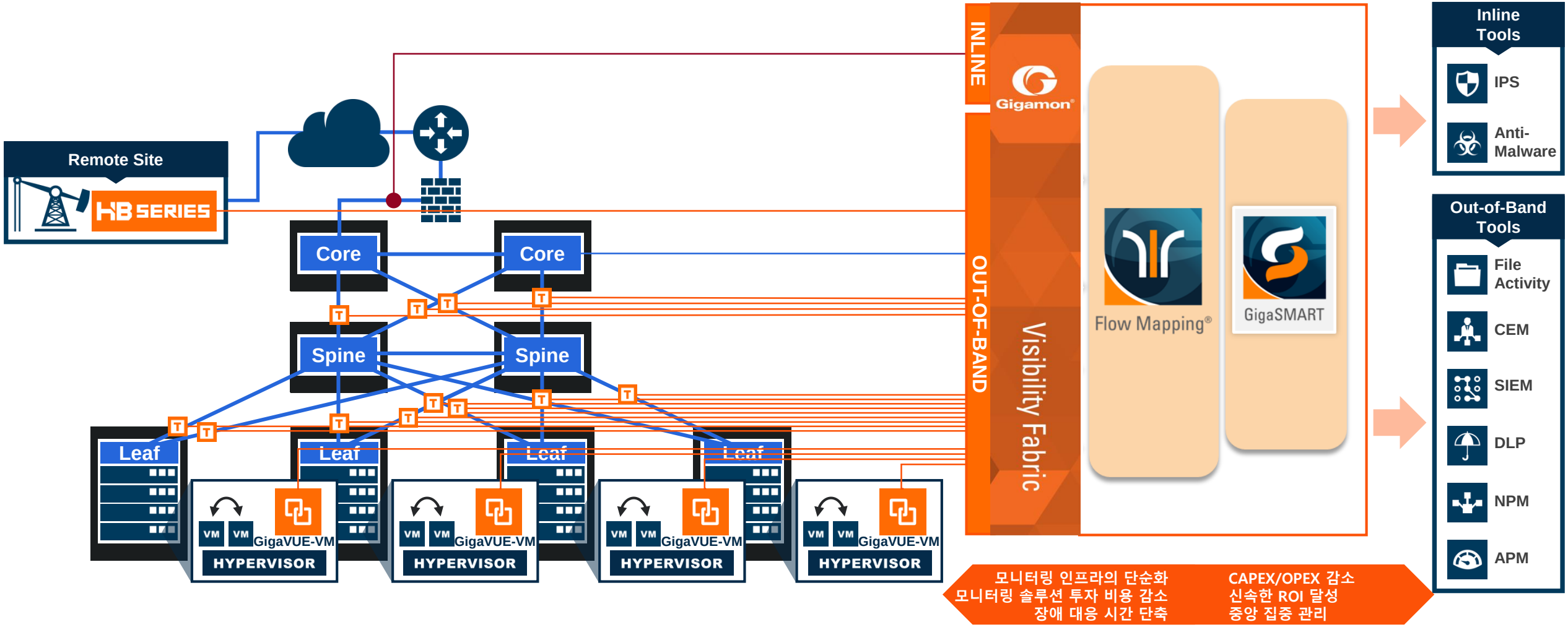
DashBoard – 변경 관리

- ✓ **보안 장비 도입** 시 **최소의 투자비용**으로 **모니터링**이 가능하도록 도와줍니다.
- ✓ 네트워크 상의 **어느 곳** 에서나 패킷 기반의 데이터 **가시성 확보** 및 활용이 가능합니다.
- ✓ 보안, 규정 준수 및 네트워크 모니터링의 **총 비용의 절감**이 가능합니다.



1. 보안 관리 전달 플랫폼 소개

1.7 VISIBILITY FABRIC™ 구조



1. 보안 관리 전달 플랫폼 소개

1.8 기가몬 VISIBILITY FABRIC™ 통합 포트폴리오

1. 보안 관리 전달 플랫폼 소개

1.9 기가몬 VISIBILITY FABRIC™ 주요 장비 사양

HD Series

GigaVUE-HD8

GigaVUE-HD4

초대형/대형 사이트급

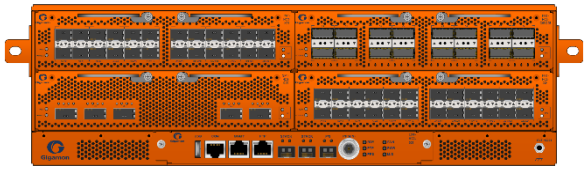
GigaVUE-HD8

포트 집적도 : 100G : 12 Ports | 40G : 64 Ports | 10G 256 Ports | 1G : 352 Ports
최대 320G GigaSMART® 성능
모니터링 처리 트래픽 : 최대 2.4 Tbps

GigaVUE-HD4

포트 집적도 : 100G : 6 Ports | 40G : 32 Ports | 10G 128 Ports | 1G : 176 Ports
최대 160G GigaSMART® 성능
모니터링 처리 트래픽 : 최대 1.2 Tbps

HC Series



GigaVUE-HC3

GigaVUE-HC2

GigaVUE-HC1

엔터프라이즈급

GigaVUE-HC3 :
10G/40G/100G 인터페이스 지원

포트 집적도 : 100G : 32 Ports | 40G : 64 Ports | 10G 96 Ports | 1G : 96 Ports
최대 500G GigaSMART® 성능
모니터링 처리 트래픽 : 최대 2.2 Tbps

GigaVUE-HC2 :
10G/40G/100G 인터페이스 지원 , Bypass Module 지원

포트 집적도 : 100G : 8 Ports | 40G : 24 Ports | 10G 96 Ports | 1G : 96 Ports
최대 200G GigaSMART® 성능
모니터링 처리 트래픽 : 최대 960 Gbps

GigaVUE-HC1 : Bypass Module 지원

포트 집적도 : 10G 12 Ports | 1G : 4 Ports
최대 20G GigaSMART® 성능
모니터링 처리 트래픽 : 최대 124 Gbps

1. 보안 관리 전달 플랫폼 소개

1.9 기가몬 VISIBILITY FABRIC™ 주요 장비 사양

HB Series

GigaVUE-HB1

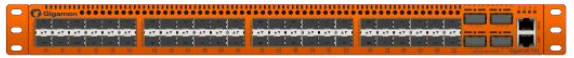
엔트리급

GigaVUE-HB1 :

지사,원격지 사이트 등 소용량 모니터링

포트 집적도 : 10G 4 Ports | 1G : 20 Ports
최대 10G GigaSMART® 성능
모니터링 처리 트래픽 : 최대 56 Gbps

TA Series



GigaVUE-TA10

TA시리즈

GigaVUE-TA10 :

0G/40G 모니터링 트래픽 Aggregation 및 L7레이어 기반 패킷 필터링

포트 집적도 : 40G 4 Ports | 1G/10G : 40 Ports
모니터링 처리 트래픽 : 최대 640 Gbps

2. 핵심 기술

2.1 Flow Mapping

2.2 Inline Bypass

2.3 GigaSMART®

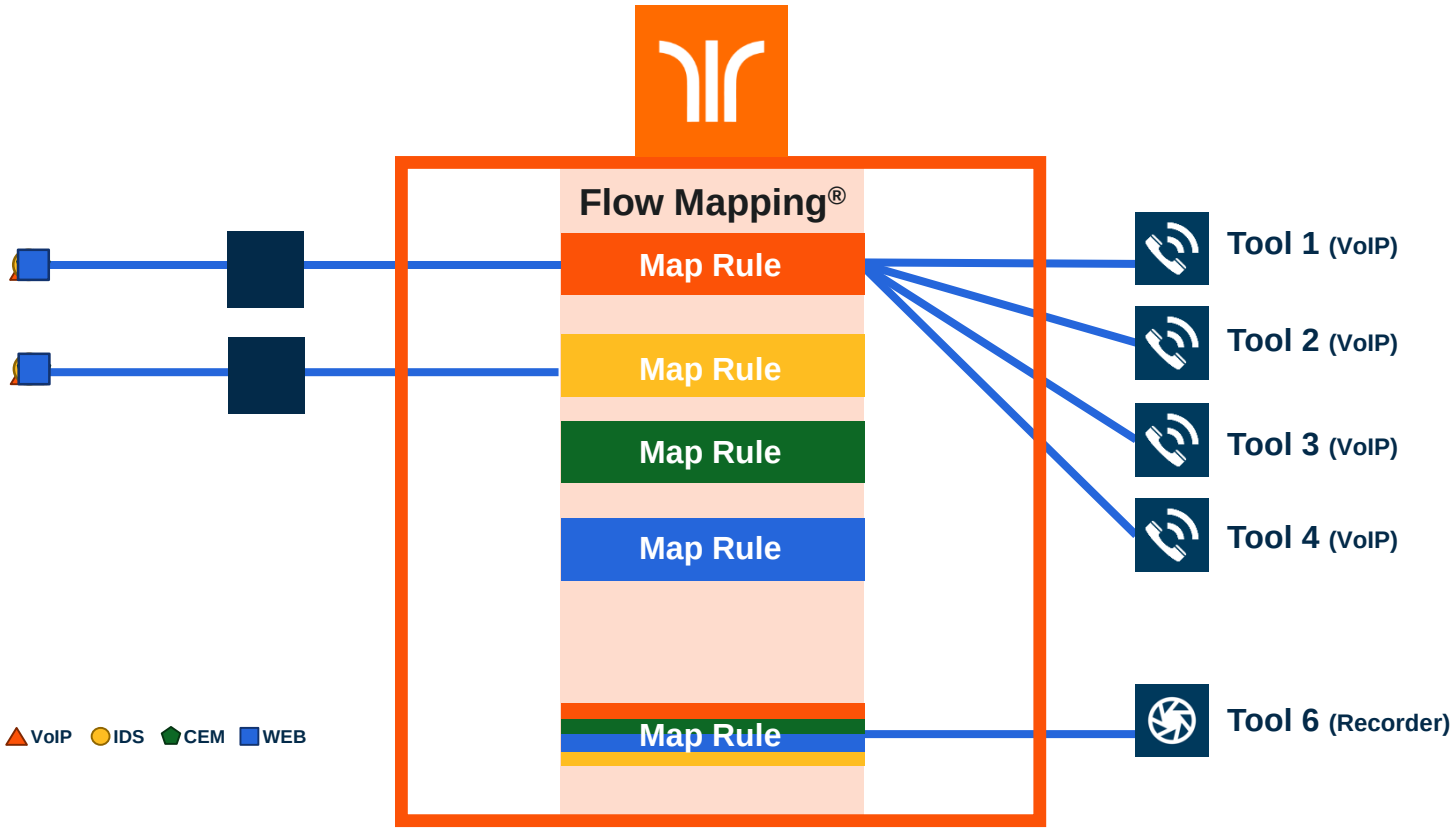
2.4 클라우드(GigaVUE-VM®)

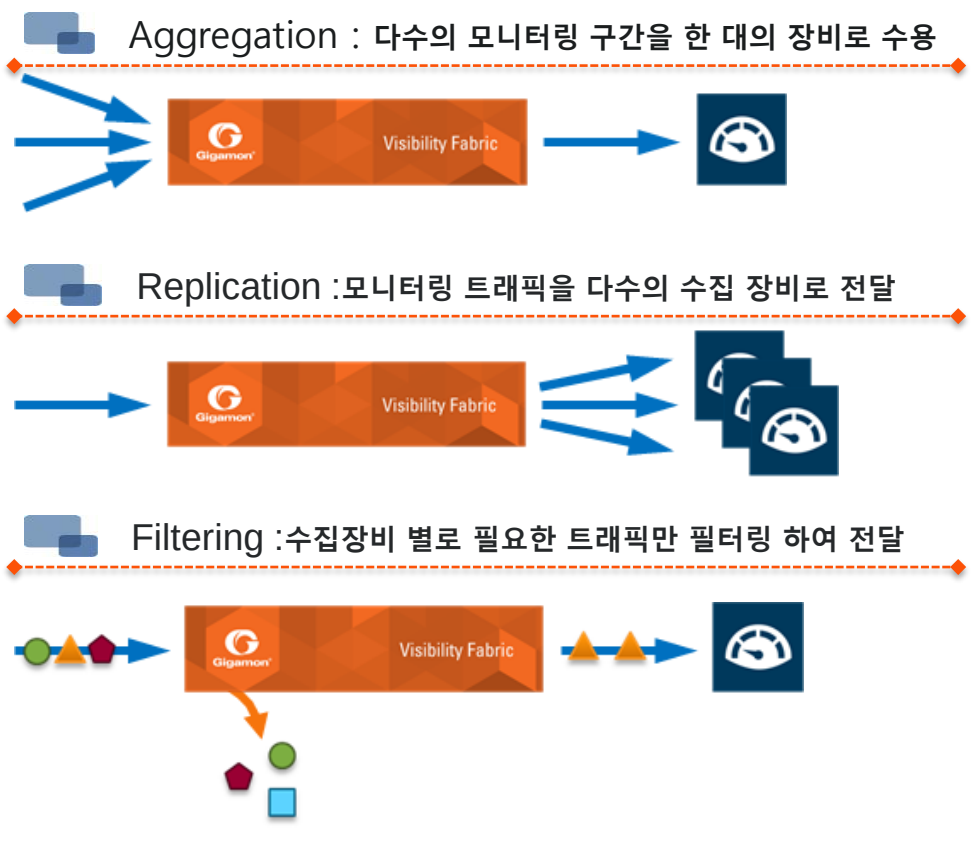
2. 핵심 기술

2.1 Flow Mapping

Flow Mapping 장점 기술

✓ 기가몬의 혁신적인 **"Flow Mapping"** 기능은 IPv4/IPv6, L2, L3 및 L4 레이어,VLAN ID, MAC 주소를 **30개 이상**의 **사전 정의된 항목**을 통하여 운영자가 **원하는 트래픽**을 다수의 **모니터링 장비**로 **분배** 및 **전달**함으로써 모니터링 장비의 부하가 감소하여 **효율**적인 보안장비/모니터링 **장비 운영**이 가능합니다.

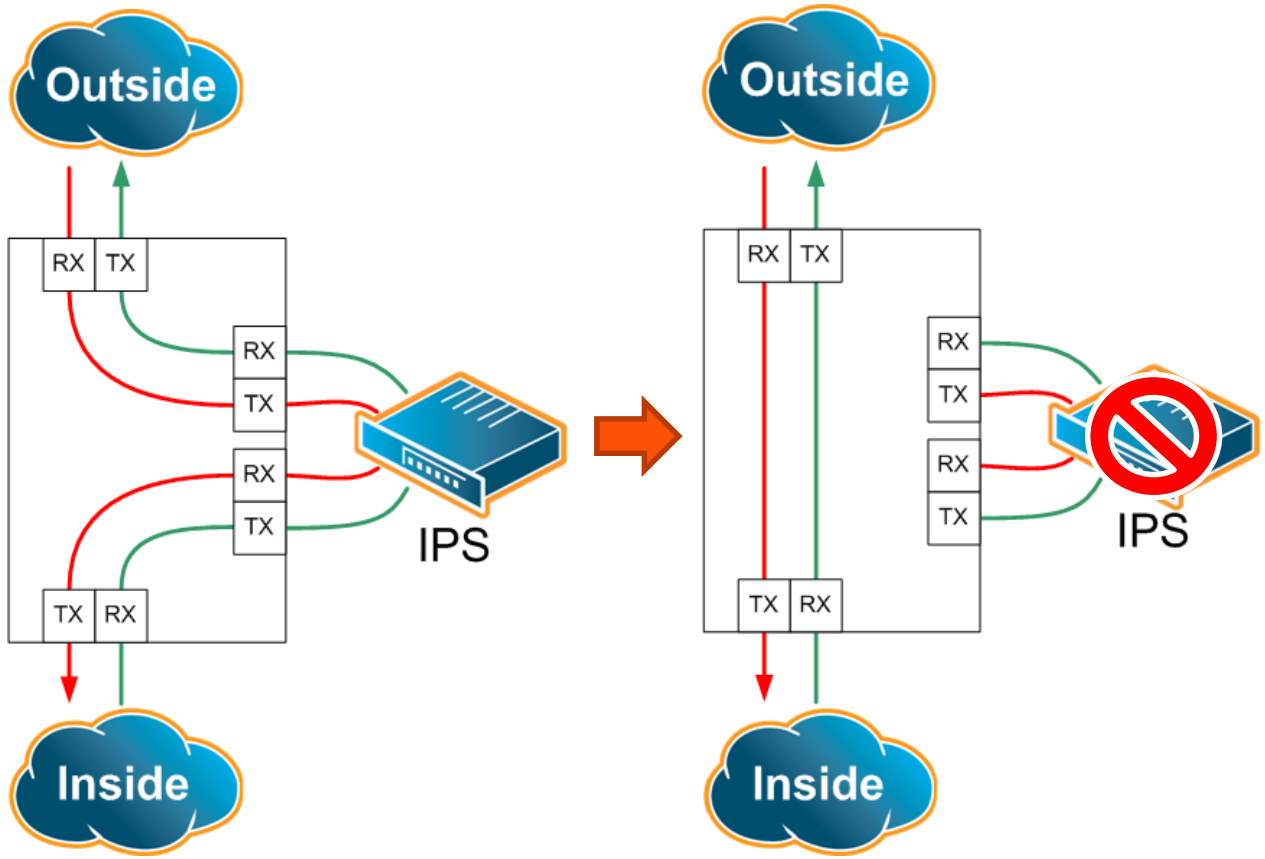




2. 핵심 기술

2.2 Inline Bypass 기능

› 인라인 장비(IPS,WAF,DDoS)와의 연동으로 **유연한 인라인 장비 운영**이 가능합니다.



물리적 바이패스 보호

- 기가몬 장비의 파워 장애 발생시 자동으로 바이패스하는 기능

논리적 바이패스 보호

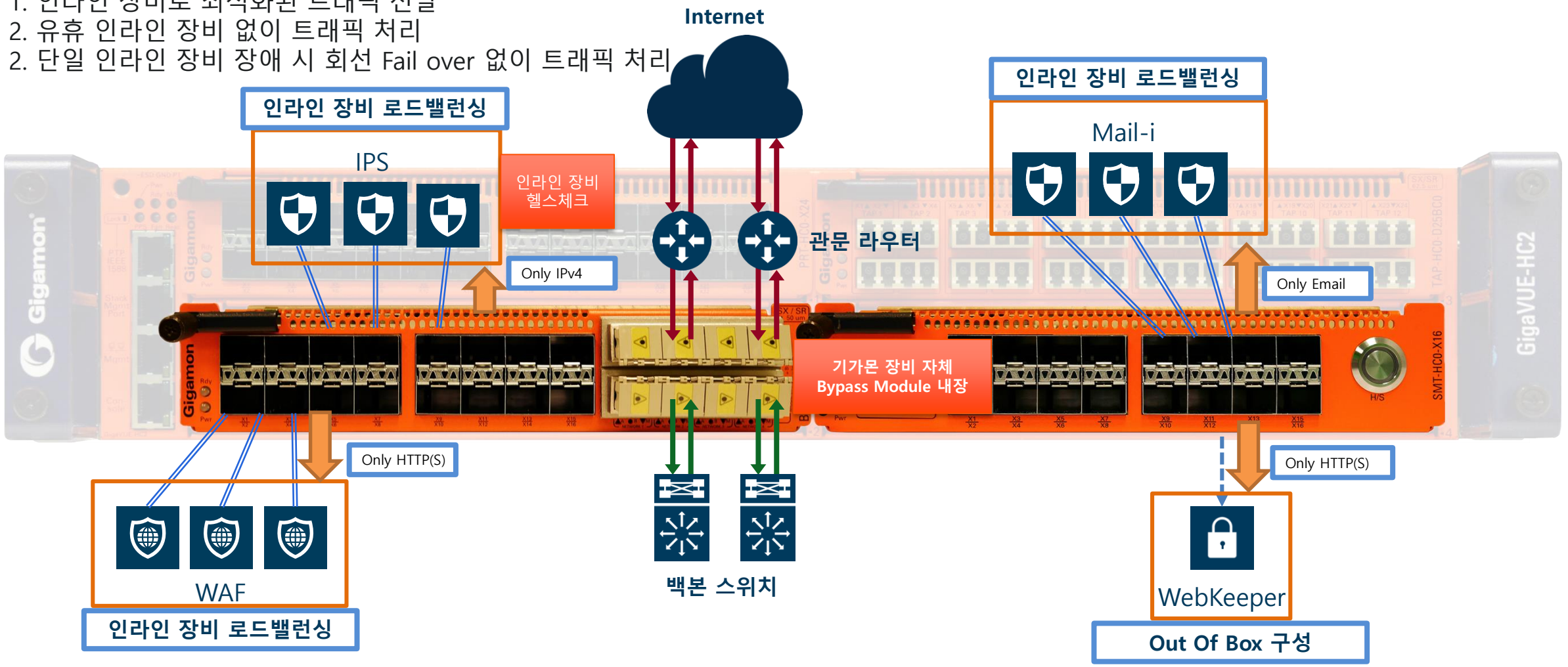
- 인라인 장비의 장애 감지:
  - 인라인 장비 다운
  - 인라인 장비 Hang up 감지(**Heartbeat**)
- 바이패스 방식:
  - 패킷 드랍 / 패킷 포워딩
  - 이중화 장비로 패킷 포워딩 (1+1, N+1)

2. 핵심 기술

2.2 Inline Bypass 기능

- 인라인 장비(IPS,WAF,DDoS)와의 연동으로 효율적인 **장비 운영**이 가능합니다.

1. 인라인 장비로 최적화된 트래픽 전달
2. 유휴 인라인 장비 없이 트래픽 처리
2. 단일 인라인 장비 장애 시 회선 Fail over 없이 트래픽 처리



2. 핵심 기술

2.3 GigaSMART® – Traffic Intelligence

기능 요약

License	Description	개선 효과
Packet Slicing *1	▪ 큰 사이즈의 패킷을 잘라서 모니터링 장비로 전달	▪ 모니터링 장비 부하 감소/모니터링 장비 스토리지 사용량 감소
Masking *1	• 패킷 내부의 개인정보(카드)를 마스킹 처리해서 모니터링 솔루션으로 전달	• 모니터링 솔루션에 대한 개인정보 관련 업무 부하 감소
Source Port Labeling *1	• 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

*1 :GigaSMART 하드웨어 구매 시 기본 제공 라이선스

2. 핵심 기술

2.3 GigaSMART® – Traffic Intelligence

기능 요약

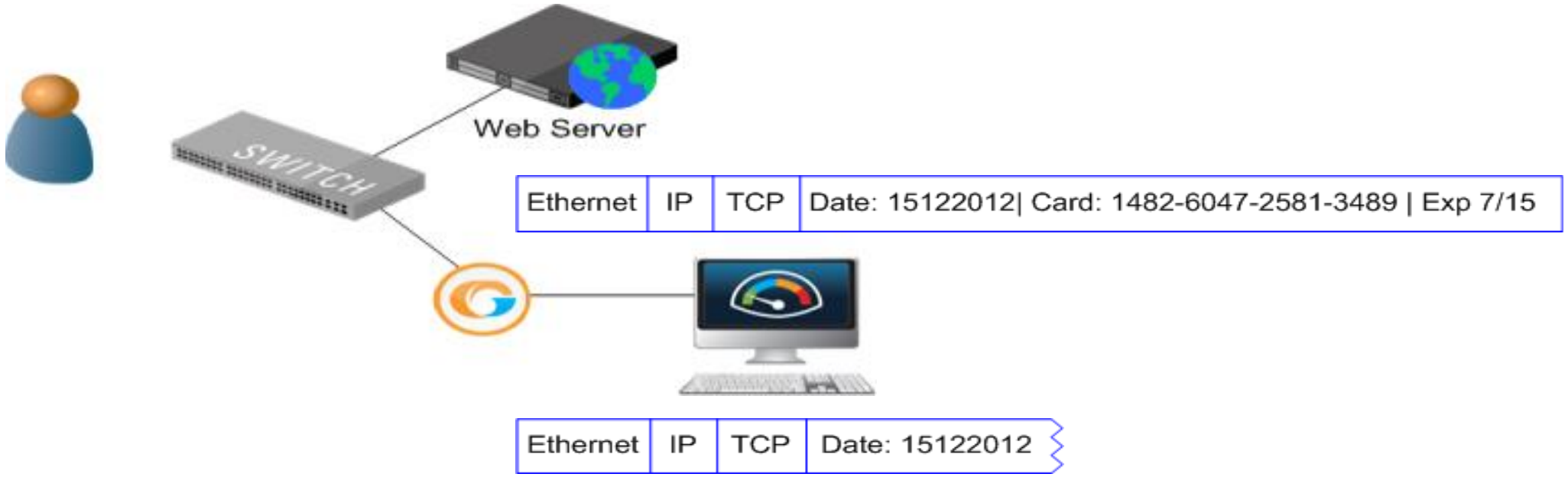
License	Description	개선 효과
Adaptive Packet Filtering, Application Session Filtering	▪ VXLAN, VN-Tag, and VGRE 기반의 패킷 필터링 ▪ 패킷 내부의 데이터 중 특정 패턴 기반으로 패킷 필터링 ▪ Application Session Filtering은 특정 패턴 기반으로 매칭되는 세션 전체를 필터링하여 모니터링 장비로 전달	▪ 모니터링 장비 부하 감소/모니터링 장비 스토리지 사용량 감소
SSL Decryption	▪ 암호화된 SSL 트래픽을 평문으로 복호화 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

2. 핵심 기술

2.3 GigaSMART - Packet Slicing

모니터링 트래픽 최적화

- ✓ 수신되는 **패킷 사이즈 최적화**를 통한 **보안/모니터링 장비 부하 경감으로 불필요한 장비 투자 비용을 줄일 수 있습니다.**
- ✓ 모니터링 장비의 **효율적인 저장공간 운영**으로 불필요한 **디스크 투자 비용을 줄일 수 있습니다.**

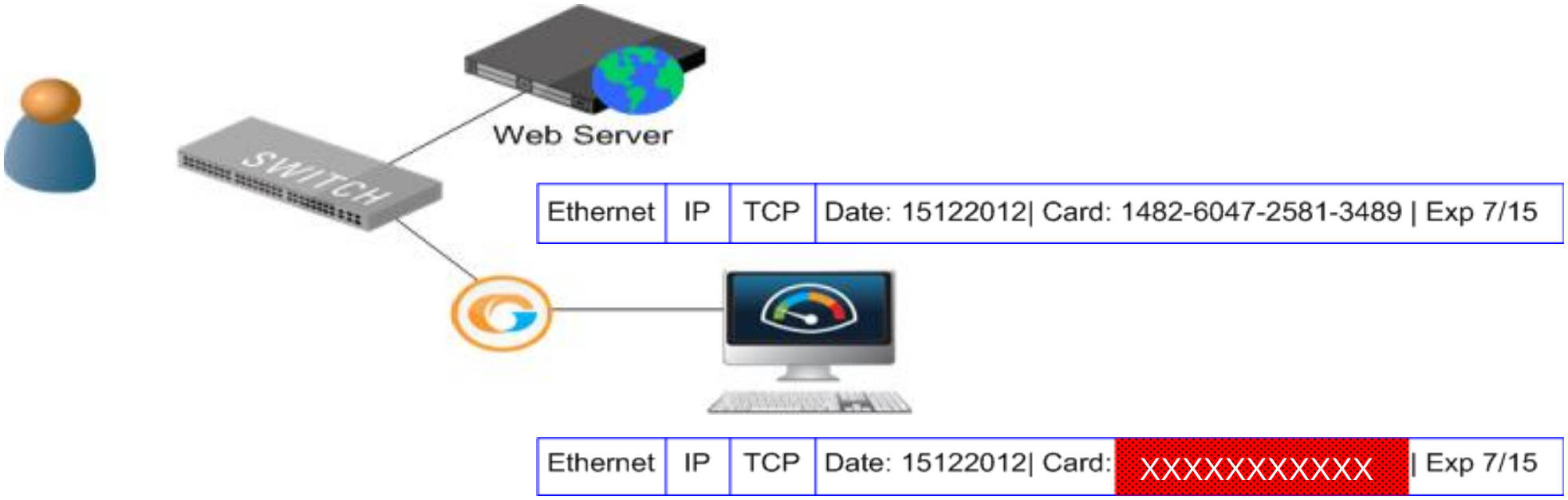


2. 핵심 기술

2.3 GigaSMART - Packet Masking

개인 정보 등 데이터 마스킹 기능 제공

✓ 패킷 내 페이로드에 포함된 **민감한 개인정보**(카드 정보,전화번호,주민등록번호 등)를 **마스킹**하여 각종 **보안 규정**(ISMS,전자금융 감독규정 등) **준수** 관련 **업무 부담 해소**가 가능 합니다.

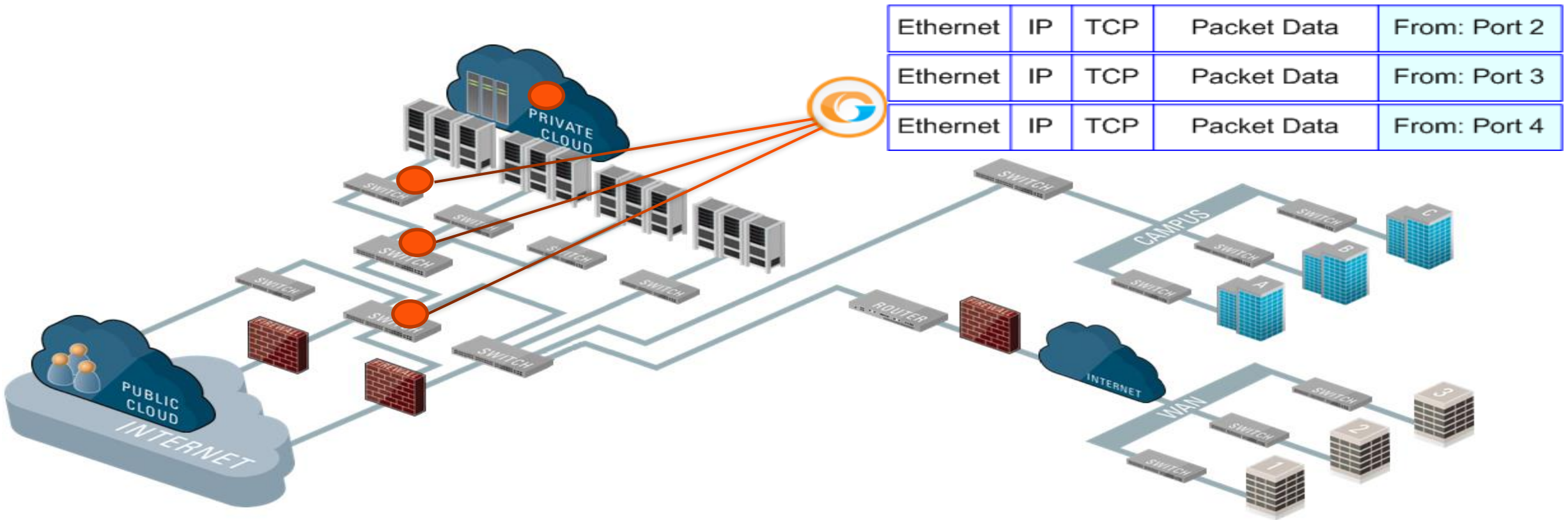


2. 핵심 기술

2.3 GigaSMART - Source Port Labeling

- 패킷이 유입된 포트에 대한 라벨링 기능

  ✓ 패킷이 **유입된 구간**에 대한 **구분**을 통해 트래픽 지연,트래픽 유실과 같은 **장애처리** 시 **신속한 트러블슈팅**이 가능 합니다.



2. 핵심 기술

2.3 GigaSMART - De-Duplication

- 중복 패킷 제거를 통한 효율적인 장비 운영

✓ **다수의 구간**에 대한 트래픽 모니터링 시 필연적으로 발생하는 **중복 패킷 제거**를 통해 **효율적인 보안장비/모니터링 장비 운영**이 가능합니다.

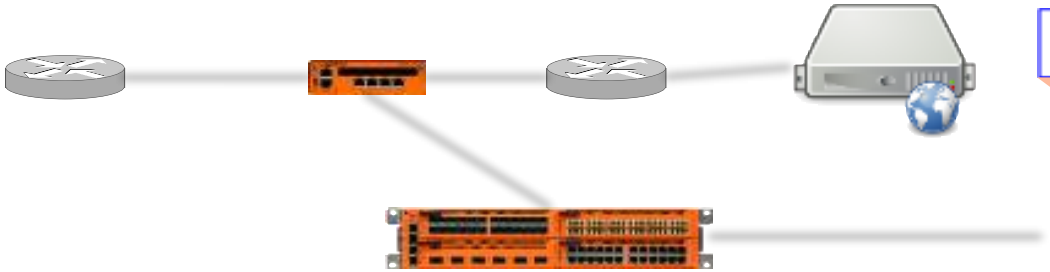
2. 핵심 기술

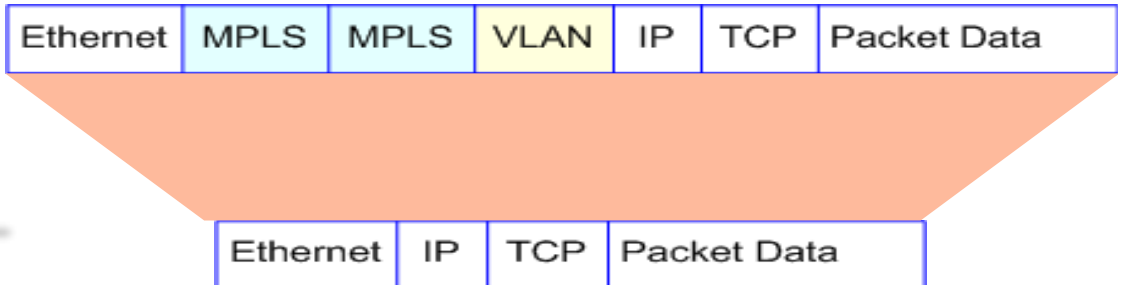
2.3 GigaSMART - Packet Header Stripping

불필요한 패킷 헤더 제거

- ✓ VLAN, MPLS, VN-Tags, VXLAN, Cisco FabricPath, GTP tunnels, ISL tunnels, GRE 등 분석/모니터링 장비에서 인식할 수 없는 **패킷 헤더 정보를 제거**하여 보안장비/모니터링 장비에서 **원활한 분석**을 지원합니다.

- ✓ 유입되는 패킷 구분을 위하여 **VLAN Tag 정보를 추가**하여 보안장비/모니터링 장비에서 네트워크 별 **트래픽 구분**이 가능하도록 지원합니다.



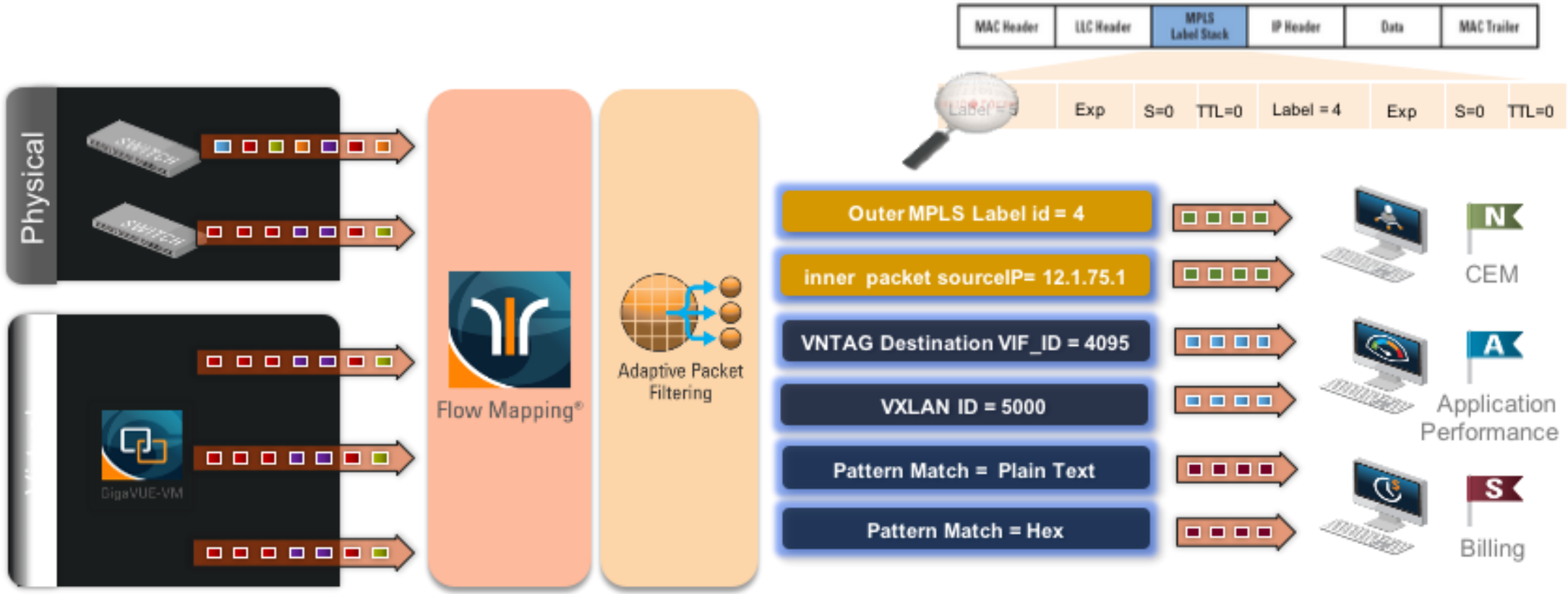


2. 핵심 기술

2.3 GigaSMART - Adaptive Packet Filtering

Layer7 기반 패킷 필터링

✓ MPLS/VLAN ID 및 패킷 내부의 **문자열 기반**으로 **트래픽을 필터링**하여 보안장비/모니터링 장비로 **전달**함으로써 보안장비/모니터링 장비에 **최적화된 트래픽만 전달**하여 트래픽 분석이 가능합니다.

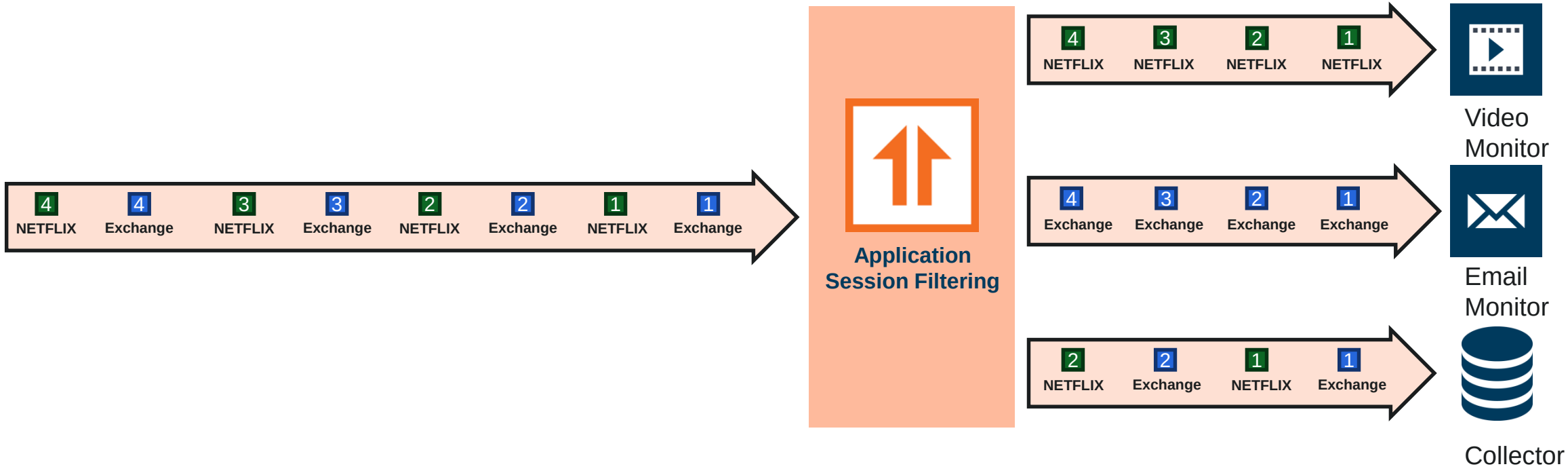


2. 핵심 기술

2.3 GigaSMART - Application Session Filtering

Layer7 기반 세션 필터링

✓ Layer7 기반의 **특정 어플리케이션 세션** 또는 **특정 도메인,URL**과 관련된 **세션을 필터링** 하여 보안장비/분석장비로 전달함으로써 **제한된 성능의 장비**에서도 **효율적인 운영**이 가능합니다.

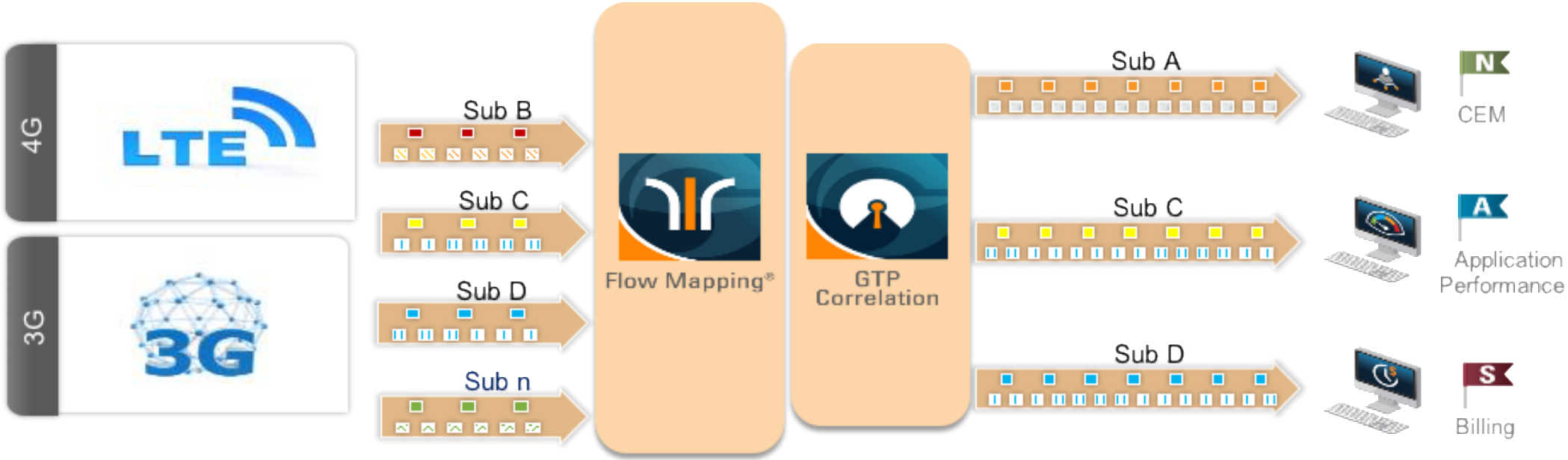


2. 핵심 기술

2.3 GigaSMART - GTP Correlation

- 3G 또는 LTE 망 내 GTP-u & GTP-c 패킷의 연관성 제공

  - ✓ GTP-u/GTP-c 연계 분석을 위하여 동일 분석 장비로 전달할 수 있습니다.
  - ✓ 가입자 기반의 플로우 샘플링 기능을 제공합니다.
  - ✓ White List 제공으로 특정 가입자의 추적기능을 제공합니다.

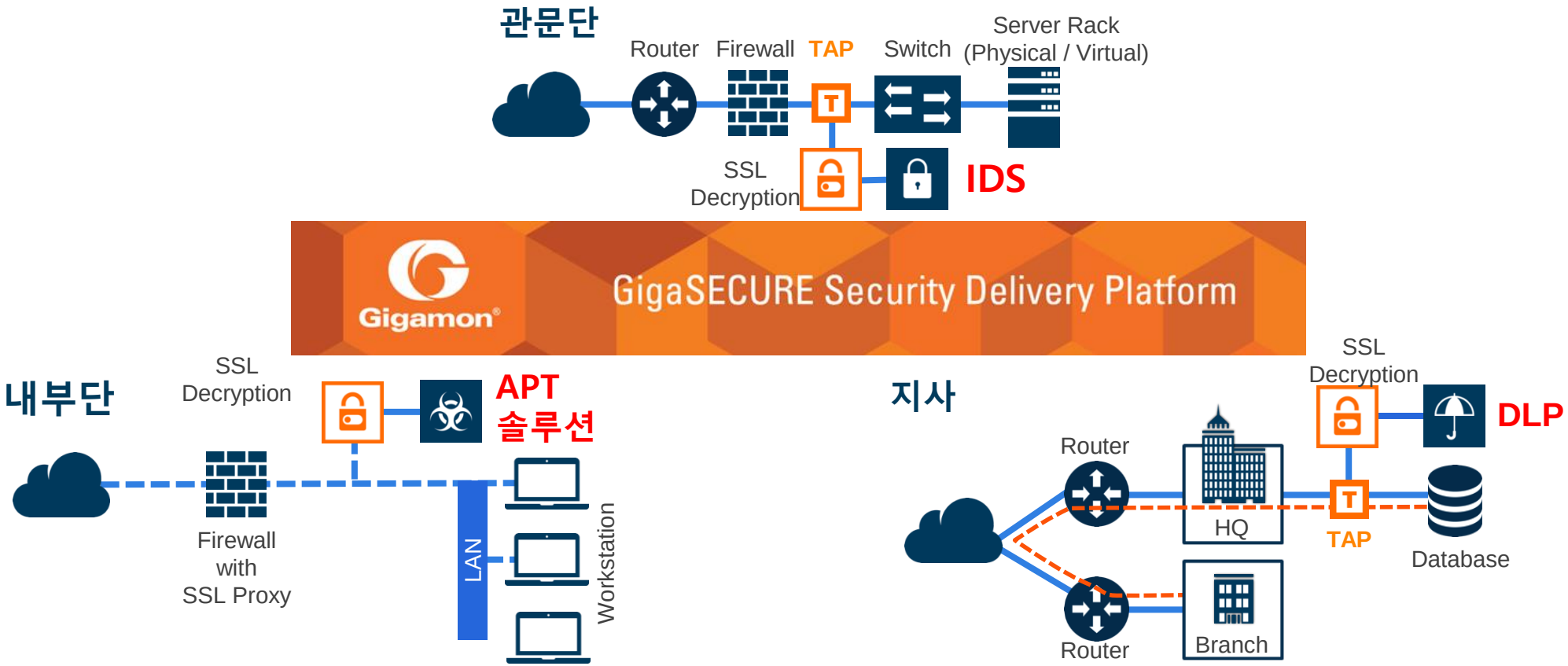


2. 핵심 기술

2.3 GigaSMART - SSL Decryption (Out of Band)

- SSL 암호화 트래픽에 대한 분석 지원

✓ **서비스 안정성에 영향없이** 미러링 또는 탭스위치를 통해 **SSL 트래픽 수집** 및 **평문화** 후 보안 장비(IDS,APT 솔루션,DLP 등)로 **전달**함으로써 **안정적인 SSL 트래픽**에 대한 **보안 위협 분석**이 가능합니다.

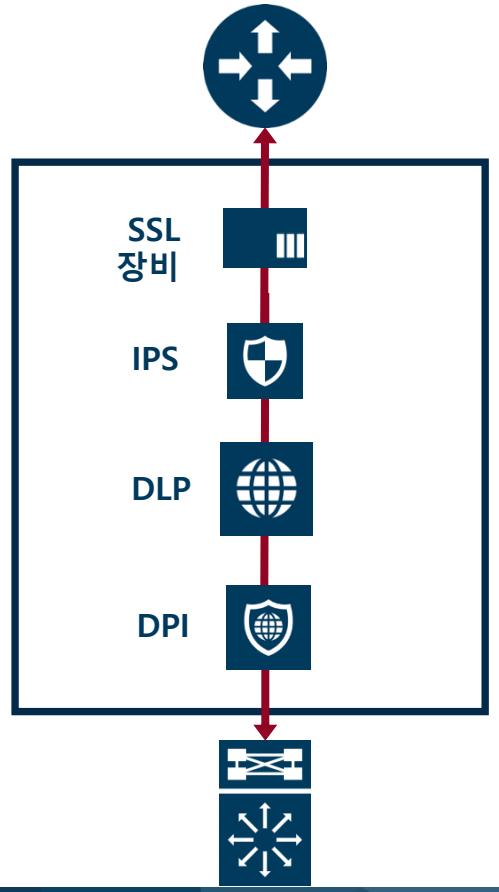


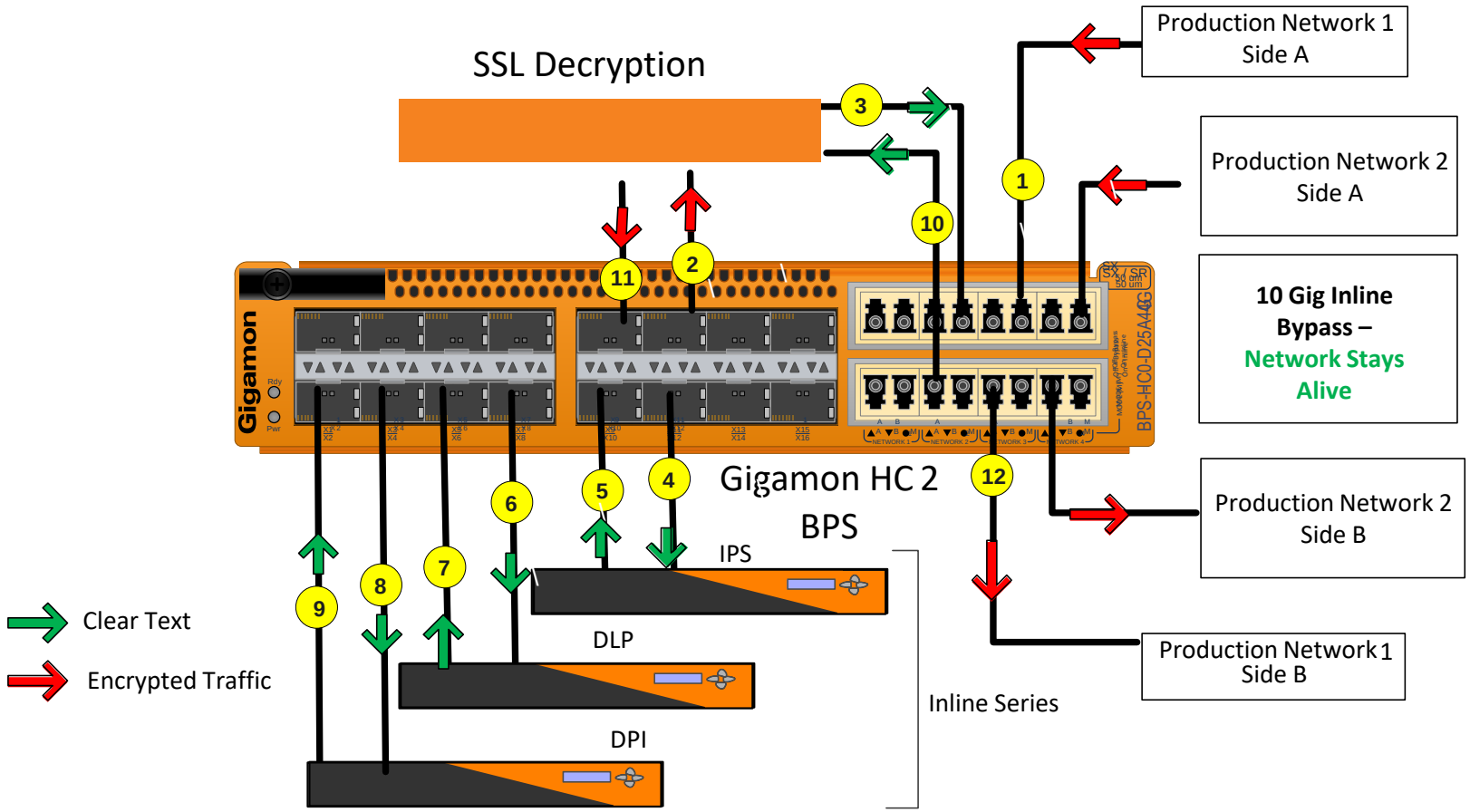
2. 핵심 기술

2.3 GigaSMART - SSL Decryption (In-Line)

- 외장형 SSL Decryption 솔루션 + DLP/IPS 결합 솔루션 :

  ✓ **인라인 장비**에 대한 **강화된 바이패스**, 인라인 장비 **이중화(HA)** 및 **로드밸런싱** 제공으로 보다 **향상된 장비의 안정성**과 **유연한 확장성**을 제공합니다.



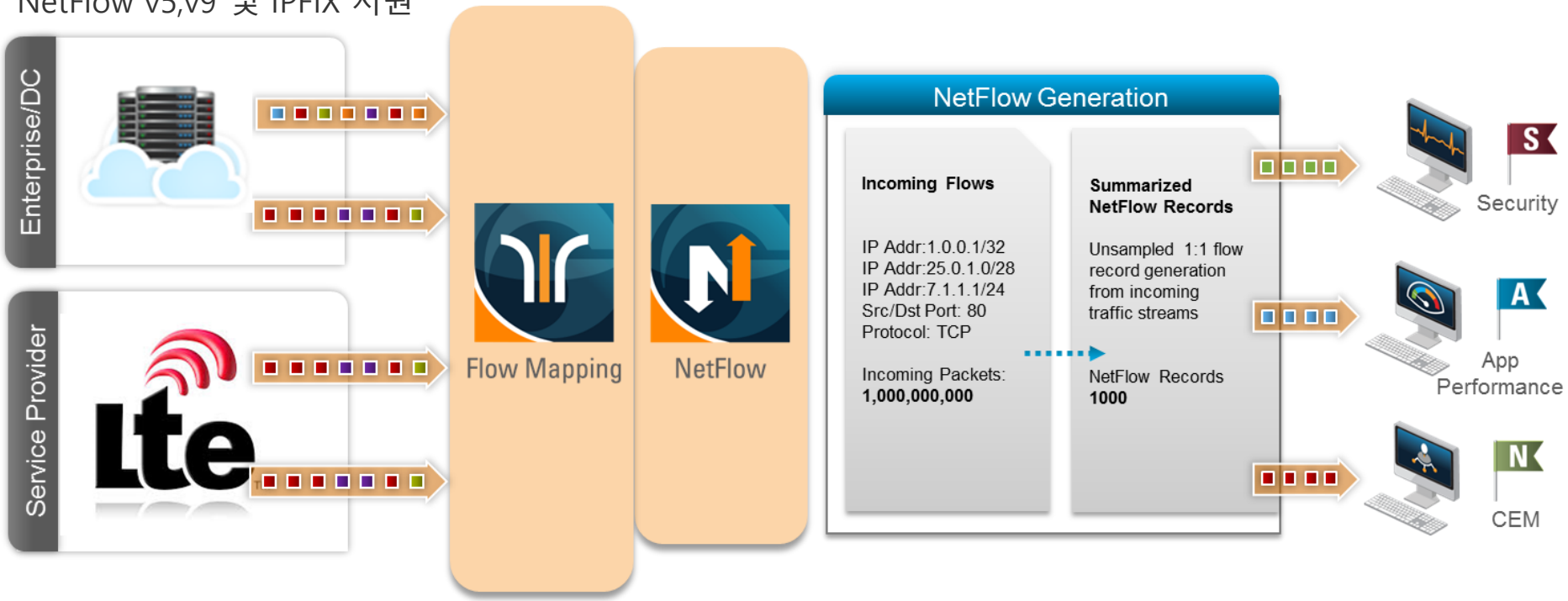


2. 핵심 기술

2.3 GigaSMART - NetFlow Generation

전수 트래픽 NetFlow 생성 기능

- ✓ 모니터링 트래픽에 대한 **전수 NetFlow 생성**을 통해 실망에서 운영 중인 네트워크 장비의 **부하 경감** 및 향후 보안사고 또는 포렌직 수행 시 관련 **접속 정보 제공**이 가능합니다.
- ✓ 최대 6개의 NetFlow 수집서버로 전송 지원
- ✓ NetFlow v5,v9 및 IPFIX 지원



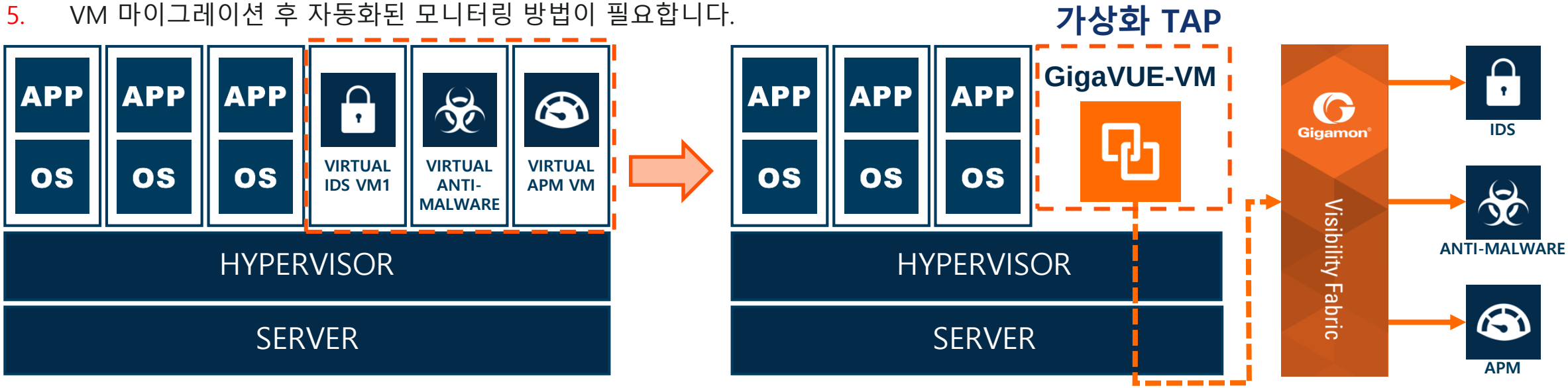
2. 핵심 기술

2.4 클라우드

가상화 트래픽의 가시성

가상화 환경에서 보안 위협 분석 시 고려사항

1. 가상화 환경에서 보안의 중요성이 강조되고 있습니다.
2. 가상화를 통한 미션 크리티컬 VM이 증가되고 있습니다.
3. 보안 및 어플리케이션 성능 분석을 위하여 VM간 트래픽에 대한 모니터링이 필요합니다.
4. 가상화 인스턴스를 생성하는 것이 전체 워크로드 성능에 영향을 줍니다.
5. VM 마이그레이션 후 자동화된 모니터링 방법이 필요합니다.

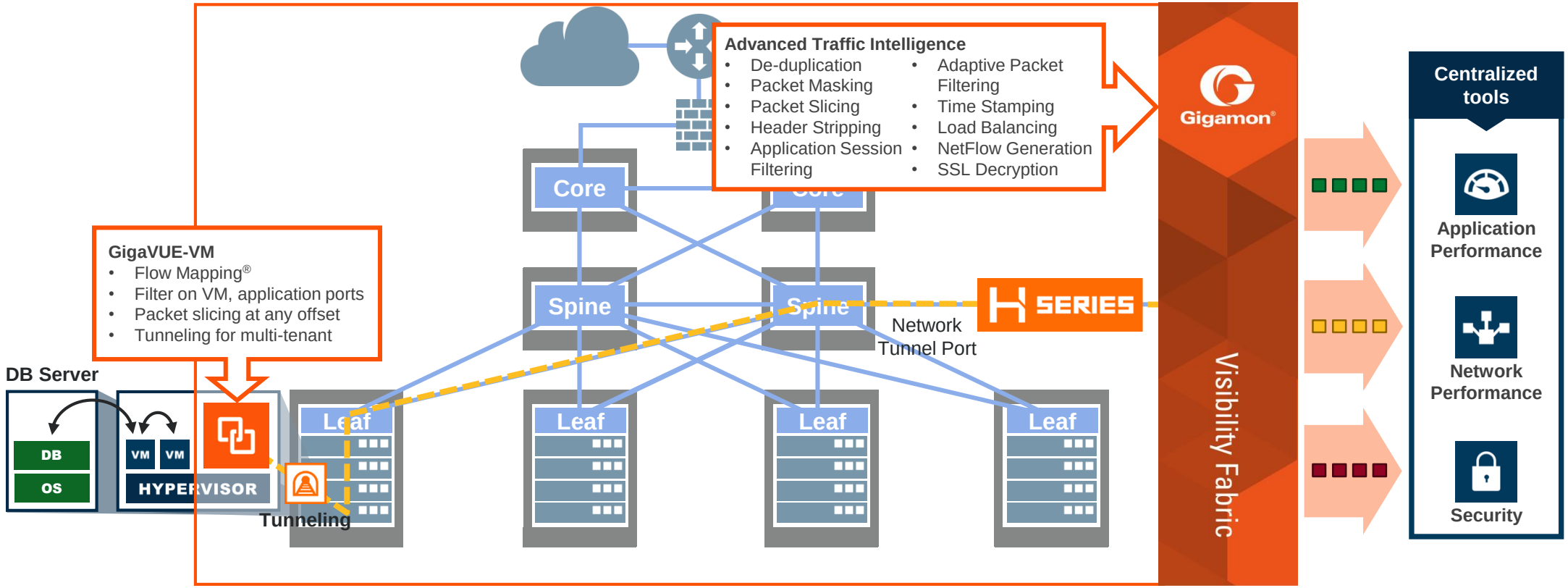


2. 핵심 기술

2.4 클라우드

가상화 환경의 모니터링 - GigaVUE-VM

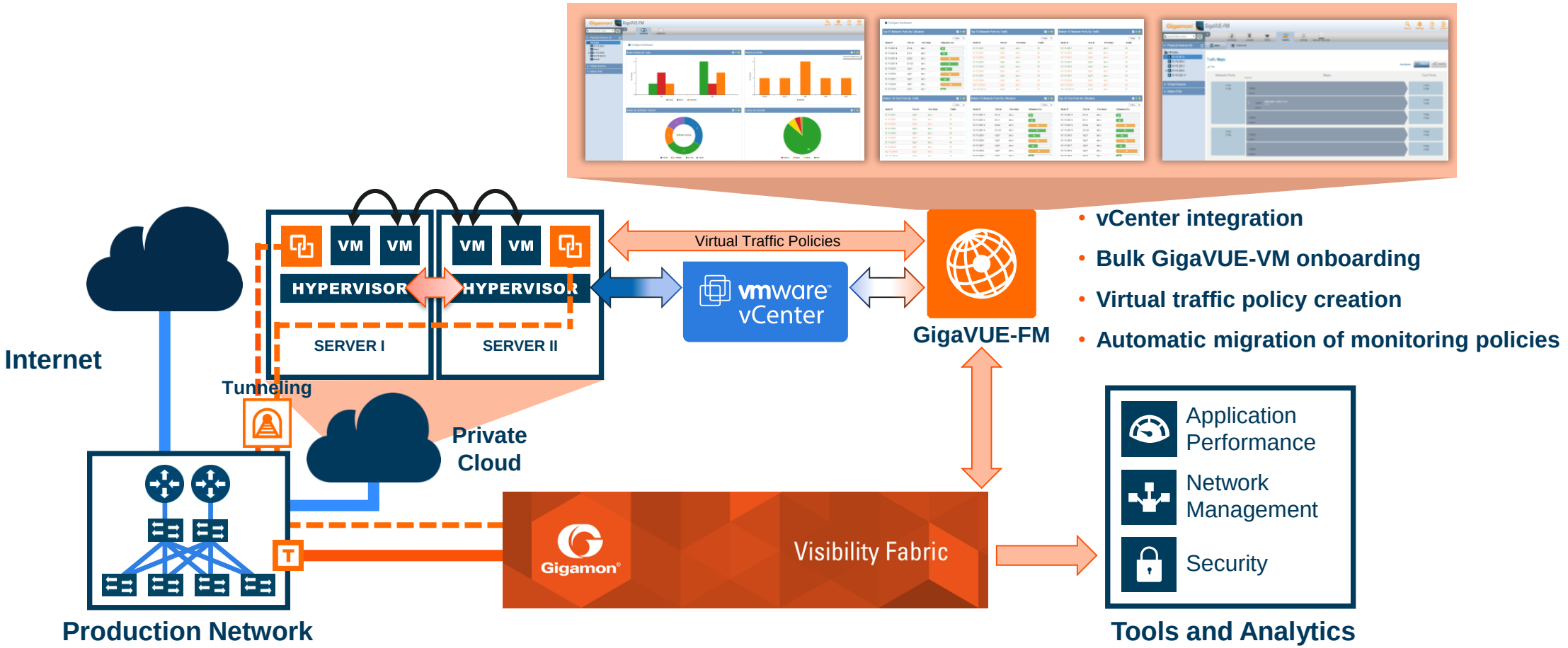
- **가상화 TAP(Virtual Tap)**용 GigaVUE-VM을 통하여 **호스트 간의 트래픽 분석이 가능**합니다.
- 가상화 내 트래픽을 **Flow Mapping** 방식으로 분류 및 터널링을 통해 분석 장비로 전달하여 **기존 보안 장비**에서 **분석이 가능**합니다.



2. 핵심 기술

2.4 클라우드

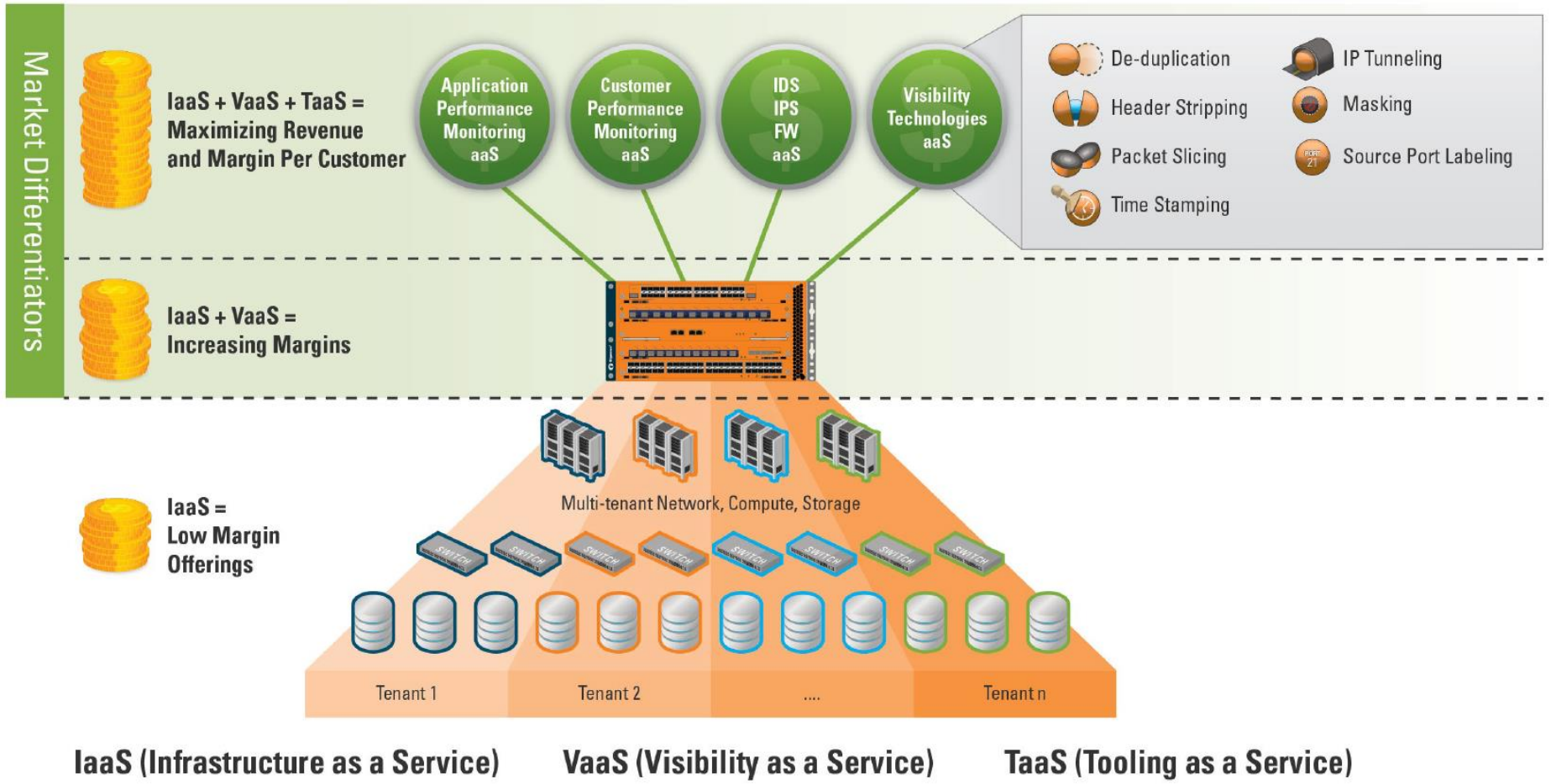
- 프라이빗 클라우드 환경 하에서의 네트워크 가시성 환경 구축 방안



2. 핵심 기술

2.4 클라우드

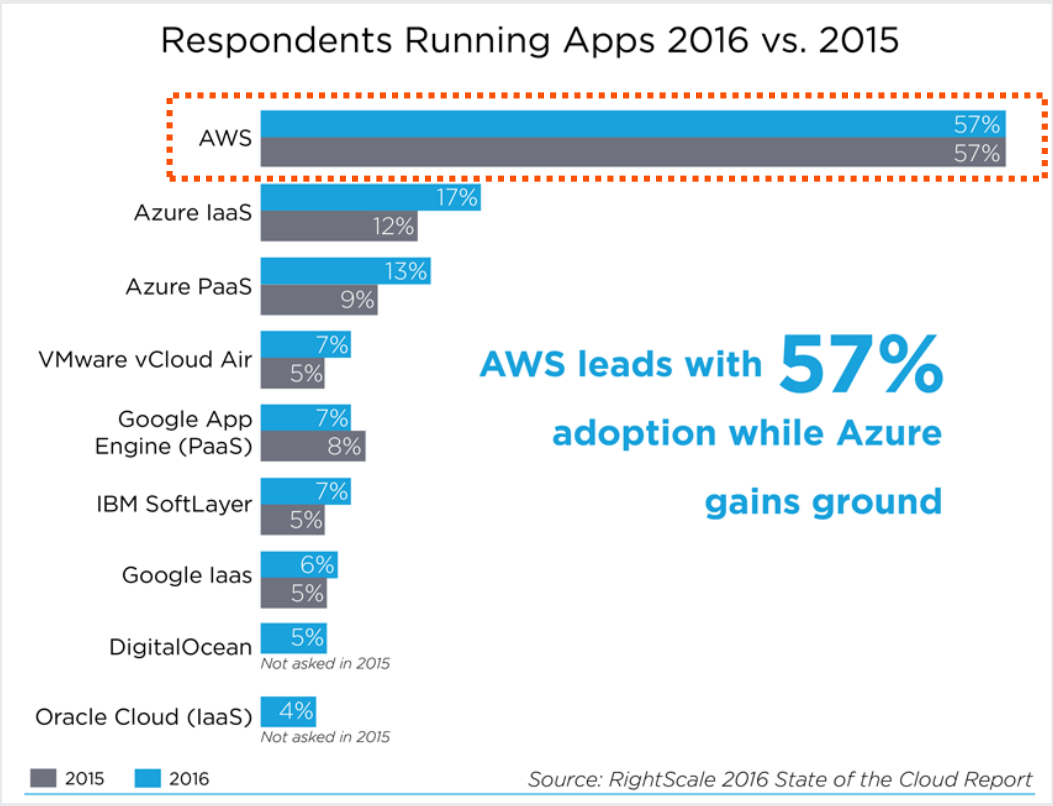
- 데이터 센터의 차별화된 서비스 제공



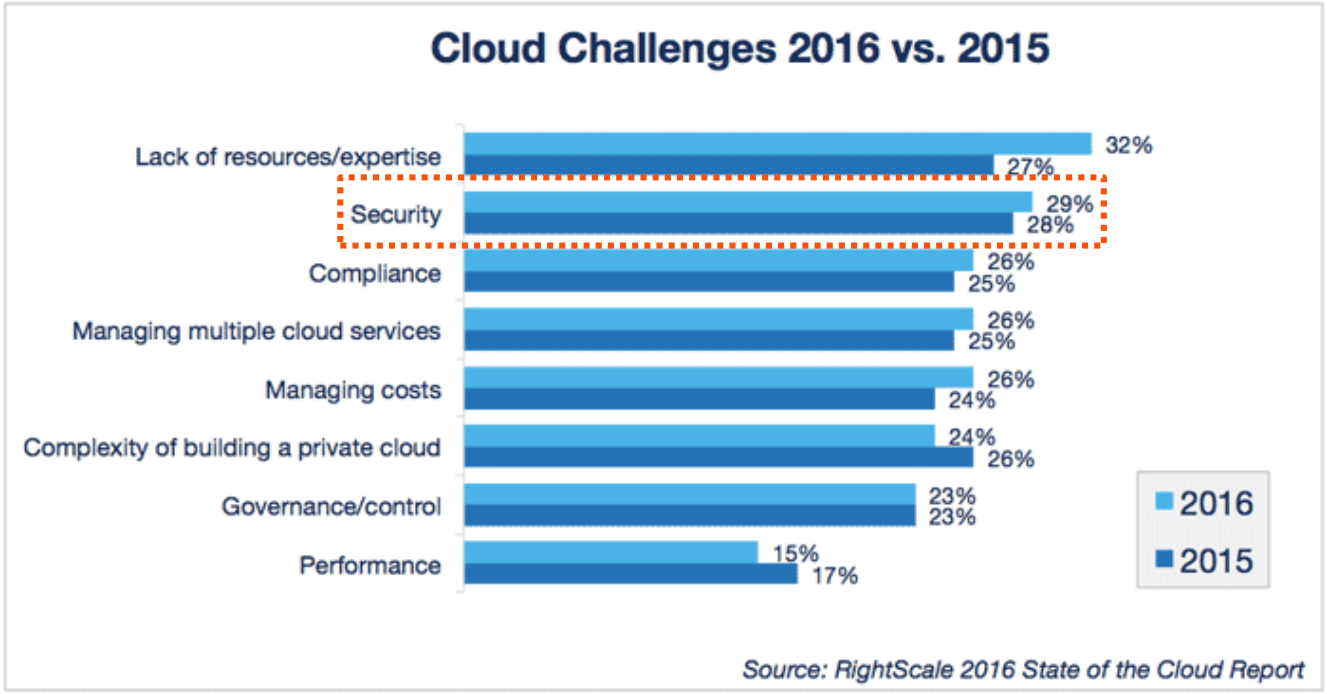
2. 핵심 기술

2.4 클라우드

퍼블릭 클라우드 - AWS



[클라우드 시장 점유율]



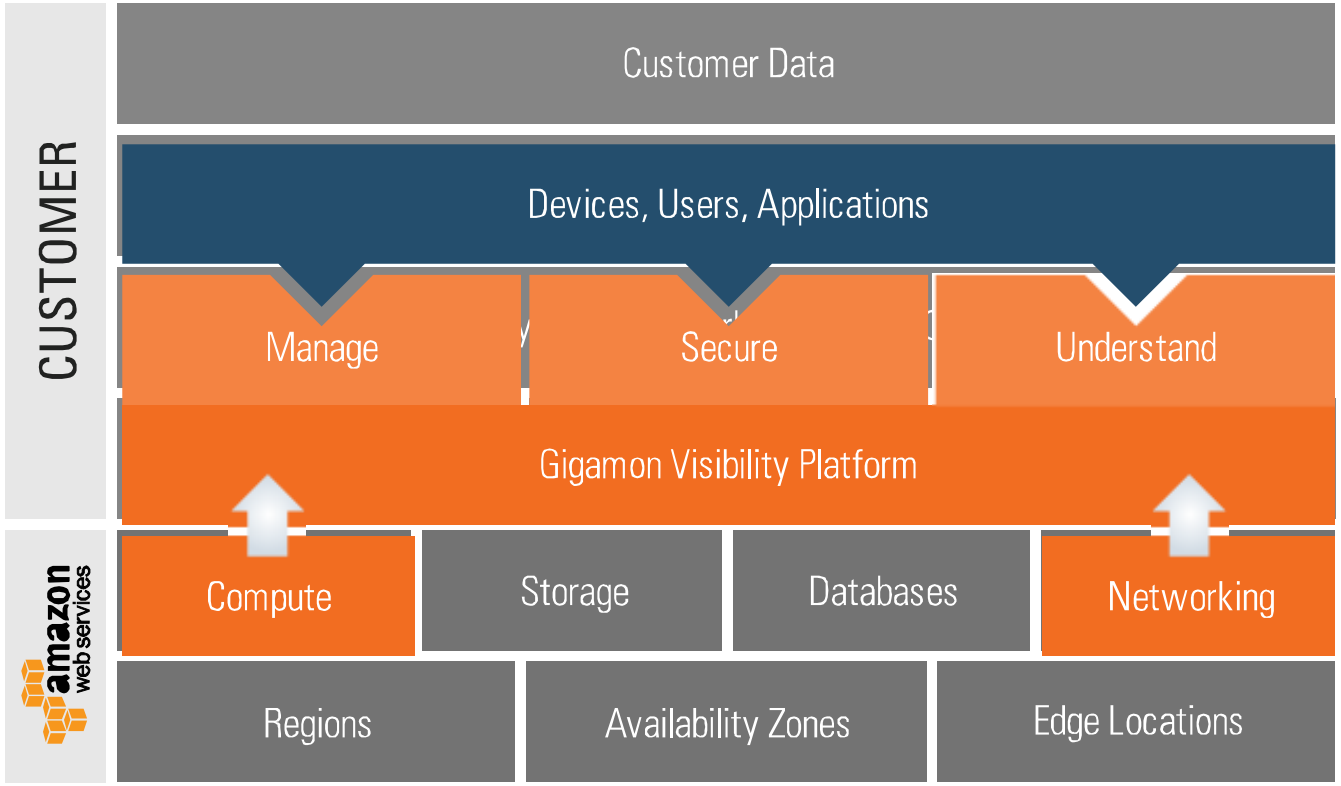
[클라우드 도입 시 고려사항]

2. 핵심 기술

2.4 클라우드

퍼블릭 클라우드 - AWS

✓ AWS에서는 물리적인 환경 외의 **운영 상의 보안**은 고객이 **직접 책임**을 지는 **"Shared Responsibility Model"**로 운영이 되므로 AWS내 EC2 간 트래픽에 대한 **트래픽 모니터링은 필수**입니다.



Manage: See What Matters

- 실제 트래픽을 모니터링 장비로 전달
- 유연한 구축 방식

Secure: See More, Secure More

- 위협에 대한 가시성 확보 및 규정 준수
- 보안/모니터링 장비의 효율성 증대
- 신속한 이슈 확인 및 트러블슈팅

Understand: Gain full transparency

- VPC 내의 트래픽에 대한 완전한 파악(EC2간 트래픽 포함)
- 신속한 이슈 확인 및 트러블슈팅

2. 핵심 기술

2.4 클라우드

- 퍼블릭 클라우드 - AWS

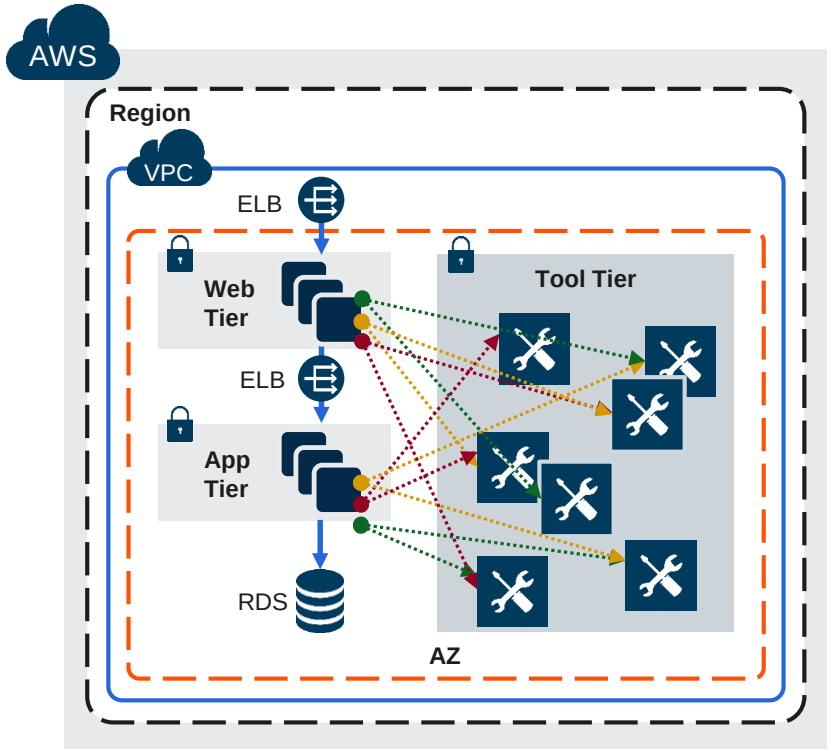
전세계 최초로
퍼블릭/프라이빗 및
하이브리드 환경에서
네트워크 보안 가시성을 제공!

지금 바로 AWS 모든 리전에서 활성화 가능!

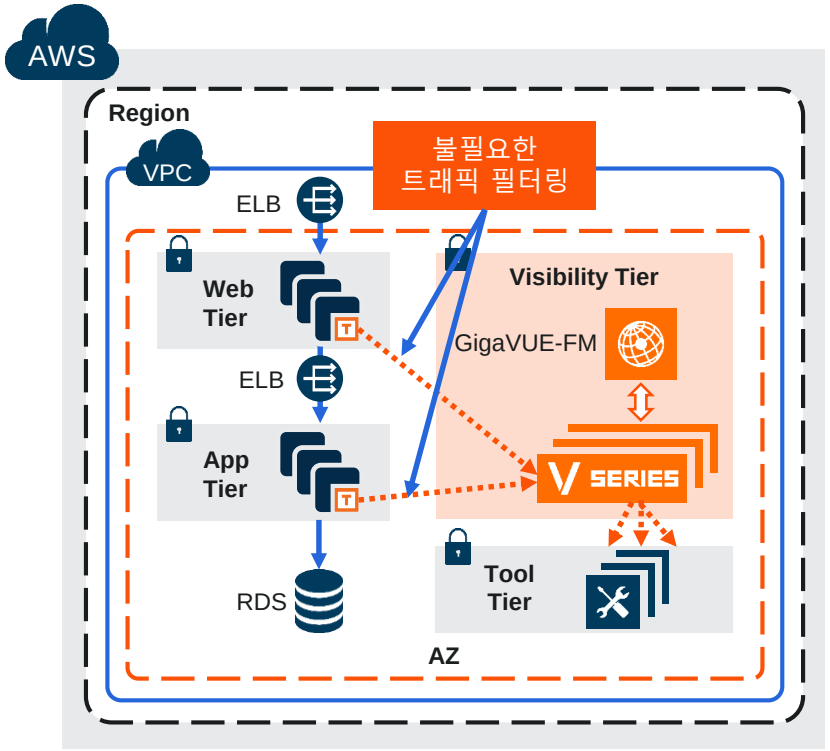
2. 핵심 기술

2.4 클라우드

퍼블릭 클라우드 - AWS



Gigamon Visibility Platform



- 전구간 실 트래픽 모니터링의 어려움
- EC2에 다중 에이전트 설치로 인한 EC2 부하 증가
- 복잡해지는 VPC내 보안 모니터링 인프라

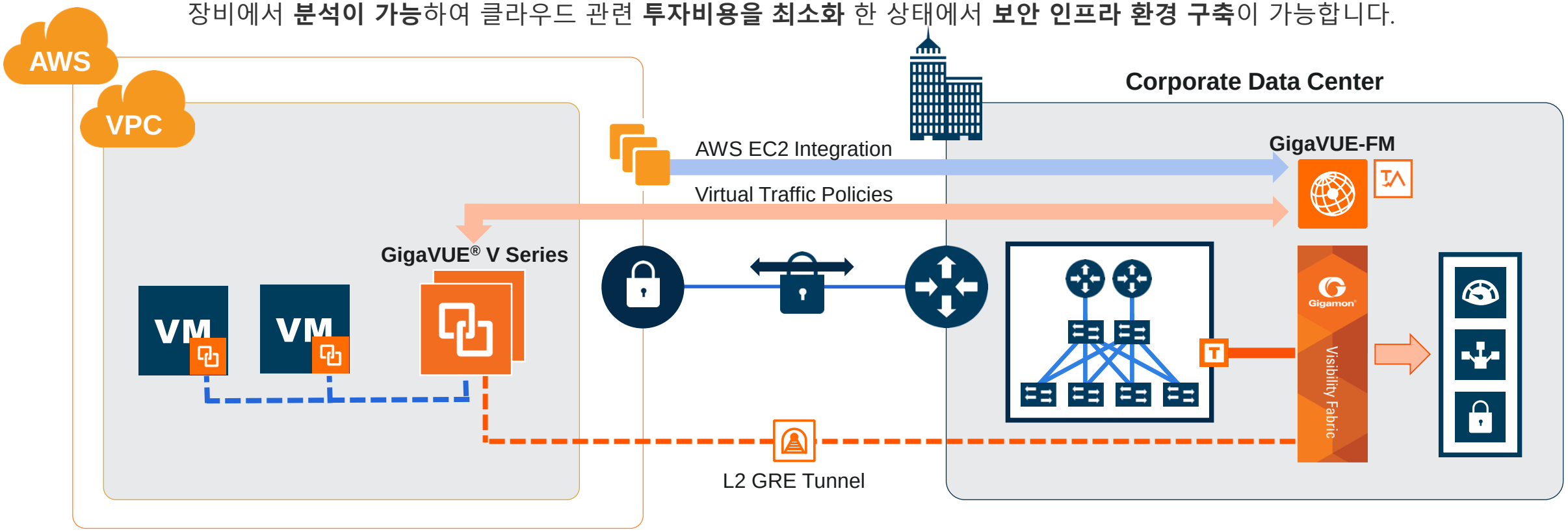
- 모니터링 인프라 구성의 단순화
- EC2에 단일 트래픽 수집 에이전트 설치를 통한 부하 경감
- 각 보안 장비에 최적화된 트래픽 전송을 통한 보안 장비 운영 효율 극대화

2. 핵심 기술

2.4 클라우드

퍼블릭 클라우드 - AWS

✓ AWS VPC 내의 **EC2에 유입되는 트래픽**을 데이터센터 내의 **기가몬 장비로 수집**하여 **기존 운영** 중인 보안 장비/모니터링 장비에서 **분석이 가능**하여 클라우드 관련 **투자비용을 최소화** 한 상태에서 **보안 인프라 환경 구축**이 가능합니다.



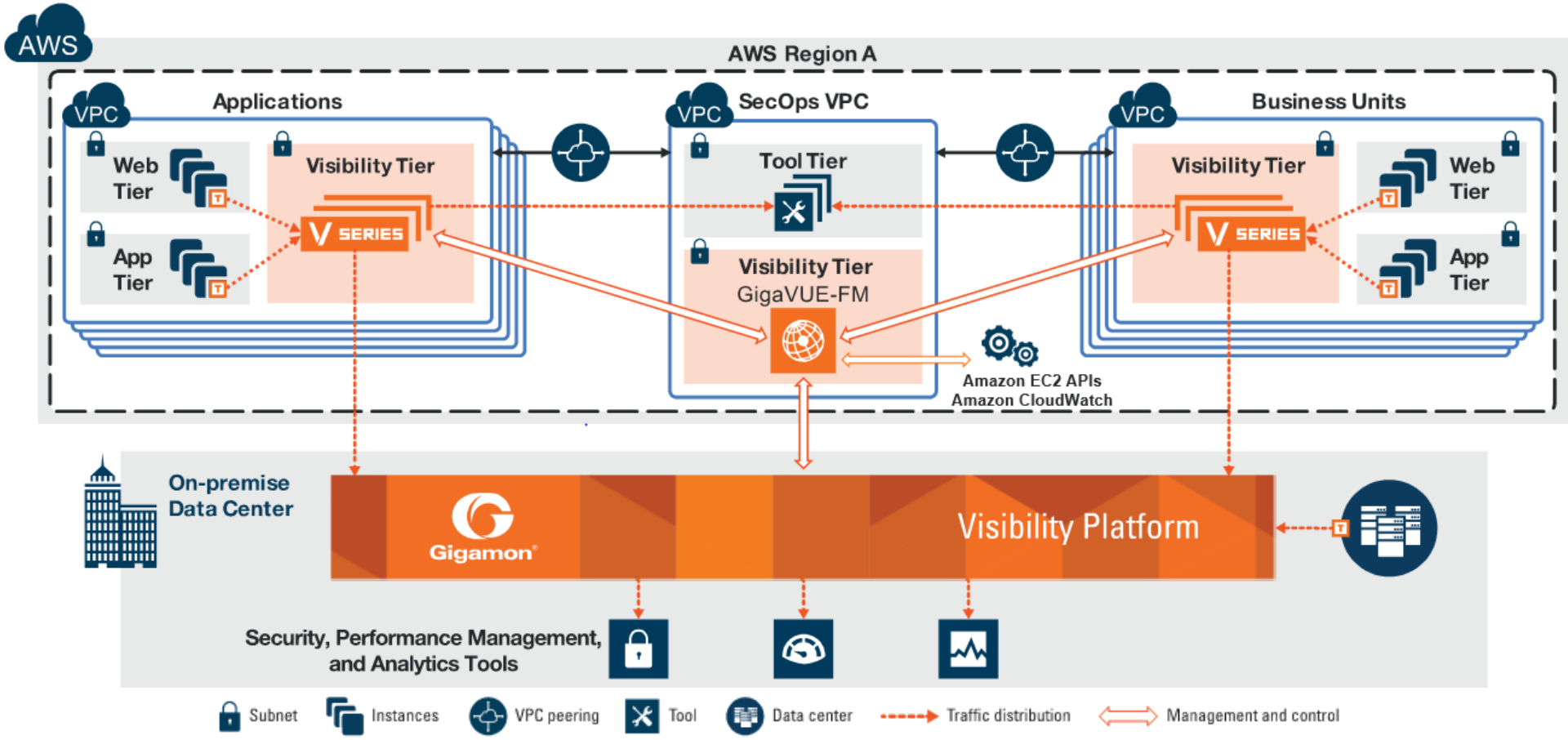
AWS VPC내의 EC2 트래픽을 자사 데이터센터의 보안 및 분석 장비로 전송

2. 핵심 기술

2.4 클라우드

퍼블릭 클라우드 - AWS

✓ AWS **리전 내**에 별도 보안 관련 VPC(SecOps VPC)로 **트래픽 수집** 또는 **물리적인 데이터센터**로 **트래픽 수집**을 통한 모니터링을 지원합니다.



Gigamon®

3. 플랫폼 이점 및 적용 사례

3.1 보안 관리 전달 플랫폼의 이점

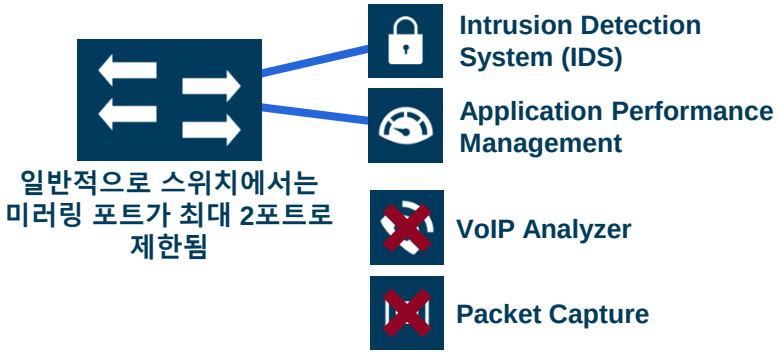
3.2 적용 사례

3. 플랫폼 이점 및 적용 사례

3.1 보안 관리 전달 플랫폼의 이점

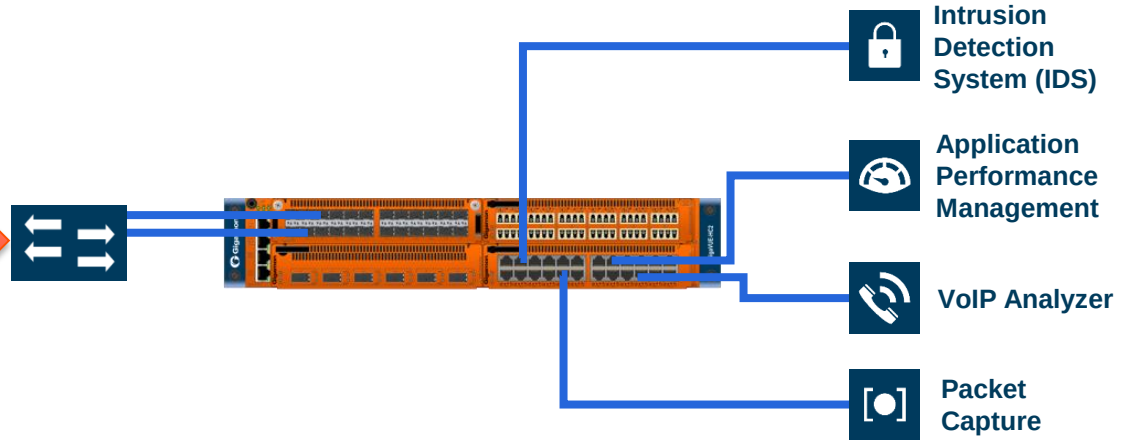
› 미러링 포트 부족으로 인한 보안장비 및 모니터링 장비 구성문제에 대한 근원적 해결이 가능합니다.

• 도입 전



• 네트워크 장비 내 미러링 (SPAN) 포트의 부족으로 인한 보안 장비 구성의 한계성 직면!

• 기가몬 도입 후



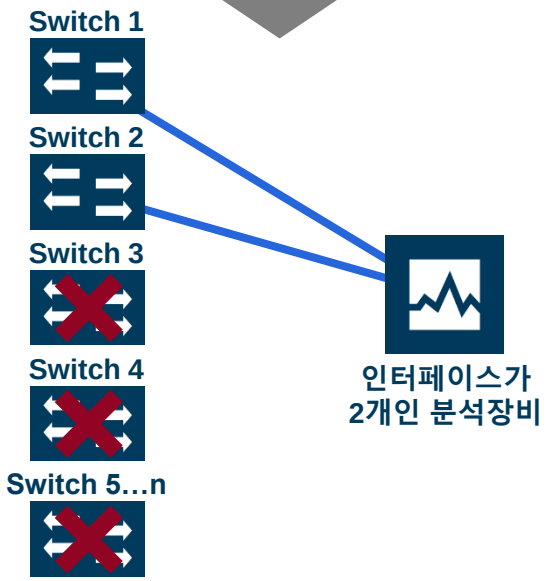
기가몬 - 보안 및 관리 전달 플랫폼 활용을 통한 확장성 및 편의성 확보

3. 플랫폼 이점 및 적용 사례

3.1 보안 관리 전달 플랫폼의 이점

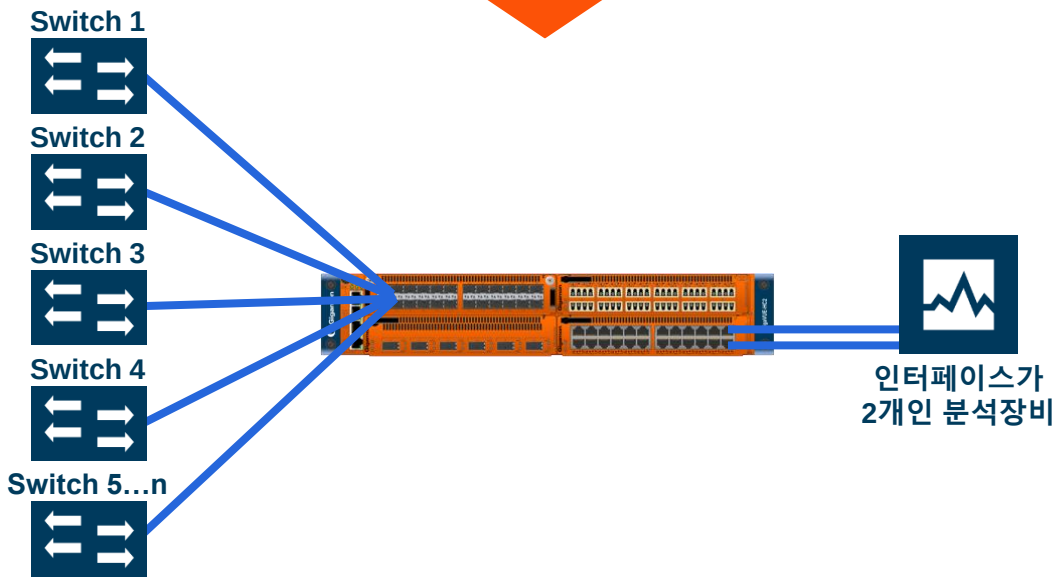
- 다수의 모니터링 구간 통합 및 트래픽 필터링

• 도입 전



- 보안 및 분석 장비의 인터페이스 제약으로 제한적 구간의 트래픽 모니터링

• 기가몬 도입 후



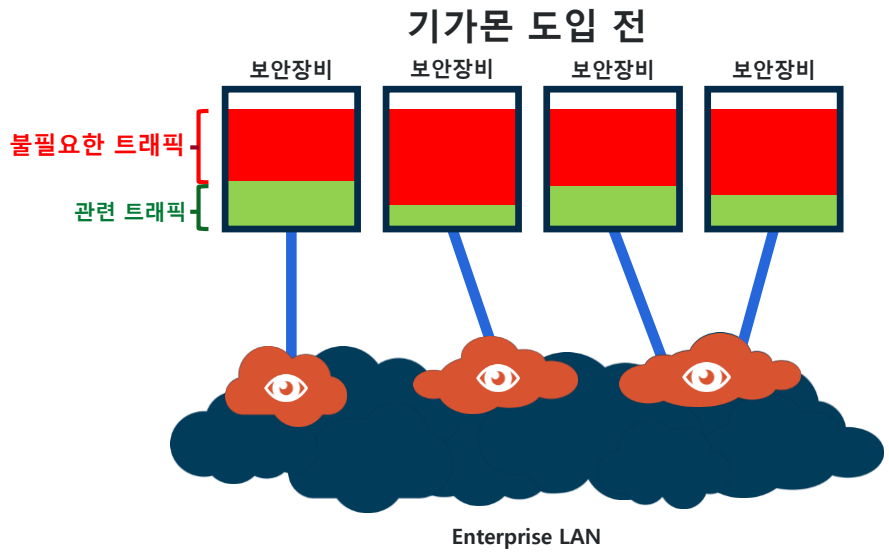
경제성 및 전 구간 가시성 확보

3. 플랫폼 이점 및 적용 사례

3.1 보안 관리 전달 플랫폼의 이점

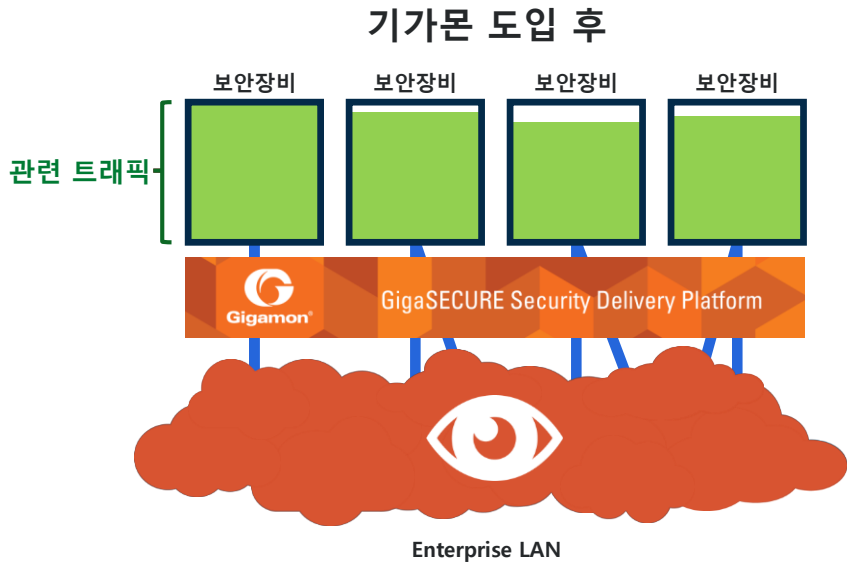
- 보안장비 운영 효율성 극대화

• 도입 전



- 불필요 트래픽 처리를 위해 보안장비 리소스 (CPU, 메모리 등) 사용으로 장비 효율 저하 발생

• 기가몬 도입 후



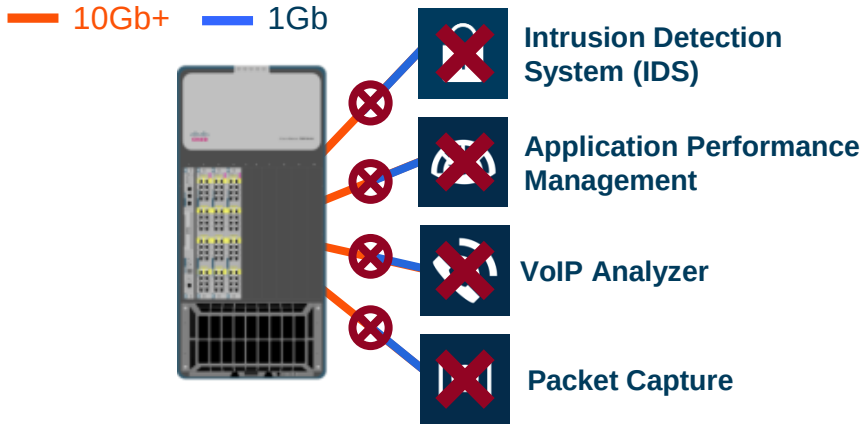
트래픽 필터링을 통한 효율적인 분석으로
동일 장비로 모니터링 구간 확대

3. 플랫폼 이점 및 적용 사례

3.1 보안 관리 전달 플랫폼의 이점

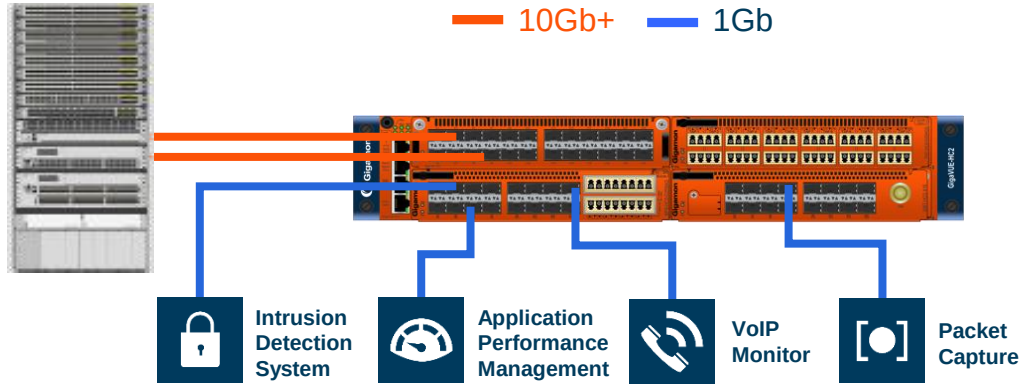
네트워크 고도화 시 장비의 투자 보호

- 도입 전



- 네트워크 업그레이드에 따라 기존 보안 및 분석 솔루션 업그레이드 필요

- 기가몬 도입 후



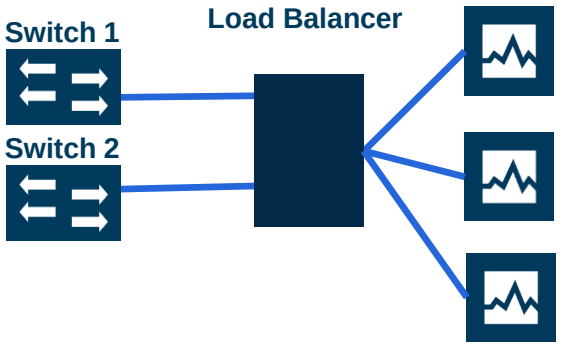
네트워크 속도 증가에 따른 보안 및 분석 솔루션의 수명을 연장하며 추가 도입 시점 조정

3. 플랫폼 이점 및 적용 사례

3.1 보안 관리 전달 플랫폼의 이점

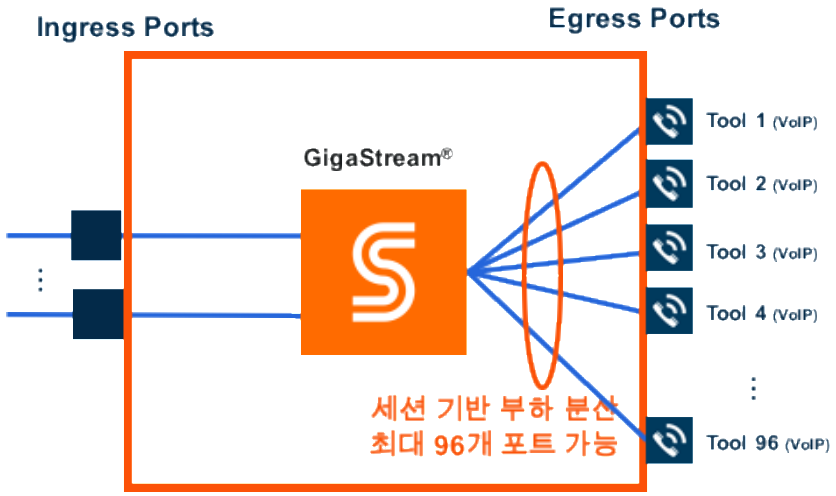
- 대용량 부하 분산 기능(최대 96대)으로 향후 투자 보호

• 도입 전



- 별도 부하분산 장비를 이용하여 제한적인 부하 분산 제공 (8개 미만)

• 기가몬 도입 후



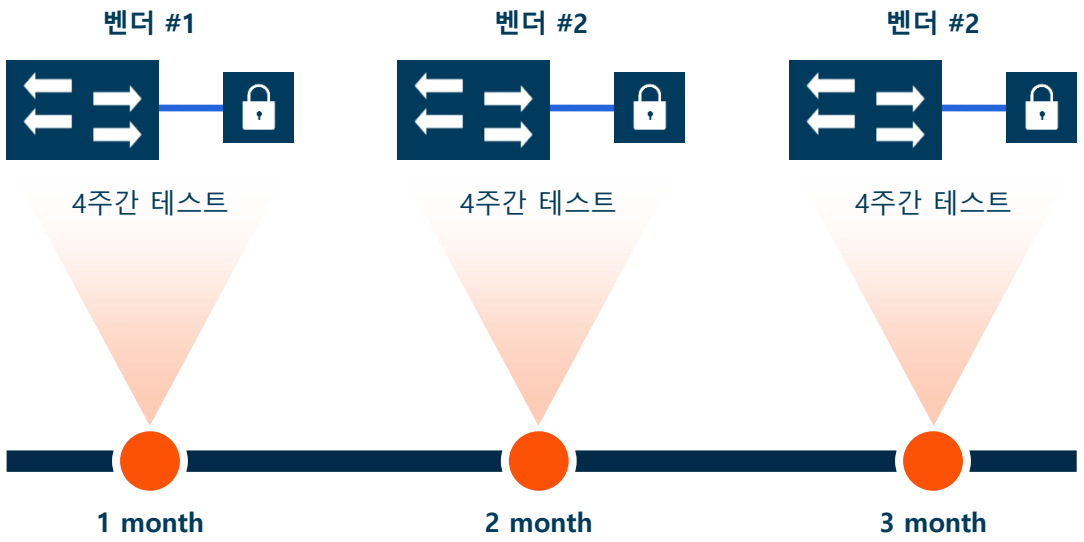
최대 96개 포트로 L2/L3/L4 세션 기반으로 부하 분산(로드 벨런싱) 제공 – Advanced Hashing

3. 플랫폼 이점 및 적용 사례

3.1 보안 관리 전달 플랫폼의 이점

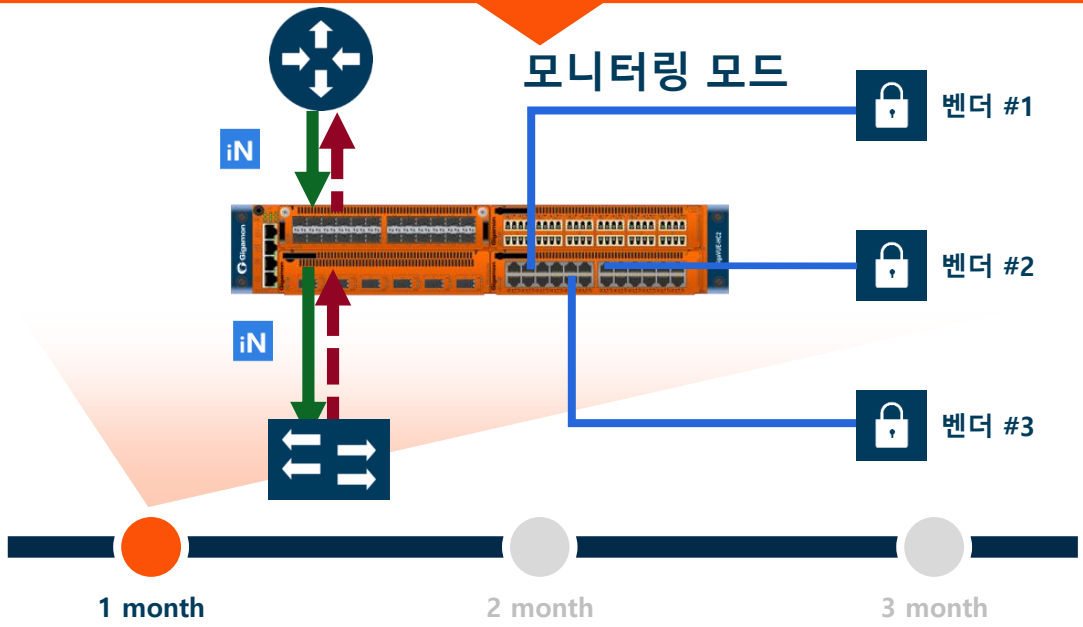
- 실망 조건에서 서비스 영향없이 동일 테스트 가능으로 솔루션 비교 분석 제공

• 도입 전



- 다른 시간대, 다른 트래픽을 대상으로 PoC 실시로 테스트 장비 비교 분석 어려움

• 기가몬 도입 후



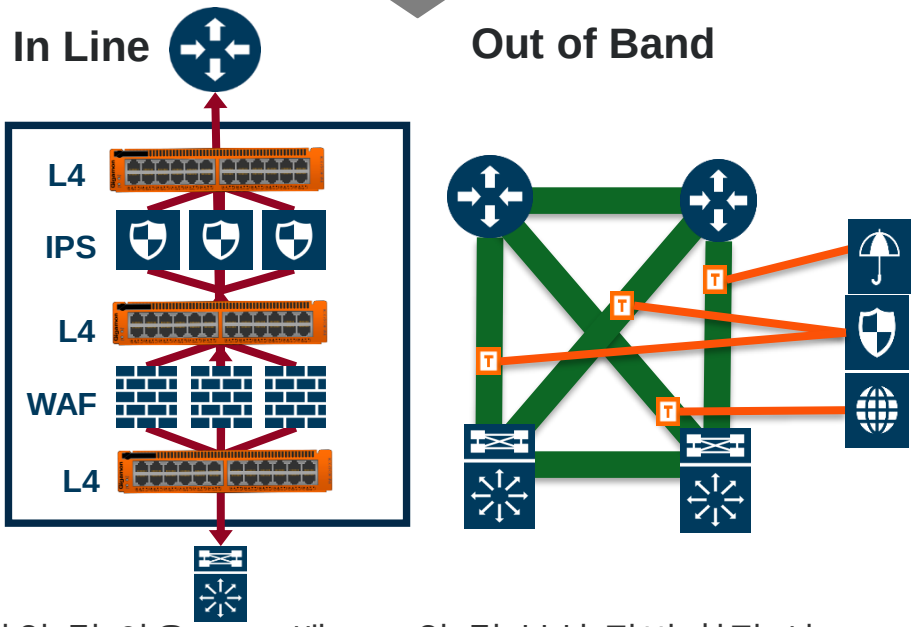
실 네트워크 영향 없이 동일 조건 PoC 수행
모니터링 모드로 장비도입 시 안정화기간 확보 가능

3. 플랫폼 이점 및 적용 사례

3.1 보안 관리 전달 플랫폼의 이점

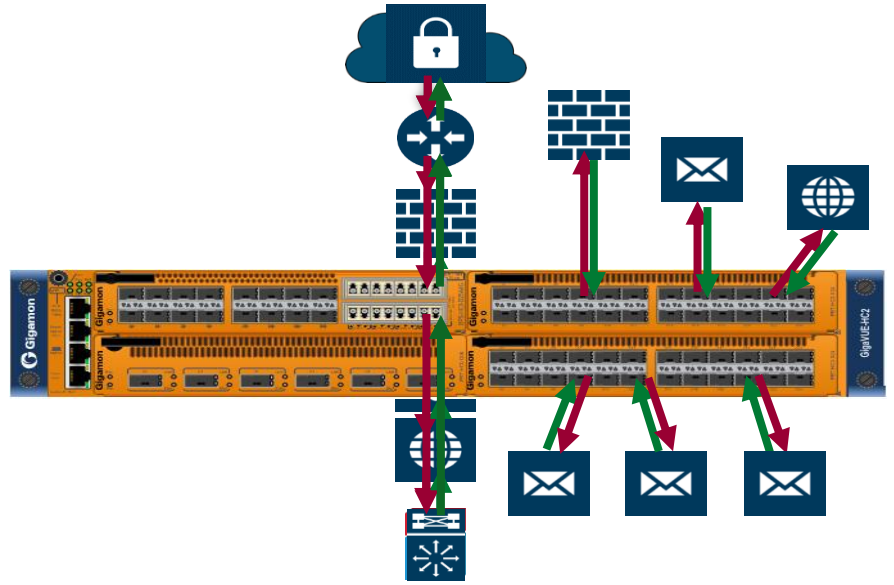
- 망 안정성 및 통합 관리를 통한 편의성 확보

• 도입 전



- 인라인 및 아웃 오브 밴드 보안 및 분석 장비 확장 시,
- 관리 포인트 지속 증가에 따른 네트워크 장애 가능성 증대
- 인라인 및 아웃오브밴드 장비구성 혼재로 관리 효율성 약화

• 기가몬 도입 후

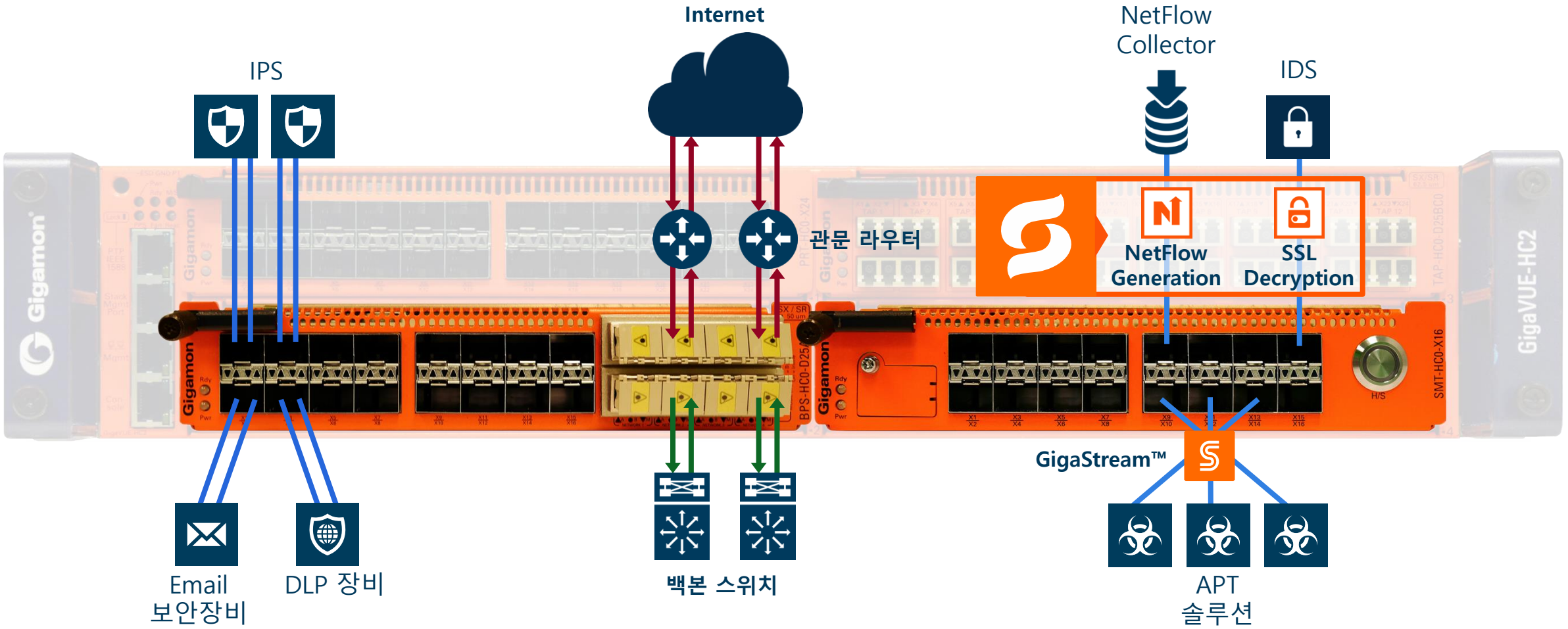


- 보안플랫폼을 통한 인라인, 아웃오브 밴드 통합 구성 관리
- 보안 장비 장애 시 Bypass 및 Heartbeat Check 기능을 통한 망 생존성 확보 가능

3. 플랫폼 이점 및 적용 사례

3.2 적용 사례 - 통합 보안 관리 전달 플랫폼

- 인라인 및 미러링 보안 장비 통합



3. 플랫폼 이점 및 적용 사례

3.2 적용 사례 – 대형 상거래 사이트

100G 트래픽 로드밸런싱

GigaVUE-HD8

GigaVUE-HD4

요구사항

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

솔루션

- 기가몬 적용 솔루션 : GigaVUE-HD4 & HD8
- 분석 장비는 A사 보안 팀에서 자체 제작

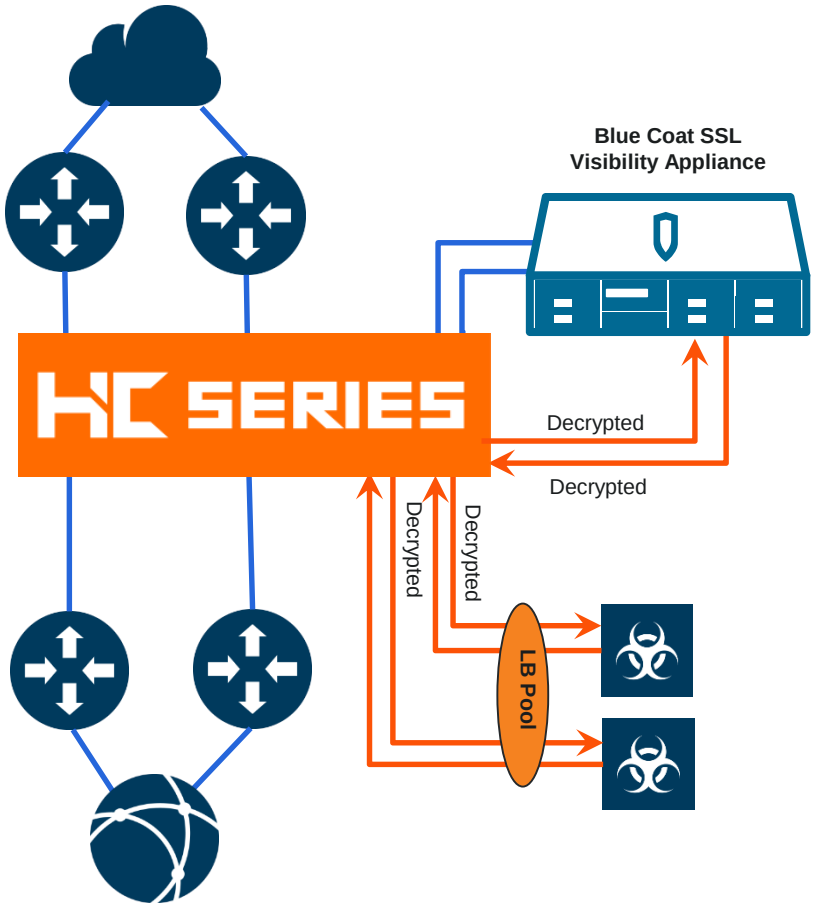
도입 후 효과

- Flow Mapping 기술로 100G 트래픽의 로드 밸런싱
- GigaSMART의 Application Session Filtering 적용으로 분석 플로우의 L7 filtering
- 100G 링크의 분석 방법 제공으로 기존 10G 솔루션 활용 및 CAPEX 절감 효과

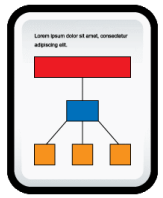
3. 플랫폼 이점 및 적용 사례

3.2 적용 사례 – 블루코트

- 인라인 장비 연동



- SSL 가시성 솔루션 **장애 발생** 시에도 **서비스 연속성 제공**
- **단일** SSL 가시성 장비로 **다중 구간**에 대한 모니터링 기능 제공



Deployment Document

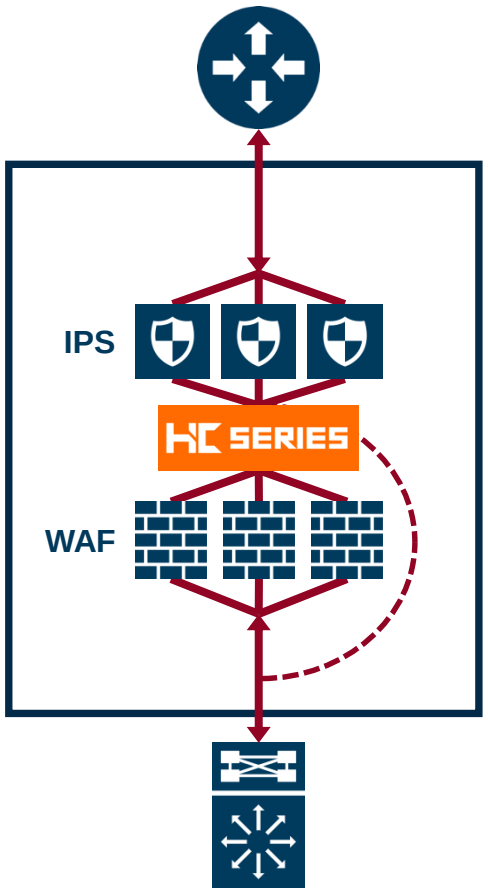
Solution Brief Available

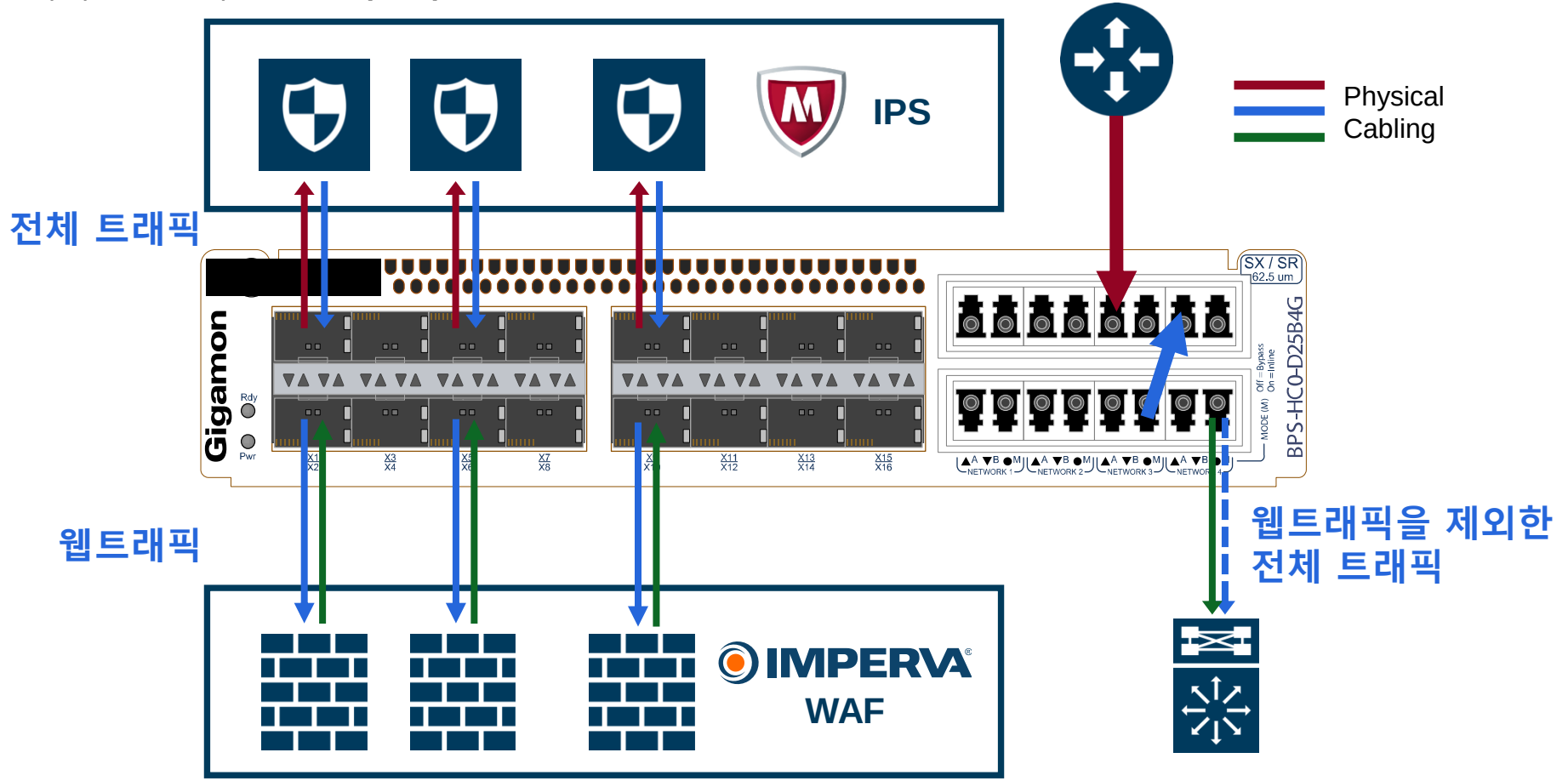
3. 플랫폼 이점 및 적용 사례

3.2 적용 사례 – 임퍼바 Web Application Firewall

인라인 장비 연동

- ✓ **인라인 장비 부하분산**을 통해 보안장비 성능 이슈 발생 시 교체가 아닌 **장비 추가**로 **CAPEX(투자비용) 최소화**
- ✓ 웹트래픽만 WAF로 전달하여 보안장비 **효율성 극대화**





4. 도입 시 기대효과

4. 도입 시 기대효과

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

Thank You!

Contact Information

㈜파인앤애플시스템즈 신동호 부장
Phone : 070-7010-5902
Mobile : 010-6855-9776
E-Mail : dhshin@pineandapple.com