See More Secure More

가시성 강화를 위한 보안 전달 플랫폼 (Security Delivery Platform)

Brian Rho

Regional Sales Director, Gigamon Korea

GIGABIT MONITORING

1Gigabit X 10 = 10Gigabit X 10 = 100Gigabit X 10 = 1 Terabit X 1000 = 1 Peta

보는 수준이 다르니 보안 수준이 다르다 !!!

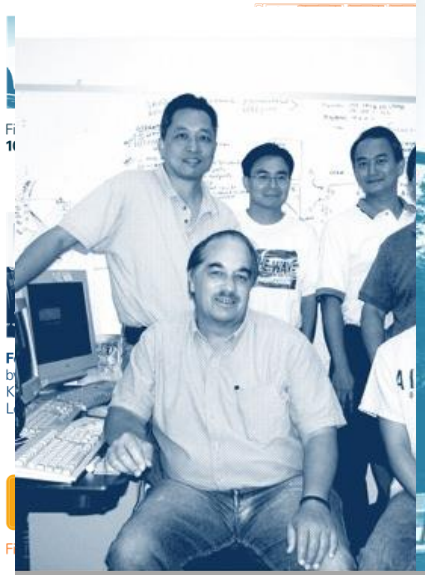
(매일경제, 2016년 8월12일, Paul Hooper)

실리콘 밸리의 많은 스타트 업들 자기들 만들어 놓은 솔루션 갖고, 억지로 문제에 끼워 맞추다 보니 실제로 고객의 욕구에 못 미쳐, 혁신 중요하지만 현장 문제와 따로 놀면 최첨단 기술도 “빛 못봐“..

목차

회사소개

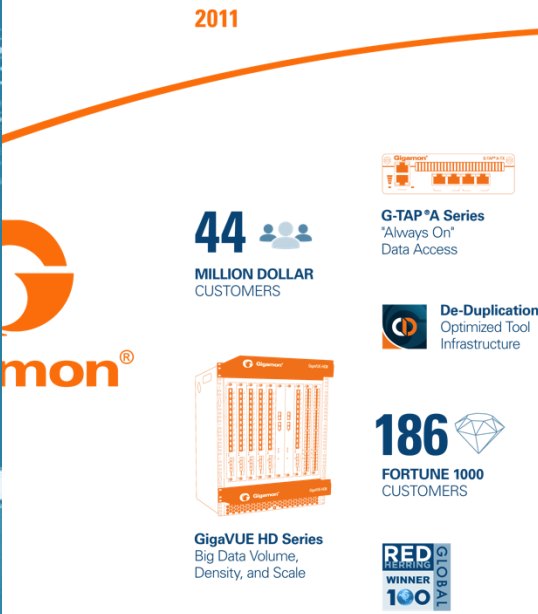
- 설립연도 : 2004년 (Pioneered Market)
- 기업공개 : 2013년 6월 (NYSE, GIMO)
- 본사위치 : 미국, 캘리포니아 Santa Clara
- 주요사업 : 보안 및 관리툴을 위한 가시성 시장의 1위 벤더 (약40%)*
- 사업분야 : 모바일(Mobile), 데이타센타 (Datacenter), 클라우드 (Cloud)
- 보유기술 : 35 개 핵심 특허권, 27개 특허권 출원 중**
- 주요고객 : 2200개+ 고객(포춘 100대 기업 중 79개+, 전세계 글로벌 100대 통신사 중 50개+)



2004년 창립기념 촬영사진

2004 2005

2015년 캘리포니아 본사 전경



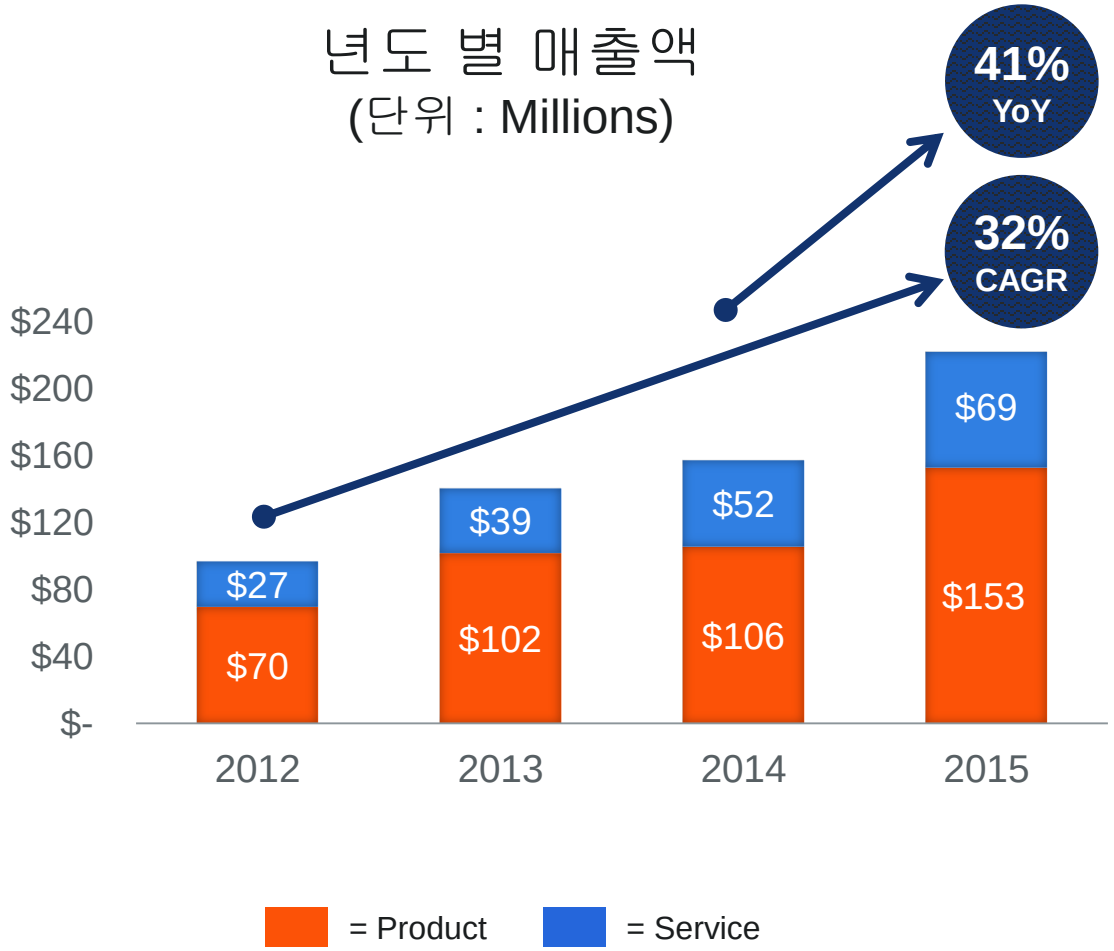
*Gartner, **Customer and patent numbers FY16Q2.

주요 하이라이트

- 미국 기술기업 내 가장 빠르게 성장하는 기업 5위.

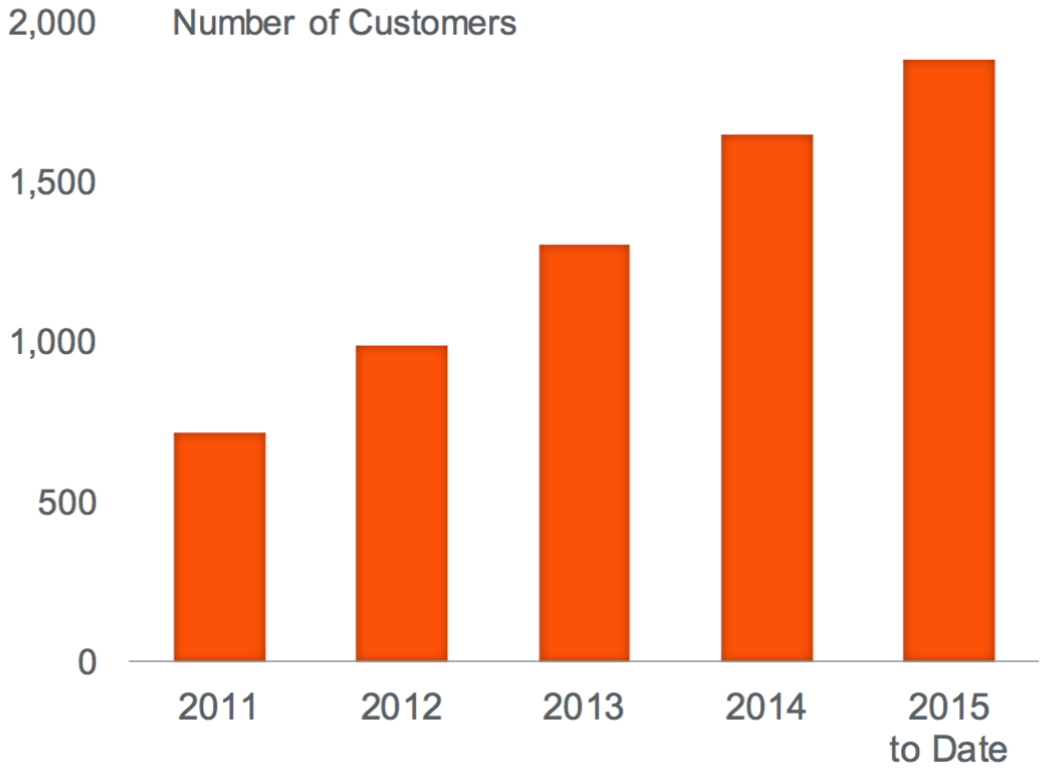
Fast Future Growth

Symbol	Company name	EPS estimate current yr % chg	Next yr % chg	Composite Rating	EPS Rating
PAYC	Paycom Software	93%	25%	99	99
FB	Facebook	73	29	99	99
SIMO	Silicon Motion Tech	56	17	99	93
HQY	HealthEquity	50	29	99	98
GIMO	Gigamon	45	21	99	95
NTES	NetEase	42	17	99	99
ESNT	Essent Group Ltd	33	18	97	99
AVGO	Broadcom Limited	25	19	99	95
GRUB	GrubHub	24	31	98	95

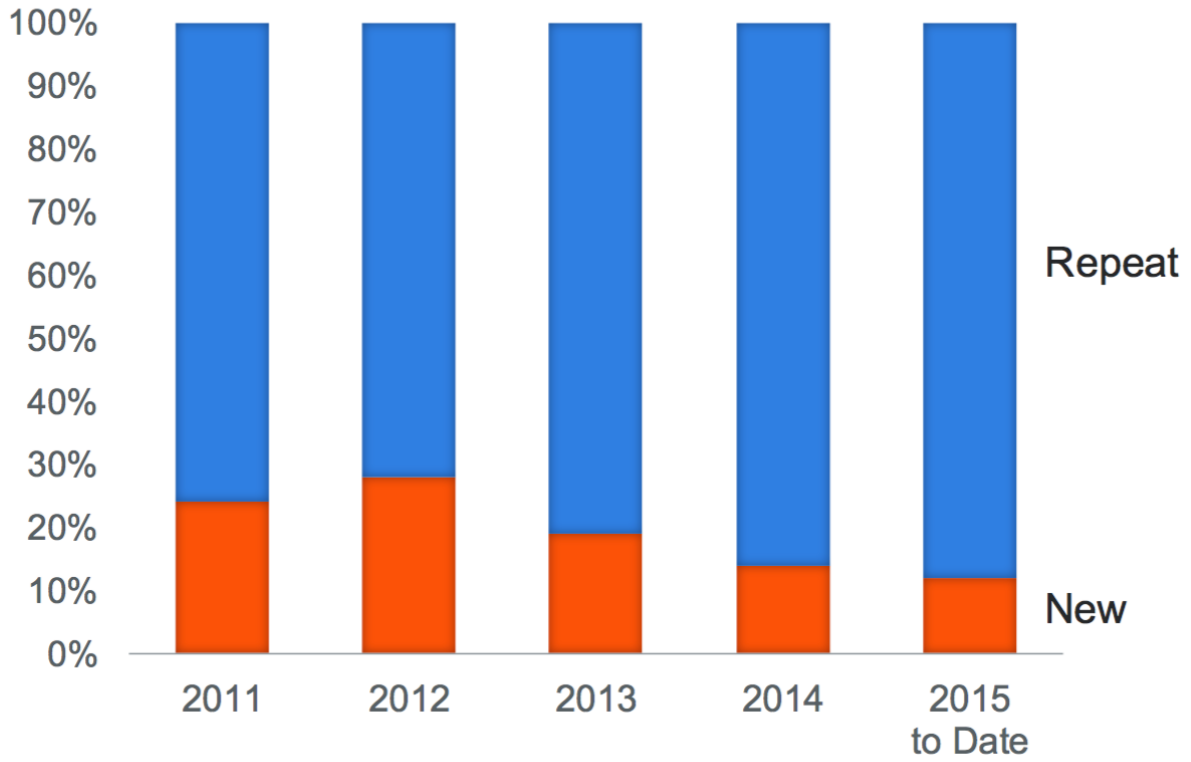


높은 고객 증가율 (고객만족도)

SEED



GROW



Percent of purchase order value from new customers acquired in the quarter vs. existing customers.

주요 국내외 고객 사

엔터프라이즈

TECHNOLOGY

monster, LINE, ebay, EMC², intel, REUTERS, Disney Online, LinkedIn, Apache, salesforce.com, Tech Data, Expedia.com

INDUSTRIAL

3M, MARATHON, NEC, BAKER HUGHES, Constellation Energy, SAMSUNG, Chevron, BNSF RAILWAY, aeso, LOCKHEED MARTIN, Genentech, HONDA, Schering-Plough

RETAIL

Sara Lee, ConAgra Foods, WAL★MART, LOTTE, Enterprise, BEST BUY, JCPenney, COSTCO WHOLESALE, General Mills

FINANCE

MasterCard, NYSE, DISCOVER, BARCLAYS, Mellon, NASDAQ, Fidelity, Bank of America, Standard Chartered, Deutsche Bank, Merrill Lynch, TD AMERITRADE, NYMEX, RBC Royal Bank, Capital One, STATE STREET

HEALTHCARE & INSURANCE

CardinalHealth, LEHIGH VALLEY HOSPITAL, CEDARS-SINAI, STANFORD HOSPITAL & CLINICS, National Institutes of Health, BJC HealthCare, APL, Medtronic

GOVERNMENT

SAIC, DARPA, SUPREME COURT, NASA, New York City Transit, VITA, U.S. DEPARTMENT OF TREASURY

2200+ 글로벌 고객

Fortune-100 내 79개 +

서비스 사업자

verizon, at&t, Sprint, U.S. Cellular, comcast, NTT Communications, vodacom, vodafone, BT, TIME WARNER CABLE, Telstra, Level (3), KDDI, BCE, COX COMMUNICATIONS, kt

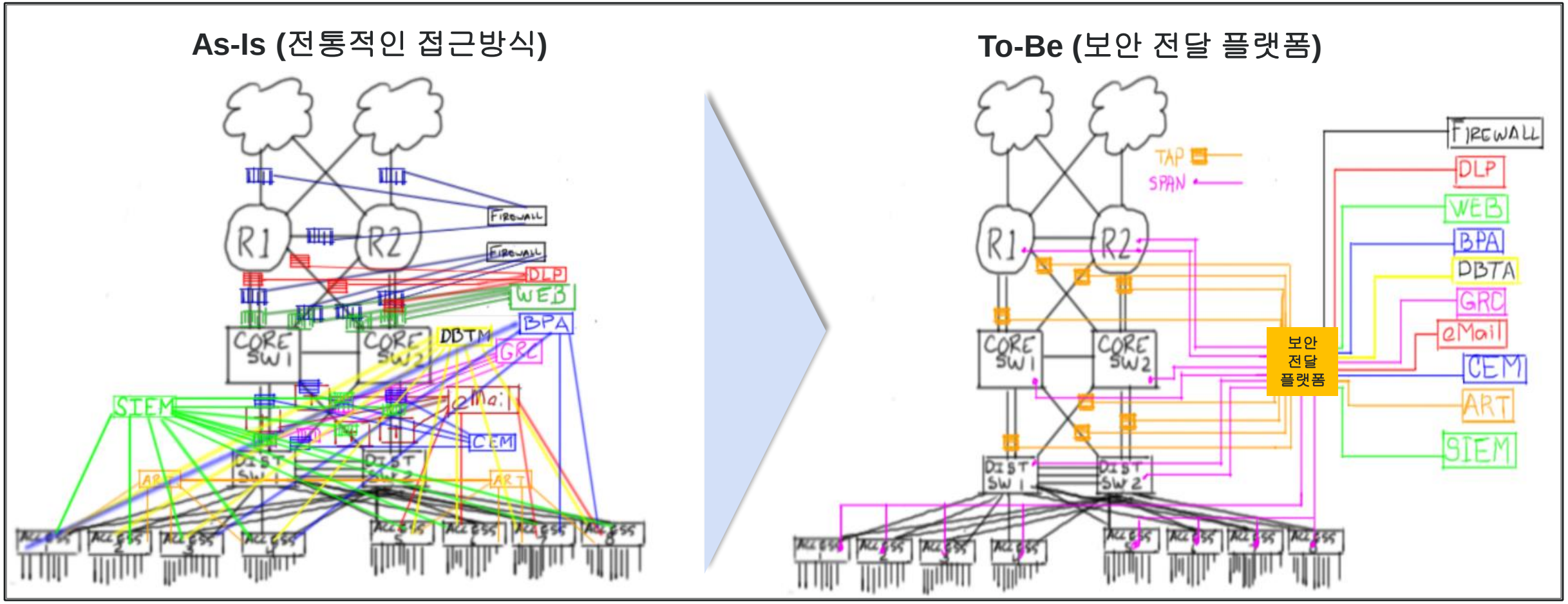
글로벌 TOP 100 SP 내 50개+

주요 에코 파트너사

*국산 보안 툴 밴더들과 호환성 보장 (윈스테크, 이글루 시큐리티, 시큐아이닷컴 등)

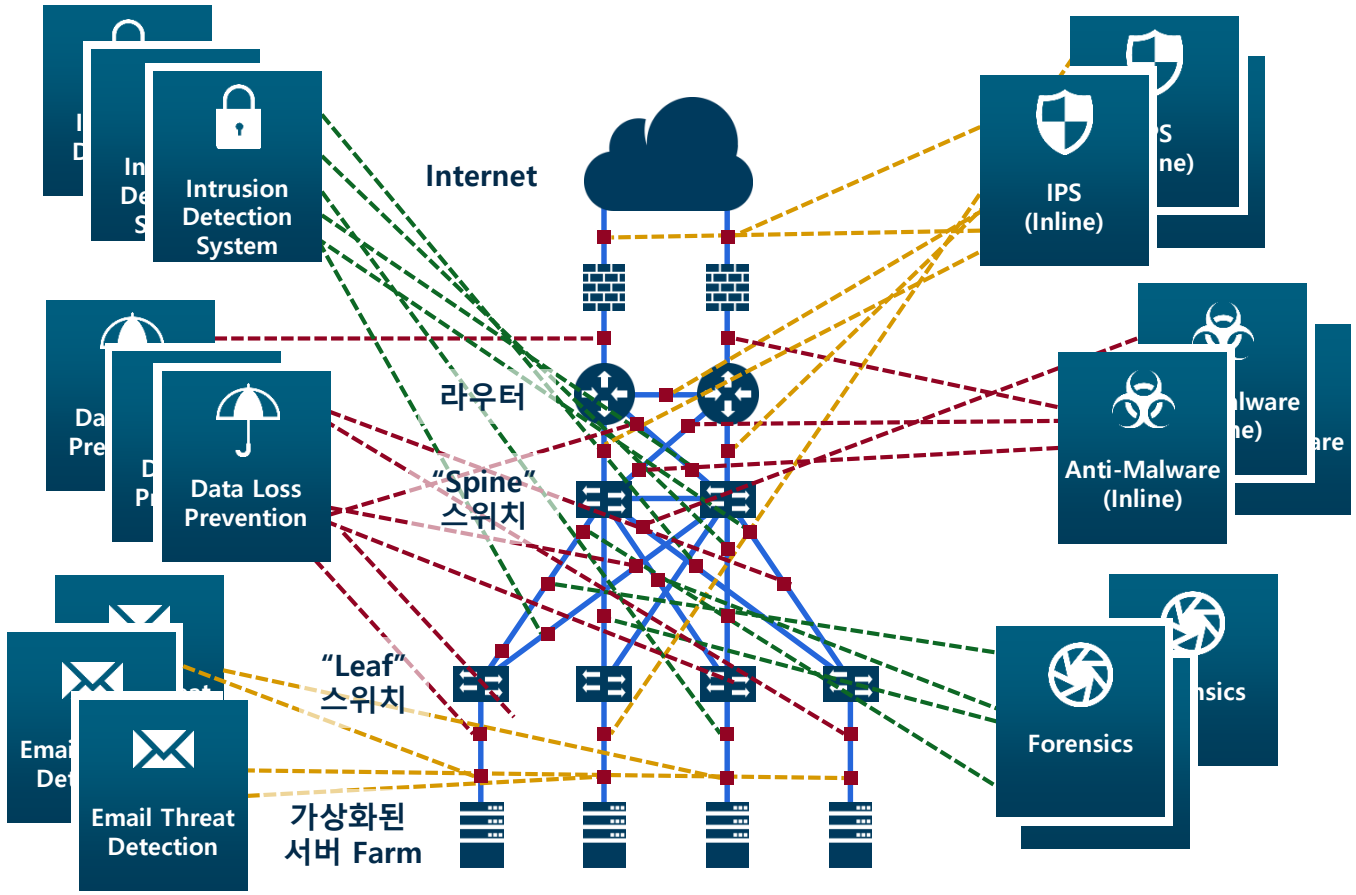
보안전달 플랫폼 구현

단순화, 통합구성 및 관리 및 운영 효율, TCO 절감의 극대화



전통적 접근 방식 (제한적 가시성)

모니터링 인프라의 복잡성 : 너무 많은 모니터링 패스와 방어 포인트



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 보안 및 관리 툴 구성 시 중복된 투자에따른 CAPEX/OPEX 증가

보안 구성에 영향을 미치는 요인

너무 많은 데이터 량 (TOO MUCH DATA)

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)

정책 및 시그니쳐 기반 → 지능형 분석 기반

보안 툴의 처리 속도 보다 빠르게 증가하는 데이터의 량

⟶ Big Data의 문제

상황인식 및 대응책 마련

네트워크 속도

네트워크 & 어플리케이션 인프라

1Gb → 10Gb → 40Gb → 100Gb

보안 구성에 영향을 미치는 요인

암호화 트래픽의 증가

SSL 트래픽 (현재) : 기업 트래픽의 25%-35% [1]

보안 및 성능관리 툴은 SSL 트래픽을 미 인지 하거나, 복호화 시 과부화가 발생

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

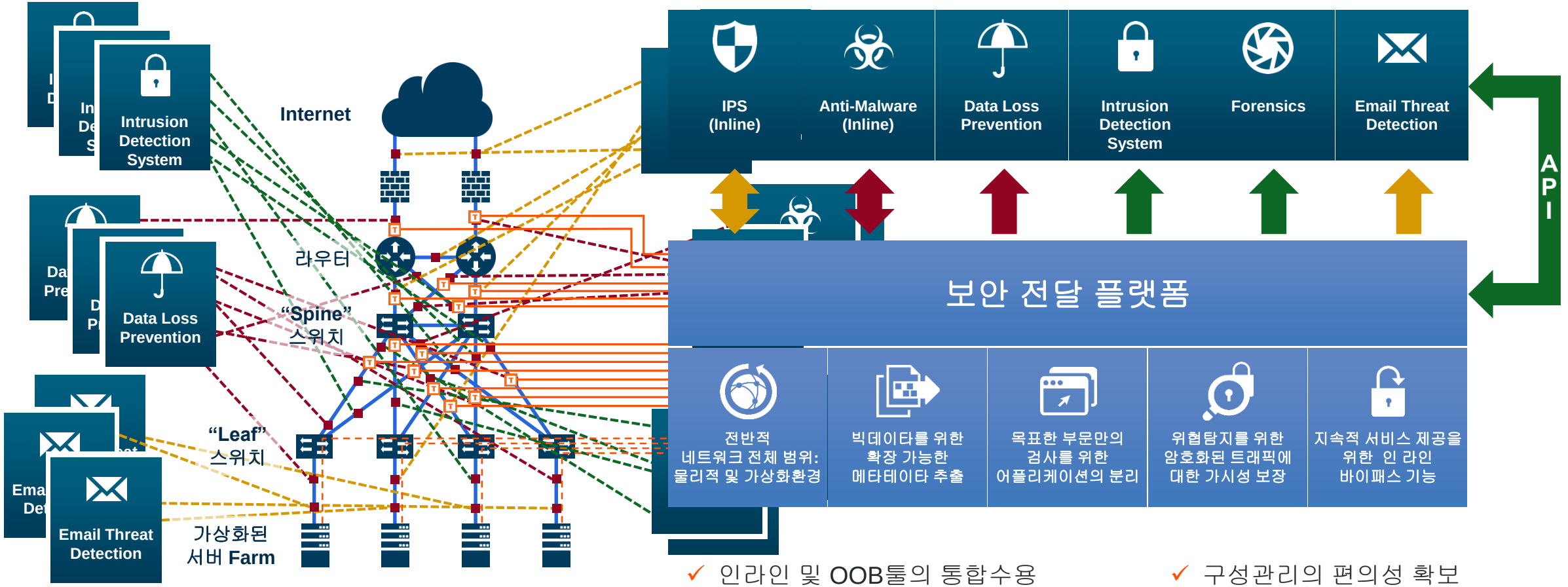
2017년, 네트워크 공격의 50% 이상 (vs. 5% today) 보안통제를 우회하기 위해 암호화된 트래픽을 이용할 것으로 예측[2]

늘어나는 암호화된 트래픽에 대응책 마련

[1] NSS Labs : 보안솔루션 전문 테스트 랩
[2] Gartner

보안 전달 플랫폼: “See Everything”

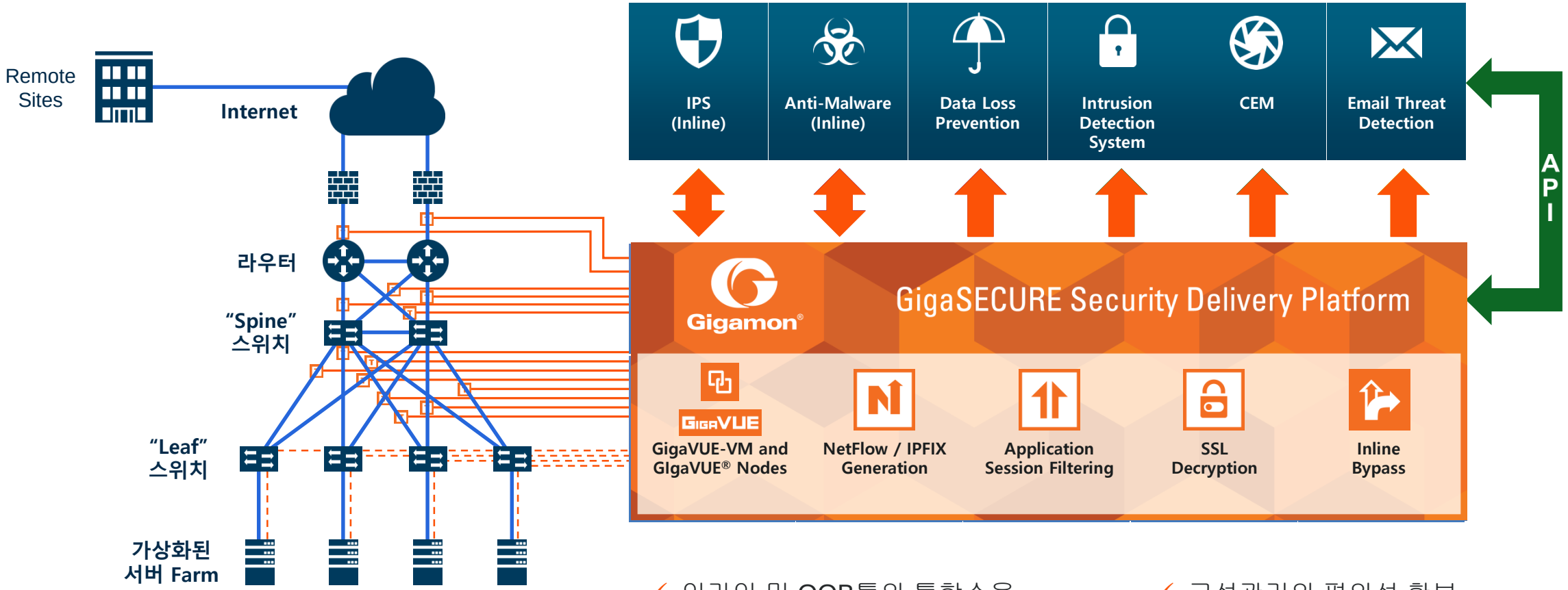
효과적인 보안을 위한 네트워크, 플랫폼 및 보안/관리 툴 블록 (BUILDING BLOCK)



- ✓ 인라인 및 OOB툴의 통합수용
- ✓ 보안 관리 툴의 성능 및 효율성 향상
- ✓ 구성관리의 편의성 확보
- ✓ CAPEX, OPEX 비용 절감

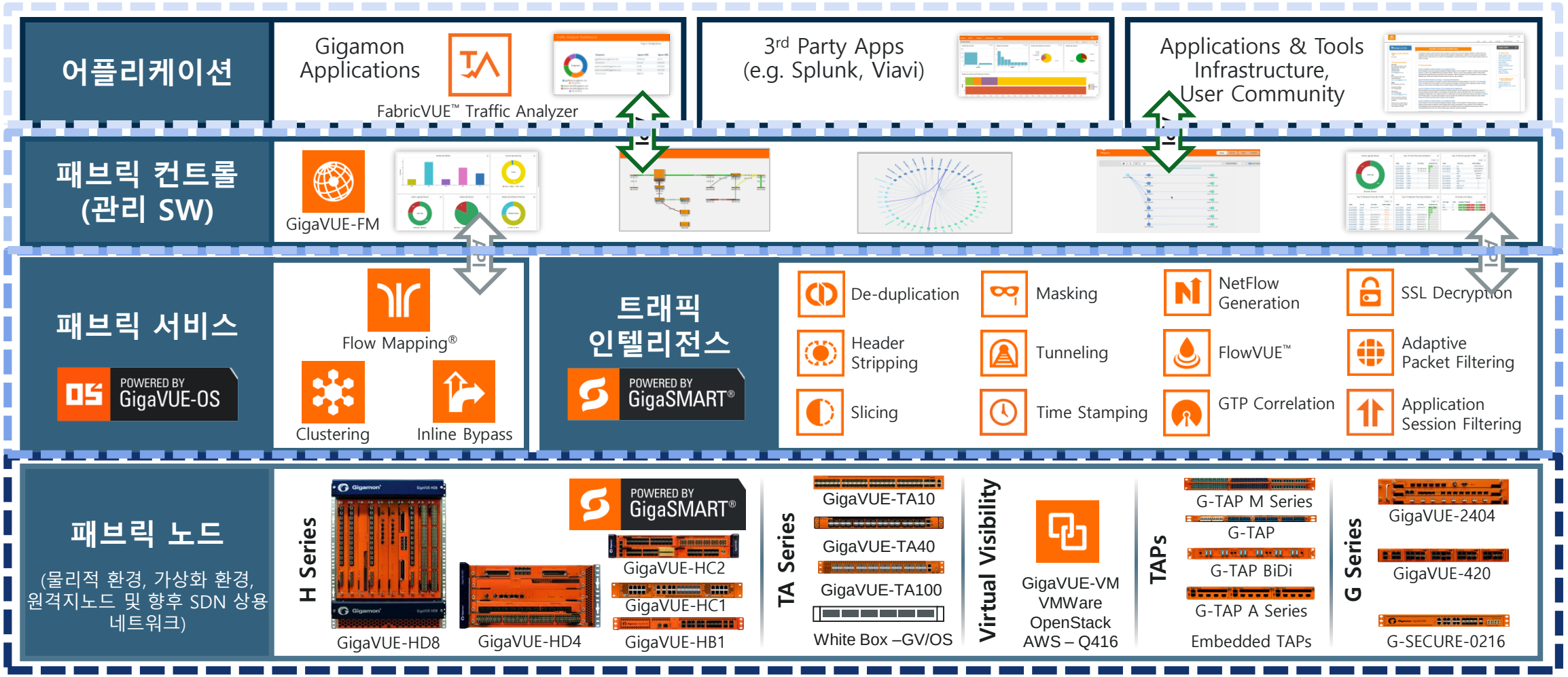
보안 전달 플랫폼: “See Everything”

산업계 최초의 보안 및 관리 플랫폼 (SECURITY & MANAGEMENT DELIVERY PLATFORM)



- ✓ 인라인 및 OOB툴의 통합수용
- ✓ 보안 관리 툴의 성능 및 효율성 향상
- ✓ 구성관리의 편의성 확보
- ✓ CAPEX, OPEX 비용 절감

보안전달 플랫폼 통합 포트폴리오

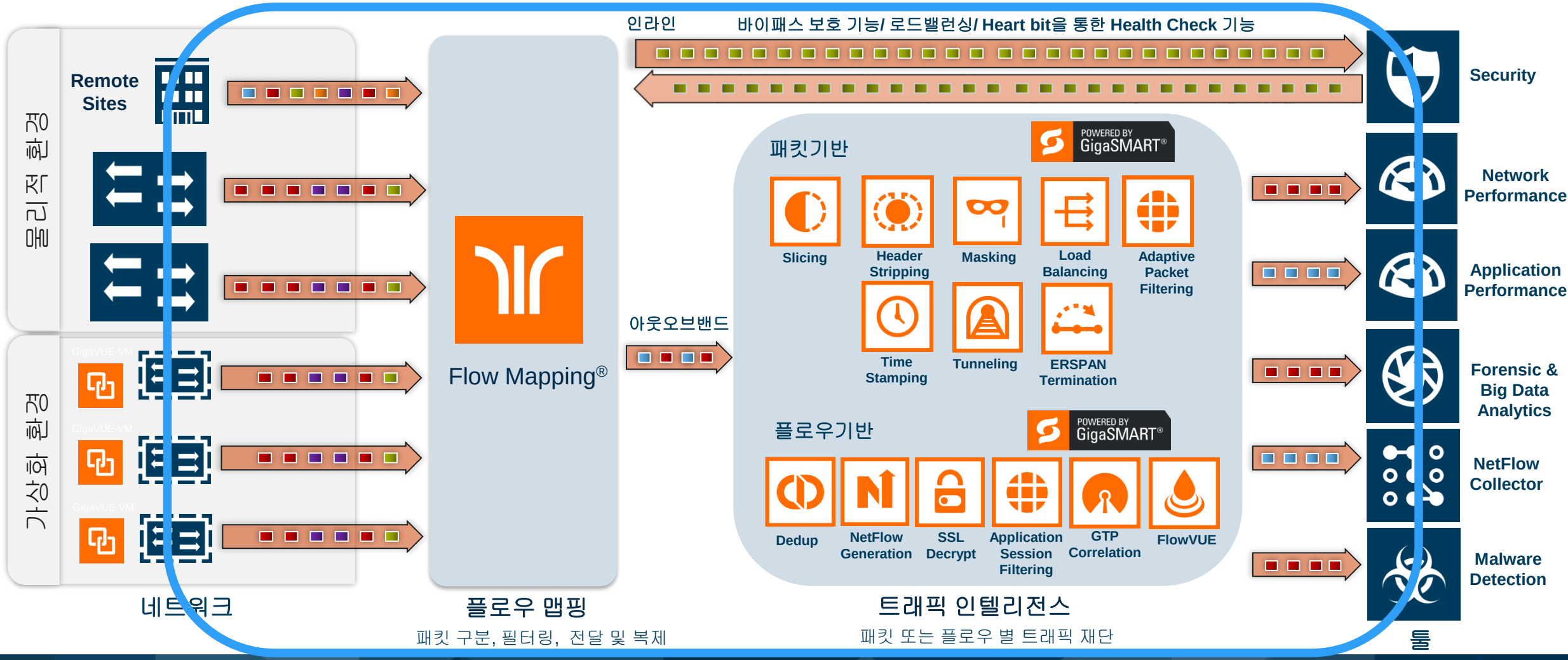


보안전달 플랫폼 패브릭노드 장비 사양

장비 모델명	장비 외관	Visibility Throughput	Port Density
GigaVUE-HD8		2.4 Tbps	100G : 48 ports 40G : 64 ports 10G : 256 ports 1G : 352 ports
GigaVUE-HD4		1.28 Tbps	100G : 24 ports 40G : 32 ports 10G : 128 ports 1G : 176 ports
GigaVUE-HC2		960 Gbps	100 : 8 ports 40G : 24 ports 1G/10G : 96 ports
GigaVUE-HC1		284 Gbps	1G/10G : 12 ports 1G : 4 ports
GigaVUE-HB1		56 Gbps	1G/10G : 4 ports 1G : 16 ports

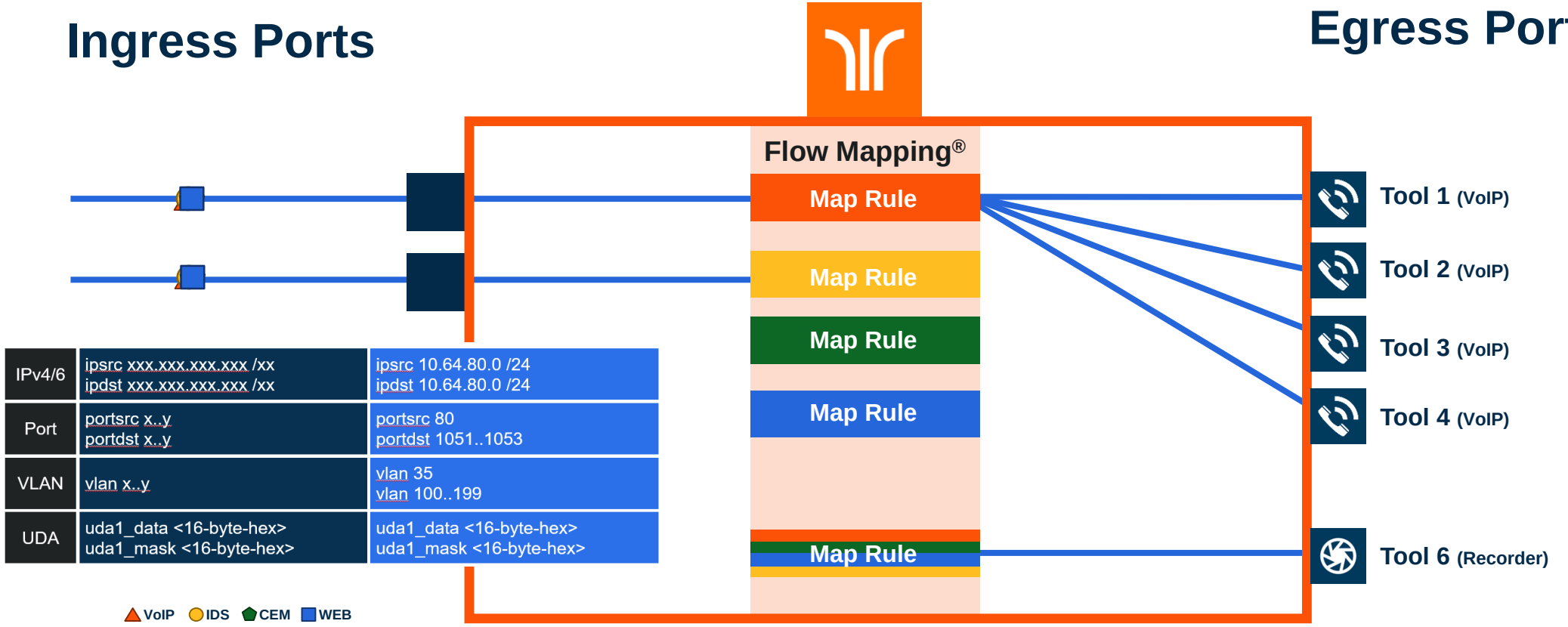
보안전달 플랫폼 기능

네트워크 → 패킷 구분, 필터링, 전달 및 복제 → 패킷 재단, 트래픽 인텔리전스 → 툴



플로우 맵핑 (Flow Mapping®)

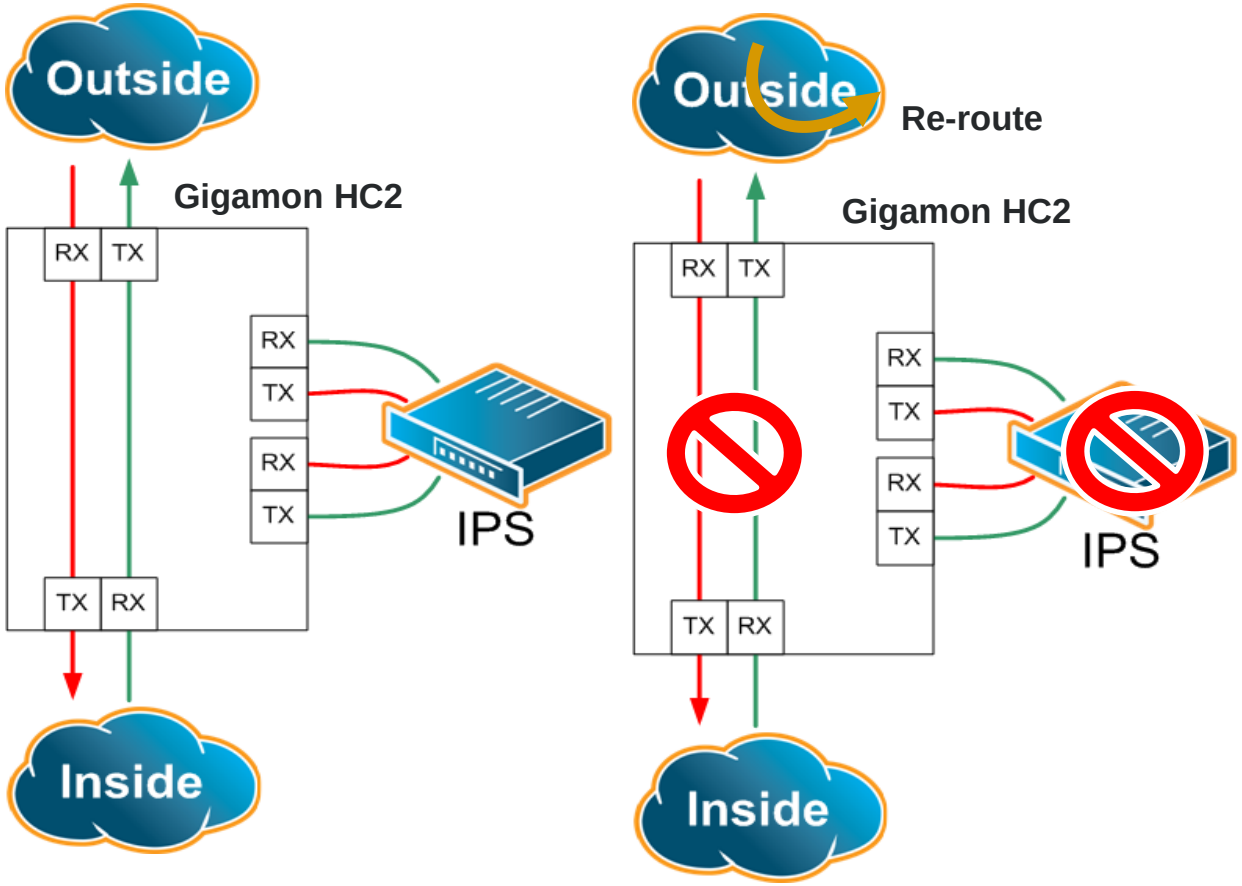
패킷을 구분하여 INGRESS/EGRESS 필터링을 통해 자유롭게 트래픽을 N:M으로 복제 및 전달가능



Configurable HW-Based Rules,
Bound to Ingress Ports

인라인 툴을 위한 보안전달기능

HEARBEAT을 이용한 툴 HEALTH CHECK, 툴 로드밸런싱 및 물리적 & 논리적 바이패스 기능제공



구분	내 용
물리적 Bypass	• 기가몬 장비의 전원 등의 장애 발생시 자동으로 네트워크 상의 모든 패킷을 바이패스
논리적 Bypass	• 장비 내 인라인 툴 장비의 장애를 감지 하여 장애발생 시 관리자 사전 정의에 따라 패킷을 바이패스 -인라인 툴의 물리적 다운 감지 -인라인 툴의 Hang up 감지(**Heartbeat**) -툴 장애 시, 패킷 드랍 / 패킷 포워딩 또는 이중화 장비로 패킷포워딩 (N+1)

아웃오브밴드 툴을 위한 보안전달기능

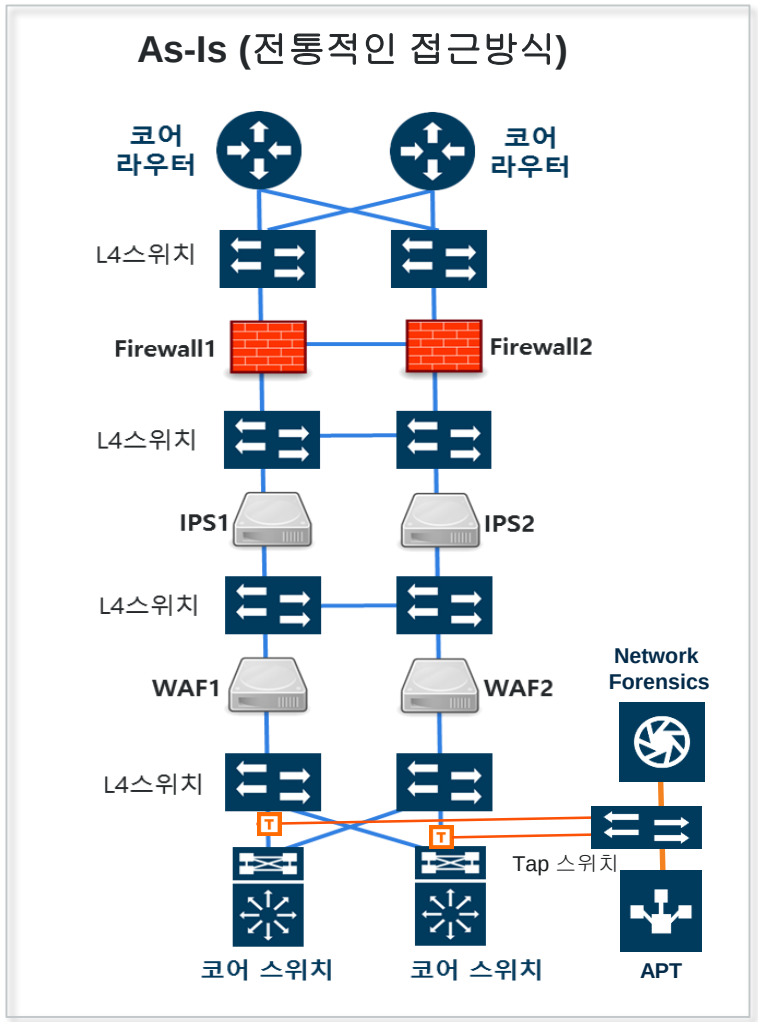
OOB형태의 보안, 측정 관리 툴에서 요구하는 패킷 재단, 툴 관리기능

기가스마트 기능

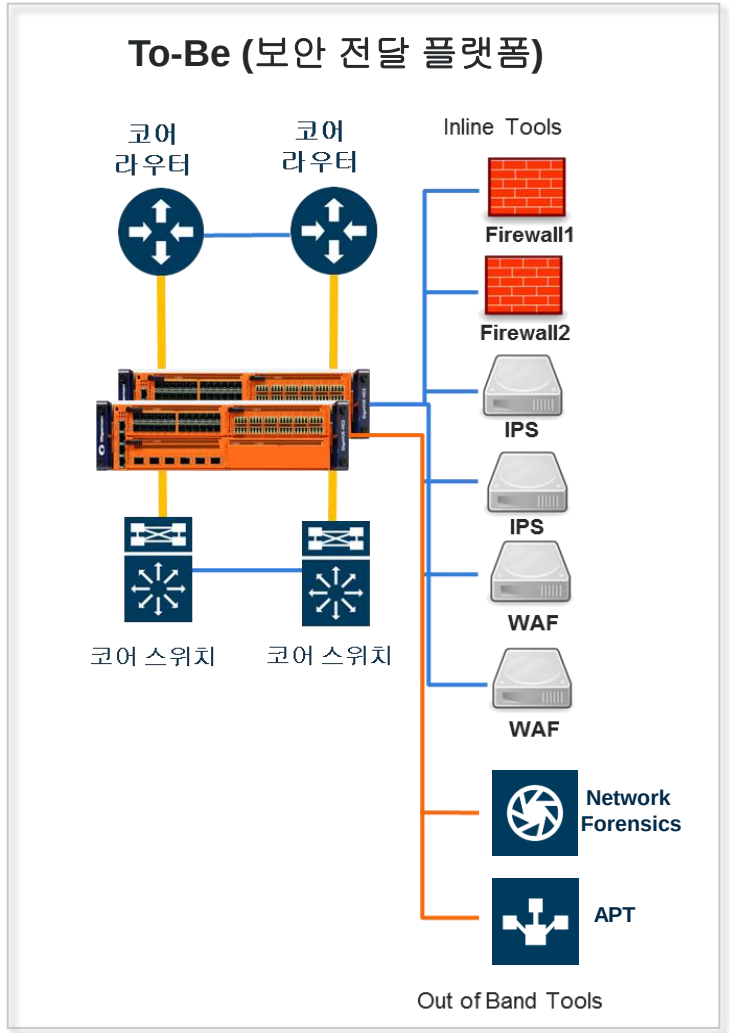
POWERED BY GigaSMART®

- De-duplication
- Masking
- NetFlow Generation
- SSL Decryption
- Header Stripping
- Tunneling
- FlowVUE™
- Adaptive Packet Filtering
- Slicing
- Time Stamping
- GTP Correlation
- Application Session Filtering

인라인 및 OOB 툴 통합구성

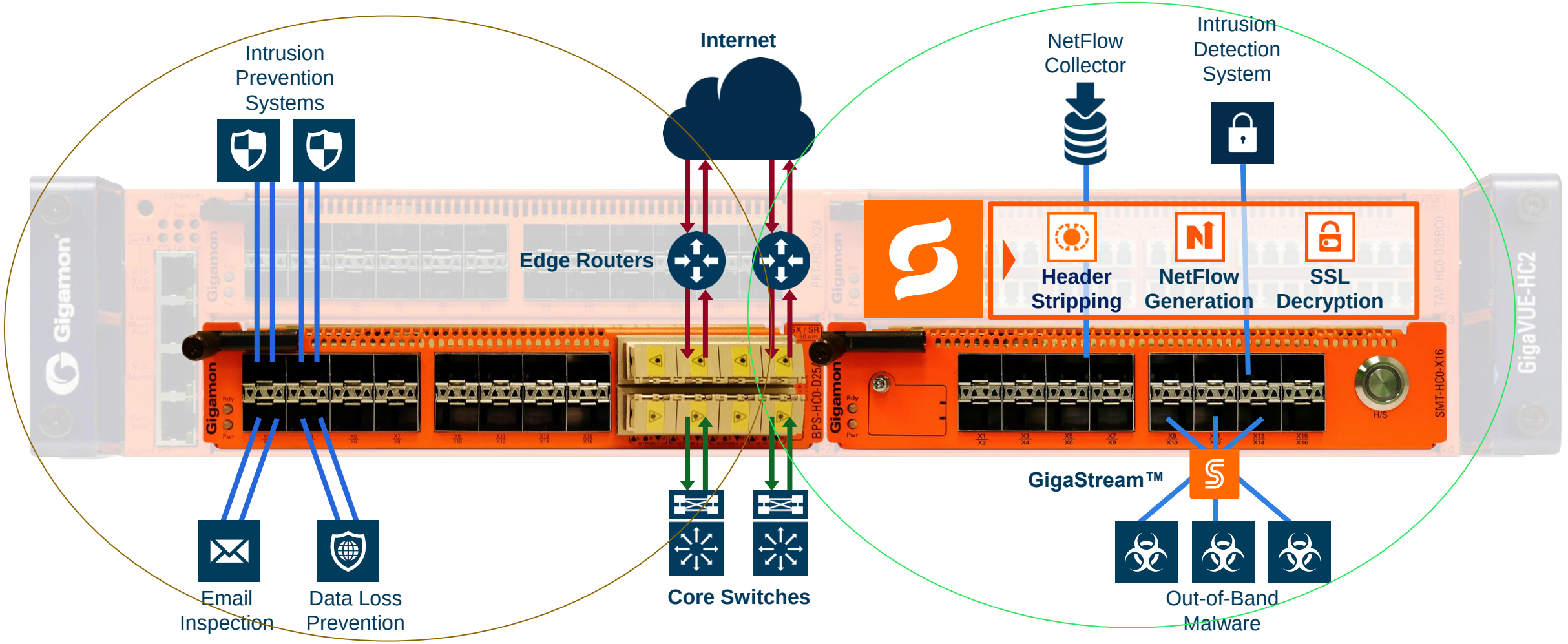


- 인라인 및 OOB 툴의 통합 구성을 통한 다 계층 보안 플랫폼 구축 가능
- 다수의 L4장비 도입 없이 인라인 장비의 로드밸런싱 및 HA 제공
  - Heartbeat 기능으로 인라인 보안 장비의 S/W Hang 감지 및 트래픽 우회
  - 기가몬의 Bypass Protection 기능으로 장애 포인트 제거
- APT, Forensic 등 OOB 툴로 SSL 복호화/중복패킷제거 기능등 패킷 제단 기능제공

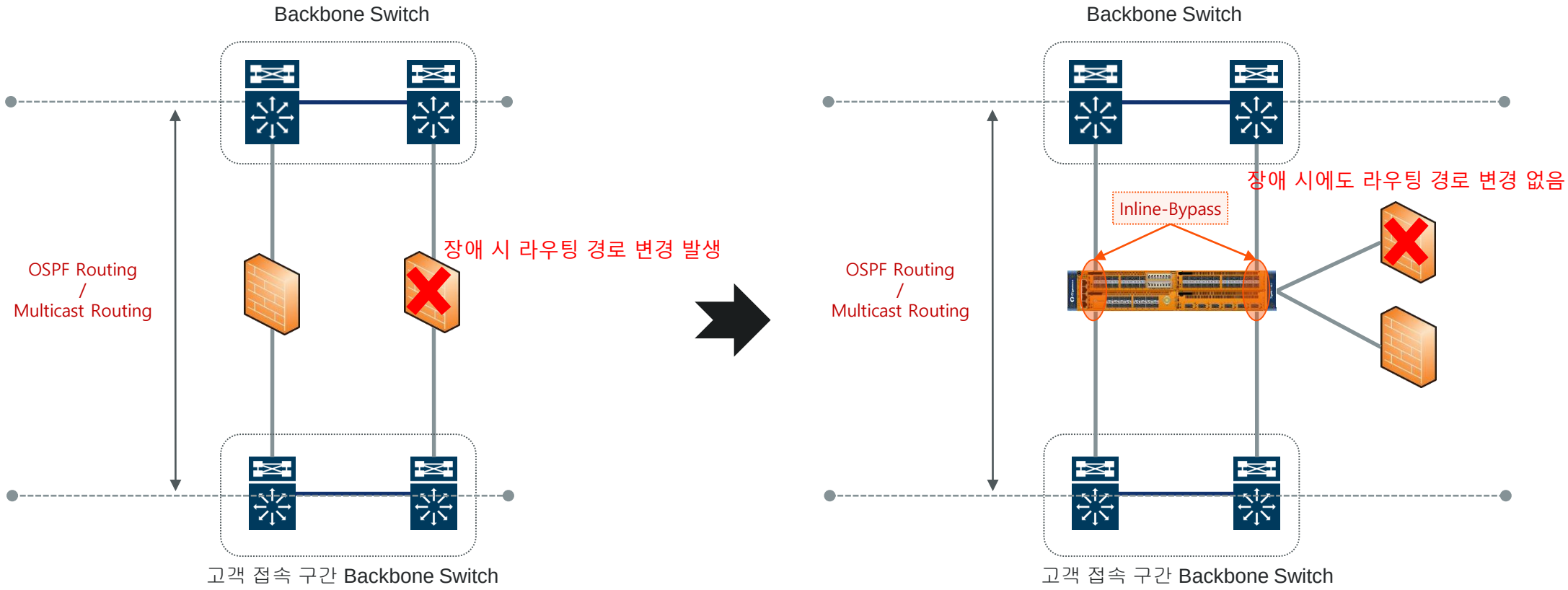


보안 전달 플랫폼 통합구성 예

인라인 및 OOB 통합 구성



단순한 네트워크 구성



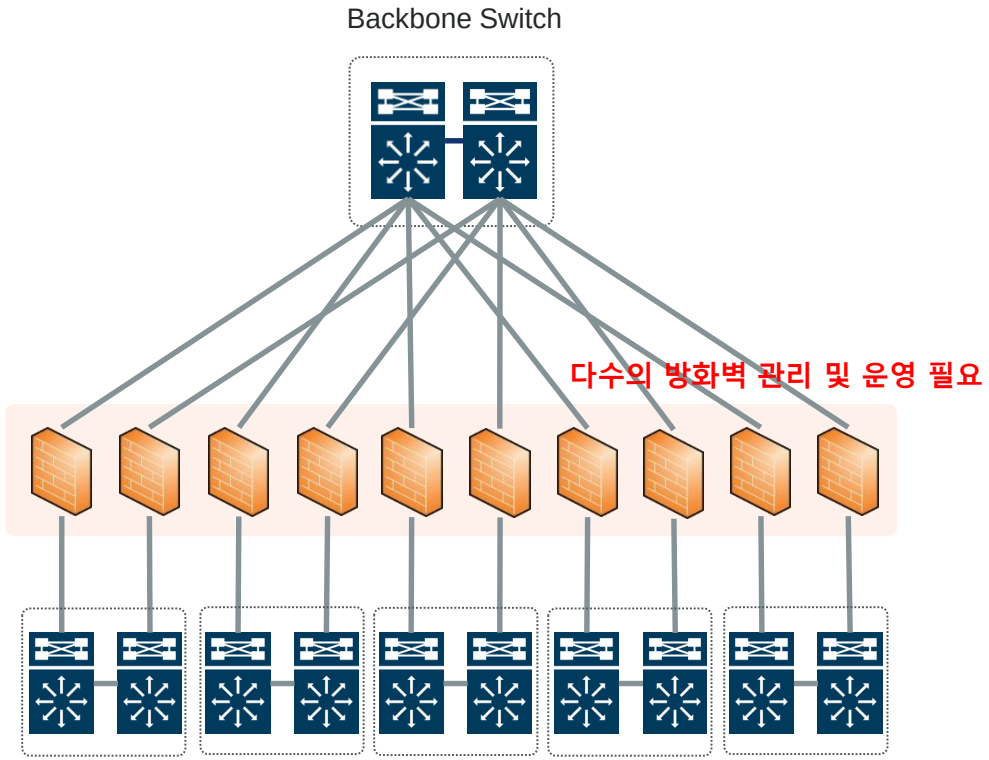
방화벽 장애 시 불필요한 라우팅 경로 변경 발생

- 방화벽 장애 발생 시 불필요한 라우팅 경로 변경에 따른 서비스 안정 저하
- 방화벽 홀딩 발생 시 트래픽 처리 불가에 따른 트래픽 손실 발생

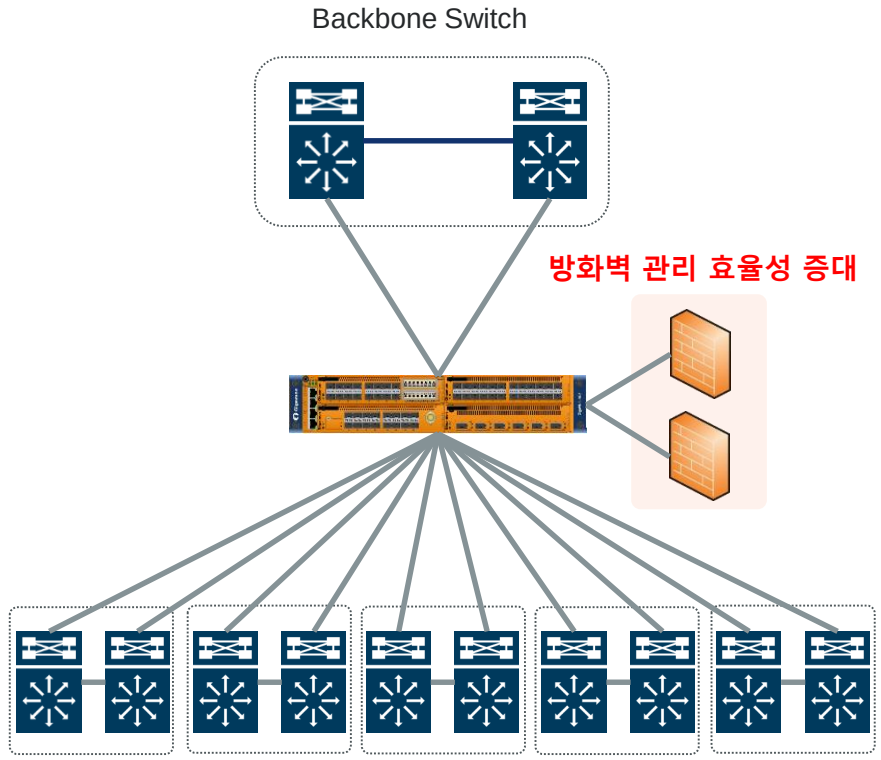
방화벽 장애 시에도 라우팅 경로 변경 없음

- 방화벽 장애 발생 시 기가몬 장비에서 트래픽 바이패스를 통한 정상 처리
- 기존 운영 네트워크망에서 불필요한 라우팅 경로 발생이 없음

인라인 보안 장비의 논리적 집선



다수 접속 구간 Backbone Switch



다수 접속 구간 Backbone Switch

다수의 방화벽 도입으로 비효율적인 운영 및 투자

- 주요 서비스 구간 내 인라인으로 다수의 방화벽 운영으로 장애 요소 증가
- 고객접속구간 각 라인 별 방화벽 도입에 따른 비효율적인 투자

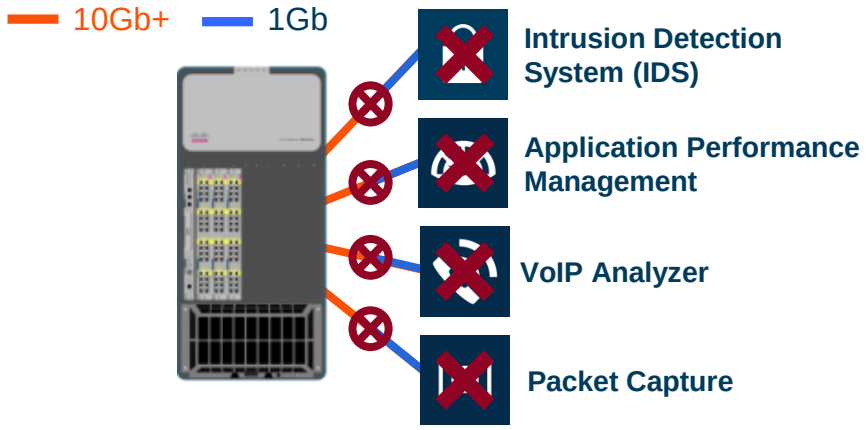
소수의 대용량 방화벽 도입으로 효율적인 방화벽 관리

- 소수의 대용량 방화벽 운영으로 장애 요소 최소화 및 효율적인 통합 보안 관리
- 방화벽 장애 시에도 기가몬 바이패스 동작으로 장애 요소 삭제

네트워크 Migration

기존 장비 사용 연수의 증가 및 자유로운 투자 시점 결정 가능

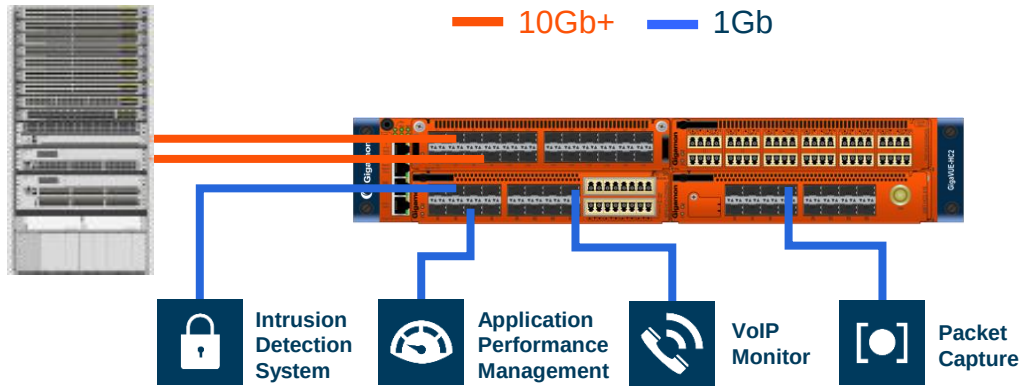
기가몬 도입 전



네트워크 업그레이드에 따라 기존 보안 및 분석 솔루션 업그레이드 필요

기가몬 도입 후

GigaVUE® Matches Your Network to Your Tools

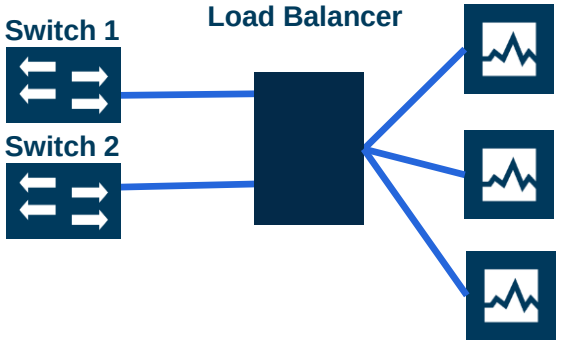


보안 및 분석 솔루션의 라이프사이클 연장 및 투자 규모 시기의 탄력적 계획 가능

대용량 부하 분산 기능으로 향후 투자 보호

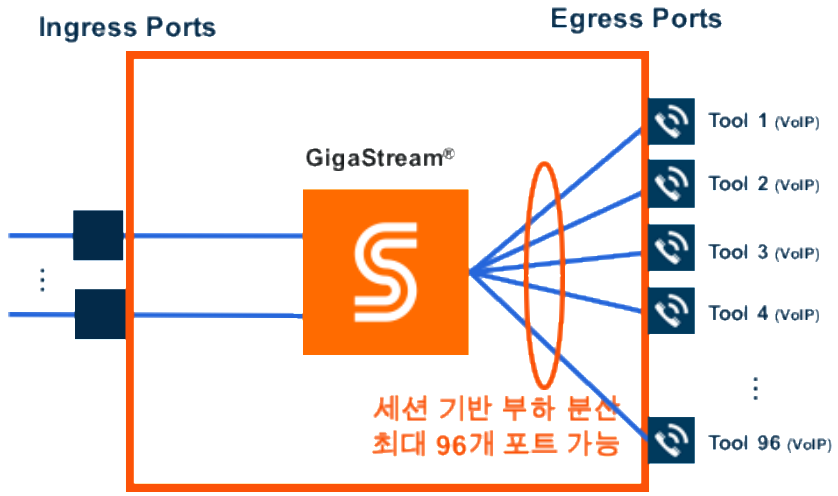
강력한 부하분산 기능을 이용하여 기존 장비 활용의 경제성 확보 및 96개의 부하분산 확장성 제공

기가몬 도입 전



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

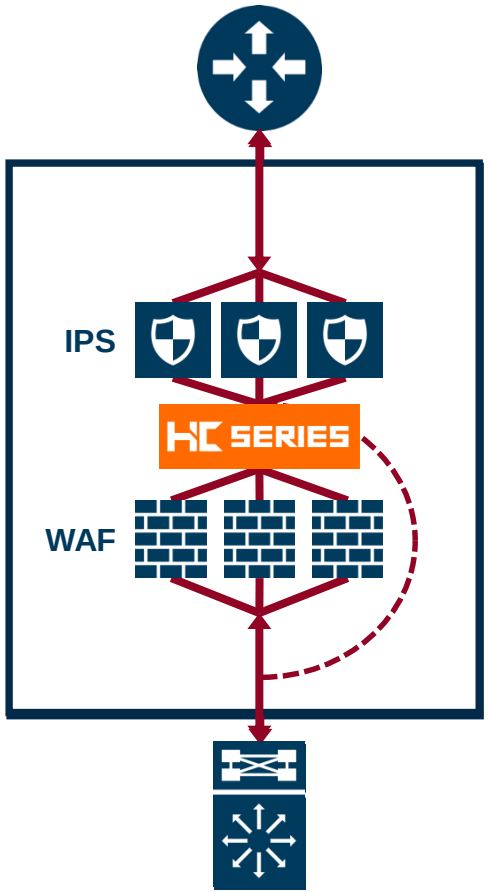
기가몬 도입 후

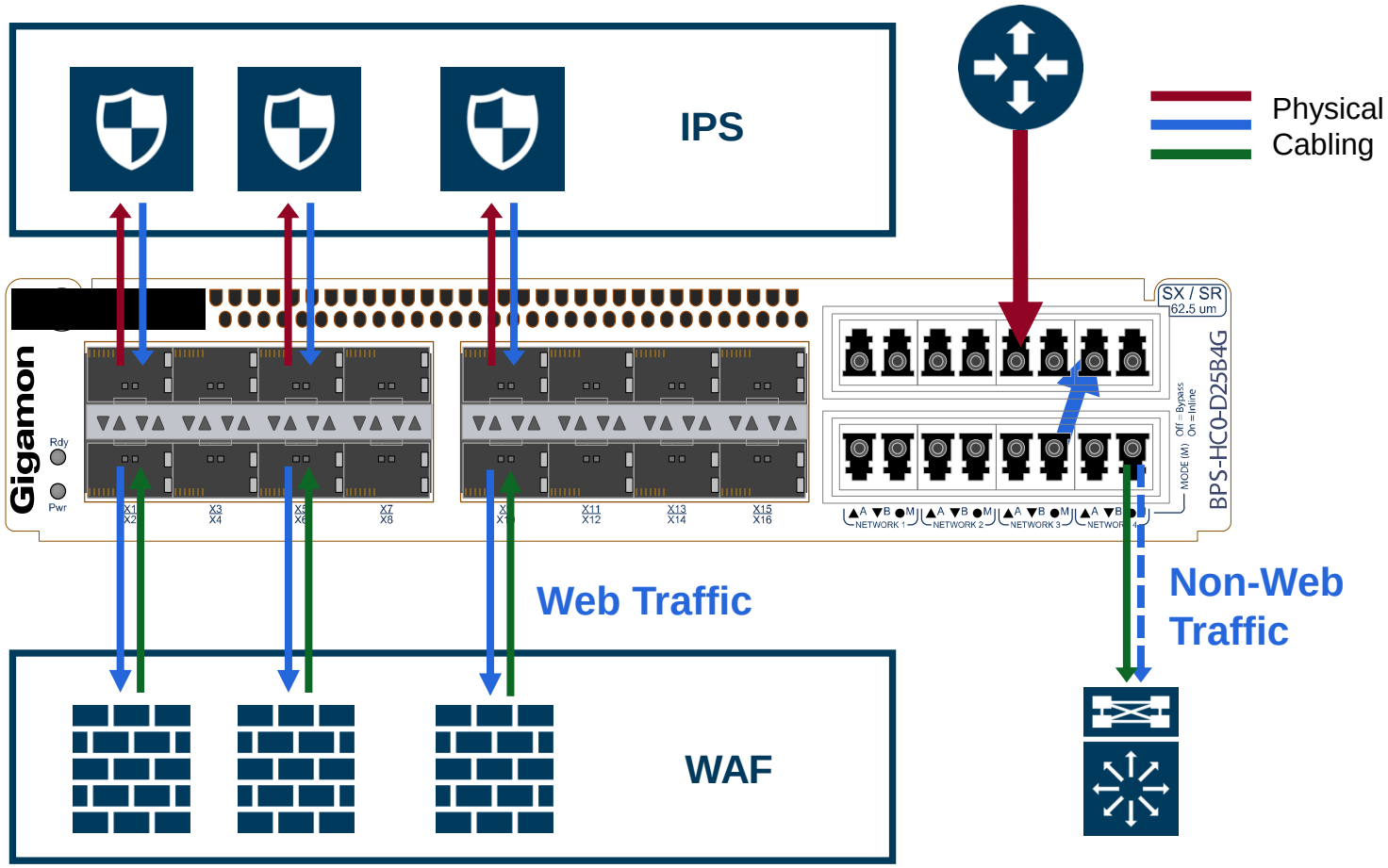


최대 96개 포트로 L2/L3/L4 세션 기반으로 부하 분산(로드 벨런싱) 제공 – Advanced Hashing

신규 보안 툴 도입 (예 : WAF)

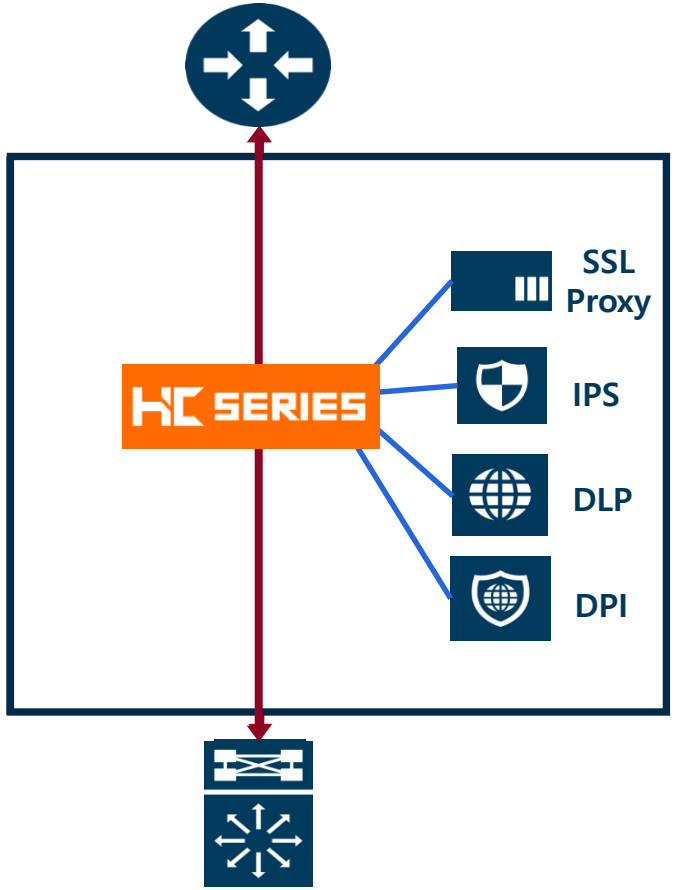
FLOW MAPPING을 활용하여 IPS 인입 트래픽 필터링 제공으로 신규 장비 성능 강화

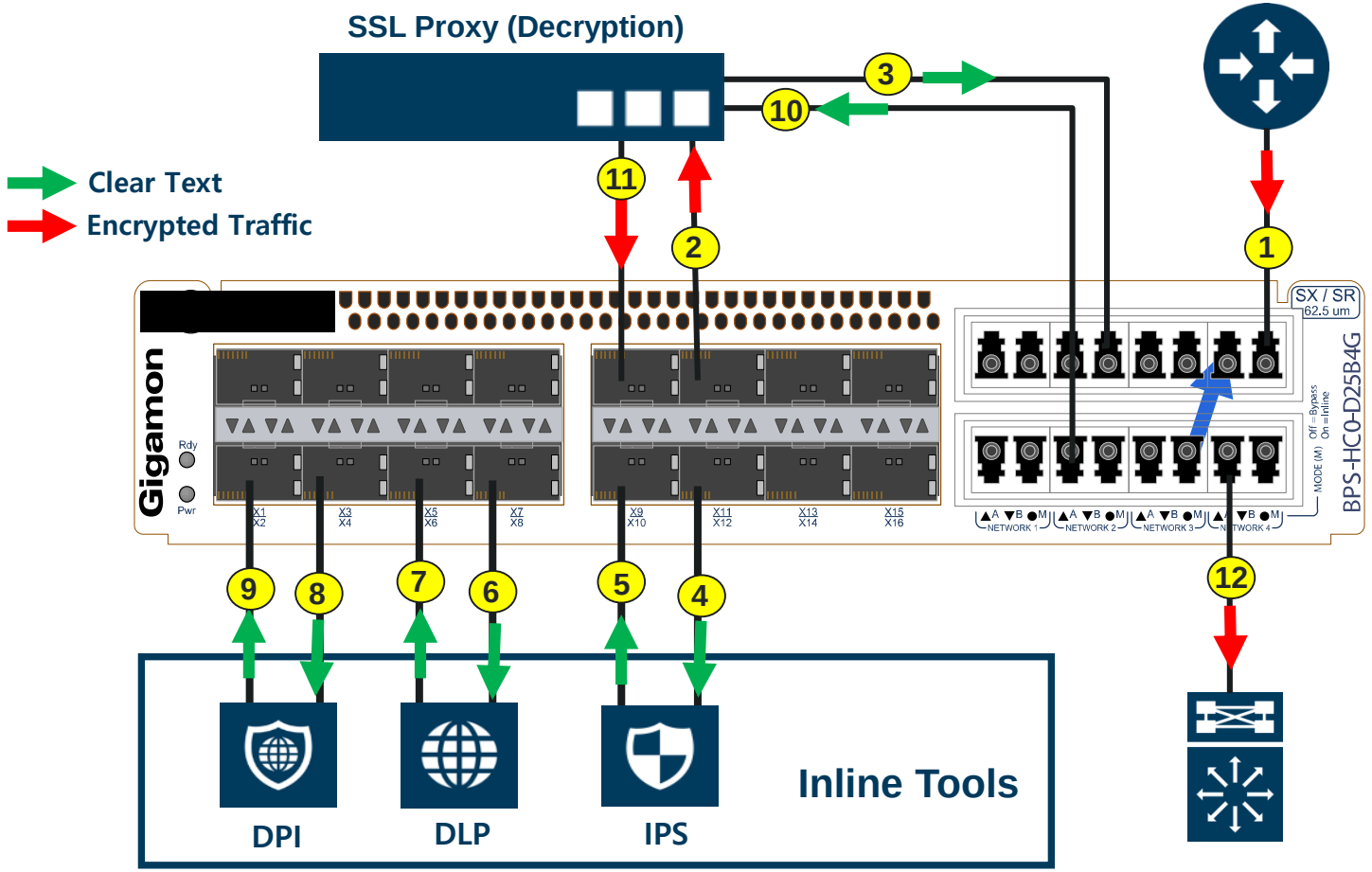




신규 보안 툴 도입 (예 : SSL 인라인 복호화)

외장형 SSL DECRYPTION 솔루션 :인라인 바이패스 보호, 로드밸런싱 기능 제공



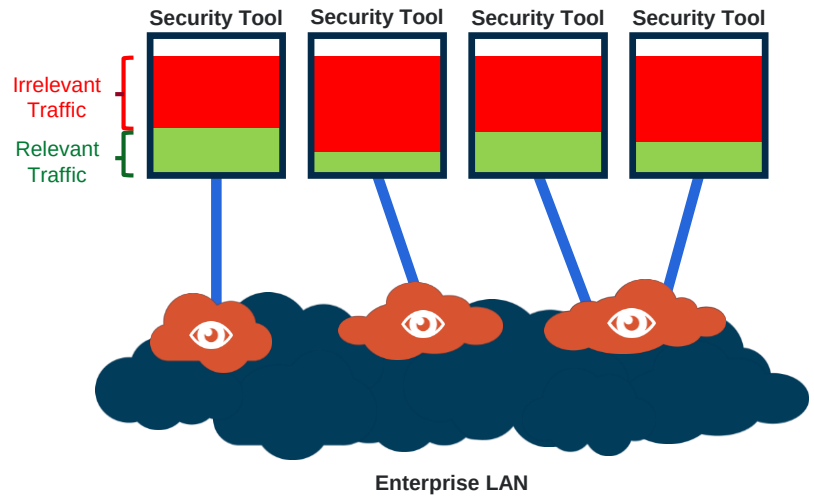


기존 및 신규 장비의 최적화

지능형 필터링을 통한 불필요한 트래픽 처리 예방으로 장비 성능 향상 및 투자비용 감소

Without Gigamon

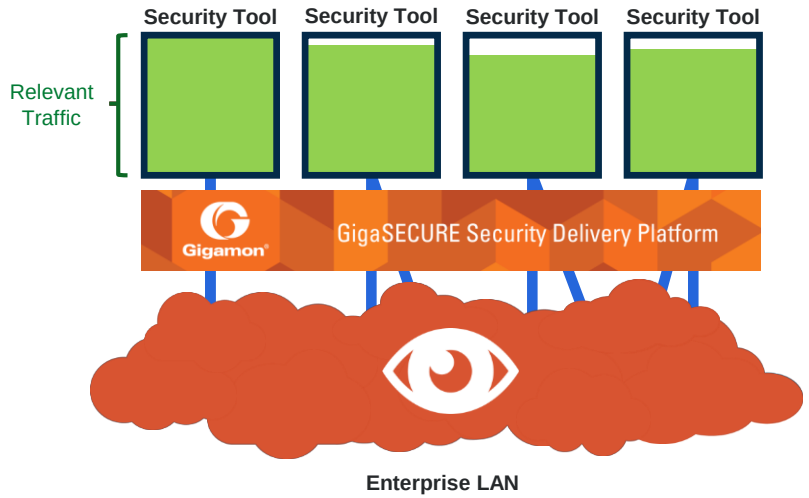
Legacy Approach Without Gigamon



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

With Gigamon

With Gigamon Security & Management Delivery Platform



트래픽 필터링을 통한 효율적인 분석으로 동일 장비로 모니터링 구간 확대

GigaSMART® : Application Session Filtering

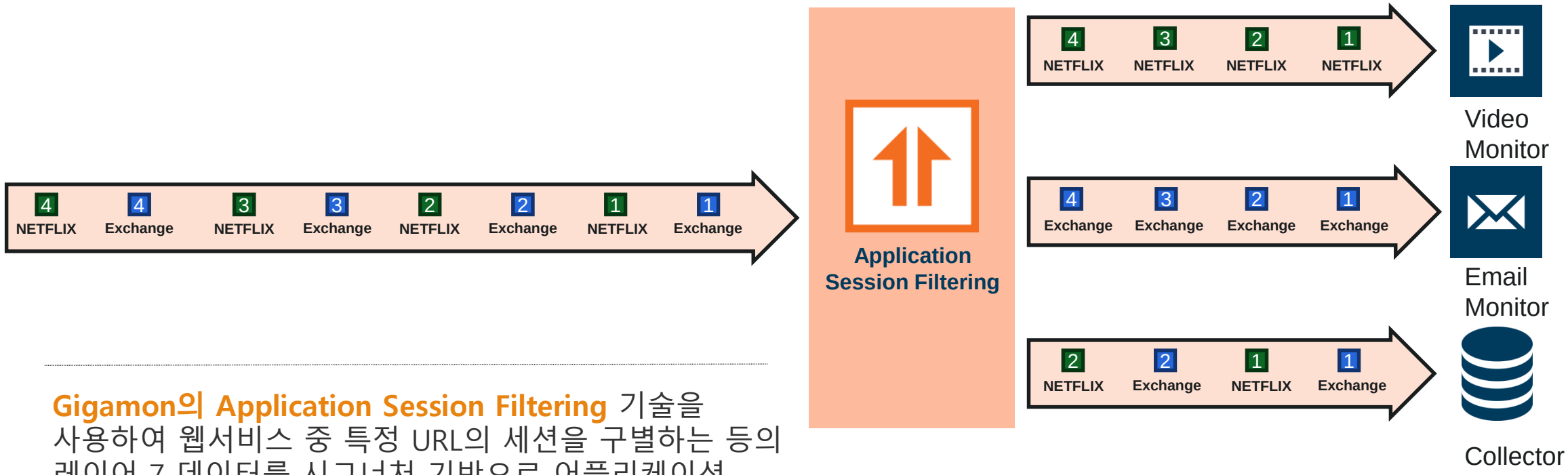
DPI 기반 특정 어플리케이션 세션 필터링 (PORT 숫자 기반 필터링 한계 극복)

Protocol	HTTP	SMTP	FTP	TELNET	NTP	BGP
TCP/UDP Port #	80	25	20/21	23	123	179

Protocols?
All Web 2.0 use port 80 & 443

GigaSMART® : Application Session Filtering

L7 기반 세션 필터링



Gigamon의 Application Session Filtering 기술을 사용하여 웹서비스 중 특정 URL의 세션을 구별하는 등의 레이어 7 데이터를 시그너처 기반으로 어플리케이션 세션을 분류 할 수 있음. 이를 통해 제한된 모니터링/분석 도구를 효율적으로 사용할 수 있는 경제성을 제공

Case Study : E-Commerce

100G LOAD BALANCING

GigaVUE-HD8

GigaVUE-HD4

Background & Challenge

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

Solution

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

Results & Key Benefits

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

Case Study : 은행

ENSURE IPS(SOURCEFIRE) DEPLOYMENT SUCCESS

Background & Challenge

- IPS 장애로 부터 네트워크 보호 (IPS : SourceFire)
- IPS 툴의 이중화 구조를 검토
- 필요한 트래픽만 필터링 구현 요구
- 기타 모니터링 도구들로 확장하여 HA 구성 및 트래픽 전달 요구

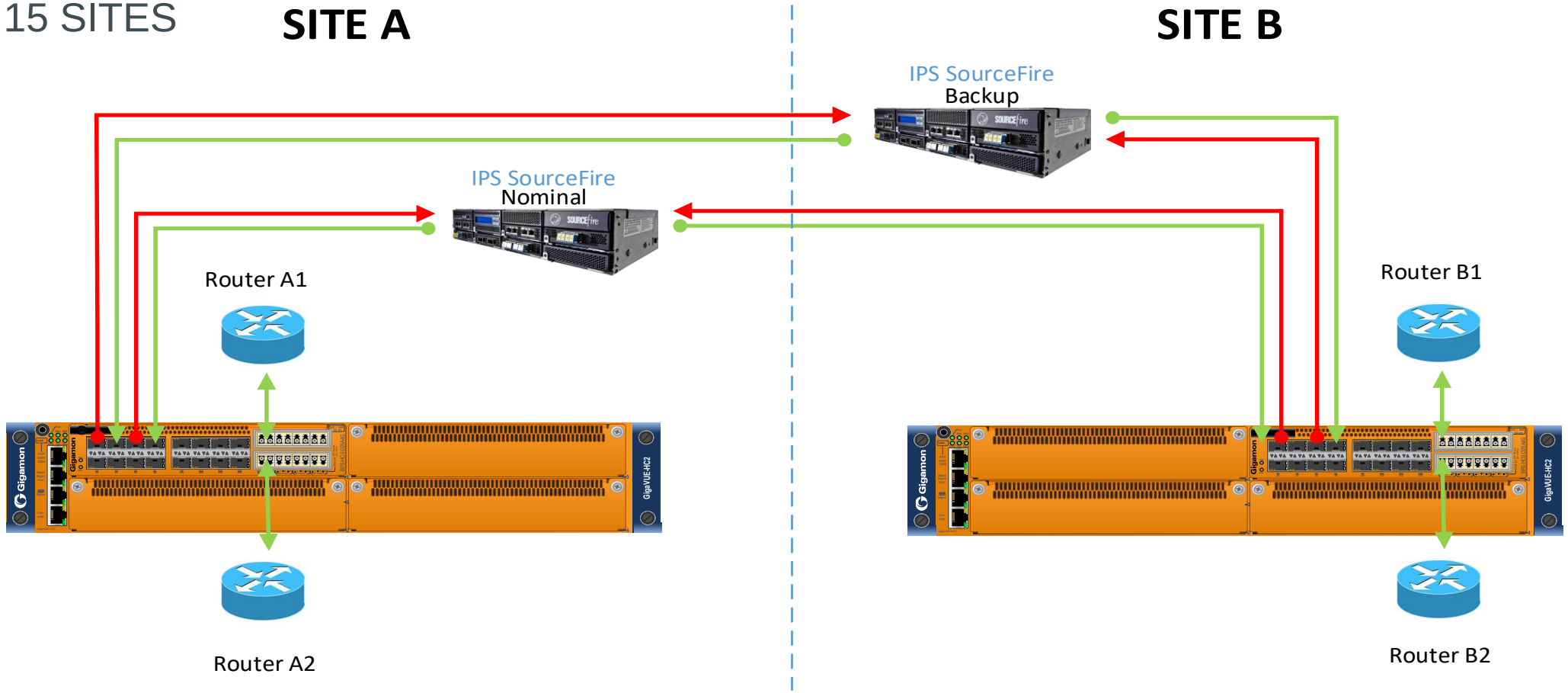
Solution

- 15개 사이트에 30 x HC2 구성
- HC2 상에 이중화된 IPS 접속 / 바이패스 모듈을 통한 IPS 와 네트워크 수용
- Heartbeat과 링크 상태 확인을 통한 장애 감지
- 플로우 맵핑 기술을 활용한 필요 트래픽 필터링

Results & Key Benefits

- IPS 유지보수 시 편의성 증가 (configuration test, OS upgrades…)
- IPS 와 네트워크 신뢰성 확보
- IPS의 asymmetric 트래픽 false positive 제한

Case Study : 은행



Case Study : 금융그룹

BUILDING AN ENTERPRISE-WIDE SECURITY DELIVERY PLATFORM

BACKGROUND & CHALLENGE

- 13백만명 고객을 보유한 대형 금융그룹 (Bank, Security & Investment etc.)
- 보안 아웃소싱으로 부터 자체적인 보안 네트워크 구축 결정
- 마스터 플랜에 입각한 단계적 진행 (1단계: inline, 2단계: security analytics)
- 다양한 보안 툴 수용 가능한 가시성 솔루션 필요 (FireEye, TippingPoint, Splunk and Palantir 등)
- 2개의 주요 데이터 센터와 각 국 및 지역 내 영업장 및 클라우드 업무 수용

APPROACH & SOLUTION

- 1단계: 코어 네트워크 상 Tipping Point (inline) 및 FireEye (out-of-band)
- 2단계: 데이타센타 및 에지 네트워크 까지의 Out-of-Band 도구 통합 수용
- GigaVUE-HC2 with inline bypass (Ph. 1). HC2 + TA10 (Ph. 2). Visibility for Vmware NSX (Ph. 3)

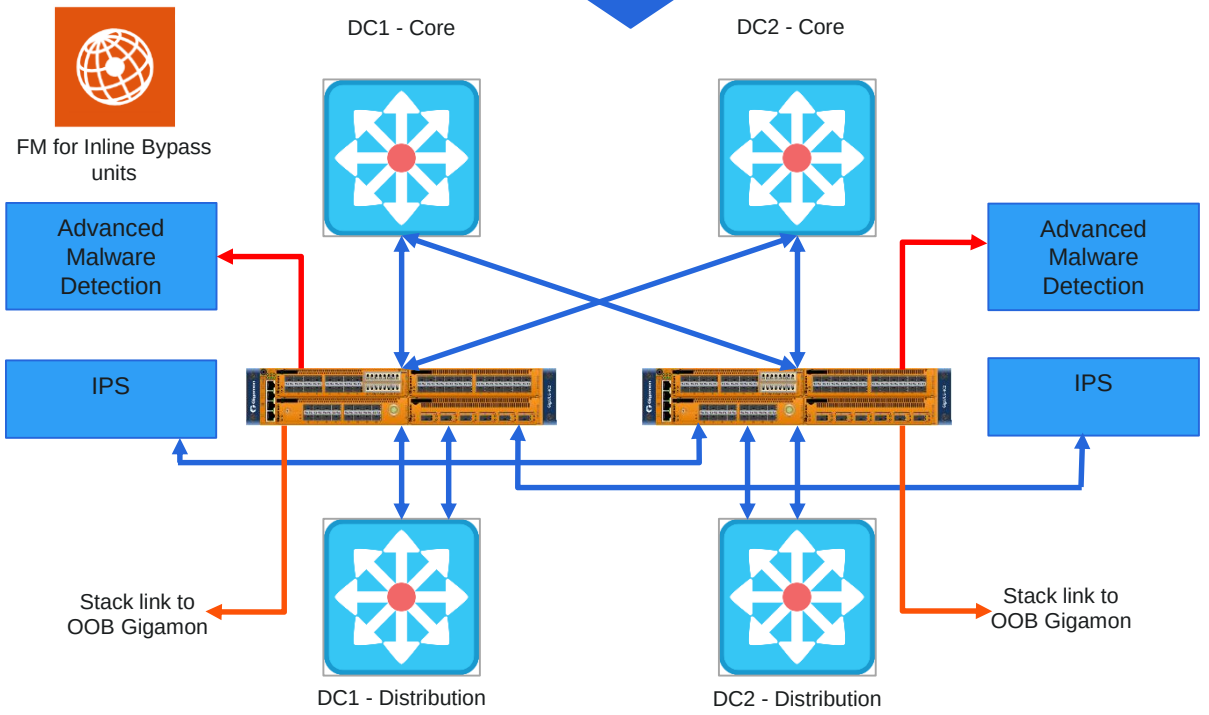
RESULTS & KEY BENEFITS

- 1단계 성공적 구축완료: HC2를 이용한 인라인 보안툴 구축 및 가시성 확보
- 2단계 구축진행 중 : TAP 구성 중, TA10 과 HC2 증설 중
- 새로운 가시성 플랫폼 구축으로 $24M 투자비 절감 효과 발생
- 아마존 퍼블릭 클라우드 와 , SSL beta 진행 예정

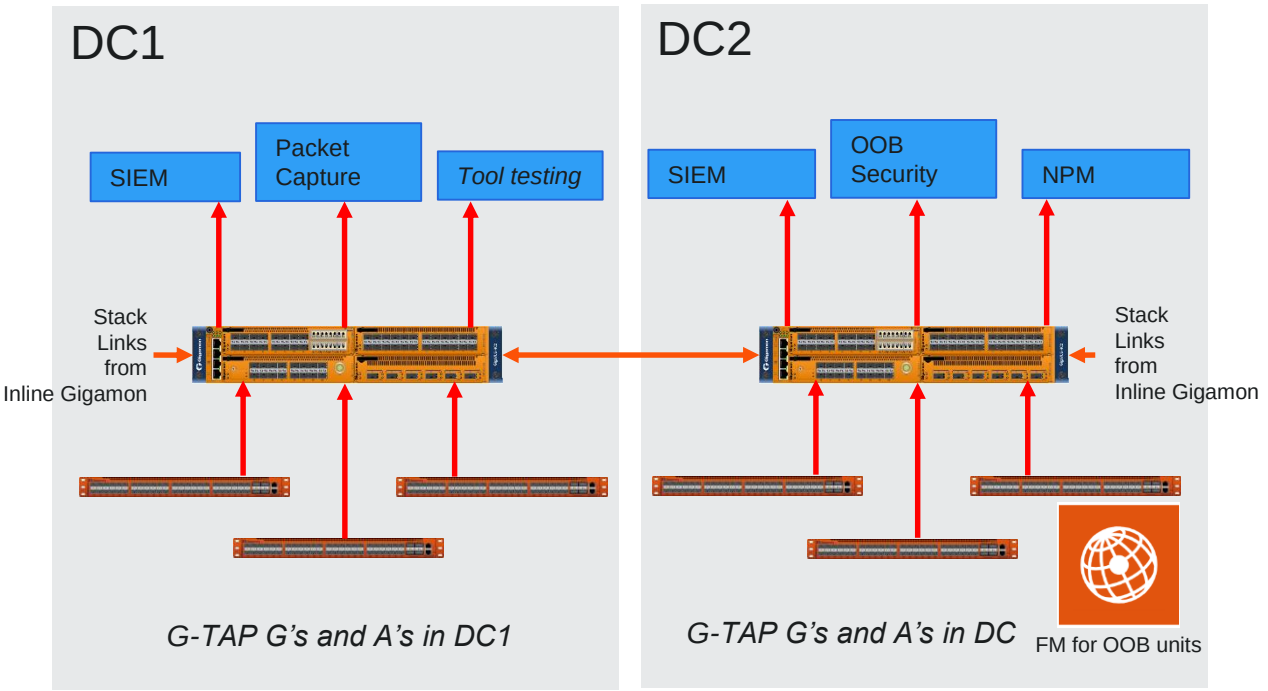
Deployment Diagram

MORE TO COME

Inline Bypass



OOB deployment



Case Study – 엔터프라이즈/제조

INLINE AND OUT-OF-BAND MONITORING

Background & Challenge

- Inline Tools : SourceFire (now Cisco FirePOWER) IPS, Imperva WAF,
- Out-of-Band tools: FireEye, ExtraHop
- 인라인 및 OOB툴의 통합 구성 및 다계층 보안 요구

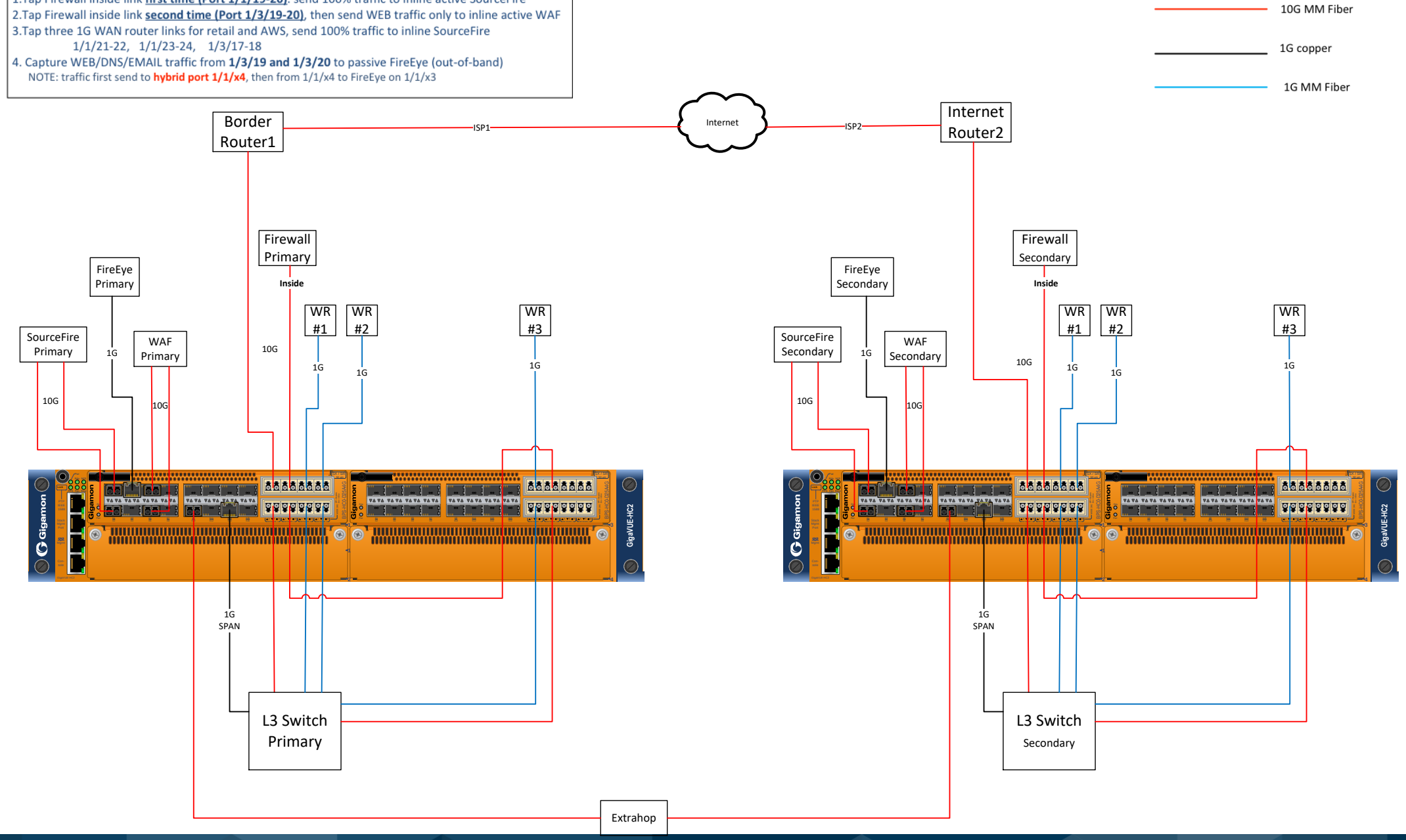
Solution

- Inline 감시 구성을 위한 GigaVUE-HC2 bypass 기술 (1 x 10Gb & 3 x 1Gb links)
- Web 트래픽 감시 성능 향상을 위한 APP aware feature
- 확보된 동일 인터넷 트래픽을 OOB 툴 FireEye 와 ExtraHop 향 동시 전달

Results & Key Benefits

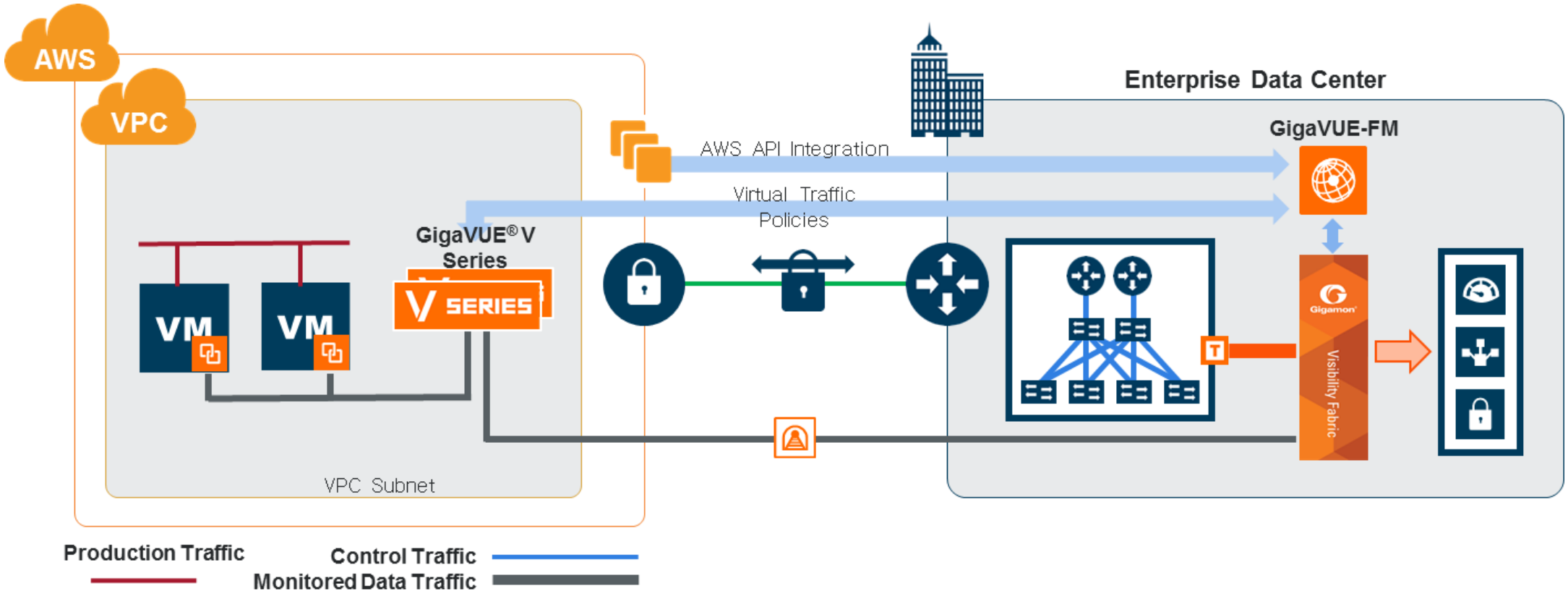
- 서로 다른 4개의 물리적 링크에 하나의 OOB 툴 활용 가능
- 인라인 및 OOB의 통합 구성 및 적은 비용으로 다계층 보안 구성 가능

1.Tap Firewall inside link **first time (Port 1/1/19-20)**. send 100% traffic to inline active SourceFire
2.Tap Firewall inside link **second time (Port 1/3/19-20)**, then send WEB traffic only to inline active WAF
3.Tap three 1G WAN router links for retail and AWS, send 100% traffic to inline SourceFire
1/1/21-22, 1/1/23-24, 1/3/17-18
4. Capture WEB/DNS/EMAIL traffic from **1/3/19 and 1/3/20** to passive FireEye (out-of-band)
NOTE: traffic first send to **hybrid port 1/1/x4**, then from 1/1/x4 to FireEye on 1/1/x3



Case Study : Public Cloud (AWS)

EXAMPLE USE CASE: TOOLS IN AN ON-PREM DATA CENTER

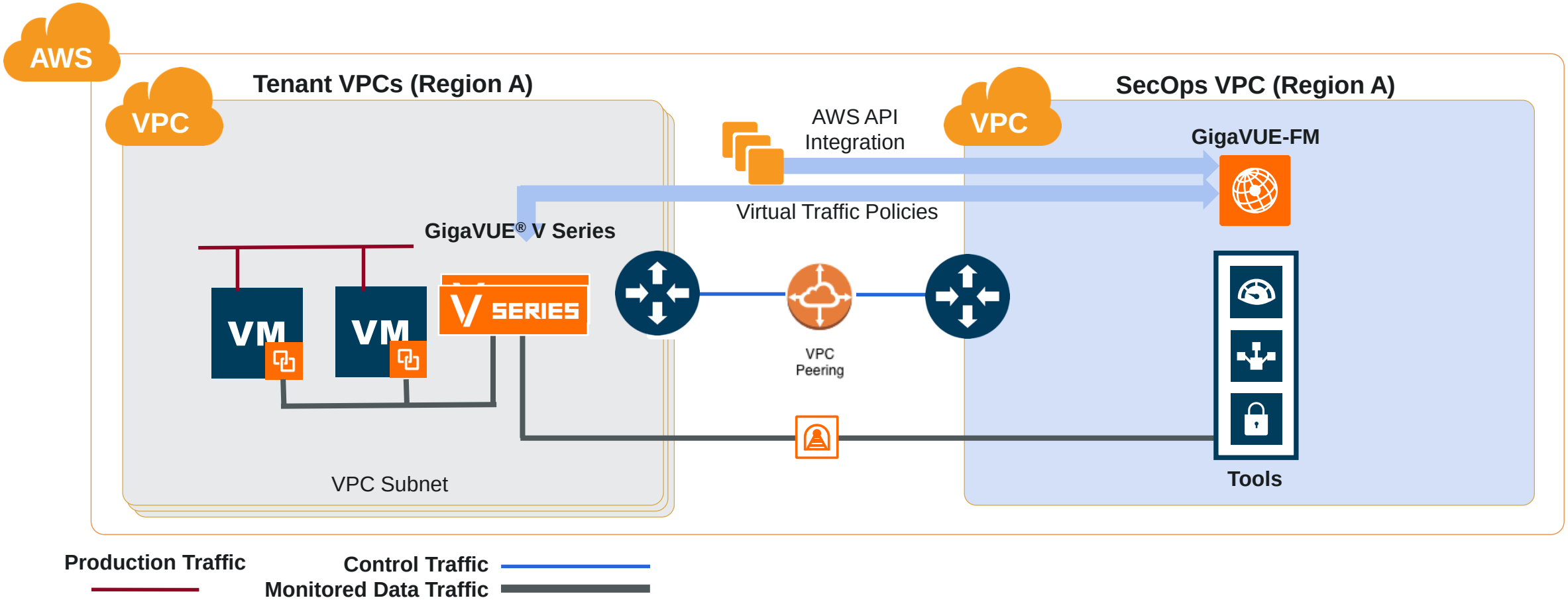


Public Could 의 트래픽을 자사 데이터센터의 보안 및 분석 장비로 전송

VPC: Virtual Private Cloud. Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and subject to change.

Case Study : Public Cloud (AWS)

USE CASE: CENTRALIZED MONITORING OF DIFFERENT VPCS



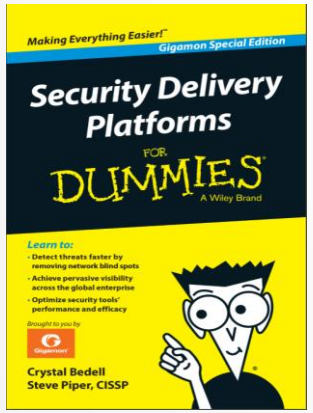
Public Could 의 트래픽을 보안 전담 VPC로 전송

기가몬의 가치

보안 전달 플랫폼

- 산업계 최초의 보안 전달 플랫폼 (Security Delivery Platform)
- SDN (Cisco ACI, VMware NSX)을 포함한 가상화 및 물리적 환경 내 전체적인 가시성 제공
- 특허 받은 Flow Mapping®기술을 통한 Zero Packet Loss 및 N:M 필터링 구현
- 클러스터링 (Clustering) 기술을 통한 구성관리의 단순화 및 유연한 확장성 보장
- 진보된 트래픽 인텔리전스와 서비스 연결성(Chaining)을 제공하는 탁월한 GigaSMART® 기능
- SSL 복호화 및 어플리케이션 세션기반 필터링 기능등의 통합된 가시성을 제공하는 유일한 회사
- 한층 넓고, 깊은 트래픽 인사이트 (Insight) 제공을 위한 전수 NetFlow / IPFIX 메타데이타 제공

Thank You!



- **Contact Points**
  -영업담당 : 노병완 전무 (010-7393-4196, brian.rho@gigamon.com)
  -기술담당 : 이민형 부장 (010-9636-8176, minhyung.lee@gigamon.com)

- **URL for downloading this SDP e-Book (https://www.gigamon.com/resources/book/security-delivery-platforms-dummies-3197)**