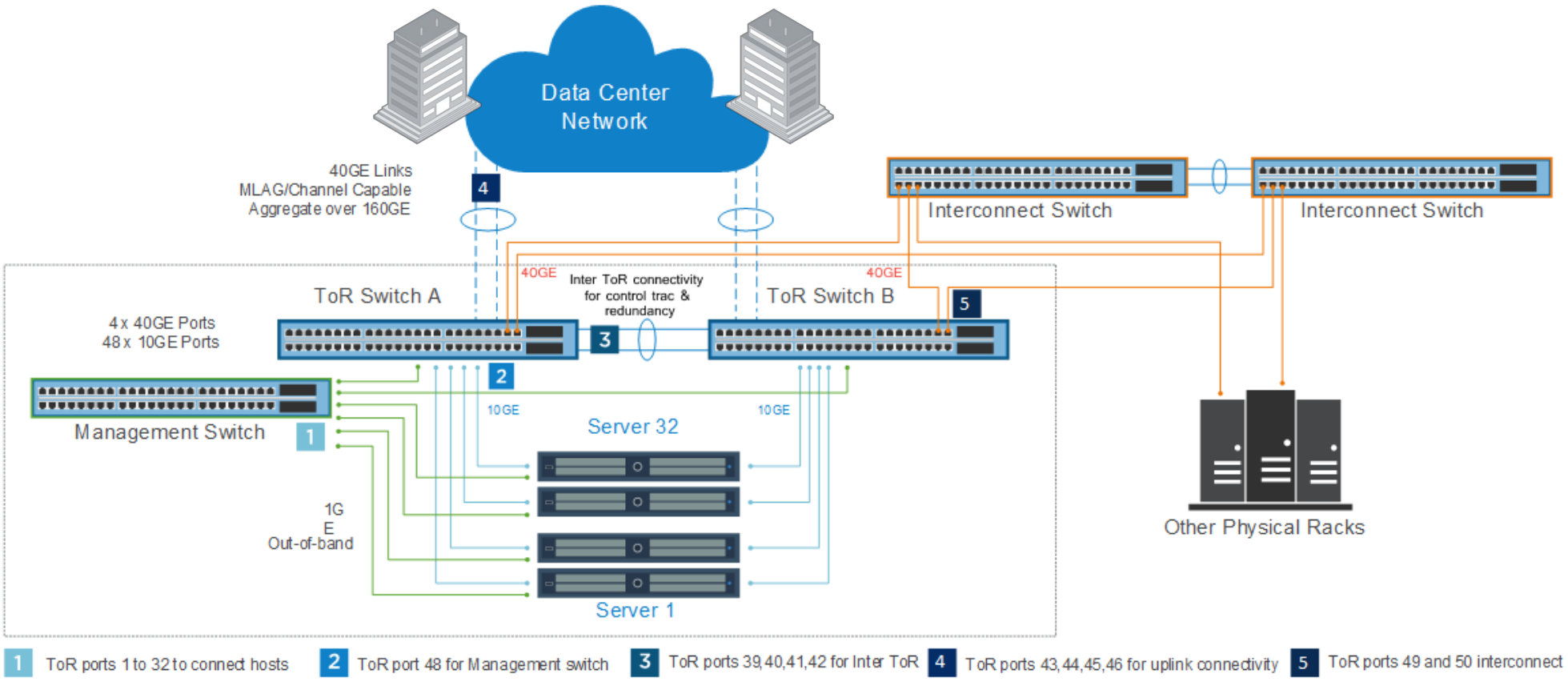
FORTINET

프라이빗 / 퍼블릭 클라우드 보안강화를 위한 포티넷 보안 구축 사례

포티넷 시큐리티 코리아
배준호 상무
2019년 2월 21일

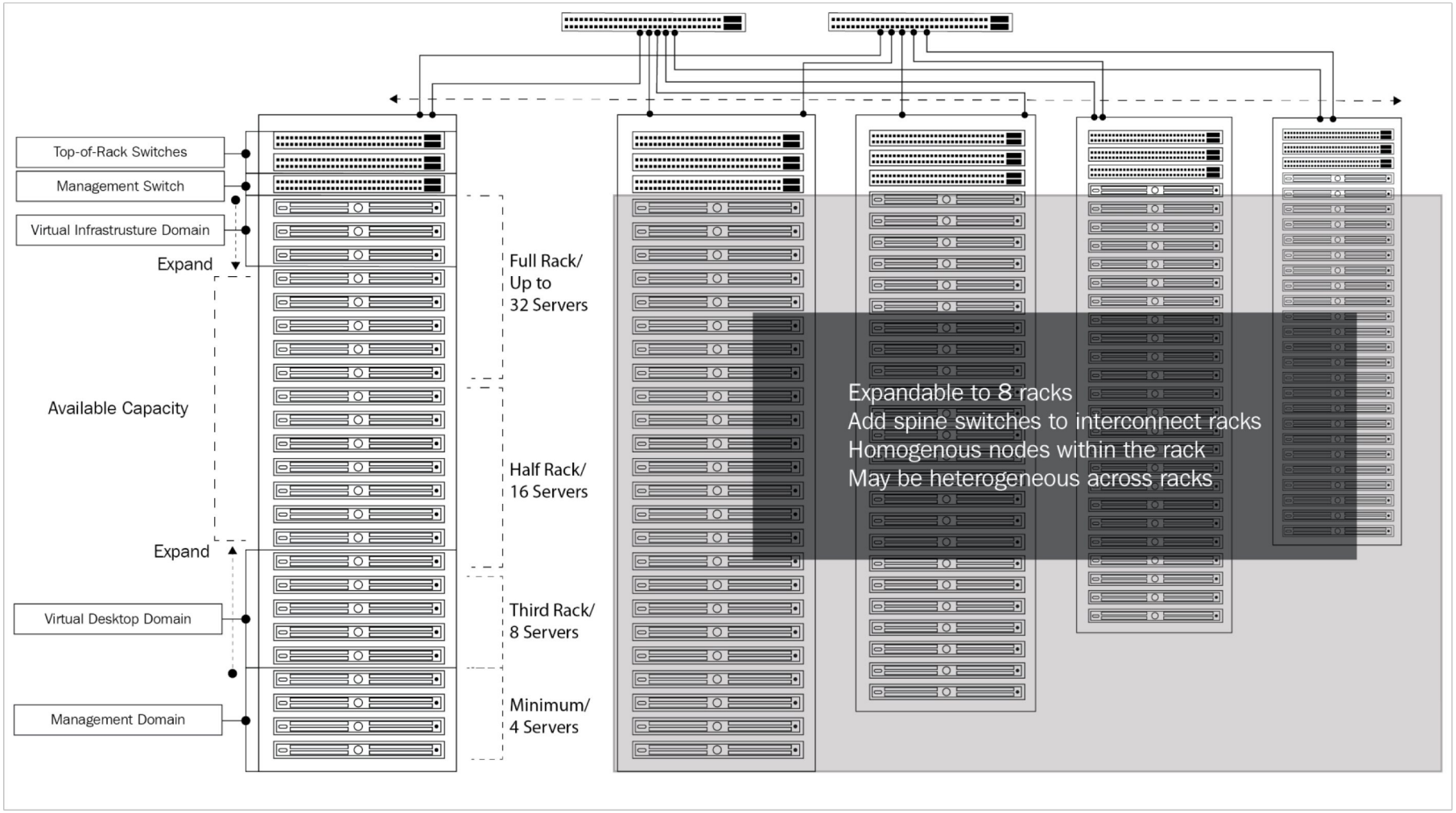
SDDC를 위한 프라이빗 클라우드 아키텍처와 포티넷 구축 사례

SDDC를 위한 프라이빗 클라우드의 물리적인 아키텍처 #1



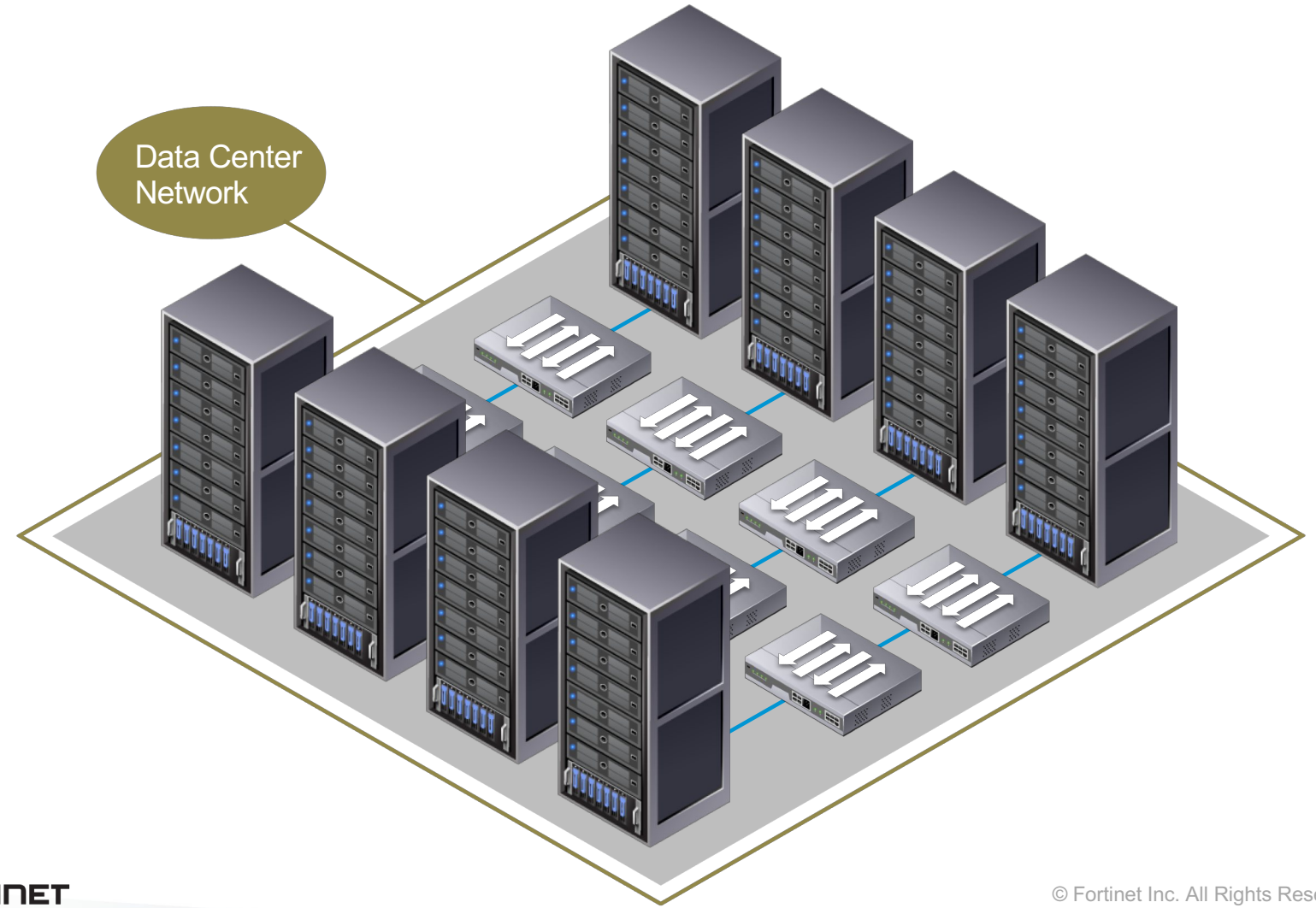
© Fortinet Inc. All Rights Reserved.

SDDC를 위한 프라이빗 클라우드의 물리적인 아키텍처 #2



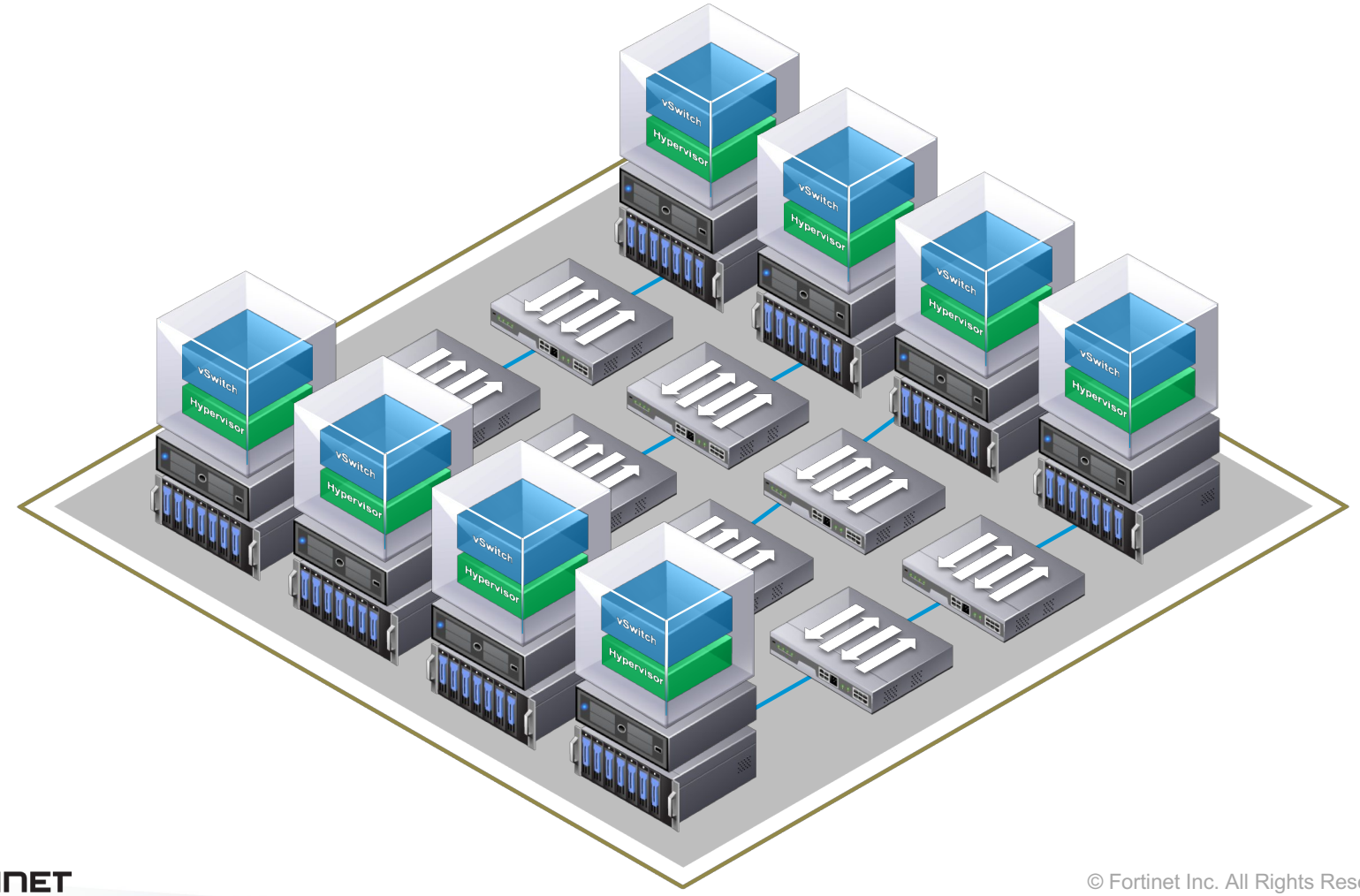
© Fortinet Inc. All Rights Reserved.

SDDC를 위한 프라이빗 클라우드의 물리적인 아키텍처 #3



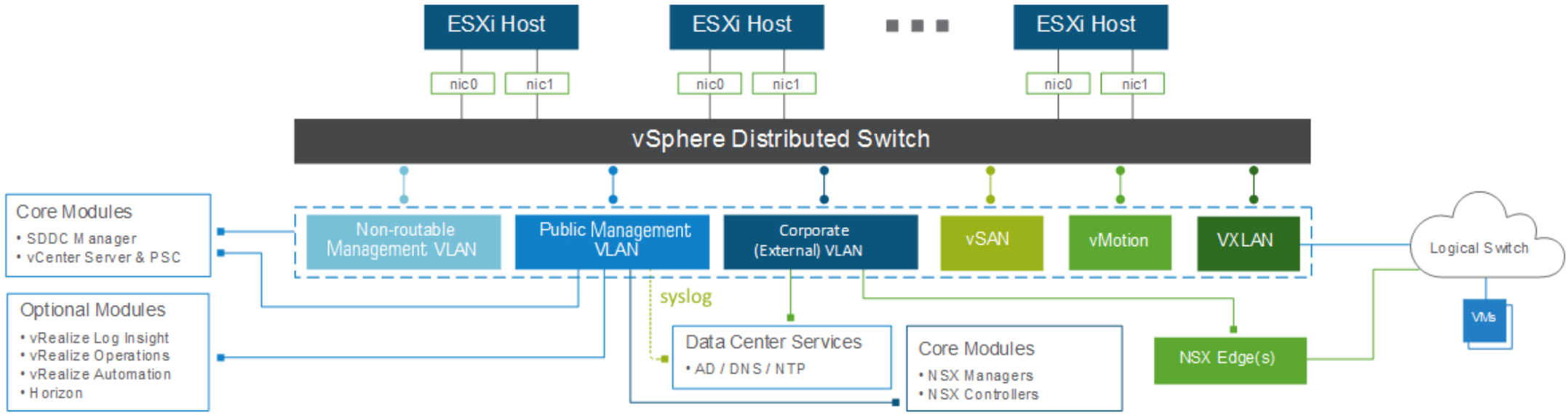
© Fortinet Inc. All Rights Reserved.

SDDC를 위한 프라이빗 클라우드의 논리적인 아키텍처 #1



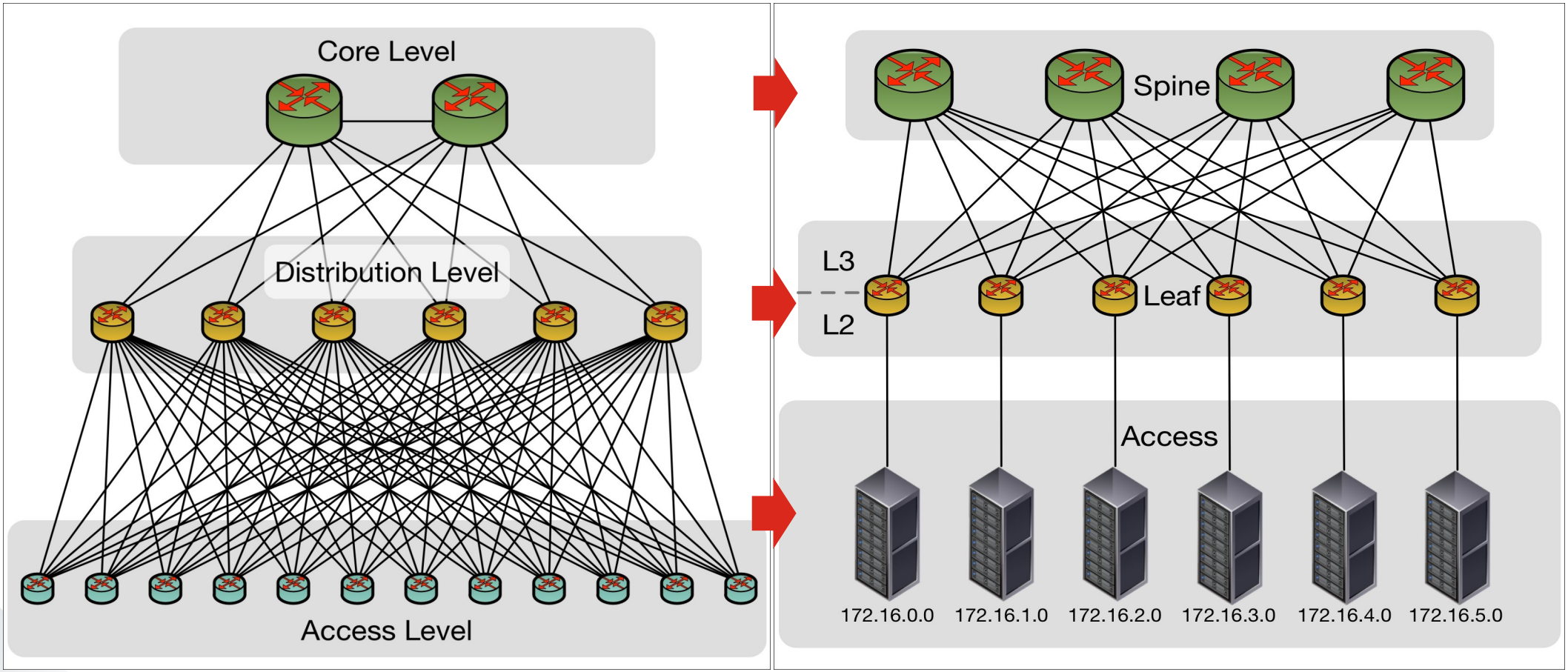
© Fortinet Inc. All Rights Reserved.

SDDC를 위한 프라이빗 클라우드의 논리적인 아키텍처 #2



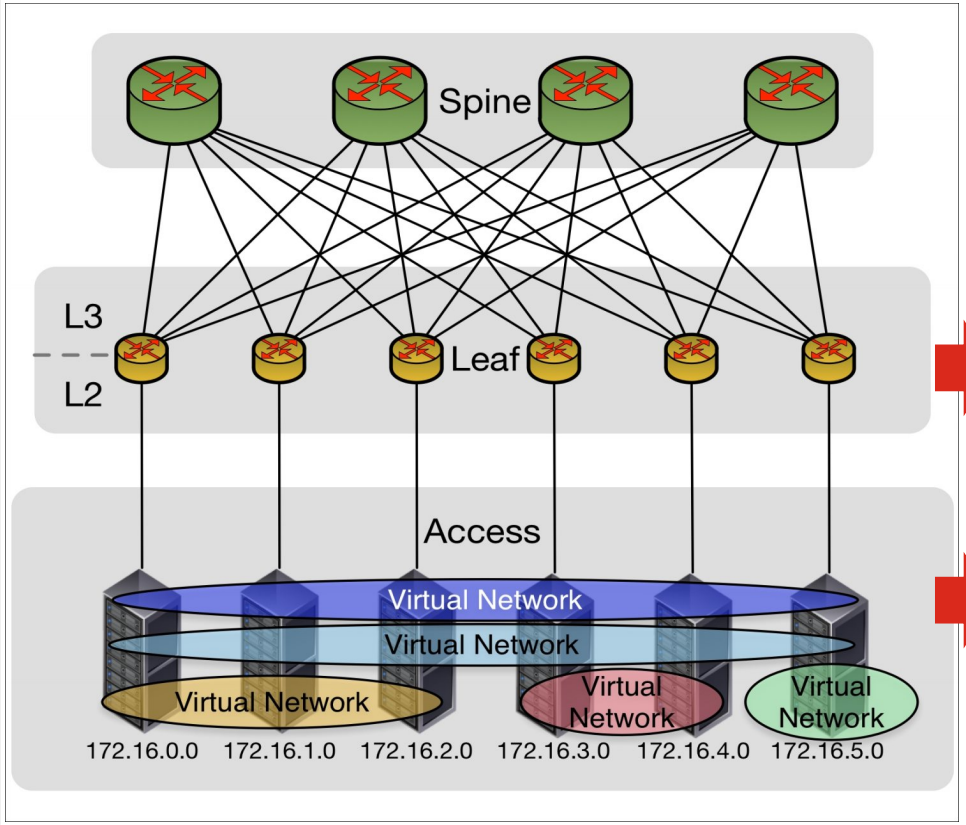
© Fortinet Inc. All Rights Reserved.

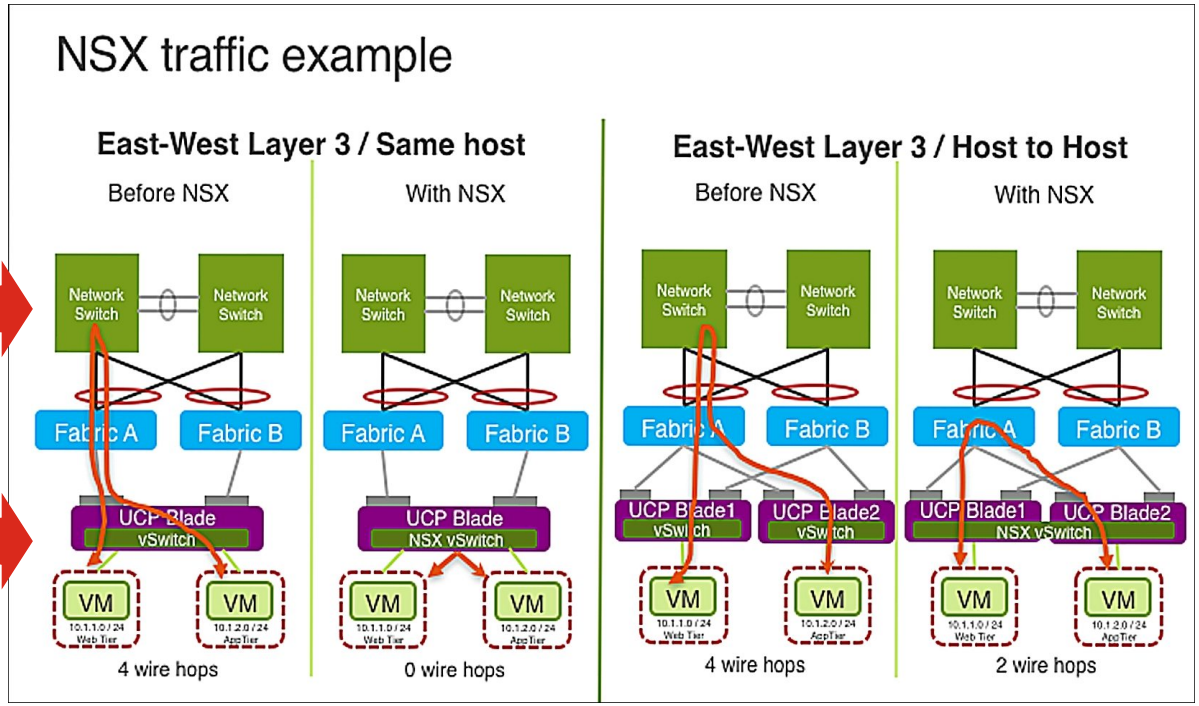
SDDC 네트워크 아키텍처의 변화 흐름 #1



© Fortinet Inc. All Rights Reserved.

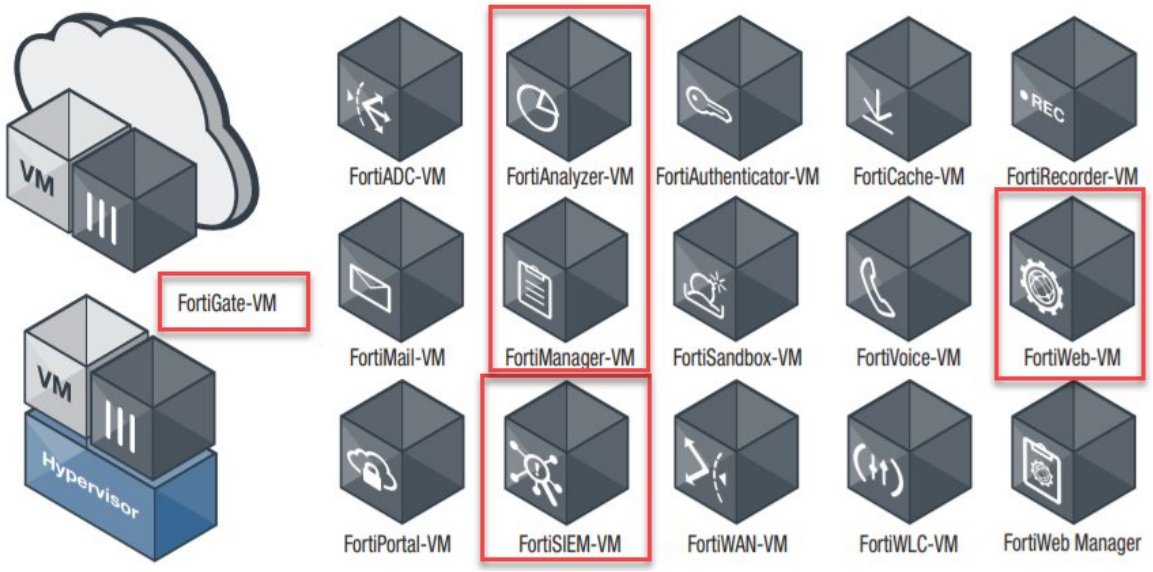
SDDC 네트워크 아키텍처의 변화 흐름 #2





© Fortinet Inc. All Rights Reserved.

SDDC 클라우드 보안 인프라를 위한 포티넷의 솔루션 지원



VM/NFV 가상머신 및 주요 보안 솔루션 구축 케이스:

-FortiGate-VM : 방화벽, 차세대방화벽(NGFW), 통합위협관리시스템 (UTM)

-FortiWeb-VM : 웹 방화벽

-FortiGate (VDOM, Virtual Domain): 멀티테넌트 지원을 위한 고속 저지연(low-latency) HW 어플라이언스 연동

-FortiGate : IPSec VPN 전용 게이트웨이

국내 고객 레퍼런스:
통신사, 항공사, 클라우드 사업자, e커너스 포탈, S그룹사 (폐쇄망), S금융계열사 등.

© Fortinet Inc. All Rights Reserved.

포티넷 SDN, NFV, 클라우드 구축 지원 범위

Public Cloud

- Amazon Web aws
- Azure/Azure Stack — Windows Azure
- Google GCP — Google Cloud
- Oracle OCI — ORACLE
- AliCloud — Alibaba Cloud

Private Cloud

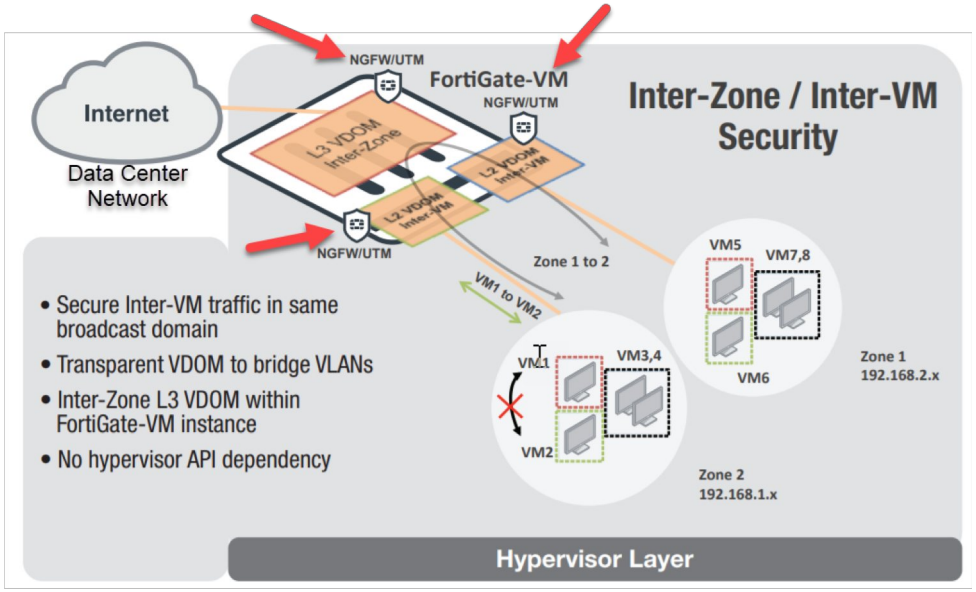
- VMWare ESXi — vmware ESXi
- VMWare NSX-V — vmware NSX
- Kernel Virtual — KVM
- Xen — Xen
- Microsoft Hyper-V — Microsoft Hyper-V Server

SDN Connector

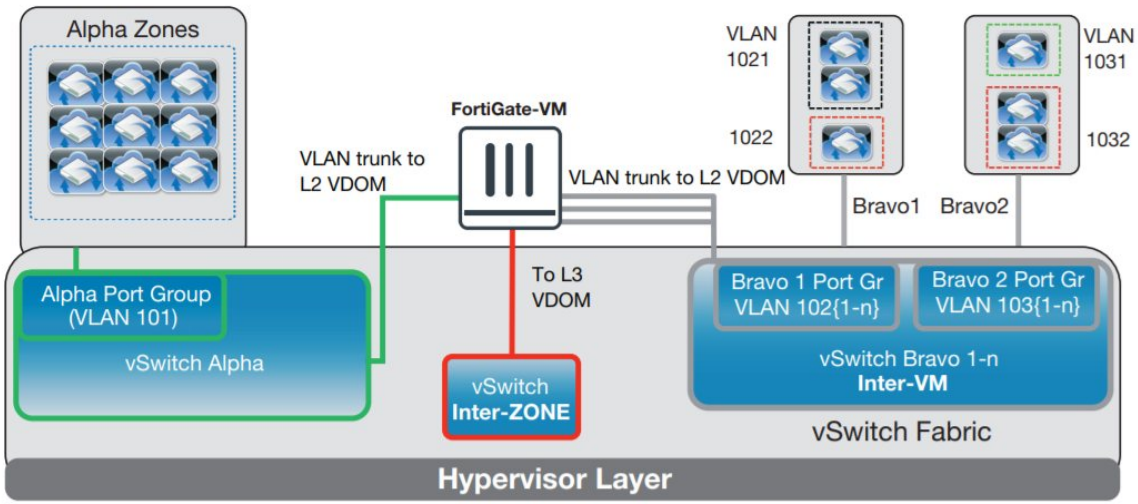
- Docker
- OpenStack — openstack
- Nutanix — NUTANIX
- CISCO ACI — CISCO
- Nuage VPC — nuagenetworks

© Fortinet Inc. All Rights Reserved.

SDDC 클라우드 인프라를 위한 포티넷 차세대방화벽(NGFW) / 통합위협관리시스템(UTM) 보안 아키텍처



- 동일 브로드캐스트 도메인 내, Inter-VM 트래픽 보안 적용.
- VLAN간 브릿지를 위한 Transparent VDOM 지원.
- FortiGate-VM 가상머신 내에서 Zone 간 연결 및 보안 적용을 위한 L3 VDOM 지원.
- 하이퍼 바이저 API 의존성 없음.



- Bravo Zones 영역의 모든 Inter-VM 트래픽은 L2 VDOM을 통해 전체 UTM 보안 검사를 받습니다.
- L3 VDOM에 의한 전체 차세대 방화벽 보안 및 UTM 보안 검사가 필요한 영역 간 트래픽 분리.
- Alpha Zone 영역의 VM은 보안 정책에 의해서 분리되어, 서로 제한없이 통신할 수 있습니다.

© Fortinet Inc. All Rights Reserved.

SDDC 클라우드 인프라에 적합한 FortiGate-VM (NGFW / UTM)의 고성능 제공

일반 방화벽 성능

IPSec VPN 성능

IPS 성능

Threat Protection 성능

	FORTIGATE-VM00	FORTIGATE-VM01/01V	FORTIGATE-VM02/02V	FORTIGATE-VM04/04V
Firewall Throughput (UDP Packets)	12 Gbps	12 Gbps	15 Gbps	28 Gbps
Concurrent Sessions (TCP)	1.0 Million	1.0 Million	2.6 Million	4.3 Million
New Sessions / Second (TCP)	85,000	85,000	100,000	125,000
IPsec VPN Throughput (AES256+SHA1, 512 Byte)	1 Gbps	1 Gbps	1.5 Gbps	3 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000	2,000	2,000	2,000
Client-to-Gateway IPsec VPN Tunnels	6,000	6,000	12,000	20,000
SSL-VPN Throughput	800 Mbps	800 Mbps	830 Mbps	2 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	1,000	1,000	2,000	4,500
IPS Throughput (HTTP / Enterprise Mix) [1]	3.5 Gbps / 1 Gbps	3.5 Gbps / 1 Gbps	5.5 Gbps / 1.5 Gbps	8 Gbps / 3 Gbps
Application Control Throughput [2]	2 Gbps	2 Gbps	2.6 Gbps	4.5 Gbps
NGFW Throughput [3]	850 Mbps	850 Mbps	1.5 Gbps	2.5 Gbps
Threat Protection Throughput [4]	700 Mbps	700 Mbps	1.2 Gbps	2 Gbps

	FORTIGATE-VM08/08V	FORTIGATE-VM16/16V	FORTIGATE-VM32/32V	FORTIGATE-VMUL/ULV
Firewall Throughput (UDP Packets)	33 Gbps	36 Gbps	50 Gbps	
Concurrent Sessions (TCP)	8.5 Million	18.0 Million	38.0 Million	
New Sessions / Second (TCP)	150,000	175,000	200,000	
IPsec VPN Throughput (AES256+SHA1, 512 Byte)	5.5 Gbps	6.5 Gbps	7 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40,000	40,000	40,000	
Client-to-Gateway IPsec VPN Tunnels	40,000	50,000	64,000	
SSL-VPN Throughput	4.5 Gbps	8.5 Gbps	8.6 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum)	10,000	25,000	40,000	
IPS Throughput (HTTP / Enterprise Mix) [1]	15.5 Gbps / 6 Gbps	25 Gbps / 12 Gbps	29 Gbps / 19 Gbps	
Application Control Throughput [2]	9 Gbps	17 Gbps	17.5 Gbps	
NGFW Throughput [3]	4.5 Gbps	9 Gbps	16.5 Gbps	
Threat Protection Throughput [4]	3.5 Gbps	7 Gbps	13 Gbps	

2019년 2월 기준 성능 데이터

FORTINET

© Fortinet Inc. All Rights Reserved.

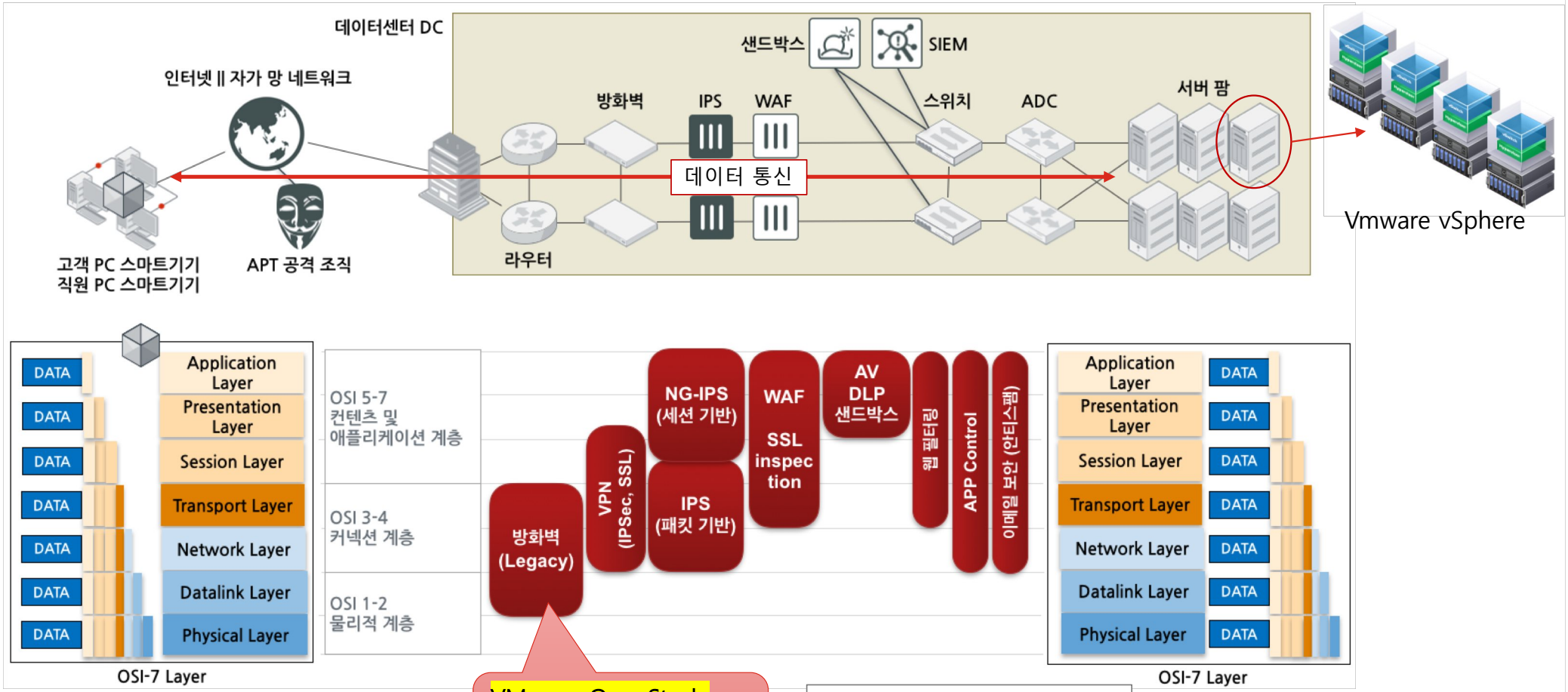
WHY?

VMware, OpenStack과 같은 플랫폼에서 제공하는 기본 보안 기능이 있는데,

"왜 포티넷과 같은 전문 보안 벤더 솔루션 도입이 필요한가?"

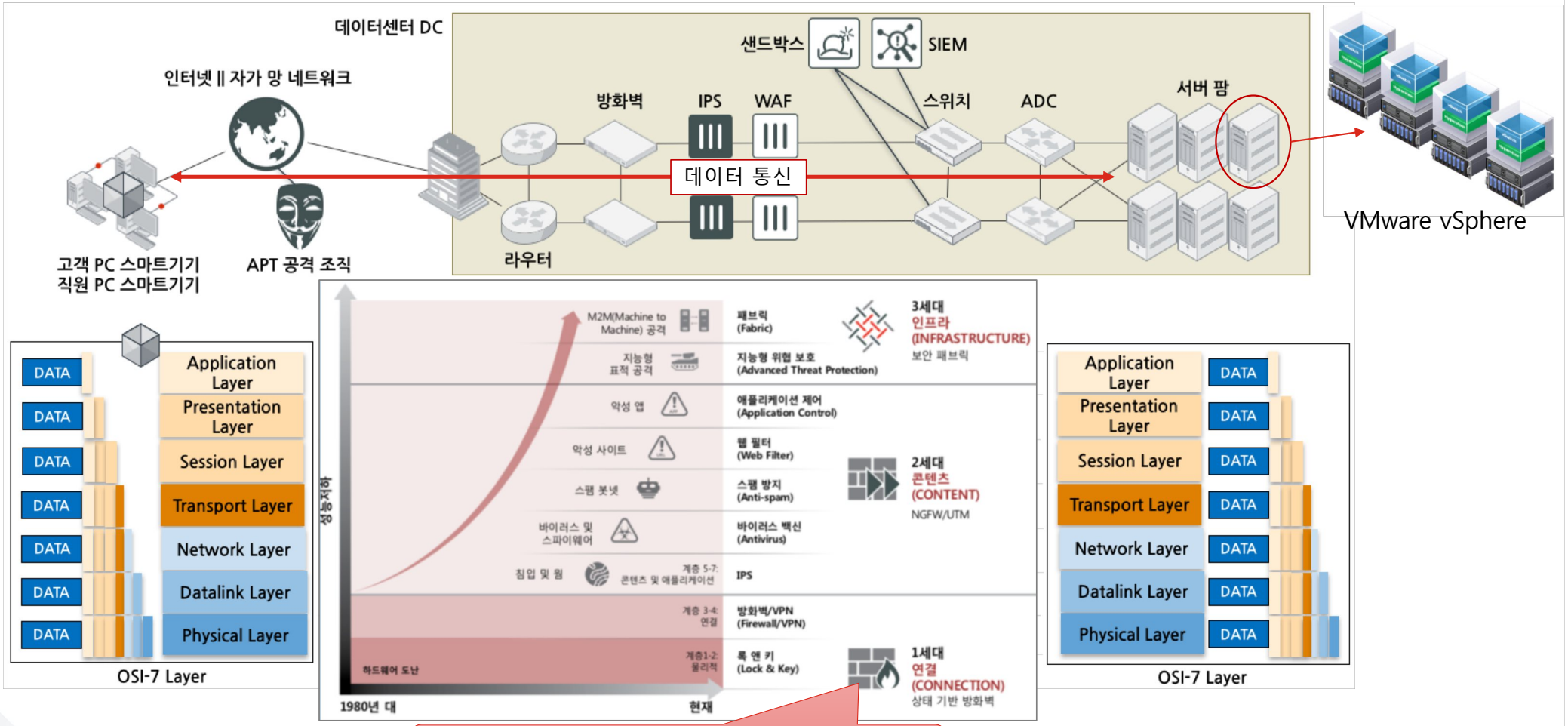
© Fortinet Inc. All Rights Reserved.

멀티-레이어드 (Multi-Layered) 보안 시스템 필요성 #1



Inc. All Rights Reserved.

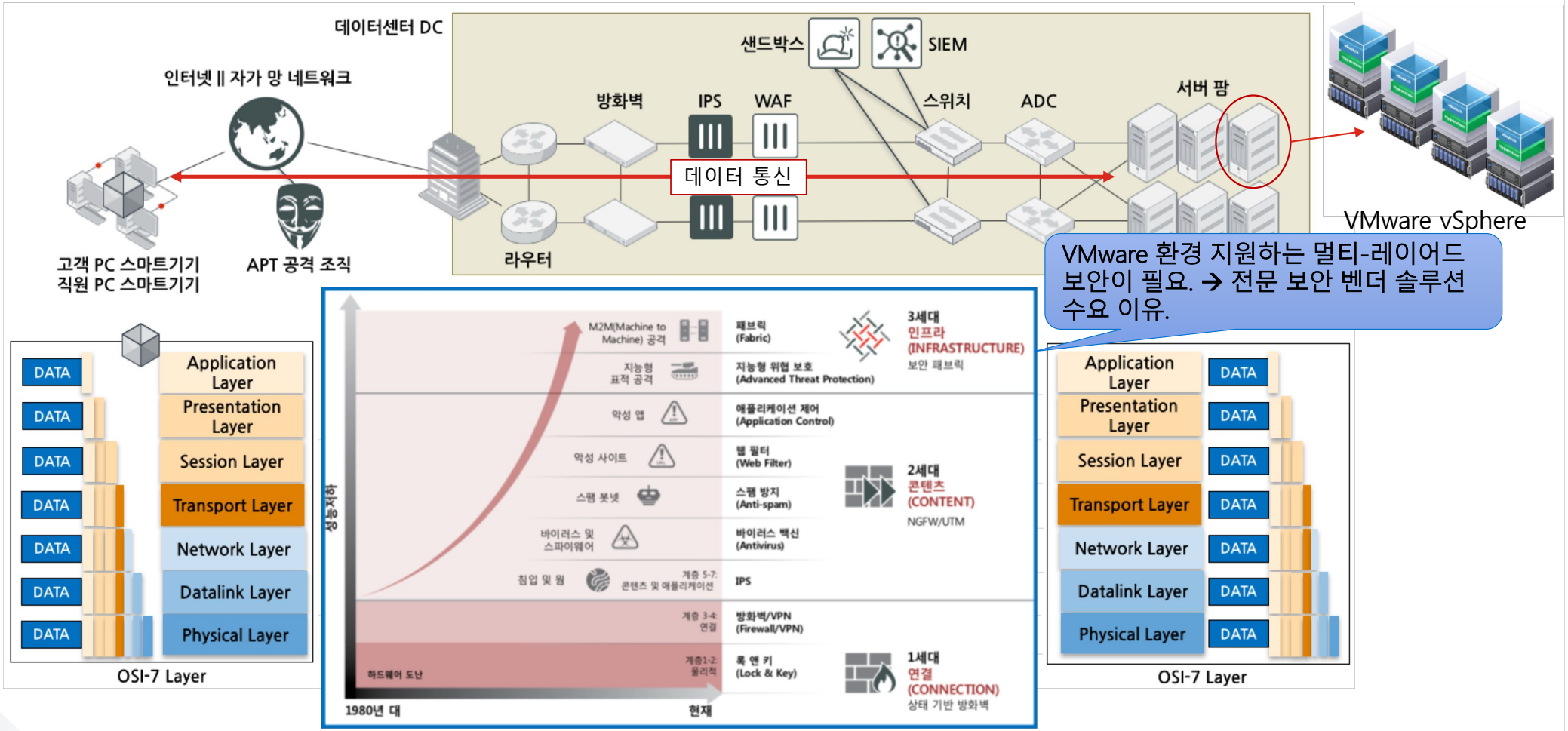
멀티-레이어드 (Multi-Layered) 보안 시스템 필요성 #2



VMware vSphere에서 제공하는 기본 보안 기능:
MAC주소/Port/IP 주소 기반의 커넥션 제어

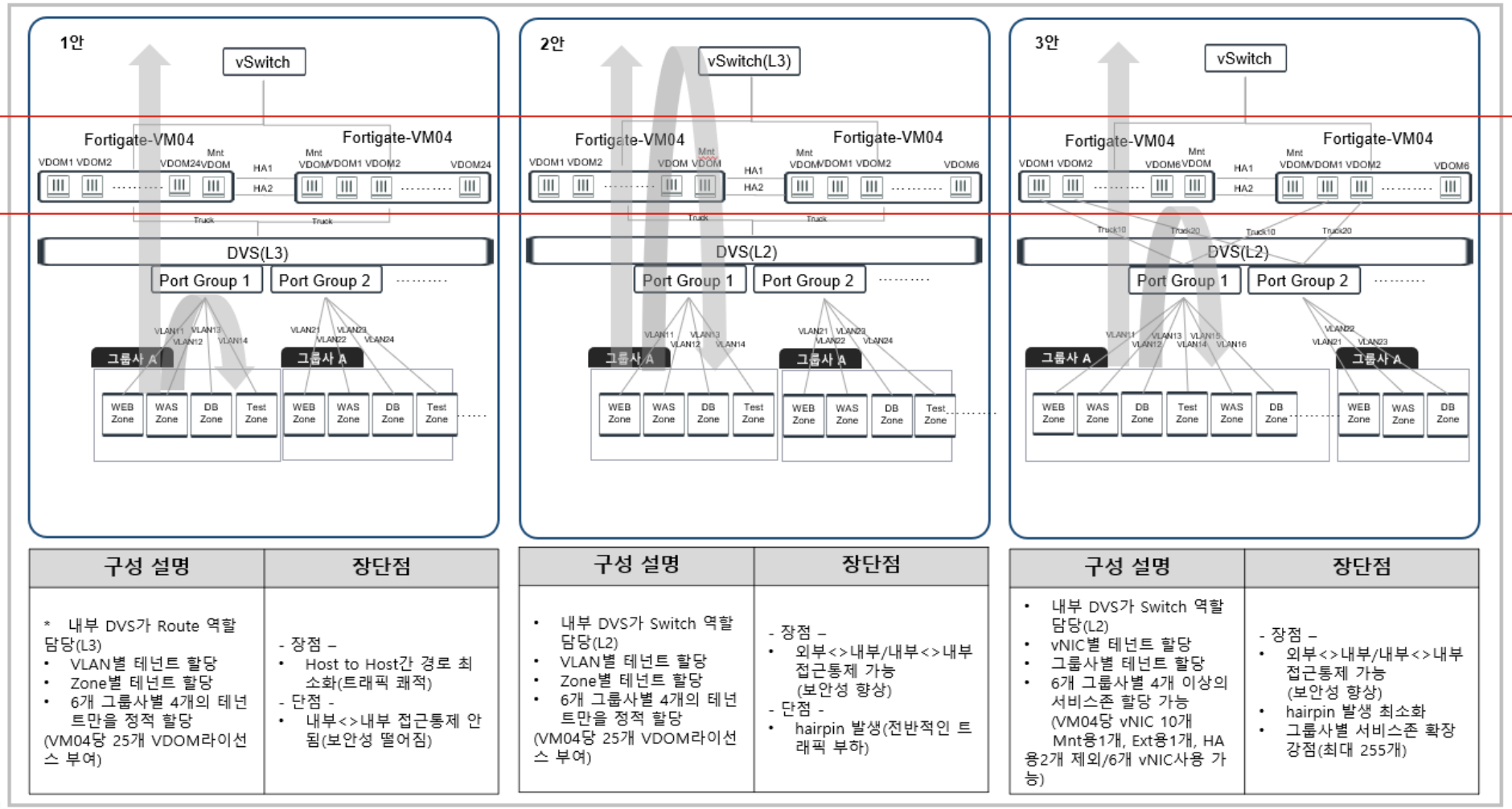
© Fortinet Inc. All Rights Reserved.

멀티-레이어드 (Multi-Layered) 보안 시스템 필요성 #3



© Fortinet Inc. All Rights Reserved.

SDDC 프라이빗 클라우드 국내 엔터프라이즈 고객 구축 사례 (VMware)



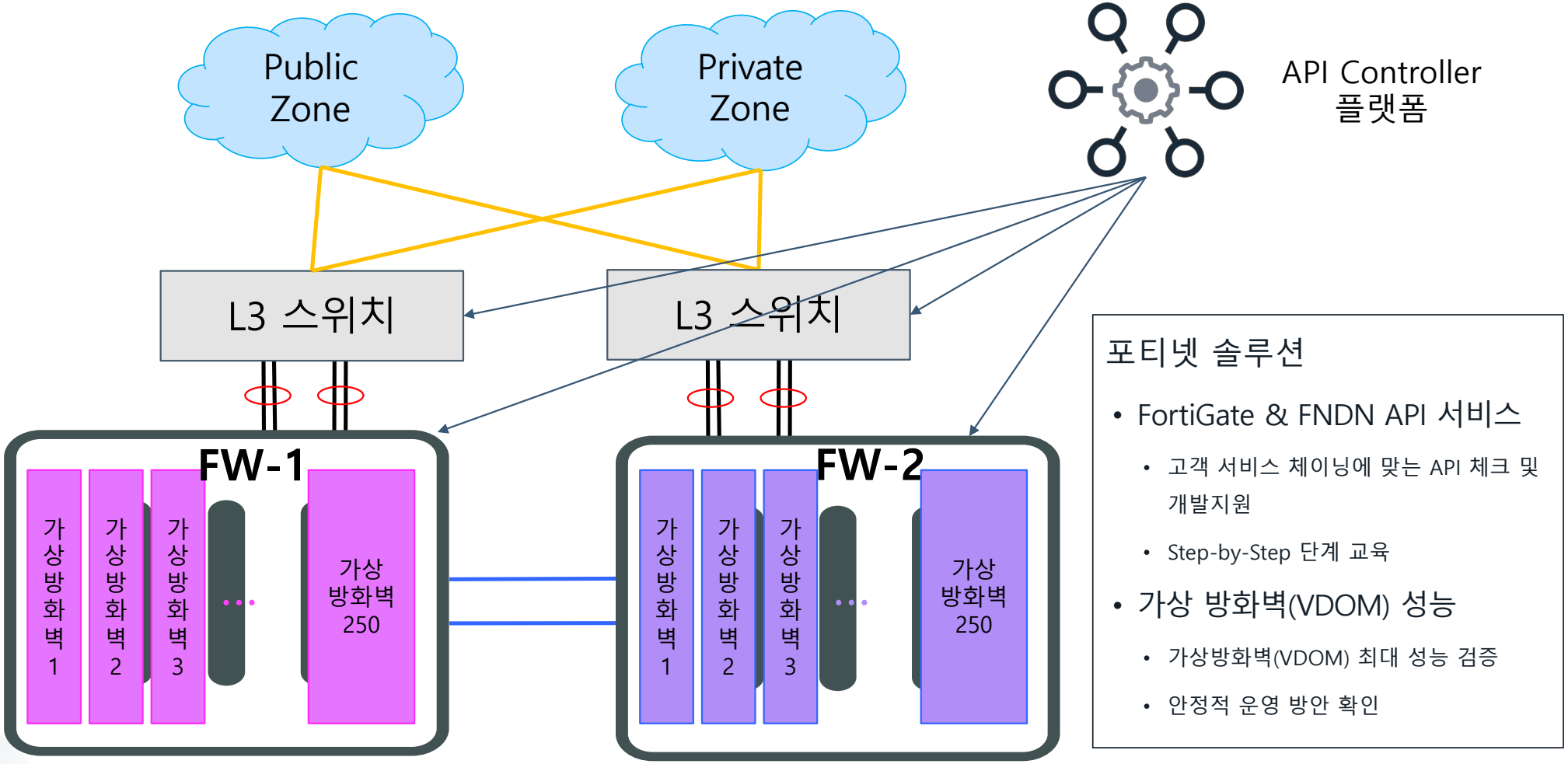
구성 설명	장단점
* 내부 DVS가 Route 역할 담당(L3) • VLAN별 테넌트 할당 • Zone별 테넌트 할당 • 6개 그룹사별 4개의 테넌트만을 정적 할당 (VM04당 25개 VDOM라이선스 부여)	- 장점 – • Host to Host간 경로 최소화(트래픽 쾌적) - 단점 - • 내부<>내부 접근통제 안됨(보안성 떨어짐)

구성 설명	장단점
• 내부 DVS가 Switch 역할 담당(L2) • VLAN별 테넌트 할당 • Zone별 테넌트 할당 • 6개 그룹사별 4개의 테넌트만을 정적 할당 (VM04당 25개 VDOM라이선스 부여)	- 장점 – • 외부<>내부/내부<>내부 접근통제 가능 (보안성 향상) - 단점 - • hairpin 발생(전반적인 트래픽 부하)

구성 설명	장단점
• 내부 DVS가 Switch 역할 담당(L2) • vNIC별 테넌트 할당 • 그룹사별 테넌트 할당 • 6개 그룹사별 4개 이상의 서비스존 할당 가능 (VM04당 vNIC 10개 Mnt용1개, Ext용1개, HA용2개 제외/6개 vNIC사용 가능)	- 장점 – • 외부<>내부/내부<>내부 접근통제 가능 (보안성 향상) • hairpin 발생 최소화 • 그룹사별 서비스존 확장 강점(최대 255개)

© Fortinet Inc. All Rights Reserved.

국내 통신사 Private Cloud SDN 플랫폼

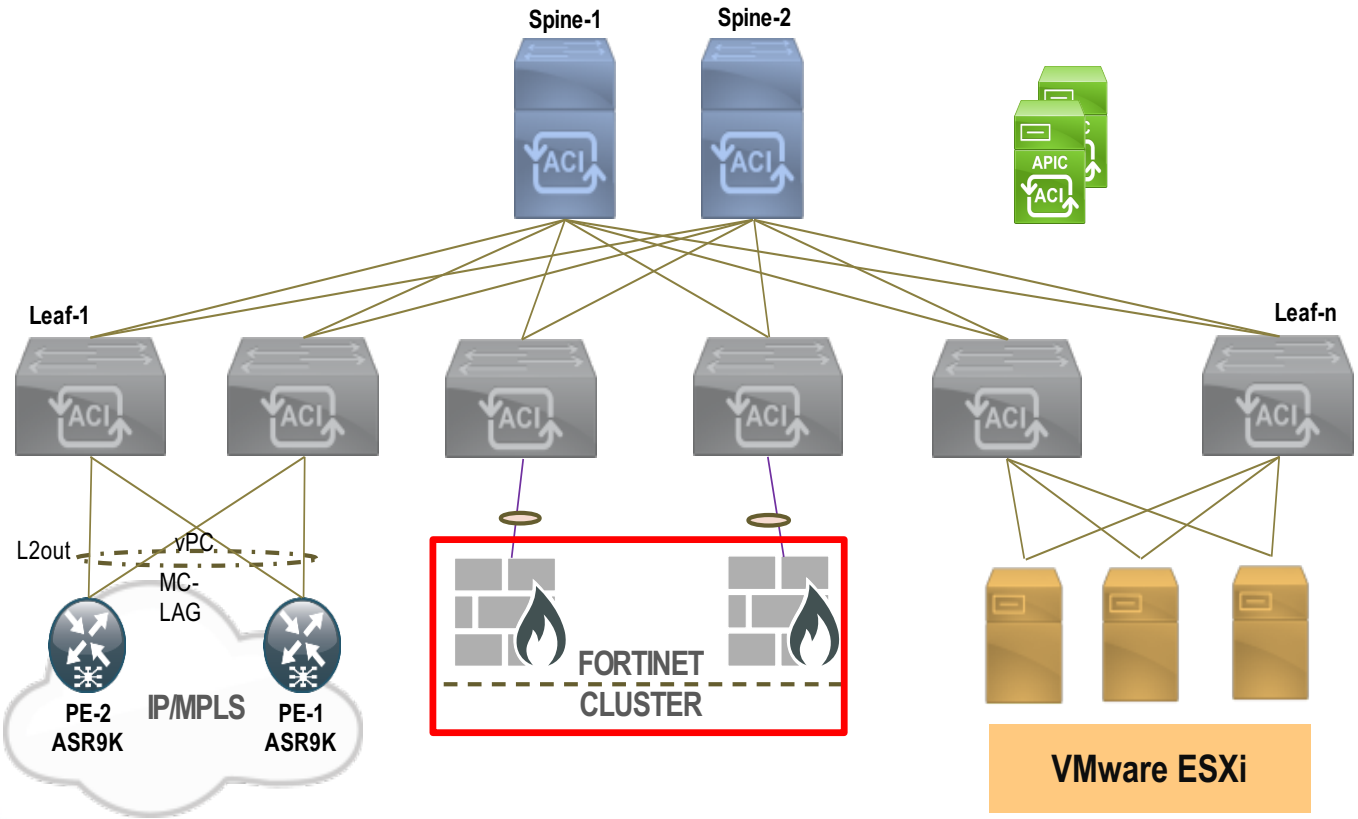


포티넷 솔루션

- FortiGate & FNDN API 서비스
  - 고객 서비스 체이닝에 맞는 API 체크 및 개발지원
  - Step-by-Step 단계 교육
- 가상 방화벽(VDOM) 성능
  - 가상방화벽(VDOM) 최대 성능 검증
  - 안정적 운영 방안 확인

© Fortinet Inc. All Rights Reserved.

국내 통신사 Private SDN 플랫폼

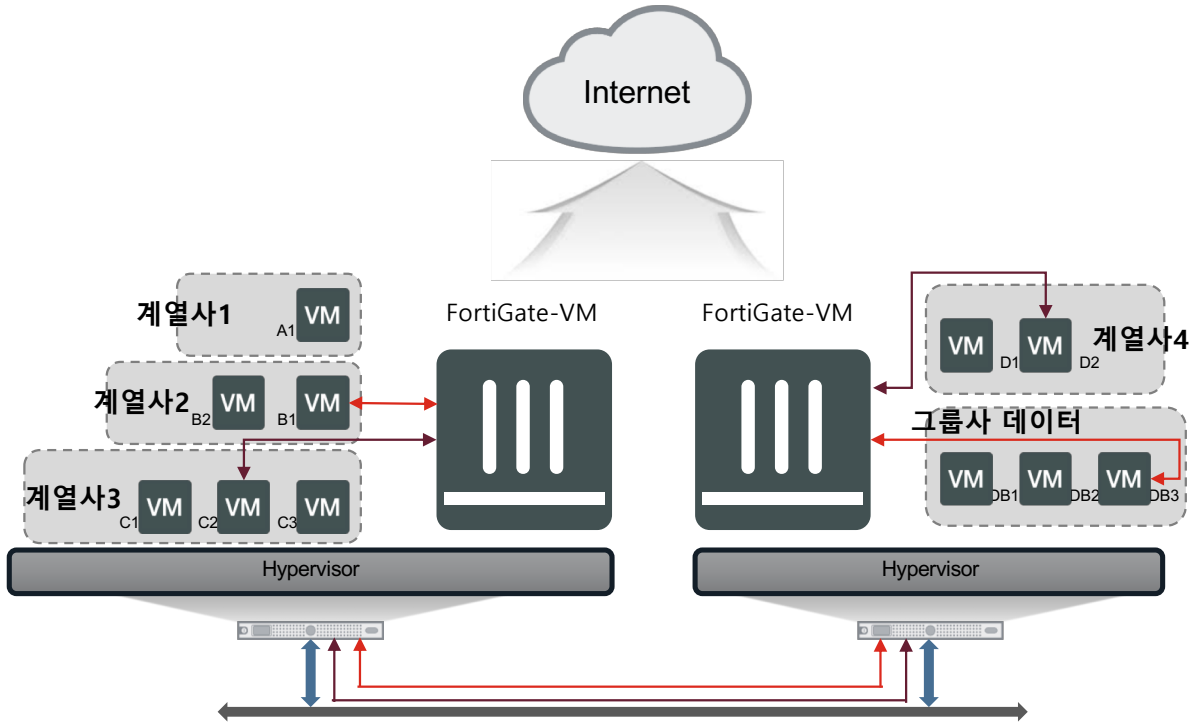


- 포티넷 솔루션
  - » FortiGate Connector
    - Cisco ACI 플랫폼과의 유연한 연동
  - » 구축 경험을 통한 모범사례 지원
    - Cisco ACI 플랫폼과 연동하는 PoC / BMT진행
    - 본사 Demo센터 및 플랫폼 학습

© Fortinet Inc. All Rights Reserved.

국내 대기업 SDN 플랫폼

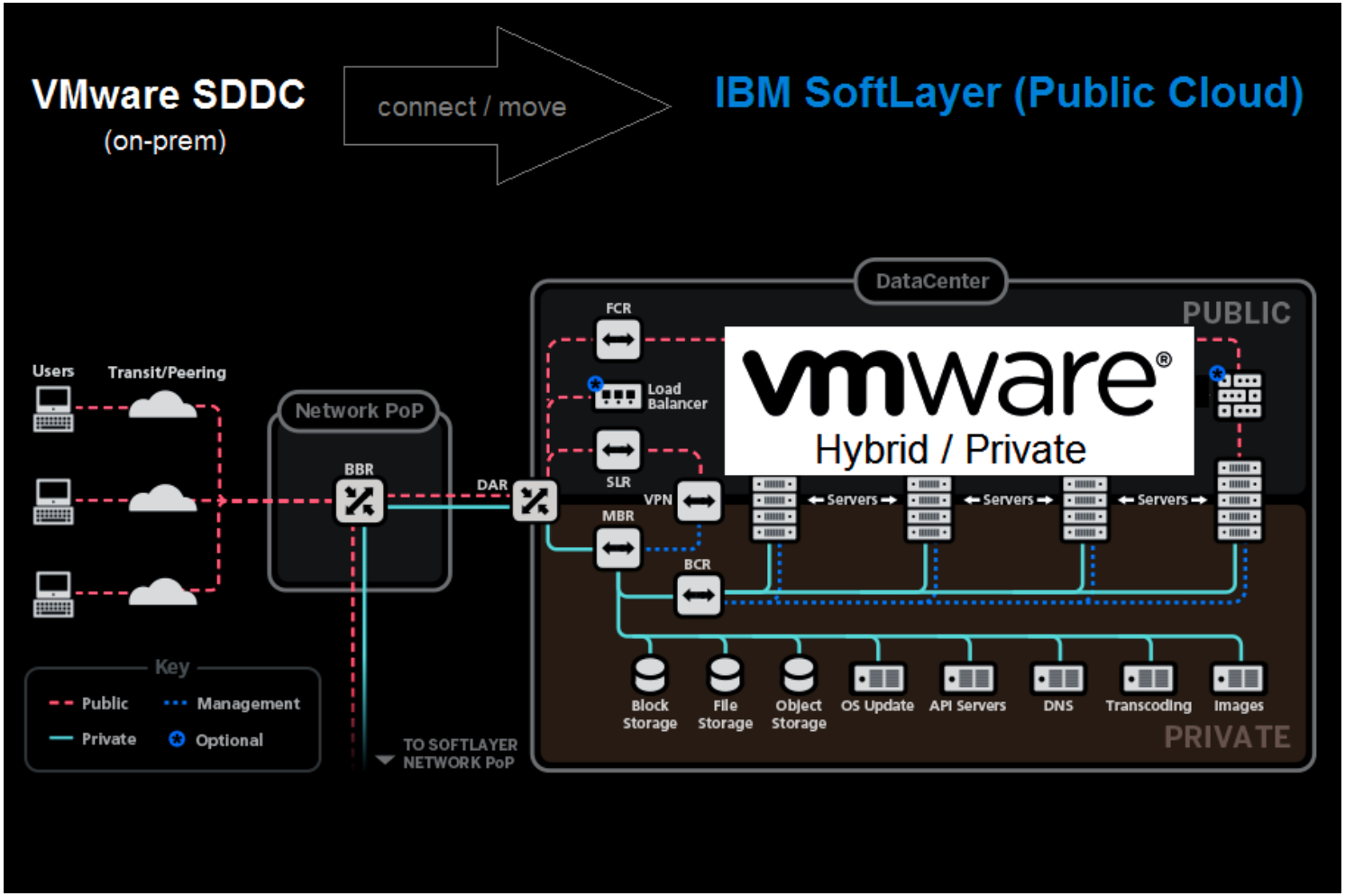
- 포티넷 솔루션
  - FortiGate-VM
    - VMware 기반에 적용
  - 그룹사 TF팀과 긴밀한 밀착 지원
    - PoC를 통한 결과 적용
    - Korea Demo센터를 이용한 Mirror 테스트
    - 수용 서비스(그룹사) 에 맞는 세그먼트 프랫폼 제공



계열사-> 인터넷 통신 트래픽: FortiGate-VM 차세대방화벽 보안 정책 적용
계열사 -> 계열사 통신 트래픽: 그룹사 데이터의 경우 FortiGate-VM 정책 바이패스 적용

© Fortinet Inc. All Rights Reserved.

국내 클라우드 사업자 SDN 플랫폼 #1

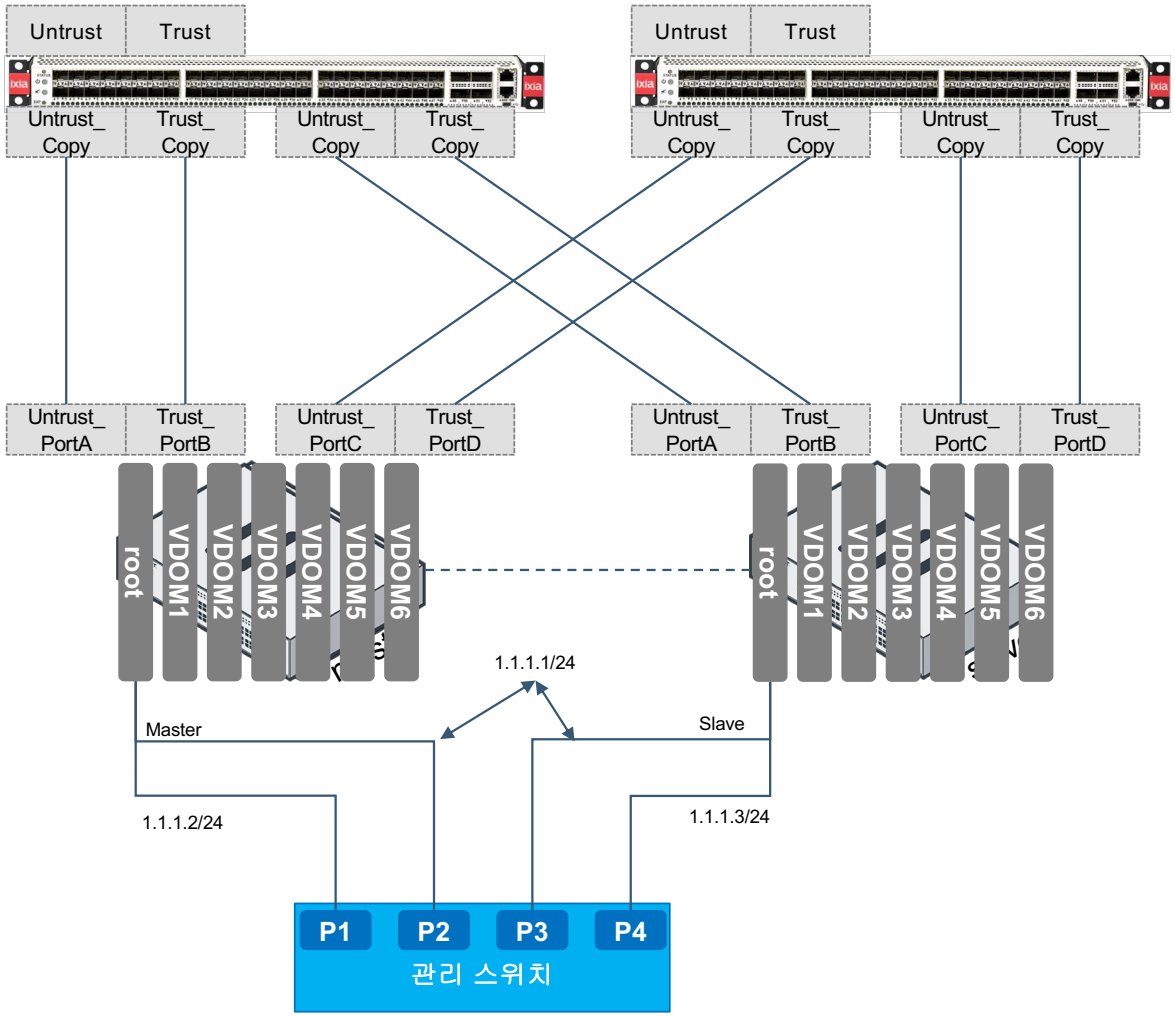


© Fortinet Inc. All Rights Reserved.

국내 클라우드 사업자 SDN 플랫폼 #2

포티넷 솔루션

- FortiGate HW 기반의 가상 방화벽 제공
  - 장점 1. Low-latency
  - 장점 2. 대용량 트래픽 수용 가능
- API 서버를 통한 관리 적용
- 공공 클라우드 고객 수용

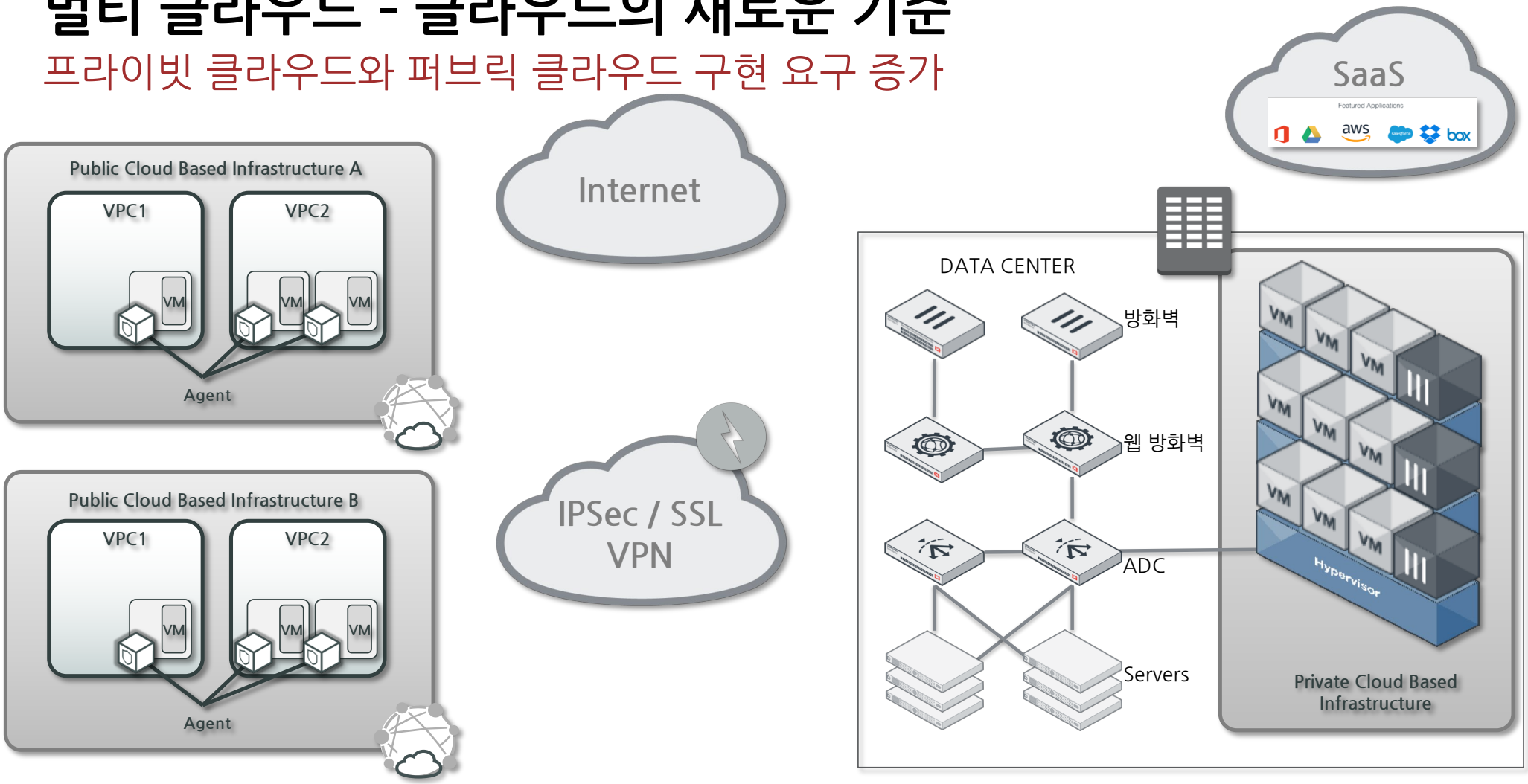


© Fortinet Inc. All Rights Reserved.

멀티-클라우드 보안 Use-Cases

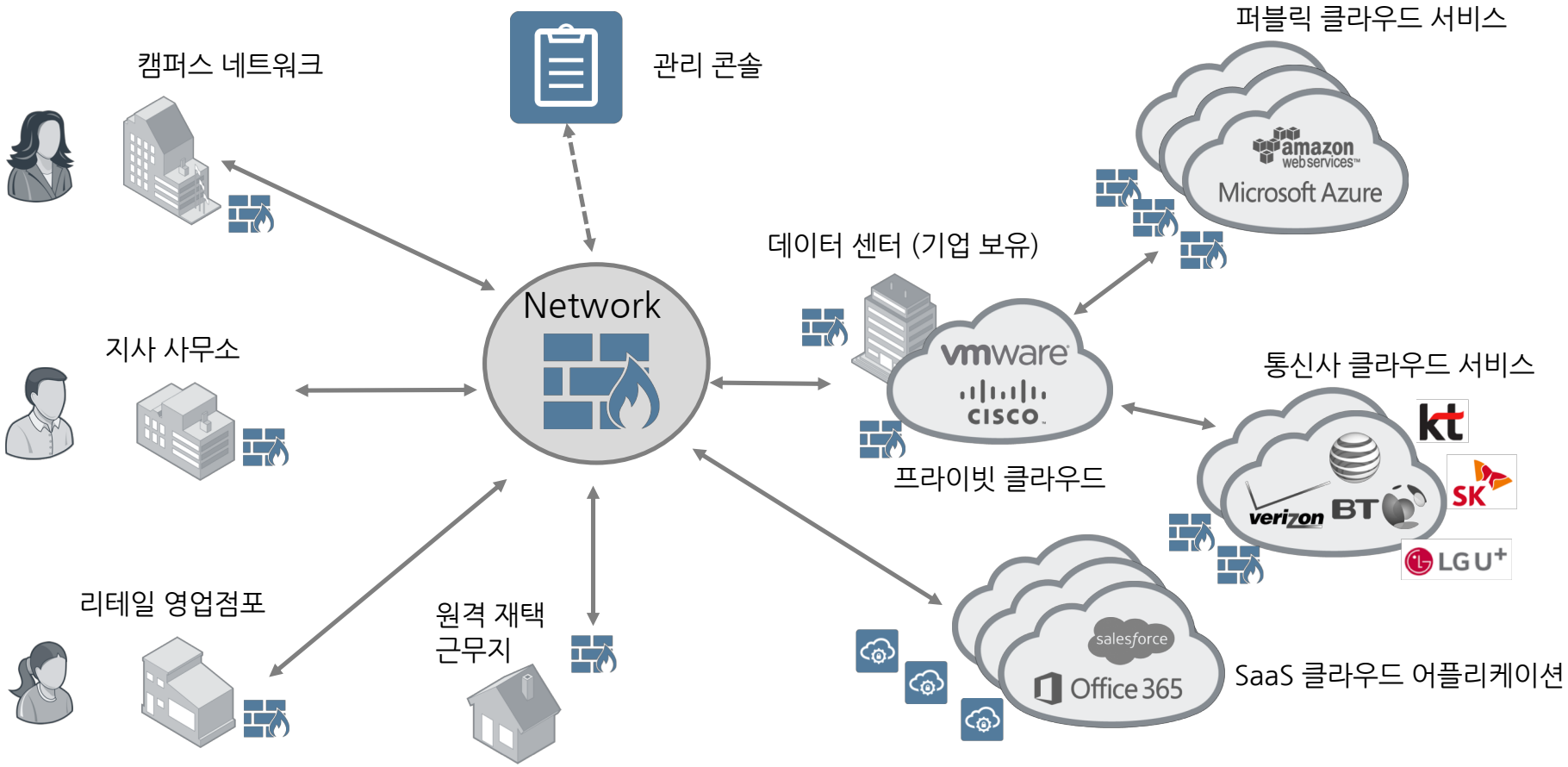
멀티 클라우드 - 클라우드의 새로운 기준

프라이빗 클라우드와 퍼브릭 클라우드 구현 요구 증가

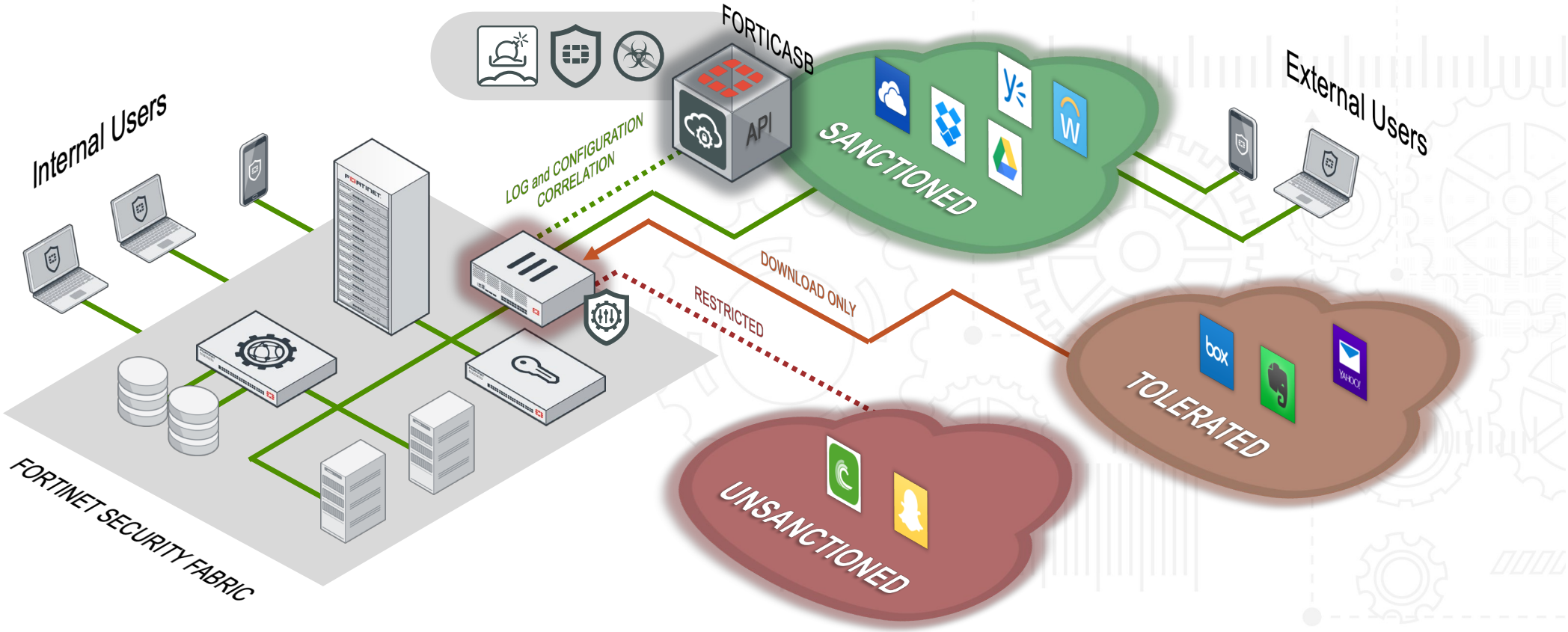


이슈: 사이버 보안 위협으로부터 보호해야 할 영역의 확대

보안 위협의 다양한 유입 경로, 고도화된 공격 방식

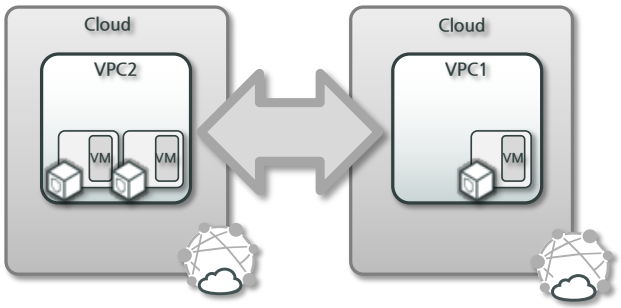


FortiCASB 솔루션 - 클라우드 SAAS 애플리케이션에 대한 보안 감사 & DLP & GDPR 컴플라이언스 감사



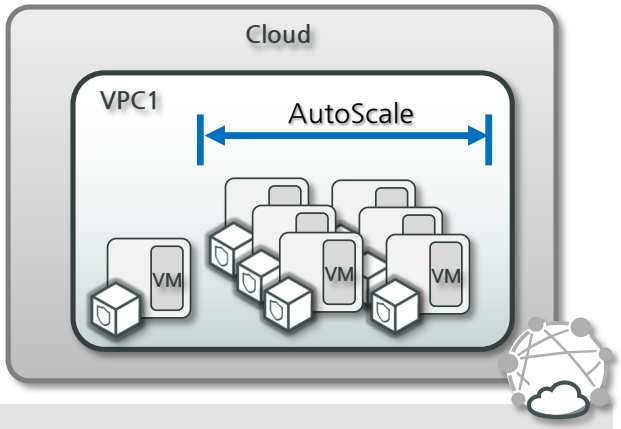
멀티 클라우드 보안 이슈

클라우드간 통신의 증가



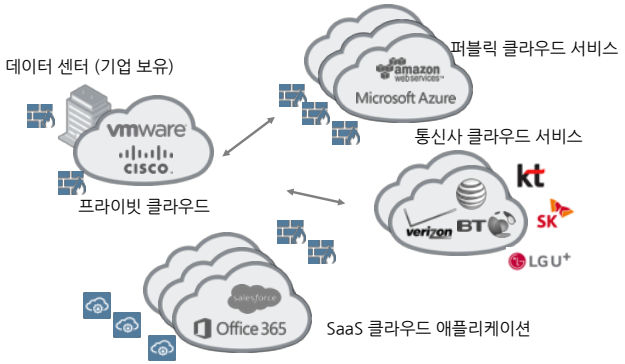
- 클라우드 커뮤니케이션 증가
- 연동되는 **엔드 포인트간의 복잡성 증가**

급격한 인프라 환경 변화



- Auto Scale등의 빈번한 인프라 변화 → **수동 제어의 한계** 발생
- 일관된 보안 정책 수립의 어려움

확대된 보안 대상 영역



- 증가한 인프라에 대한 **가시성 확보**의 어려움
- 정보 교류 및 **확대된 Attack Surface** 보호
- **Shadow IT** 환경 제어

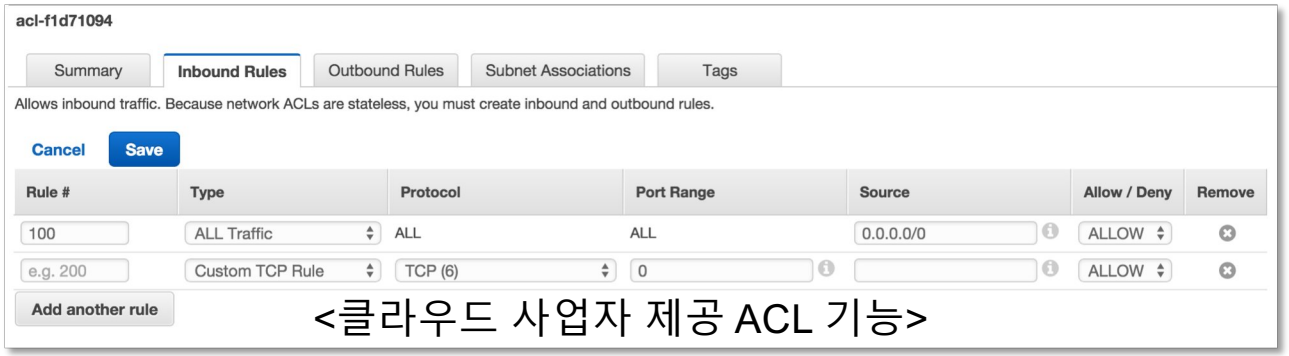
클라우드 사업자에서 제공하는 보안 기능의 보호 영역

인스턴스 보안

분산된 관리 패널

- 서브넷, 인스턴스 단위 제어
- Stateful 방화벽
  - VPC당 갯수 제한.
  - 허용 정책 기반 동작
- 네트워크 ACL
  - Top Down 방식
  - 양방향 정책 필요
  - 허용/차단 기반 동작
- 로그 및 정책 관리의 어려움

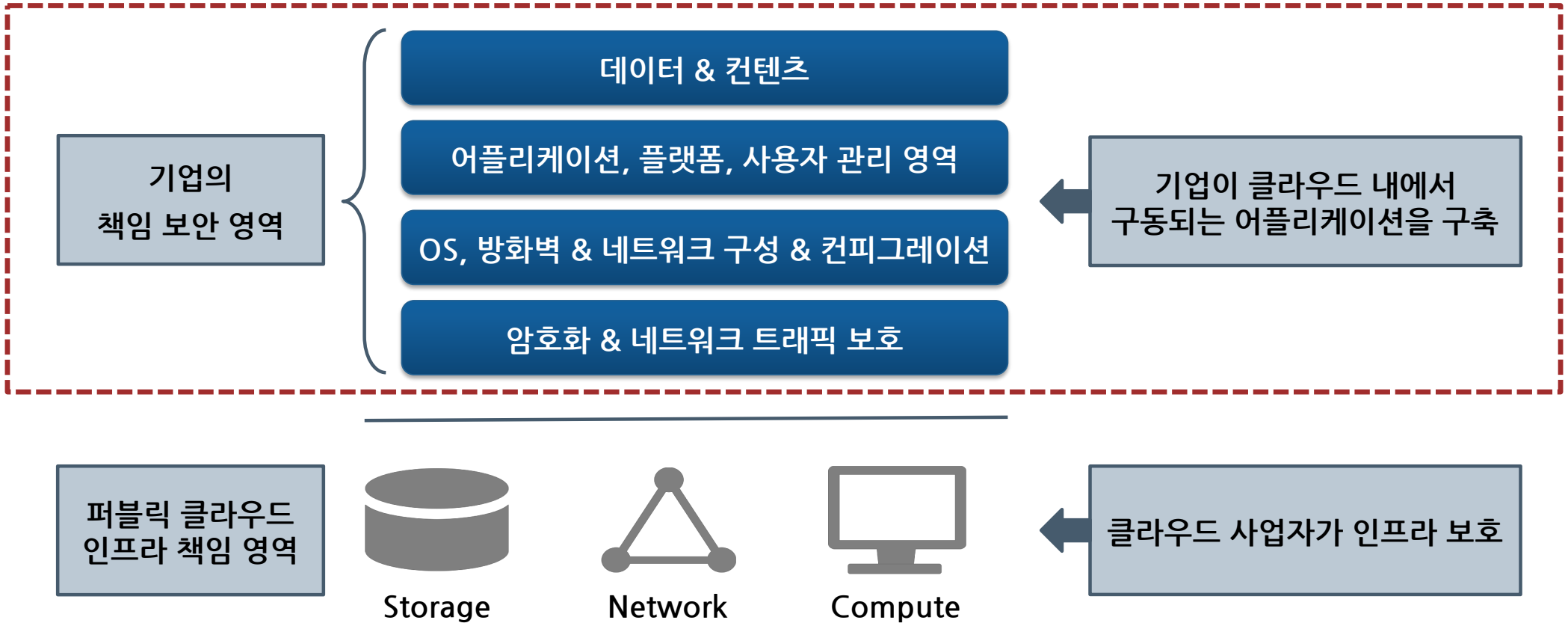
<클라우드 사업자 제공 방화벽 기능>



<클라우드 사업자 제공 ACL 기능>

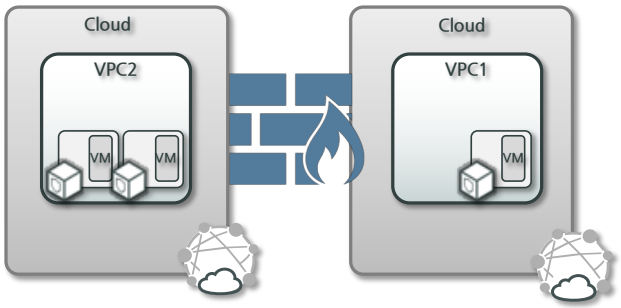
클라우드 사업자와 기업간의 책임 공유 모델

인스턴스 보안



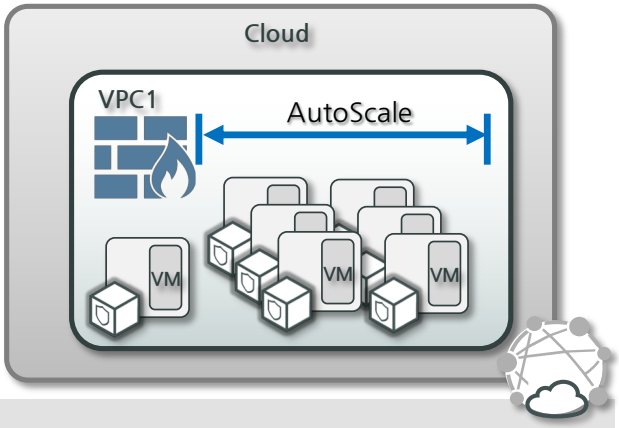
멀티 클라우드 보안 전략

인프라 경계 제어



- 연동 **경로에서 커뮤니케이션 제어**
- 기업의 데이터 영역, 컨텐츠 영역 보안

자동화 및 통합관리

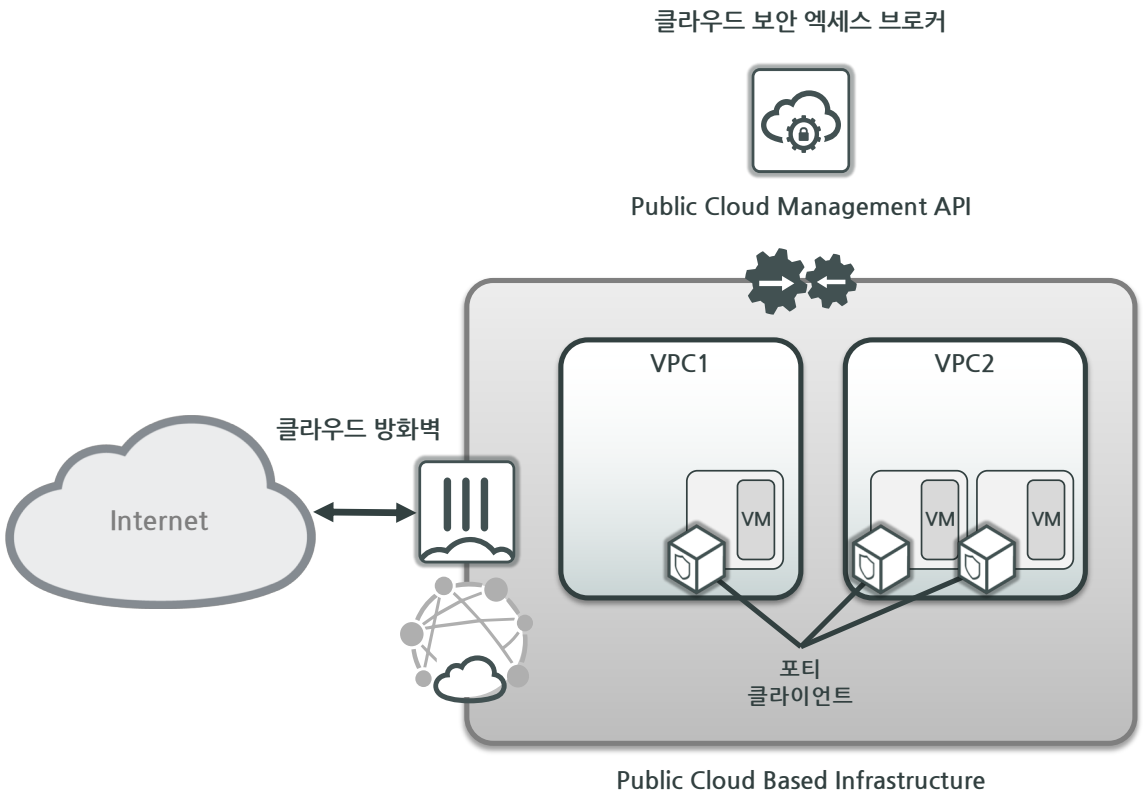


- Auto Scale등의 빈번한 인프라 변화 → **자동 제어**
- 일관된 보안 정책 제공
- 모든 클라우드 환경에서 일관된 아키텍처 제공

가시성 및 자산 접근 제어

- 기업 데이터, 가변적 인프라에 대한 **가시성 확보**
- **SaaS Cloud** 직접 제어(CASB)

Use Case#1: 대외 서비스 인프라 보안 아키텍처



목 적

- 기본 보안 기능 극복, 기업의 데이터 보호
- 외부 리소스(클라우드)와 연동 제어

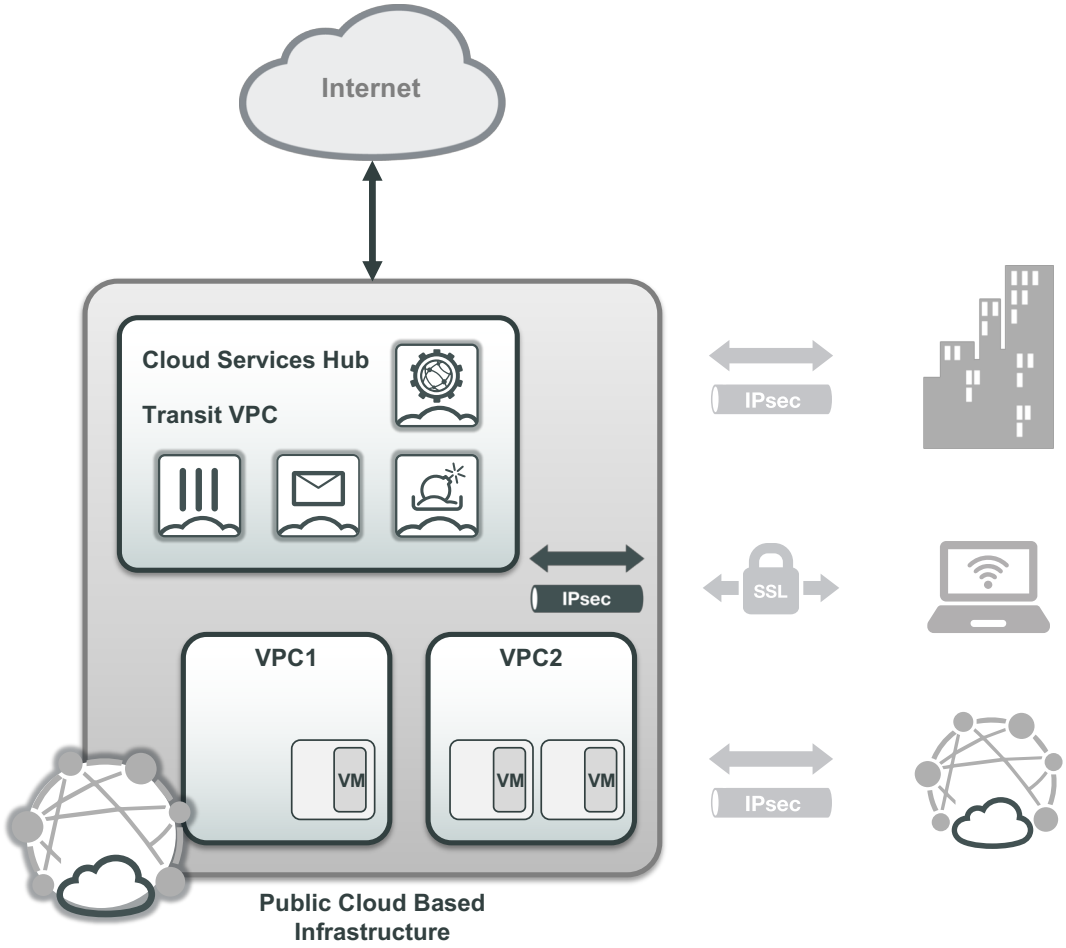
적용 솔루션

- 포티넷 클라우드 방화벽(차세대 방화벽)
- 포티 클라이언트
- 포티CASB

역 할

- 어플리케이션간 **커뮤니케이션 제어** 및 **상위 레이어 보안** 기능 제공
- 인스턴스 변화 시, 오브젝트 **자동 업데이트**
- VPC / vNET 네트워크 방화벽
- 호스트 **보호/정보(보안, 트래픽, 연동 정보 등) 제공**
- 데이터 무결성 강화, 컴플라이언스 준수
- 사례 : e 커머스

Use Case#2: 클라우드 보안 서비스 허브



목 적

- 분산된 서비스 환경을 위한 중앙 집중형 보안 인프라 구성

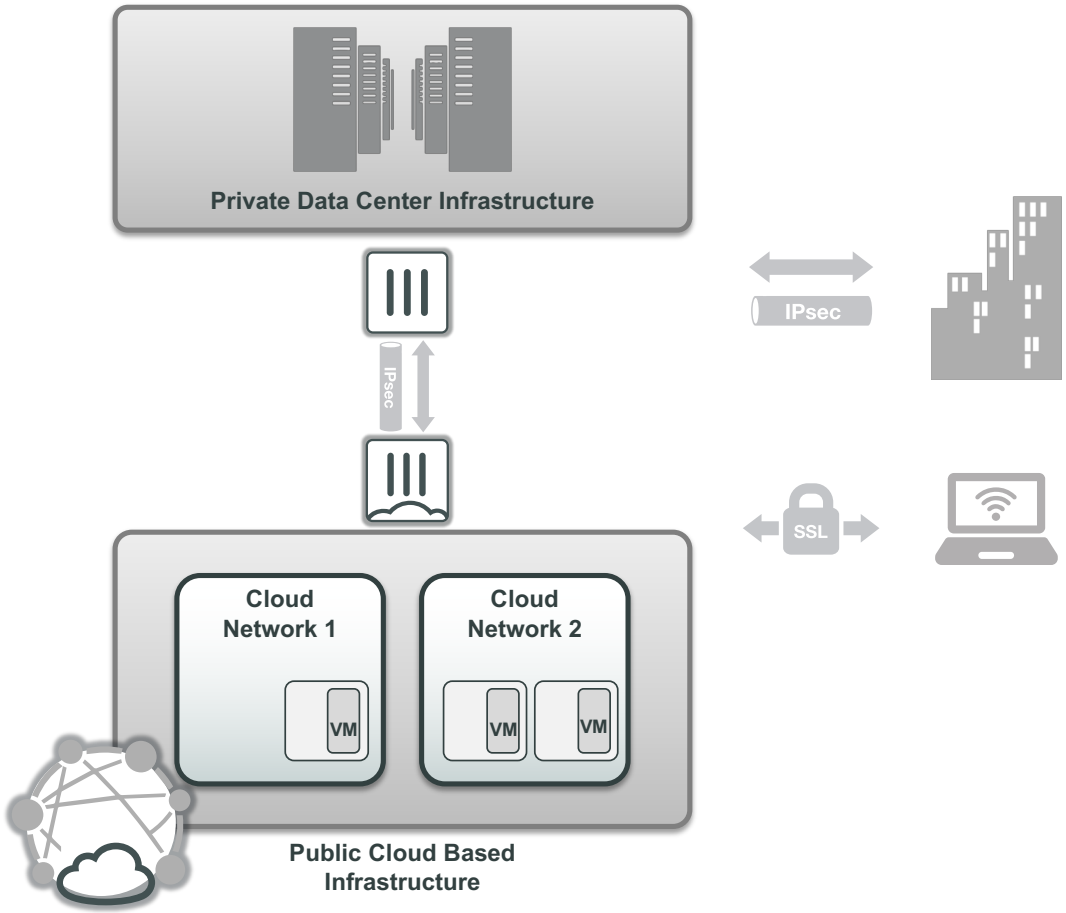
적용 솔루션

- 포티넷 클라우드 방화벽(NGFW, VPN)
- 웹 방화벽, 이메일 방화벽, 샌드박스

장 점

- 인프라의 탄력성, 가용성, 확장성을 보장
- **보안 서비스 공유 및 집중**
- **모든** 사이트, 클라우드, 서비스, 네트워크 등을 **보안 서비스 허브를 통해 연결**
- 필요에 따른 보안 서비스 확장
- 물리적인 지역에 상관 없이 확장

Use Case#3: 하이브리드 클라우드



목 적

- 점진적/선택적으로 클라우드 마이그레이션 과정에서 필요
- 고객의 주요 정보가 데이터 센터 내 위치

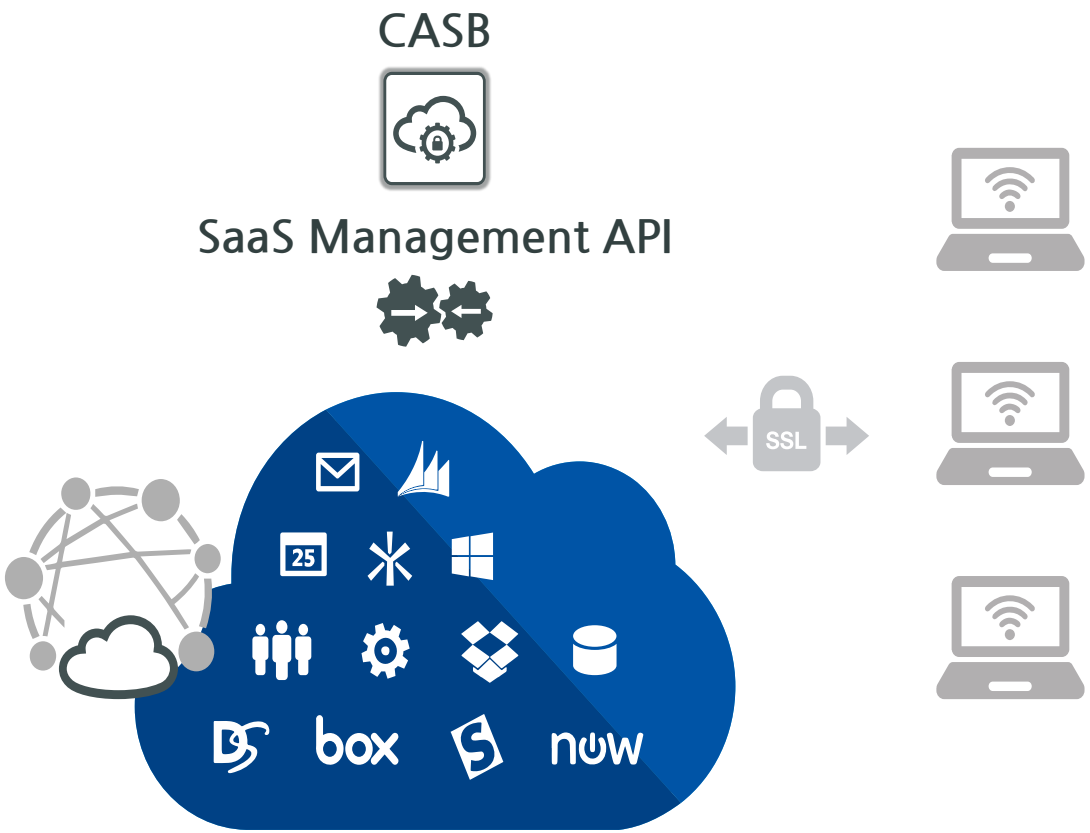
적용 솔루션

- 포티넷 방화벽(IPSEC VPN)

장 점

- 퍼블릭 클라우드를 추가 인프라로 활용
- 기업의 데이터 센터와 함께 비즈니스에 IT 솔루션 개발 및 제공
- **데이터 센터 및 클라우드에서의 IPSec 터널 운용**
- 인프라 전반에서 **일관된 보안 정책**
- 사례 : 항공사

Use Case#4: SaaS 어플리케이션 보안



목 적

- SaaS 어플리케이션 데이터 제어

적용 솔루션

- 포티CASB
- 포티클라우드 샌드박스(Optional)

장 점

- **악성 코드** 유포 또는 잠재적 인 **데이터 누출** 등 SaaS 어플리케이션 데이터에 대한 가시성/컴플라이언스를 확보
- 쉐도우 IT 환경 제어
- 로그인,로그아웃,데이터 보안 이벤트 관련 로그 발생
- 맬웨어 전파로부터 보호하기 위해 **포티넷 클라우드 샌드박스**에서 파일을 검사

마무리 및 Q&A

마무리 요약

- 포티넷은 다년간 SDDC를 위한 프라이빗 클라우드와 퍼블릭 클라우드 구축 사례 보유 (국내 기술력 입증).
- SDN, NFV, VM 연동되는 고성능-저지연(low-latency) FortiGate 포티게이트 구축 사례 보유.

Q&A

- 고객 문의 및 답변

FORTINET®

감사합니다.