

네트워크 가상화 환경에서의 침해대응

ksnoh

ugginsung2@gmail.com

노기성





네트워크 가상화 시대

🏠 > 뉴스

좋아요 { 2 } 트윗 { 4 } g+1 { 2 } Share { 1 }



데이터센터 / 클라우드

🕒 2012.07.24

VM웨어, 오픈플로우 선도업체 '니시라' 인수

Joab Jackson | IDG News Service

데이터센터의 모든 요소를 가상화한다는 전략을 펼치고 있는 VM웨어가 SDN(Software Defined Networking) 전문업체인 니시라(Nicira)를 12억 6,000만 달러에 인수한다고 밝혔다.

🏠 > 뉴스

좋아요 { 0 } 트윗 { 6 } g+1 { 0 } Share { 0 }



데이터센터 / 애플리케이션 / 클라우드

🕒 2012.12.27

SDN, 시스코-VM웨어-오픈플로우 '3국 시대'로 파편화

Jim Duffy | Network World

주니퍼 네트워크 수석 부회장 밥 무글리아는 소프트웨어 정의 네트워킹(Software-Defined Networking) 초기 시장을 오픈플로우(OpenFlow)/오픈 소스, 시스코, 그리고 VM웨어 등 세 개의 진영으로 요약했다.



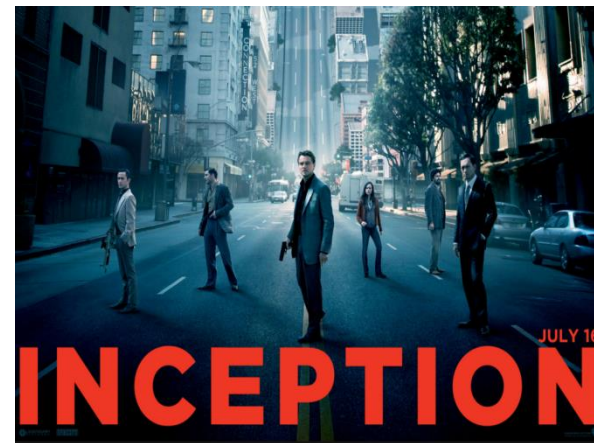
가상네트워크 구축 현황

- 미국 : 잘팔려요~
- 일본 : 정보보호를 목적으로 100개 사이트 이상 실 망 도입
- 한국 : 아직은 테스트 용이 지배적..



네트워크 가상화

- **물리** 네트워크를 기반으로 **가상**의 네트워크를 만드는 기술(GRE STT VXLAN 등Overlay 기반)
- x86 가상화 기술로 네트워크 가상화가 구현되면 금상첨화





1. 가상네트워크를 통한 침해대응 환경 개선 범위

2. 네트워크 가상화 기술의 이해

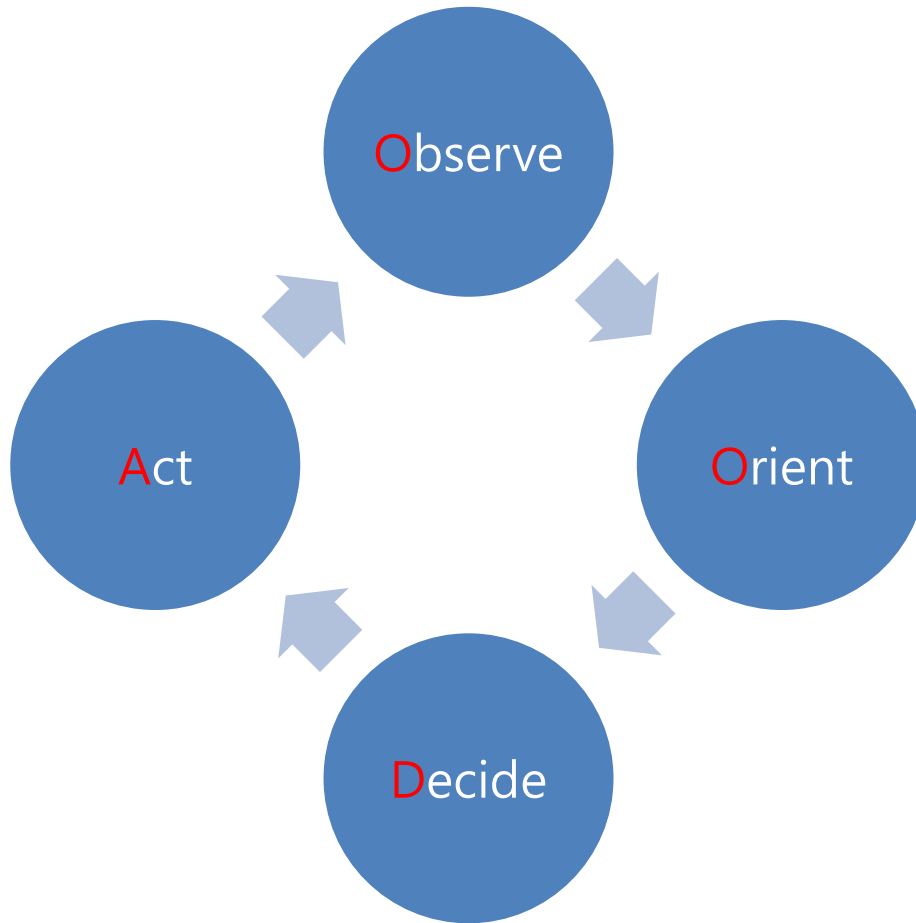
- 기반기술 이해
 - ✓ 서버 가상화
 - ✓ 데스크탑 가상화
- SDN

3. 가상네트워크 보안 장치

1. 가상네트워크를 통한 침해대응 환경 개선 범위



OODA Loop

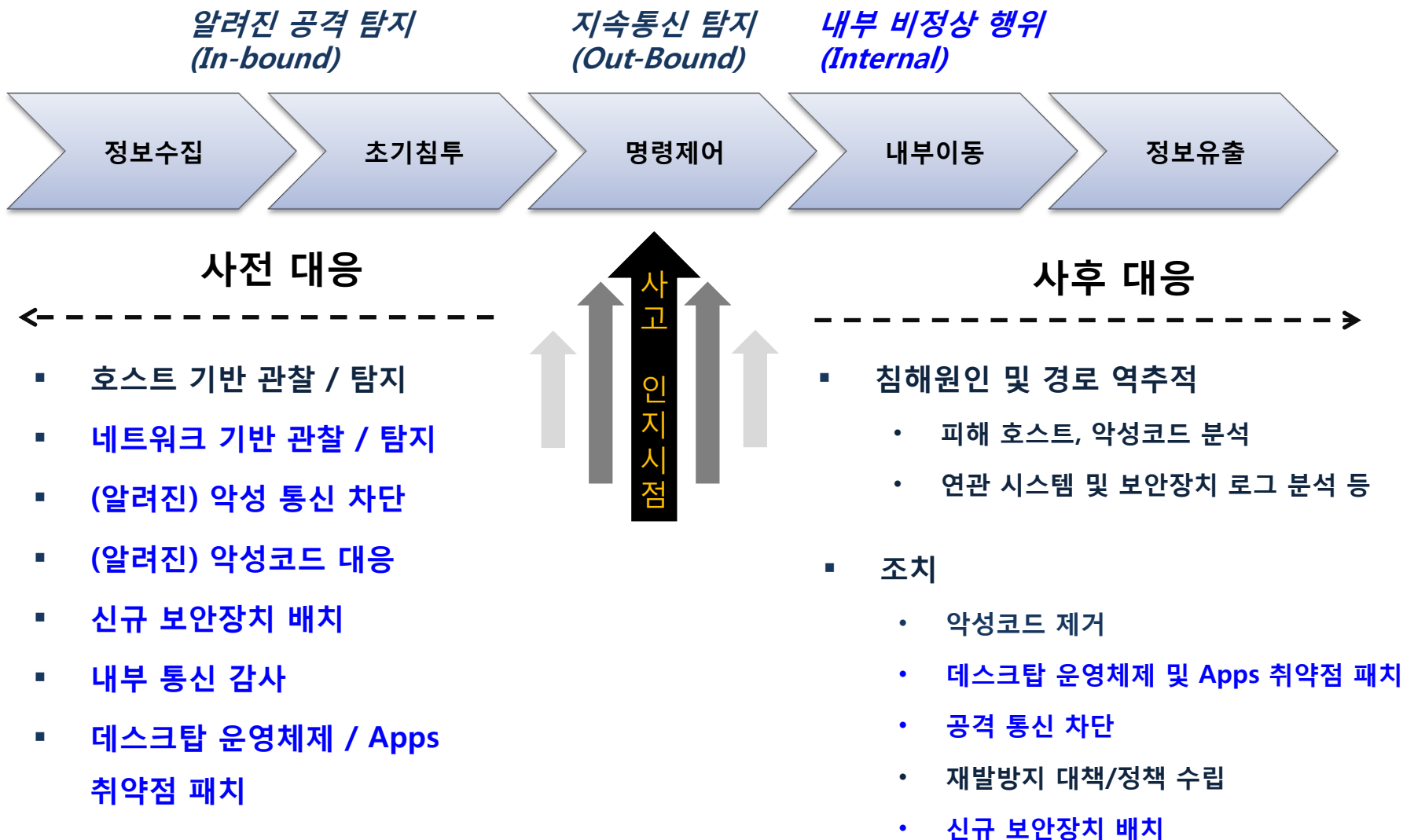


- 관찰할 데이터도 많고 모든 것을 다 볼수도 없고..
- 신규 대응 인프라가 필요한데 구매 및 실배치 까지 여러 난관이 있고..
 - 예산, 시간, 안정성 등..
- 대응하다 운영중인 서비스에 영향 주면 안되는데..
- 사람도 없고...

1. 가상네트워크를 통한 침해대응 환경 개선 범위



네트워크 가상화 기술이 기대되는 침해 대응 영역



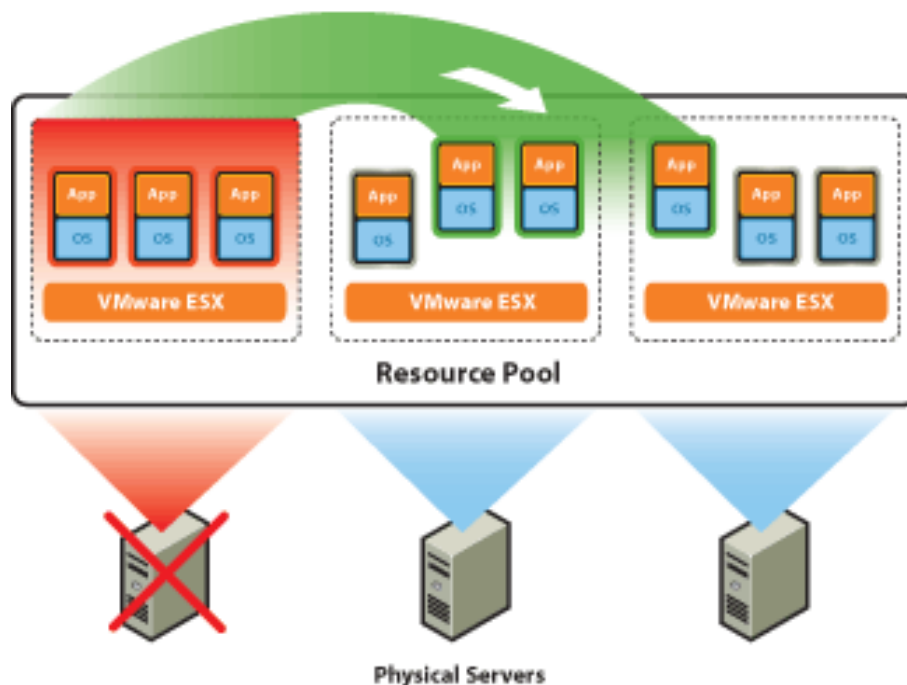
2. 네트워크 가상화 기술의 이해



서버 가상화

- 목적 : 안정적인 서버 통합운영을 통한 비용 절감 (소프트웨어 정의 IDC 구축)
- 주요 기능
 - 장애 예방 및 복구 (HA, 클러스터, Fault Tolerance)
 - 패치 통합 관리 (물리서버 + 가상머신)
 - 백업 관리
 - 파워관리(전기세 절약)

**서버 운영체제 가상머신을
구동하는 기술 아님!!**



데스크탑 가상화

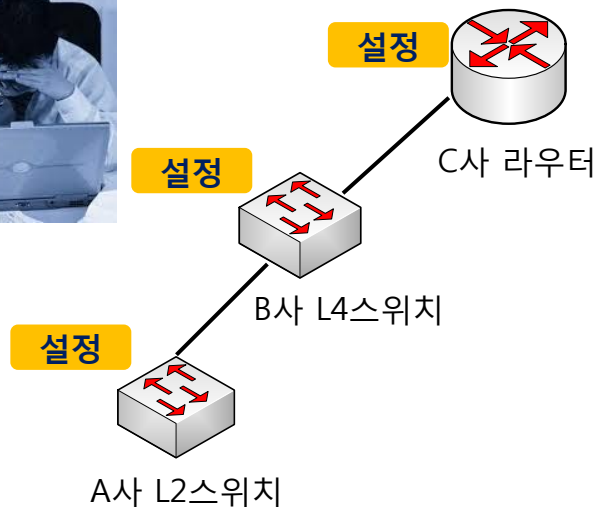
- 목적 : 서버가상화 인프라를 기반으로 Desktop OS 환경을 사용자에게 통합 관리
- 주요 기능
 - 보안(망분리)
 - 사용자 데이터 통합 관리
 - 응용프로그램 / OS 관리
(패치, 사용권한 등)
 - 언제 어디서나 업무환경
 - 비용절감





SDN(Software Defined Network)

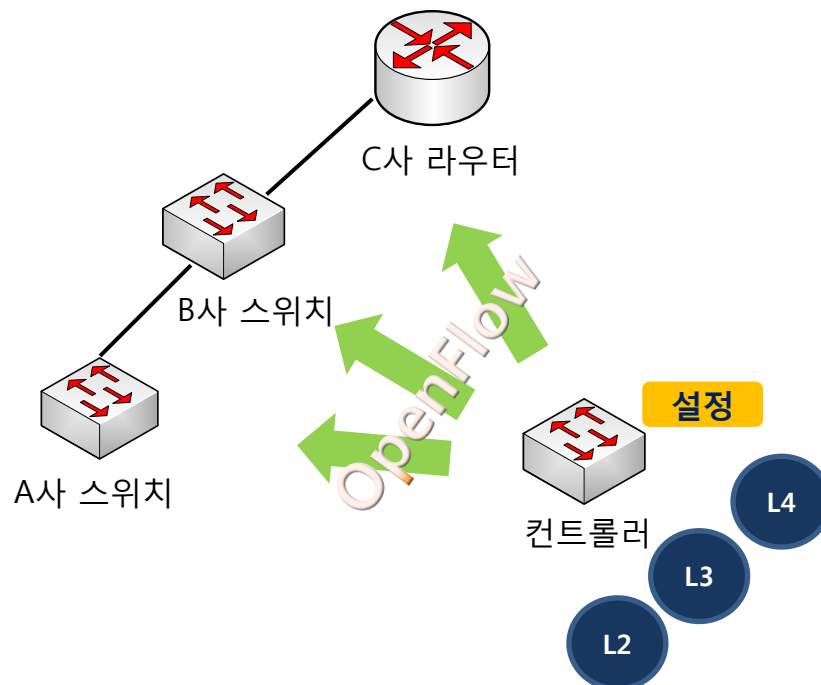
- 모든 네트워크 장비를 따로 관리하지 않고 통합관리 할 수 있어 좋네..
 - 하지만 SDN 지원하는 전용 장비로 교체해야하네...;; 전문인력도 필요하고..



S/W - 동작상태 및 성능 관리

S/W - 패킷 경로설정, 관리, 제어

H/W - 패킷 송수신





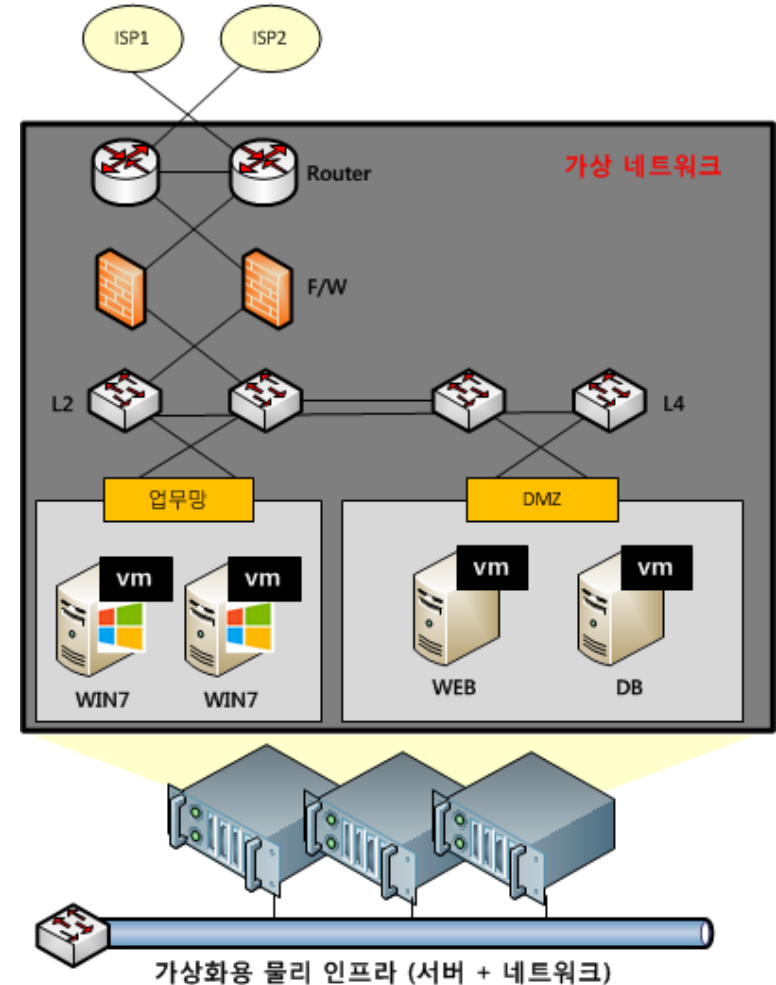
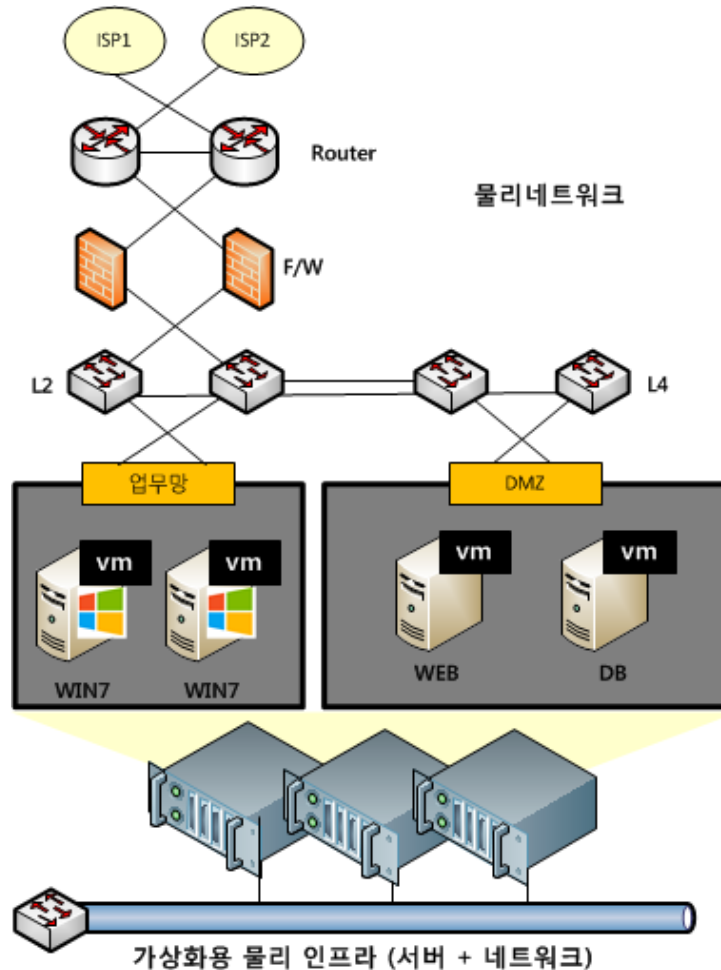
네트워크 가상화 이점

- 모든 네트워크 장비를 통합 관리할 수 있으면서 (SDN 아키텍처를 따르면서)
- 네트워크 / 보안 장비 배치 작업도 빠르게 하고..
- 네트워크 장비들도 가상머신으로 만들어서 유지 관리를 편하게 하고
- 이러한 모든 것들을 전용장비 구매 없이 기존 네트워크 인프라를 활용해서 할수는 없을까?
- 사용자 보안을 강화할 수는 없을까? (악성코드, 운영체제 취약점 관리, DLP, 망분리..)



네트워크 가상화

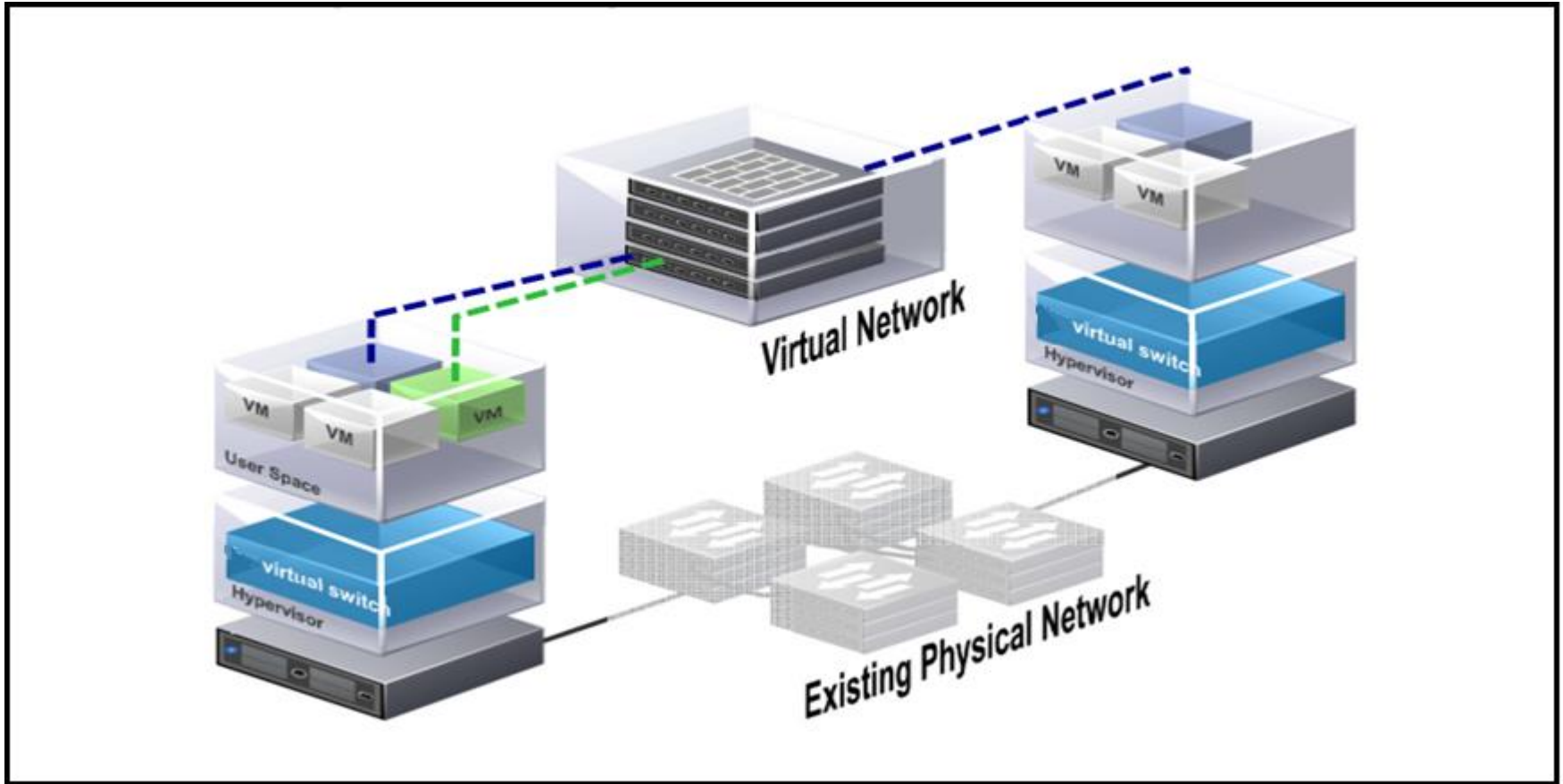
- 목적 : 서버가상화 인프라를 기반으로 편리하고 효율적인 네트워크 인프라 운용 / 보안성





네트워크 가상화

- 물리 스위치를 기반으로 가상의 네트워크를 만드는 기술 (Overlay)

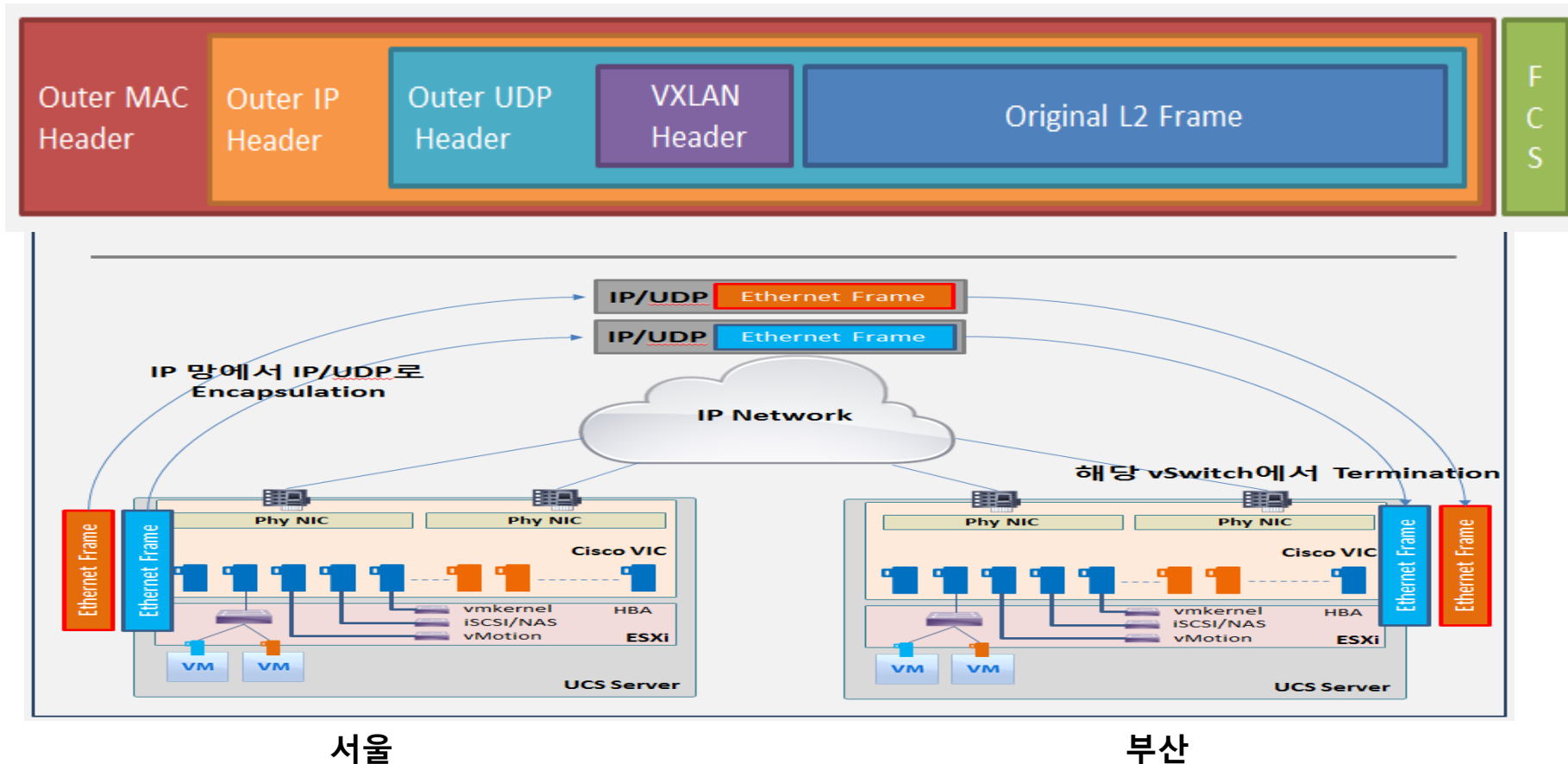


2. 네트워크 가상화 기술의 이해



Overlay ?

- VXLAN Overlay 기반 L2 확장 예시(L2 over L3)



출처 : <http://youngmind.tistory.com/entry/Network-Overlay-VXLAN-%EB%B6%84%EC%84%9D-2>



네트워크 가상화 제품

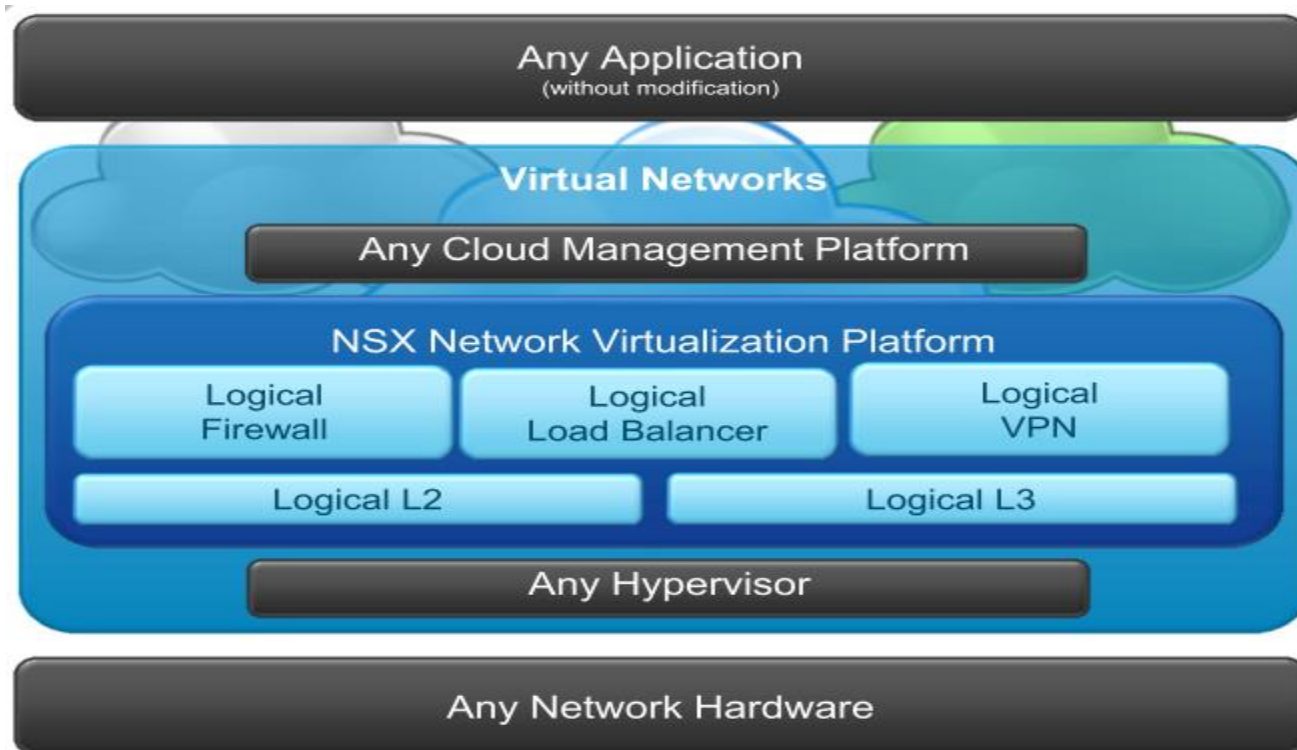
- 시스코 ACI
- Nuage Networks VSP
- VMware NSX
 - 다양한 3rd 파트너사와 협력을 통해 가상네트워크 보안 어플라이언스 제공



네트워크 가상화 제품

▪ VMware NSX

- L2,L3,L4,F/W,NAT,VPN, Control API 제공
- 기존 네트워크 장비 교체 필요 없으며, 타 하이퍼바이저에서도 사용 가능



출처 : VMware.com



VMware NSX 기능

Layer	기능
L2	<ul style="list-style-type: none">• VLAN / PVLAN• LACP• Port Mirror
L3	<ul style="list-style-type: none">• Routing<ul style="list-style-type: none">- OSPF- IS-IS- BGP• NAT• F/W
L4-L7	<ul style="list-style-type: none">• LB• QoS• HA• VPN<ul style="list-style-type: none">- L2 VPN- IPSec- SSL VPN-Plus
보안 및 모니터링	개 별 3 rd Party Plugins (F/W, AV, IDS, sFlow 등)

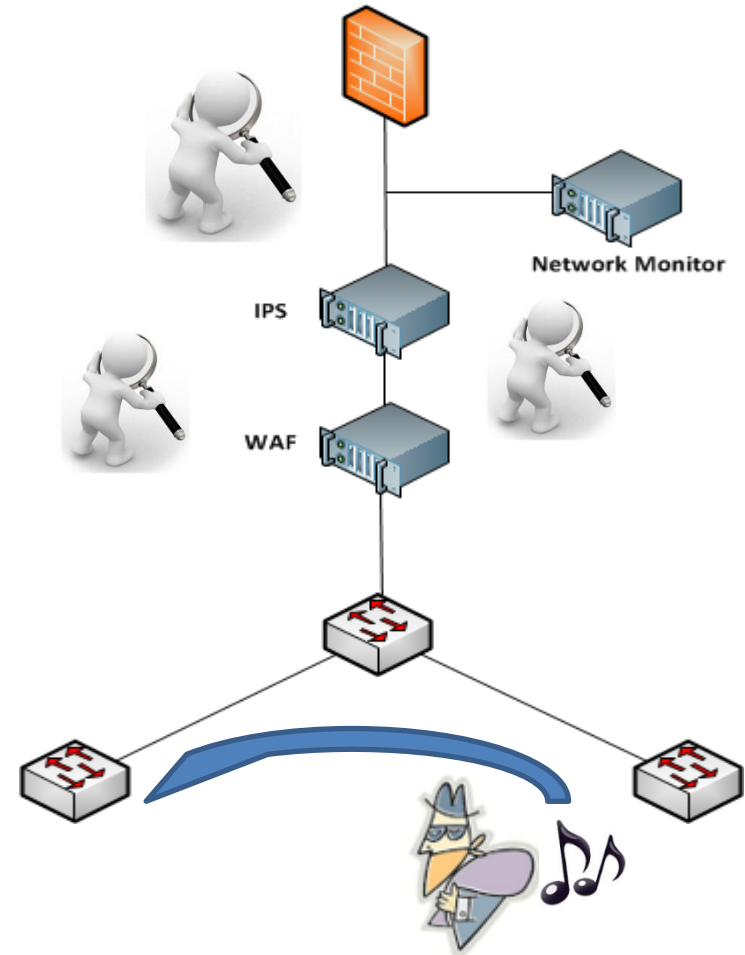
3. 가상 네트워크 보안 장치

3. 가상 네트워크 보안장치



고민 ..

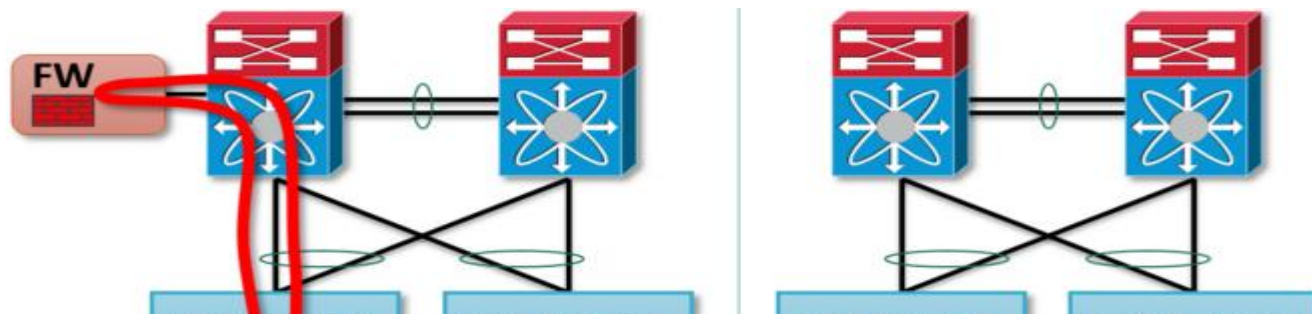
- 보안 / 트래픽 모니터 장비를 구석구석 넣고 관찰하고 싶지만 금전적, 구조적 한계가..
- 공격자가 특정 구간만 우회할 수 있으니
구석구석 관찰할 수는 없을까 ?
- 신규 보안장비 배치를 안전하고 빠르게
할 수 없을까?
- 네트워크 보안 감사 처리 부하를 낮출수는
없을까?



분산 방화벽



- 가상머신과 가상머신 사이에는 무조건 가상 방화벽 및 트래픽 수집/제어가 가능하다면?
 - Access Control 및 트래픽 관찰을 중앙에서..L2 까지도
 - 트래픽 처리 효율성 증대 및 보안성 강화



No.	Name	Type	Source	Destination	Service	Action
✓ 1	firewall	Internal	<i>i</i> vse	any	any	Accept
✓ 2	ipsec	Internal	<i>i</i> 192.168.130.4 <i>i</i> 192.168.100.10	<i>i</i> 192.168.130.4 <i>i</i> 192.168.100.10	<i>i</i> udp:500,4500:any <i>i</i> esp:any:any	Accept
✓ 3	sslvpn	Internal	any	<i>i</i> 192.168.130.4	<i>i</i> tcp:443:any	Accept
✓ 4	Default Rule	Default	any	any	any	Deny

3. 가상 네트워크 보안장치



접근통제외 내,외부 알려진 위협 트래픽, 취약점 관리, 악성코드 탐지등은 어디에서?



3. 가상 네트워크 보안장치



Third-party 보안도구 설치 및 통합 운용

L2 Gateway

ADC/LB

Firewall

IDS/IPS

AV/FIM

Vulnerability Management

Security Services

New Service Definition

✓ 1 General properties

2 Service Categories

3 Add service configurations

4 Add profile configurations

5 Select transports

6 Ready to complete

Service Categories

Choose one or more service categories to associate v
Optional: Define a set of attributes for each selected c

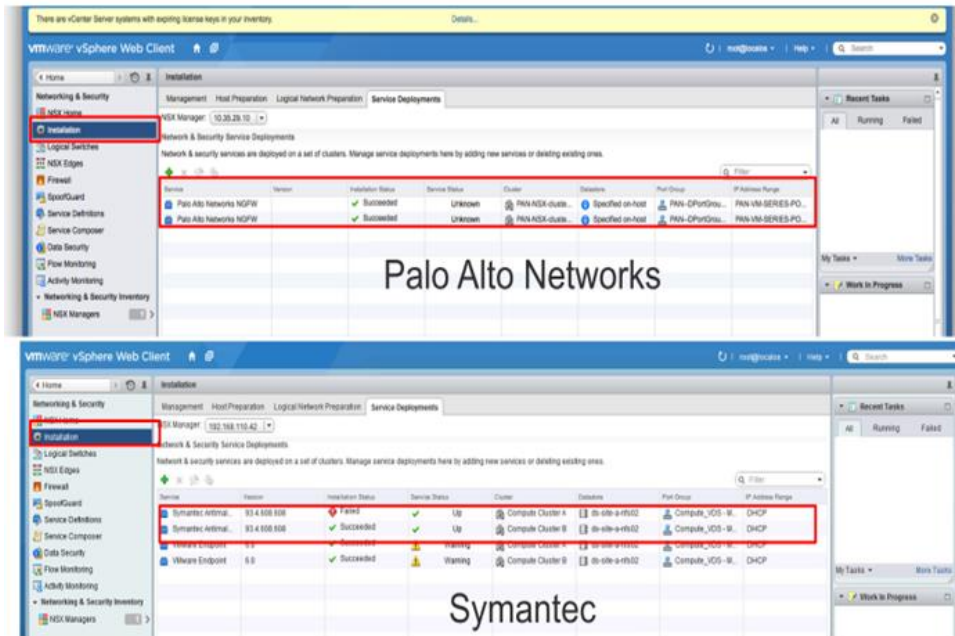
Service Category
<input type="checkbox"/> ADC
<input type="checkbox"/> Anti virus
<input type="checkbox"/> Data Collection
<input type="checkbox"/> Data security
<input type="checkbox"/> DLP
<input type="checkbox"/> File Integrity Monitoring
<input type="checkbox"/> Firewall
<input type="checkbox"/> IDS IPS
<input type="checkbox"/> Load balancer
<input type="checkbox"/> Network Monitoring
<input type="checkbox"/> Vulnerability management
<input type="checkbox"/> WAN optimizer

3. 가상 네트워크 보안장치



유해 트래픽 탐지시 분산 방화벽 필터와 연동하여 차단까지 연계

- 설치도 편하고 관리도 편하고 커버리지도 넓고..

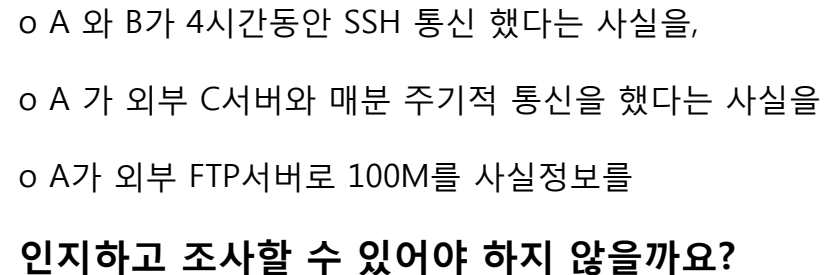


Detect
& Block



공격수행

- 전용 트래픽 수집 분석 장치를 구석구석 배치하여 관찰 하기엔 네트워크 구간이 너무 많고..



3. 가상 네트워크 보안장치




가상 네트워크 트래픽 모니터링

- 장점 : 전 구간 트래픽 흐름 관찰 가능

[Dashboard](#) [Details By Service](#) [Live Flow](#) [Configuration](#)

NSX Manager: 192.168.110.42

Live Flow will be shown for the selected vNIC. Please select a vNIC and press start to see the live flows

vNIC:  apache-w-01a - Network adapter 1 [Browse](#) [Start](#) [Stop](#)

Refresh Rate: 5 Seconds

New active flows Flows with state change Terminated flows

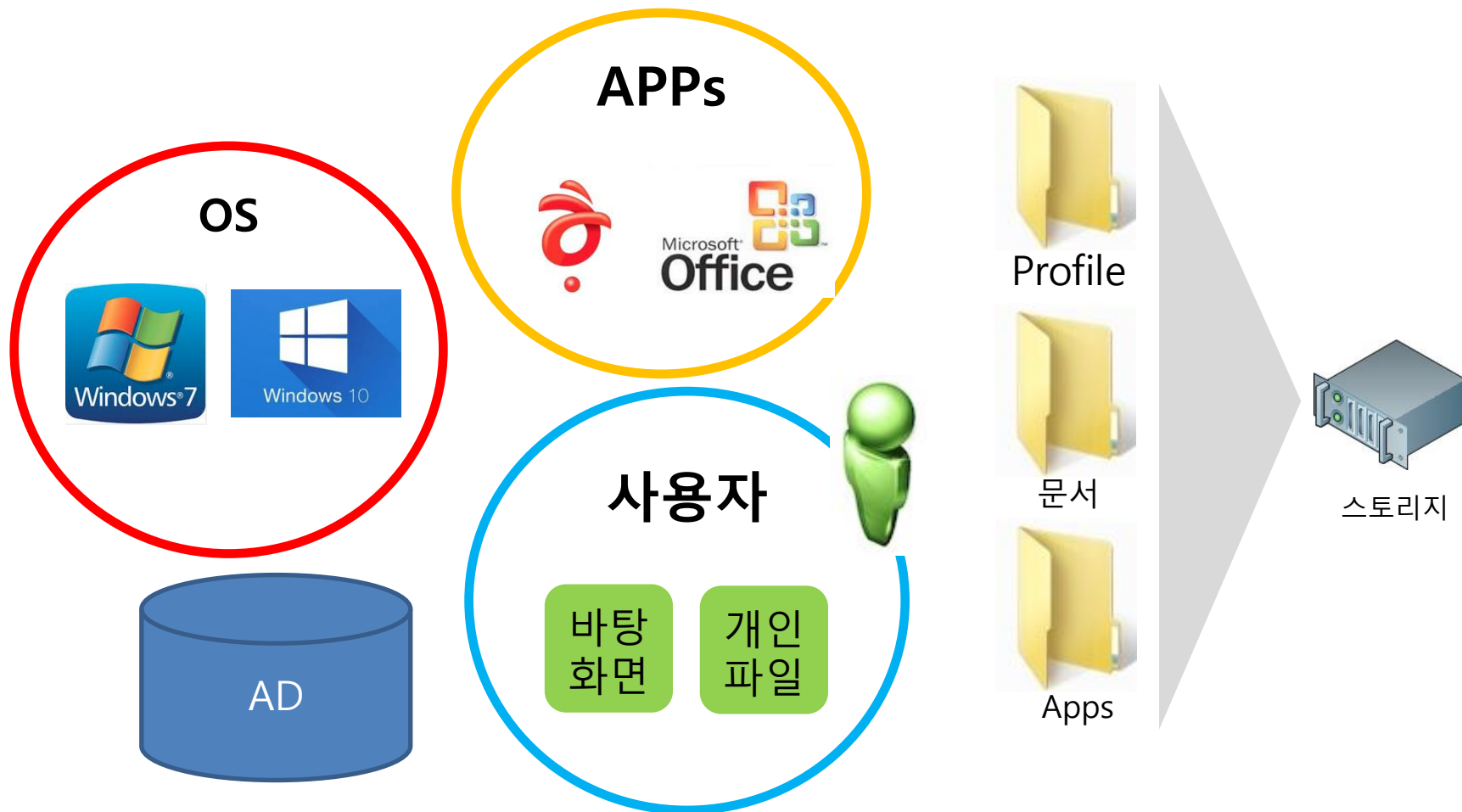
RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	State	Incoming Bytes	Incoming Packets	Outgoing Bytes
1002	OUT	Active	UDP	192.168.100.75	138	192.168.100.255	138		229	1	0
1002	IN	Active	UDP	192.168.100.76	138	192.168.100.255	138		236	1	0

3. 가상 네트워크 보안장치



데스크탑 가상화 보안 관리 이점

- OS, App 패치관리 용이성





결론

- 넓은 네트워크 관찰 범위
- 빠르고 편리한 네트워크 보안 아키텍처 구성
- 네트워크 접근 제어 관리 용이
- 다양한 구간에서의 탐지 / 차단 프로세스 연계 용이

