

가상화/클라우드를 위한 혁신적인 데이터센터 보안 디자인

Cisco Systems Korea

Woo Hyung Choi

Mail : whchoi@cisco.com / whchoi98@gmail.com

Blog : <http://youngmind.tistory.com>

Date : 2013-01-24

우리는 클라우드 컴퓨팅을 거부할 수 있는가?

가트너 10대 전략 키워드

[2010년 ~ 2013년]

2010 년

1. Cloud Computing
2. Virtualization for Availability
3. IT for Green
4. Client Computing
5. Mobile Applications
6. Advanced Analytics
7. Social Software and Social Computing
8. Flash Memory
9. User Activity Monitoring (Security)
10. Reshaping the Data Center

2011 년

1. Cloud Computing
2. Next-Generation Analytics
3. Social Communications and Collaboration
4. Mobile Applications and Media Tablets
5. Storage class memory
6. Social Analysis
7. Context-Aware Computing
8. Video
9. Fabric-Based Infrastructure and Computing
10. Ubiquitous Computing

2012 년

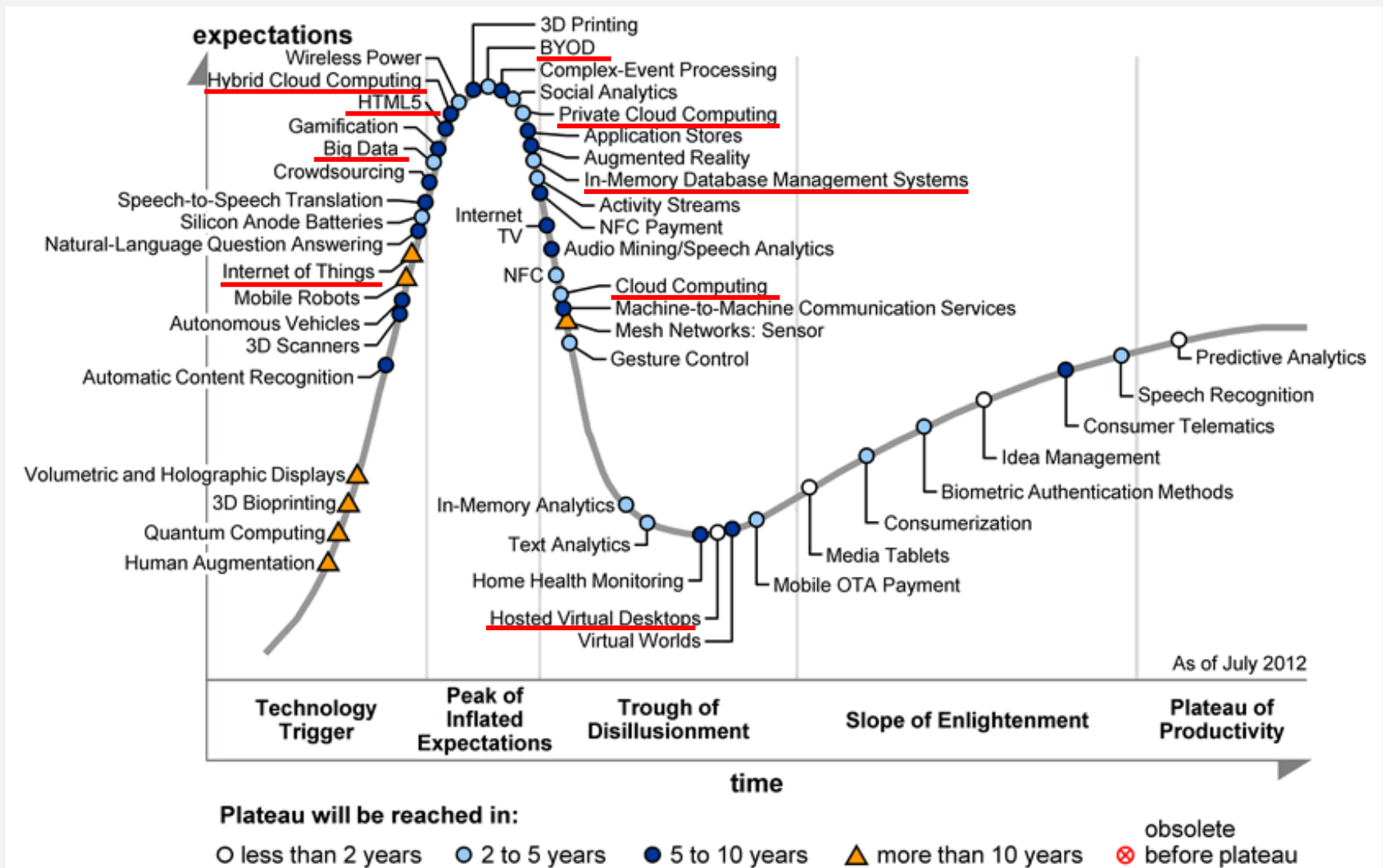
1. Media tablets and beyond
2. Mobile-centric application and interface
3. Contextual and social user experience
4. Internet of things
5. App stores and market places
6. Next-generation analytics
7. Big data
8. In-memory computing
9. Extreme low-energy servers
10. Cloud computing

2013 년

1. Mobile Devices Battles
2. Mobile Applications & HTML5
3. Personal Cloud
4. Internet of Things
5. Hybrid IT & Cloud Computing
6. Strategic Big Data
7. Actionable Analytics
8. Mainstream In-Memory Computing
9. Integrated Eco-Systems
10. Enterprise App Stores

* Source : Gartner, Top 10 Strategic Technology Trend, 2010~2013

가트너 2012년 Technology Hype Cycle



그래도 우리는 클라우드 컴퓨팅과 가상화로 갈 것이다.

G A F A

Google : Cloud Computing & Mobile



Apple : Mobile & Cloud Computing



FaceBook : Social Networking & Cloud Computing



Aamazon : Cloud Computing No.1



TCO/ROI



비즈니스 = IT



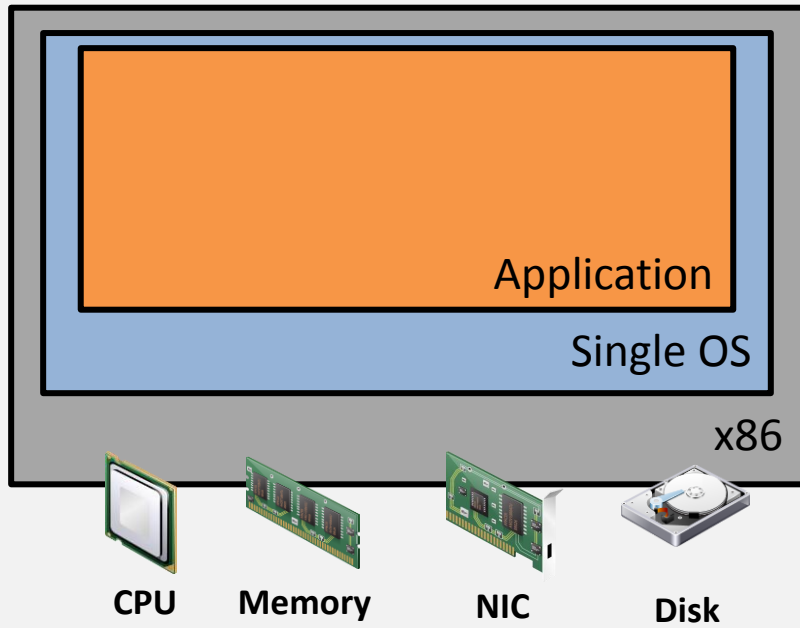
무중단



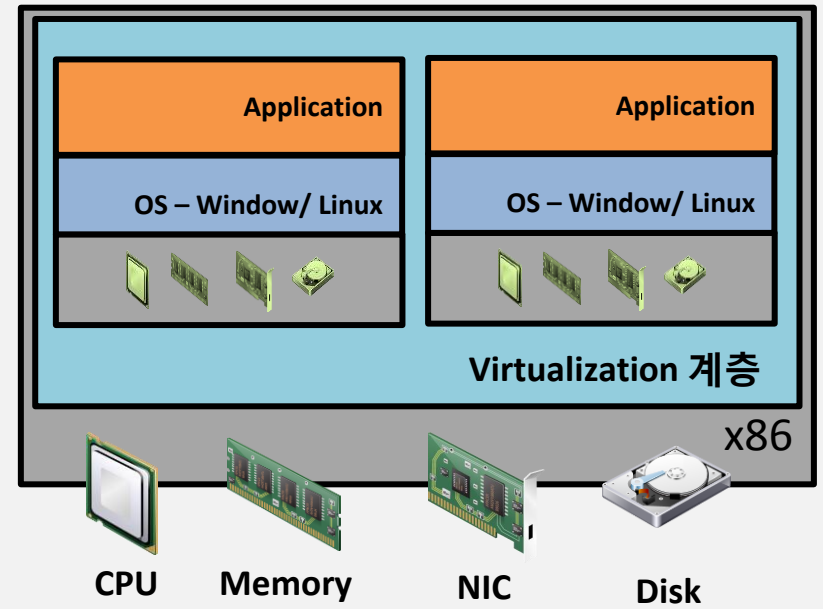
저전력

클라우드 컴퓨팅의 기본, 가상화... 무엇인가?

서버 가상화란?



전통적인 x86 서버 환경



가상화 기반의 x86

네트워크 가상화란?



데이터 부 (Data Plane)

데이터 처리 역할

Segmentation : VLAN , VRF , MPLS ...



관리 부 (Management Plane)

네트워크 장비의 구성 관리

Config, Log, SNMP, Telnet ...



제어 부 (Control Plane)

네트워크 제어 역할

BPDU, Routing Message, ARP ...

네트워크 가상화란?



데이터 부



관리 부



제어 부

VDC1

Shares = 2

VDC2

Shares = 4

VDC3

Shares=1

VDC4

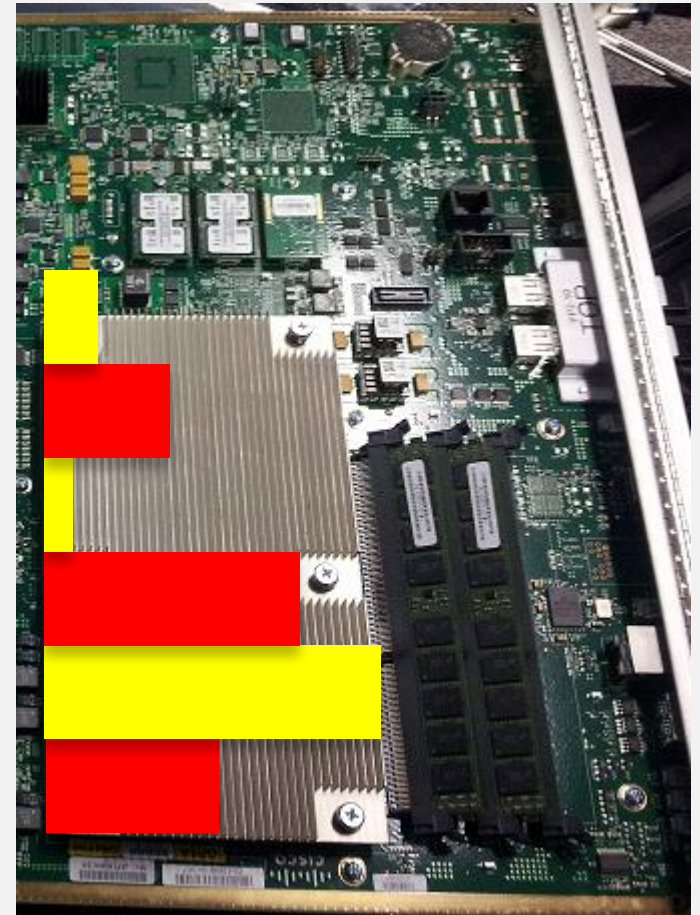
Shares=8

VDC5

Shares=10

VDC6

Shares=5



Cisco Nexus 7000 기반의 가상화 – VDC (Virtual Device Context)

가상화를 두려워 하는 이유?



- 보이지 않는다.
- 관리의 주체가 애매하다.
- 물리적 가상화 보다 보안적 이슈가 많다.

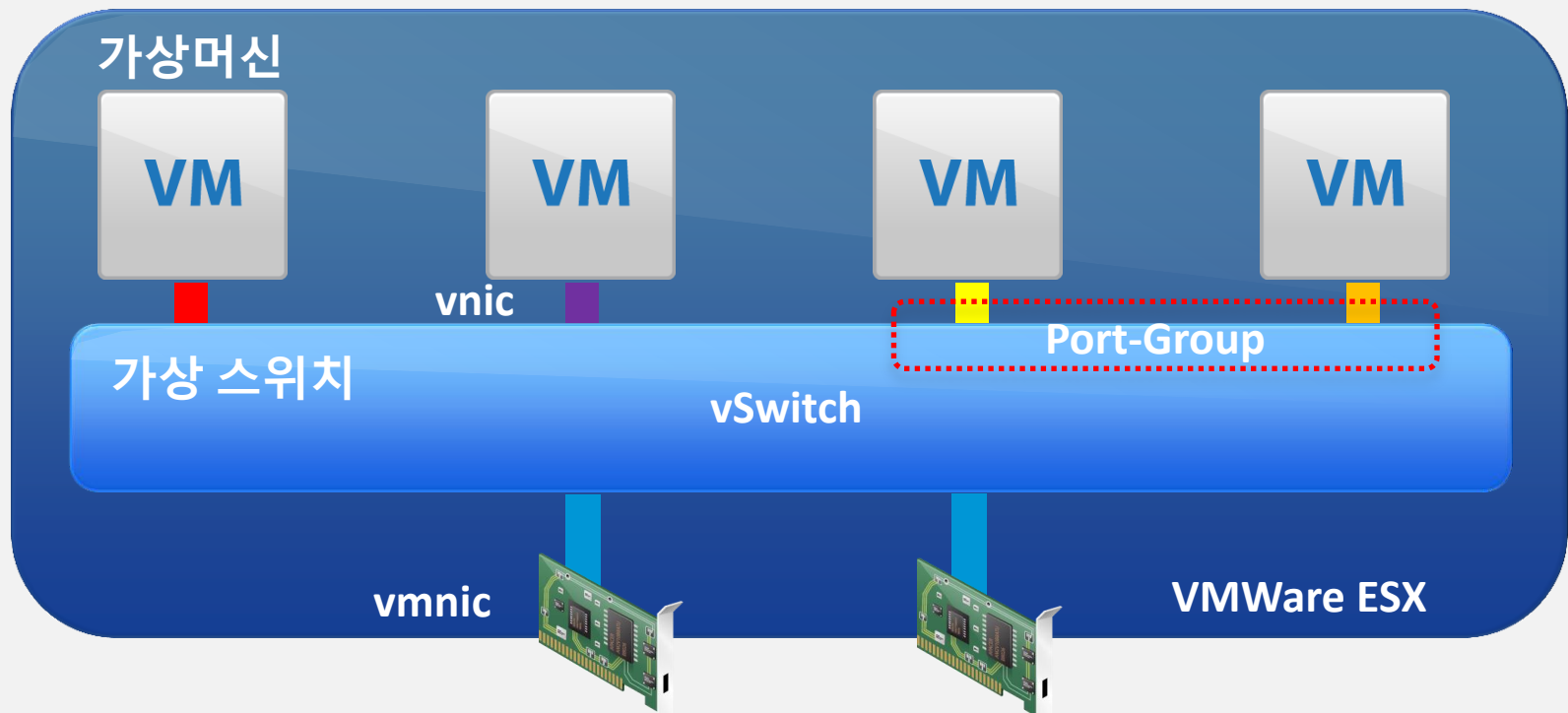




가상화와 네트워킹 관계에서의 보안

가상화와 네트워킹 관계의 이해

[vmware & vswitch]

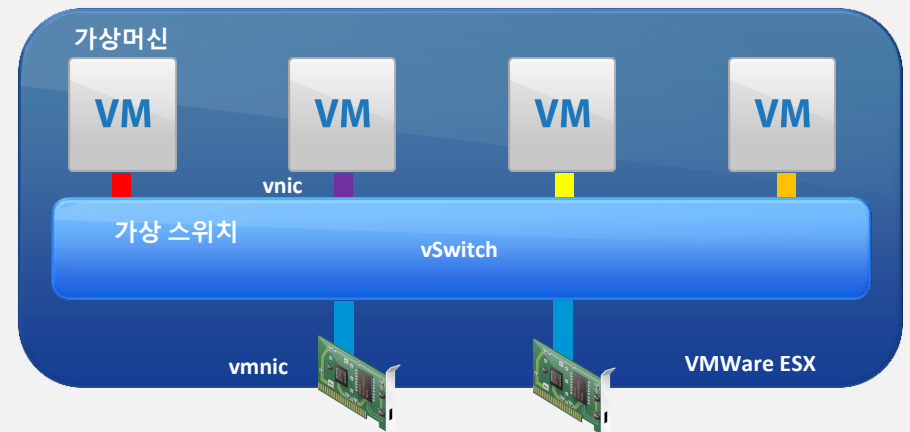
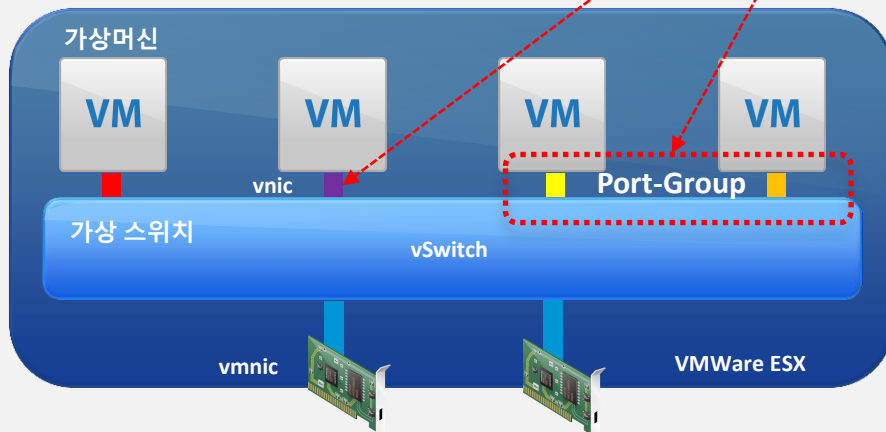


가상화와 네트워킹 관계의 이해

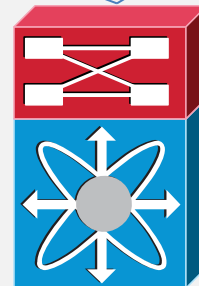
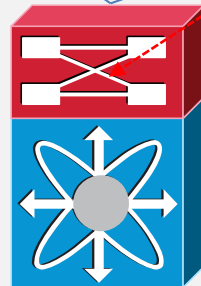
[vmware & vswitch]

VGT (Virtual Guest Tagging) : NIC Level Tag

VST (Virtual Switch Tagging) : vSwitch Level Tag

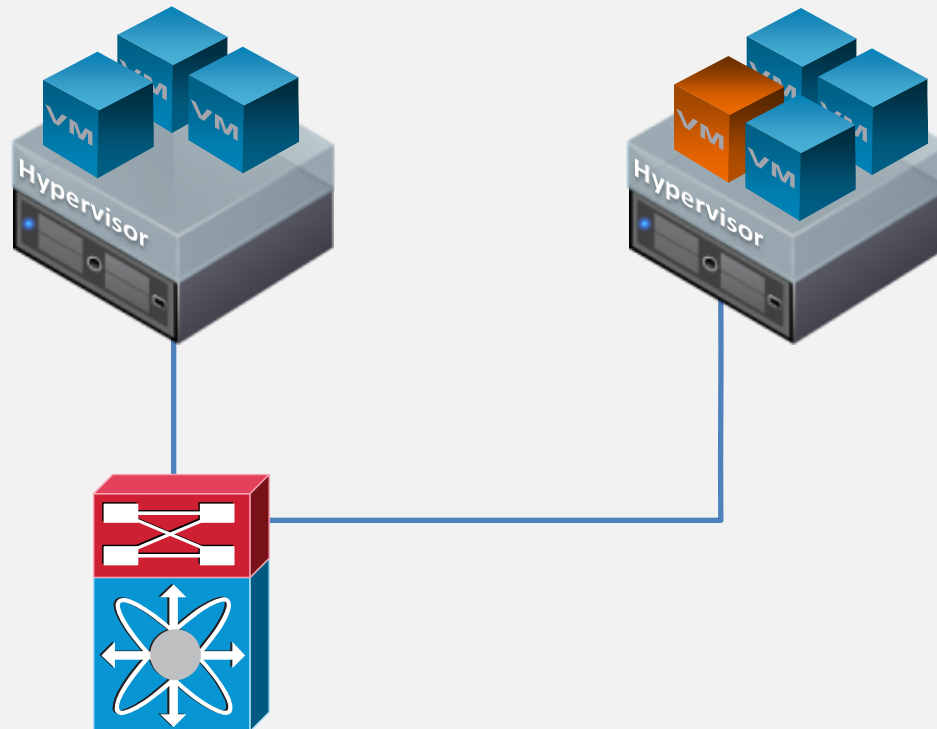


**EST (External Switch Tagging) :
Access Switch Tag (ex. Switch access vlan)**



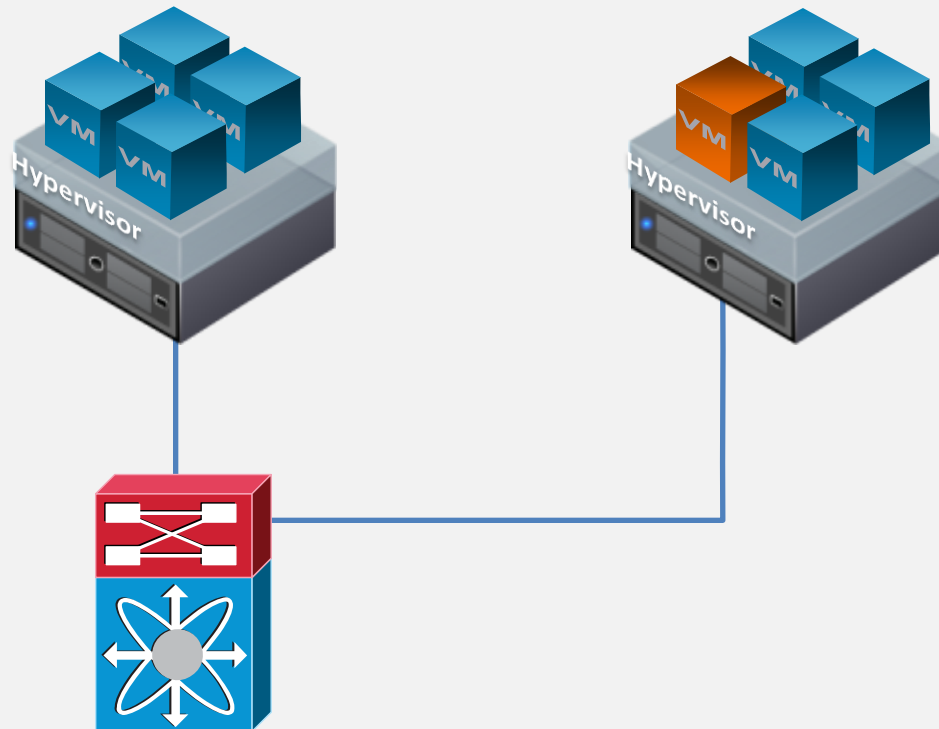
가상화와 네트워킹 관계의 불편한 진실

1 네트워크 정책 적용 불가 네트워크 모니터링 불가



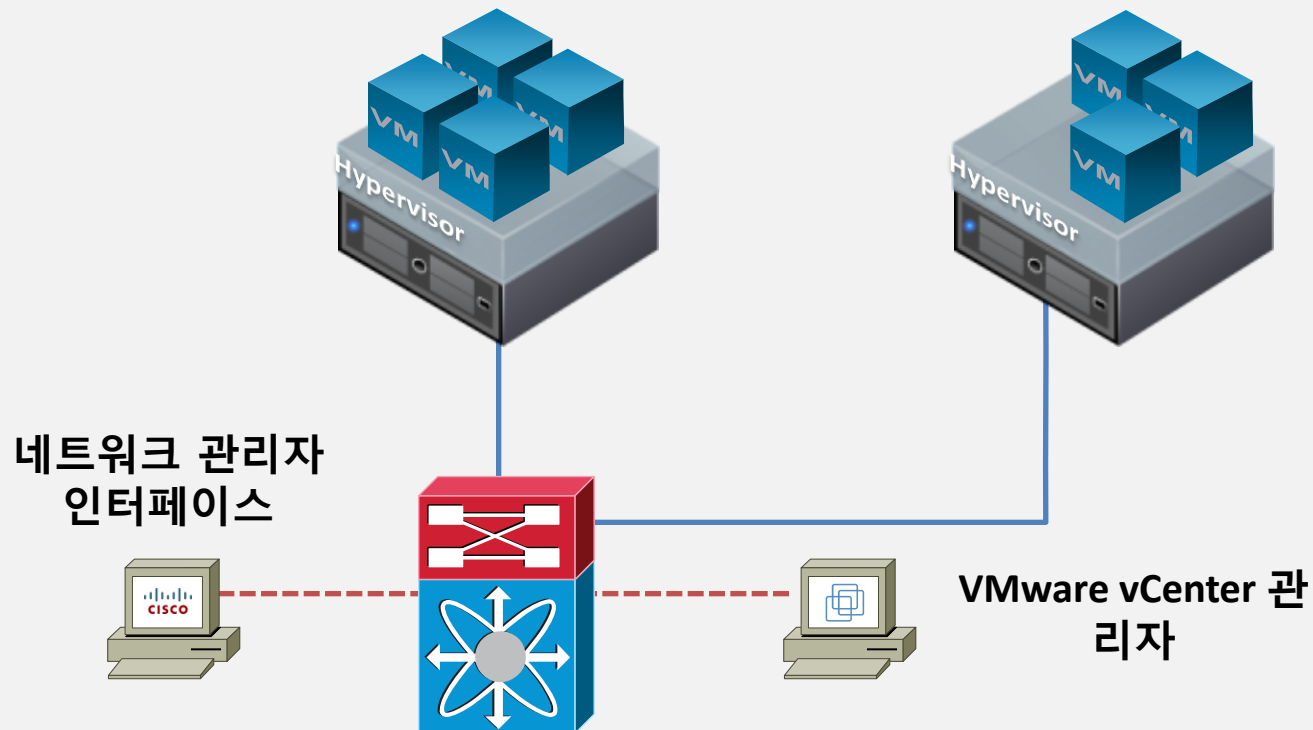
가상화와 네트워킹 관계의 불편한 진실

2 정책의 이동성 보장 불가능



가상화와 네트워킹 관계의 불편한 진실

3 가상스위치...그리고, 네트워크 담당자와 서버 담당자



가상화와 네트워킹 관계의 불편한 진실

4 데이터센터 서버 액세스 스위치의 새로운 패러다임...그리고 관리 포인트 이슈



가상화와 네트워킹 관계의 불편한 진실

5 진짜...이슈

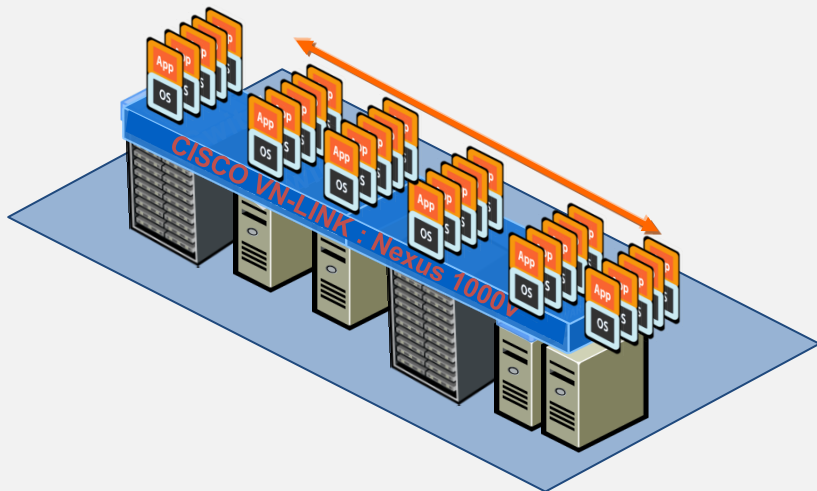
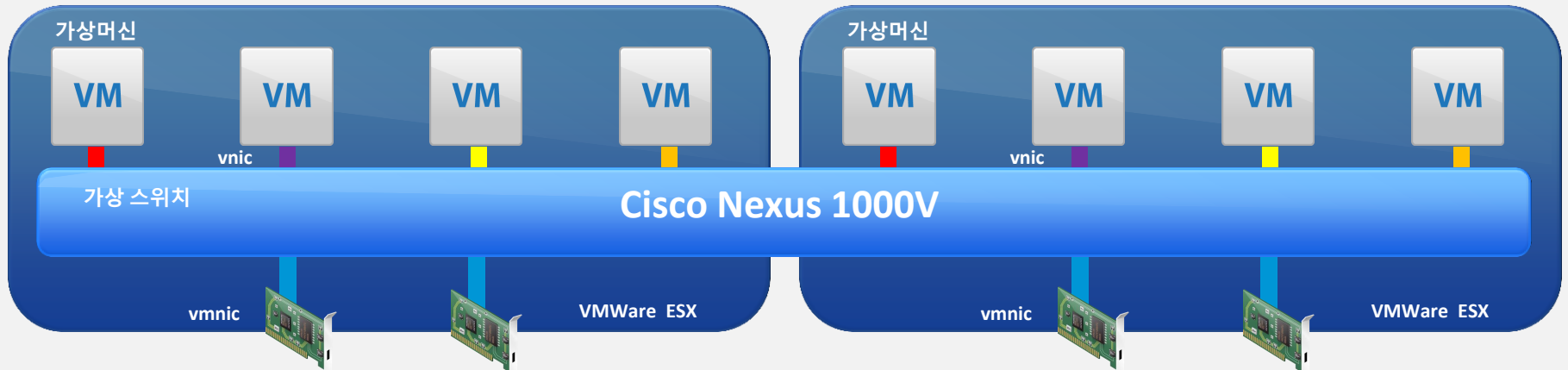
가상화 업체, 가상화 파트너, Server 벤더들 중 vSwitch의 정체를 제대로 아는 사람이 별로 없다.

vSwitch를 매우 단순하게 구성한다.

가상화 기반의 물리적 서버가 증가 할 수록, vSwitch가 가장 큰 이슈가 된다.

가상화 서버에 대한 SLA 개념이 전혀 없다.

Cisco VSN 의 핵심 Cisco Nexus 1000V Switch



다양한 정책 할당 및 구성 가능

- ACL, QoS, Netflow, Portmirroring 과 같은 기능 구현 가능
- DAI 와 같은 보안 기능 설정 가능

VM 이동시에도 기존 정책 유지 가능

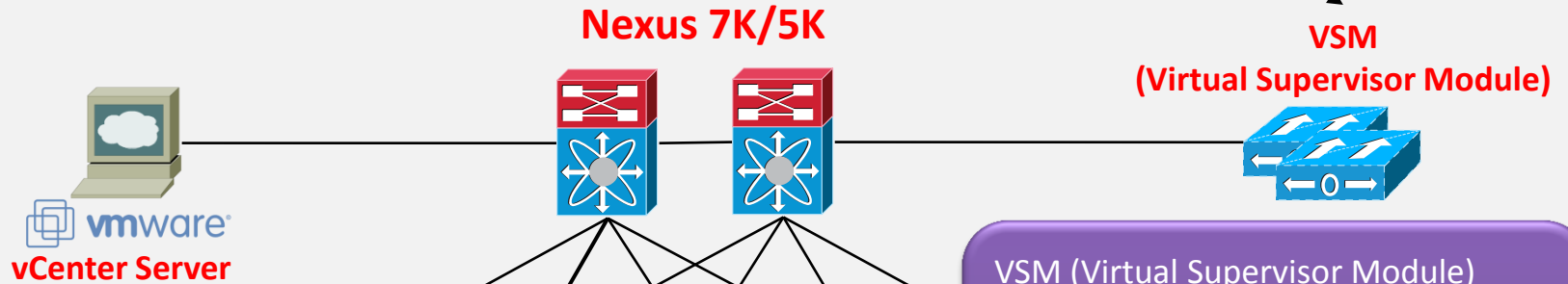
- Port profile 형태로 구성하여, vCenter 와 API 연동으로 VM 이동성 보장

무중단 운영 모델

- N1K Switch 통합 운영을 위한 VSM 구현으로 서버운영자와 네트워크 운영자 독립성 확보

Nexus 1000V 소개

나는 Nexus 7K/5K의 Supervisor 소프트웨어다.

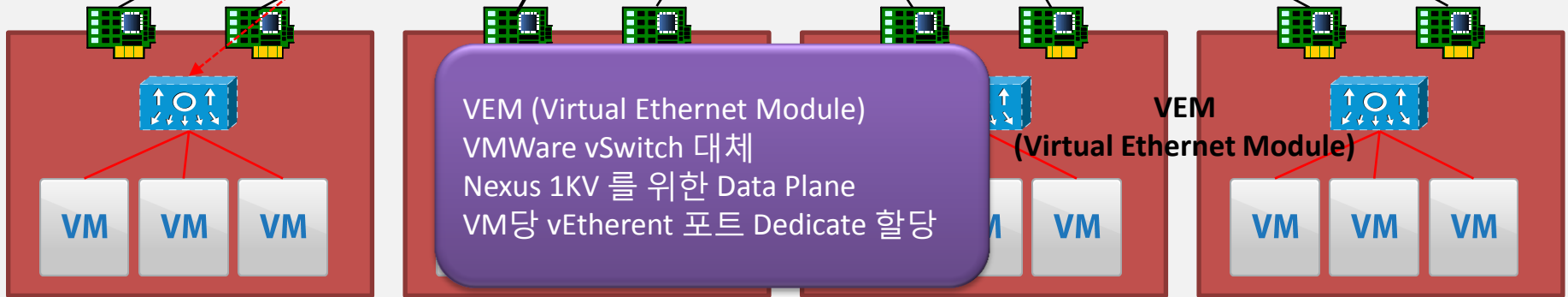


나는 Nexus 2000의 소프트웨어다.

VSM (Virtual Supervisor Module)
Nexus 1KV 기반의 CLI 구성
Nexus 1KV 를 위한 Control Plane
NX OS 기반
Virtual Chassis 형태의 구성

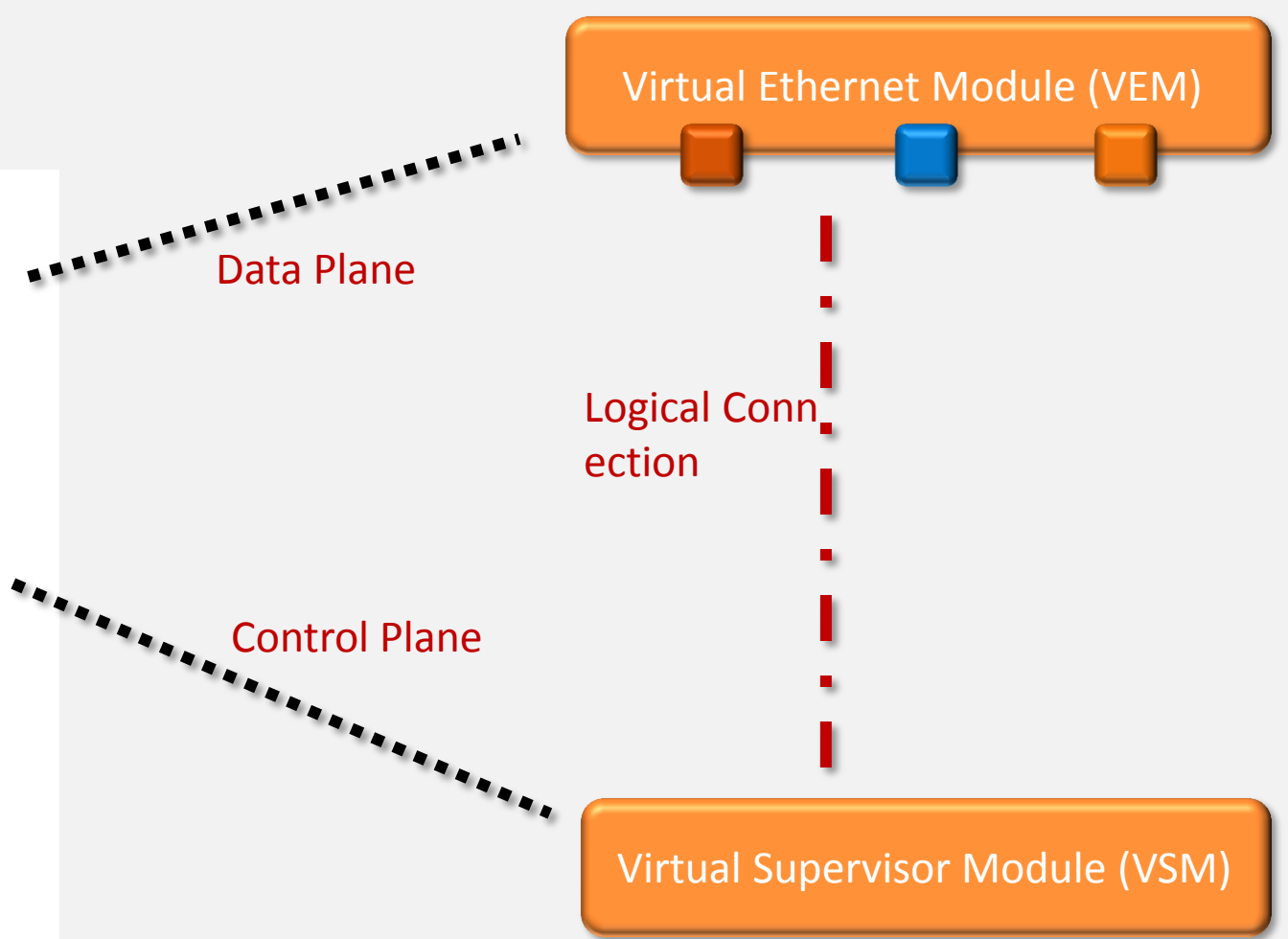
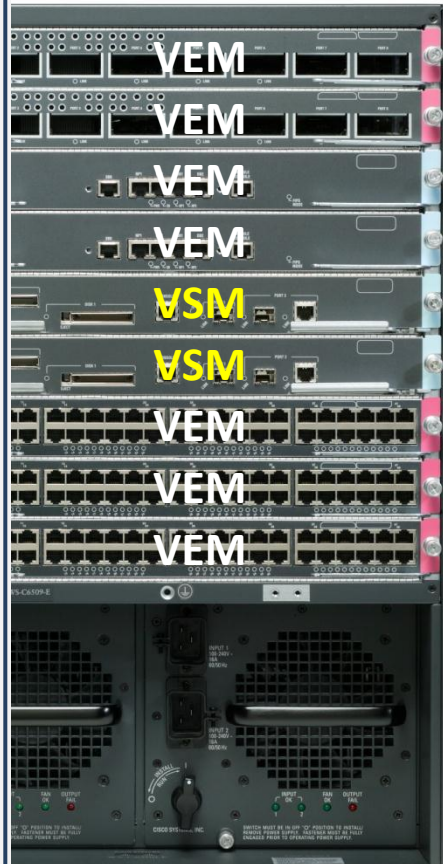
VEM (Virtual Ethernet Module)
VMWare vSwitch 대체
Nexus 1KV 를 위한 Data Plane
VM당 vEthernet 포트 Dedicate 할당

VEM (Virtual Ethernet Module)



Nexus 1000V 소개

가상 샤시



Virtual Ethernet Module (VEM)

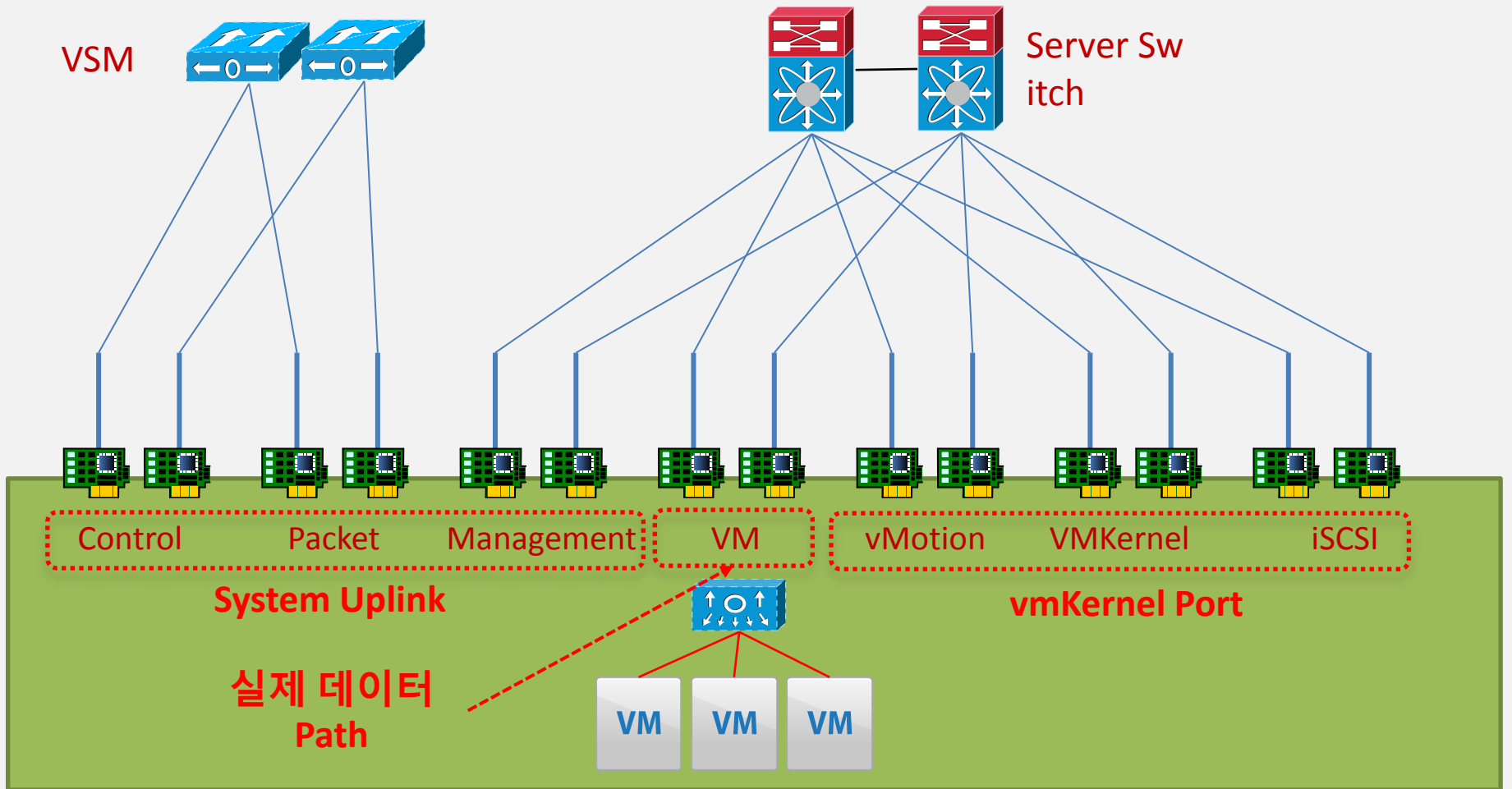
Data Plane

Logical Connection

Control Plane

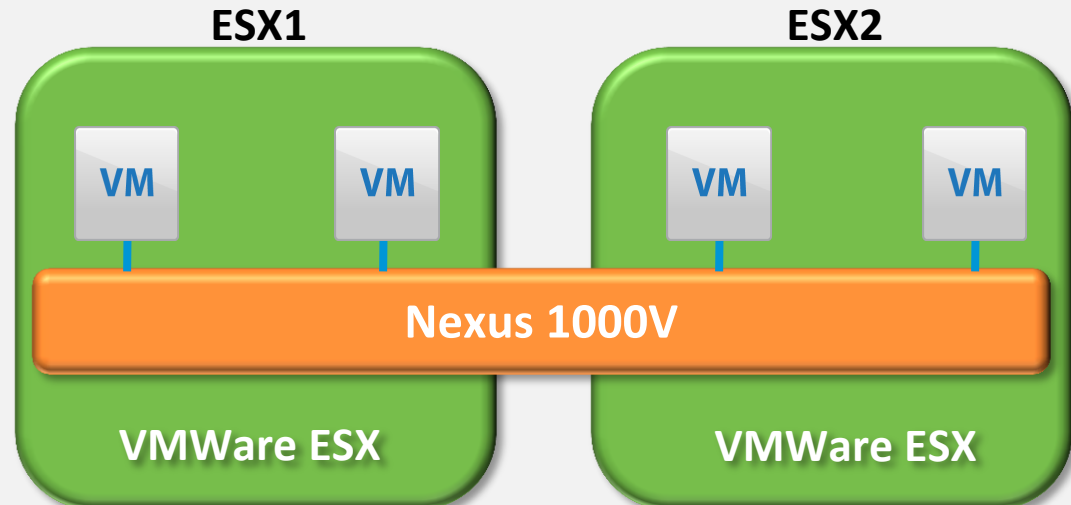
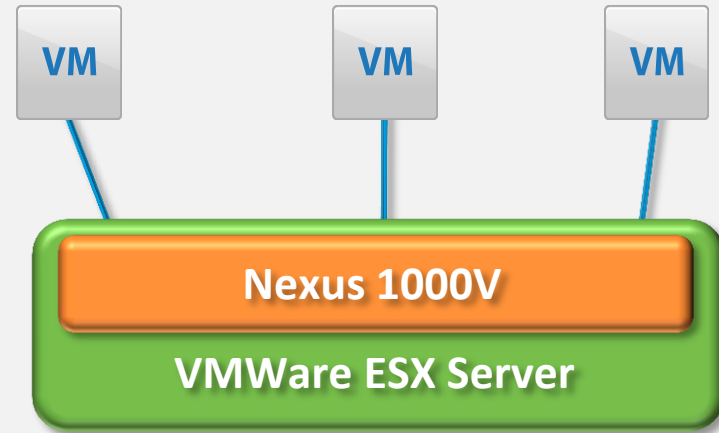
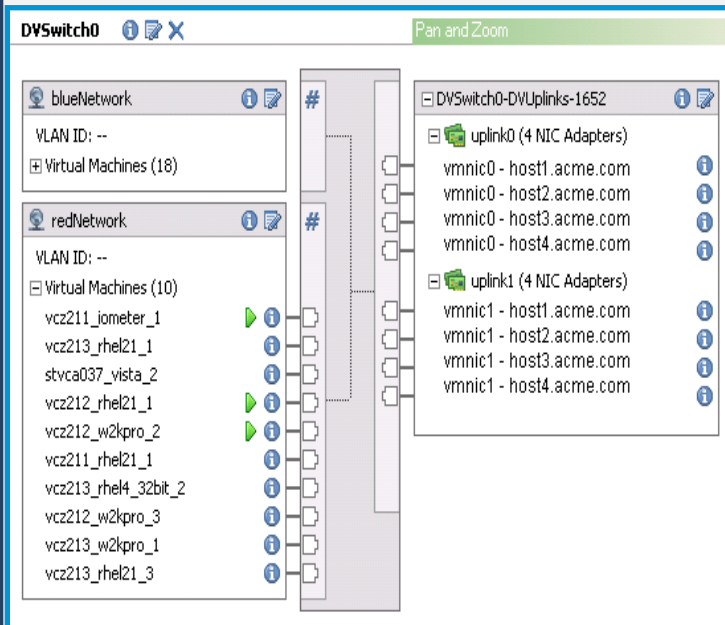
Virtual Supervisor Module (VSM)

Nexus 1000V IO 구성

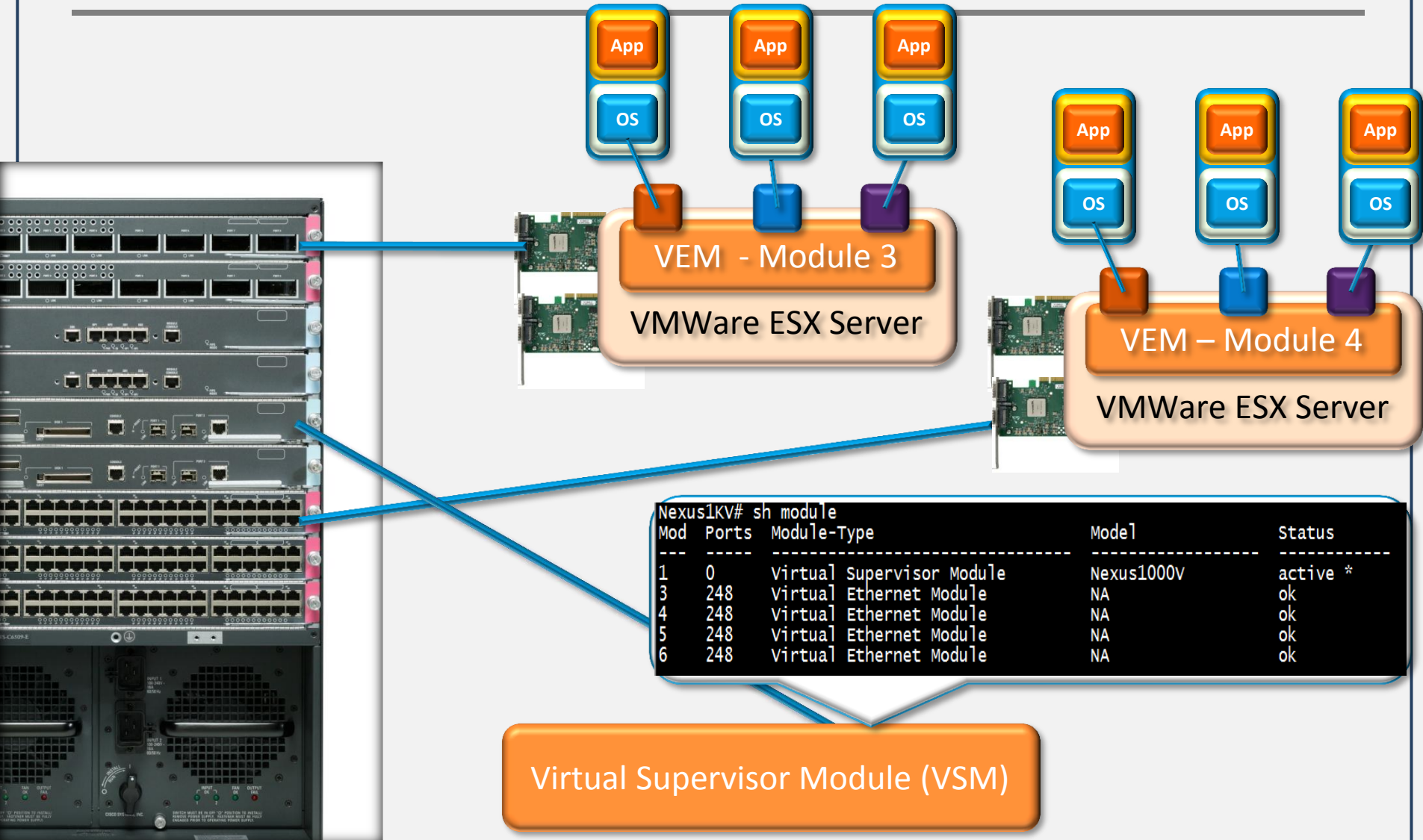


Nexus 1000V 소개 구성

Nexus 1000V 는 DVS를 대체하며,
vCetner와 API로 연동하여
VN-Link를 구현.



Nexus 1000V 소개 구성

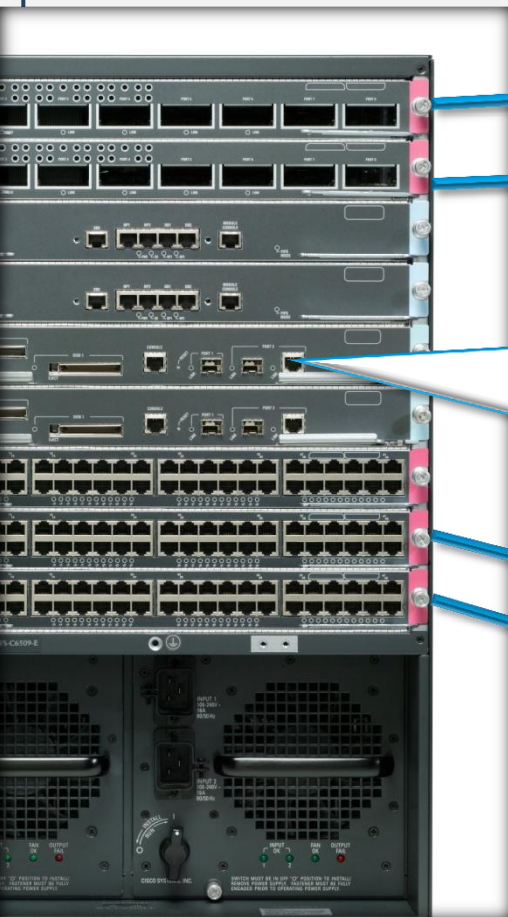


```
Nexus1KV# sh module
Mod Ports Module-Type Model Status
-----
1 0 Virtual Supervisor Module Nexus1000V active *
3 248 Virtual Ethernet Module NA ok
4 248 Virtual Ethernet Module NA ok
5 248 Virtual Ethernet Module NA ok
6 248 Virtual Ethernet Module NA ok
```

Virtual Supervisor Module (VSM)

Nexus 1000V 소개 구성

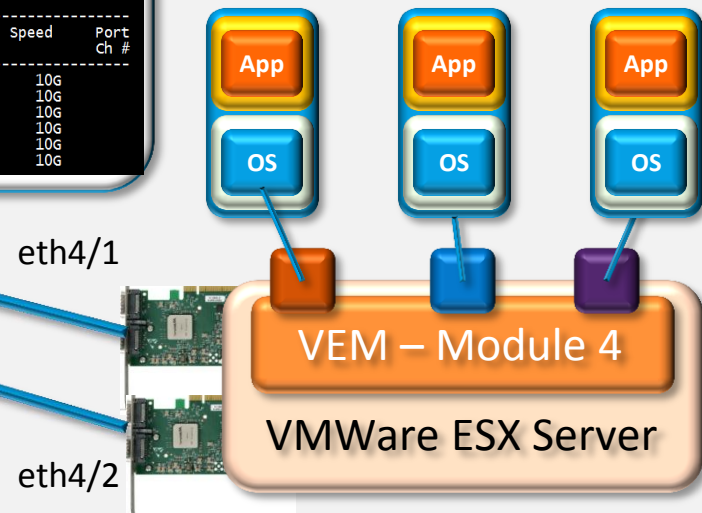
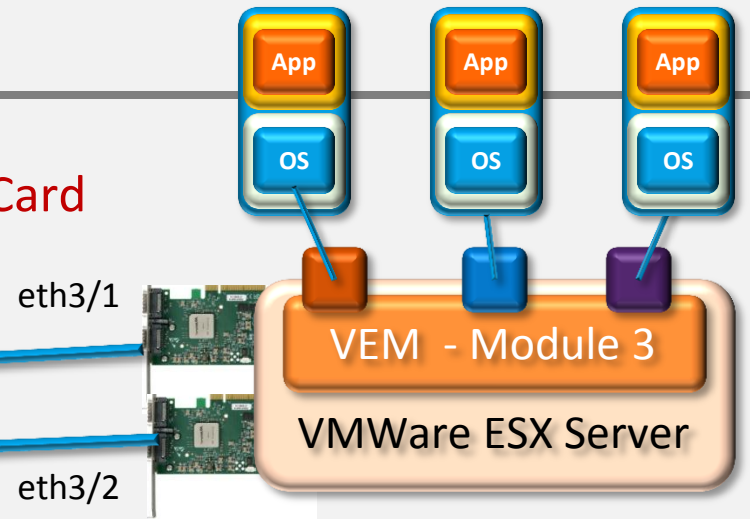
“ethernet” = ESX 서버의 업링크/물리적 NIC Card



```
Nexus1KV# sh interface brief
```

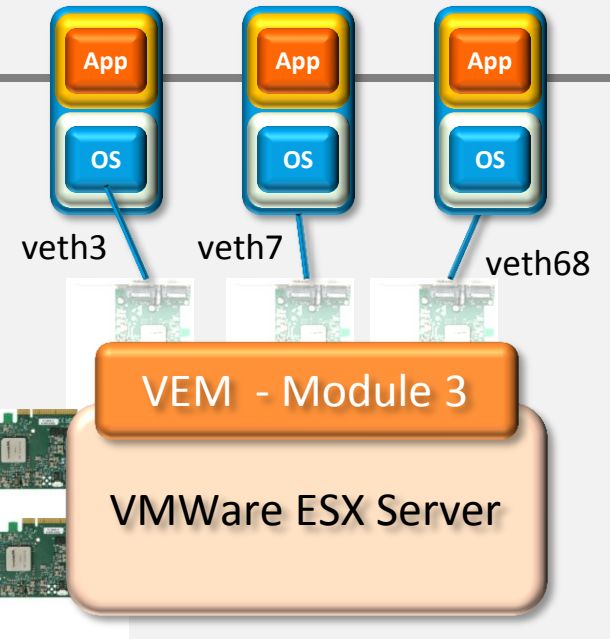
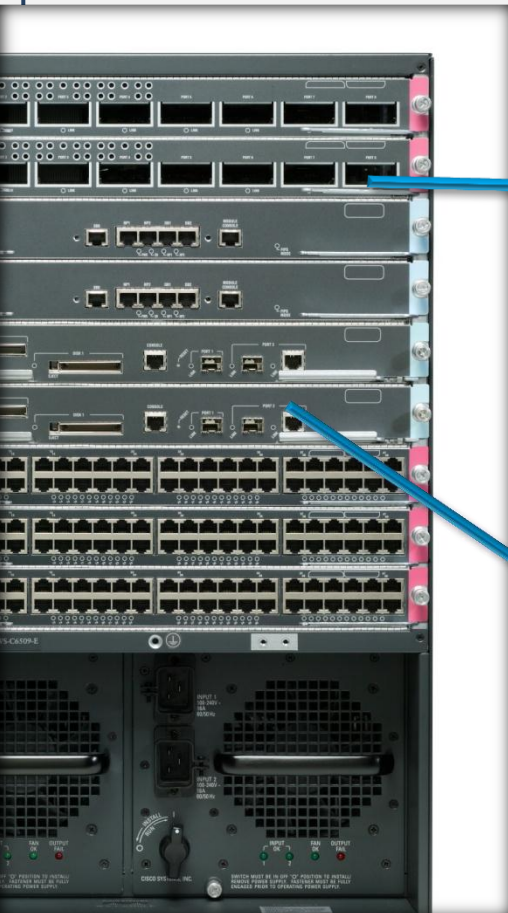
Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	10.72.83.91	1000	1500

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch #
Eth3/2	1	eth	trunk	up	none	10G	
Eth3/7	4	eth	access	up	none	10G	
Eth4/2	1	eth	trunk	up	none	10G	
Eth4/7	4	eth	access	up	none	10G	
Eth5/2	1	eth	trunk	up	none	10G	
Eth6/2	1	eth	trunk	up	none	10G	



Nexus 1000V 소개 구성

vethernet = ESX의 vNIC과 동일

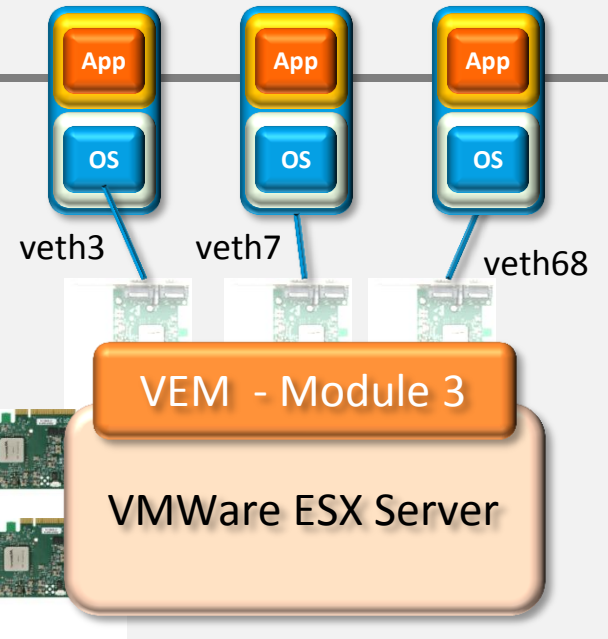
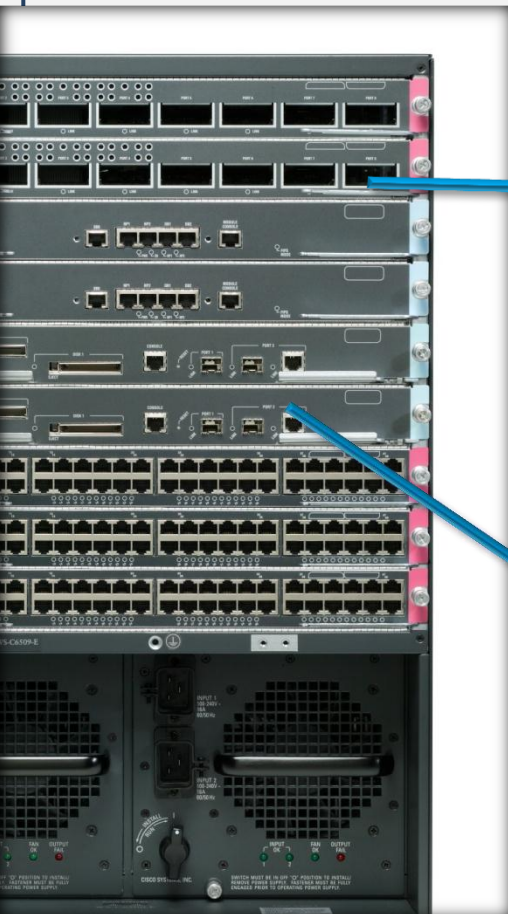


```
Nexus1KV# sh interface virtual
-----
Port      Adapter      Owner                               Mod Host
-----
Veth1     Net Adapter 2 Nexus1000VSG                       4 10.72.83.82
Veth2     Net Adapter 1 w2K8-DEMO-02                       4 10.72.83.82
Veth3     Net Adapter 1 Virtual Network Manageme          3 10.72.83.81
Veth4     Net Adapter 3 Nexus1000VSG                       4 10.72.83.82
Veth5     Net Adapter 1 Nexus1000VSG                       4 10.72.83.82
Veth6     Net Adapter 1 w2K8-DEMO-04                       4 10.72.83.82
Veth7     Net Adapter 1 w2K8-DEMO-01                       4 10.72.83.82
Veth8     Net Adapter 1 w2K8-DEMO-03                       4 10.72.83.82
```

Virtual Supervisor Module (VSM)

Nexus 1000V 소개 구성

Port-Profile = ESX의 Port-Group과 동일



```
Nexus1KV# sh port-profile brief
```

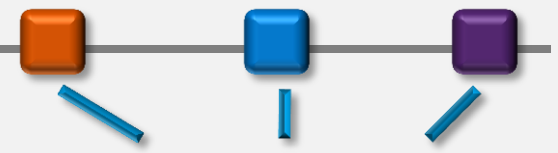
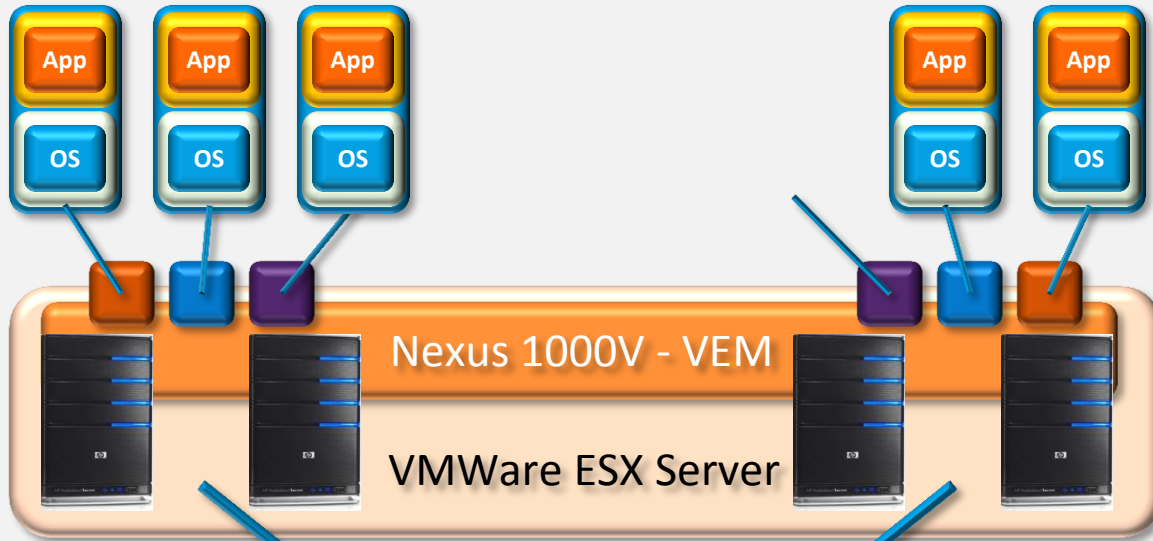
Port Profile	Profile Type	Profile State	Conf Items	Eval Items	Assigned Intfs	Child Profs
Gold-SVC	Vethernet	1	3	3	2	0
Mgmt_Net	Vethernet	1	3	3	2	0
N1KV_Control	Vethernet	1	3	3	0	0
N1KV_Packet	Vethernet	1	3	3	0	0
N1KV_SVC_Network	Vethernet	1	6	6	1	0
N1KV_SVC_UpLink	Ethernet	1	3	3	2	0

Virtual Supervisor Module (VSM)

Nexus 1000V 소개 구성

Port-Profile 은 일반적인 스위치에서 속성값을 의미

VM Motion이 발생해도 Port-Profile에 의해 속성값 유지



- Port Profile**
- VLAN, PVLAN settings
 - ACL, Port Security, ACL Redirect
 - Cisco TrustSec (SGT)
 - NetFlow Collection
 - Rate Limiting
 - QoS Marking (COS/DSCP)
 - Remote Port Mirror (ERSPAN)



클라우드/가상화를 위한 보안을 그린다.

Physical | Virtual | Cloud Journey

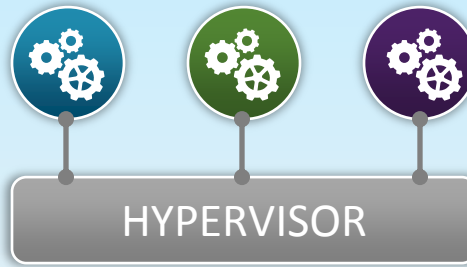
PHYSICAL WORKLOAD

- 서버당 1개 App
- Static
- 수동 provisioning



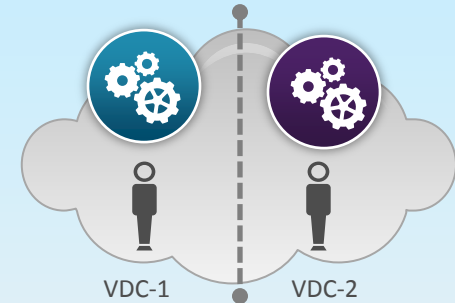
VIRTUAL WORKLOAD

- 서버당 여러 개 App
- Mobile
- 동적 provisioning



CLOUD WORKLOAD

- 서버당 Multi-Tenant
- Elastic
- Automated Scaling



정책, 기능, 보안, 관리, 역할의 분리

스위칭

Nexus 7K/5K/3K/2K

Nexus 1000V, VM-FEX

라우팅

ASR, ISR

Cloud Services Router (CSR 1000V)

서비스

WAAS, ASA, NAM

vWAAS, VSG, ASA 1000V, vNAM

컴퓨팅

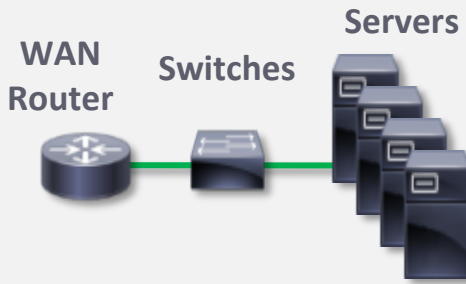
Bare Metal 기반 UCS

가상화된 Workload 기반의 UCS

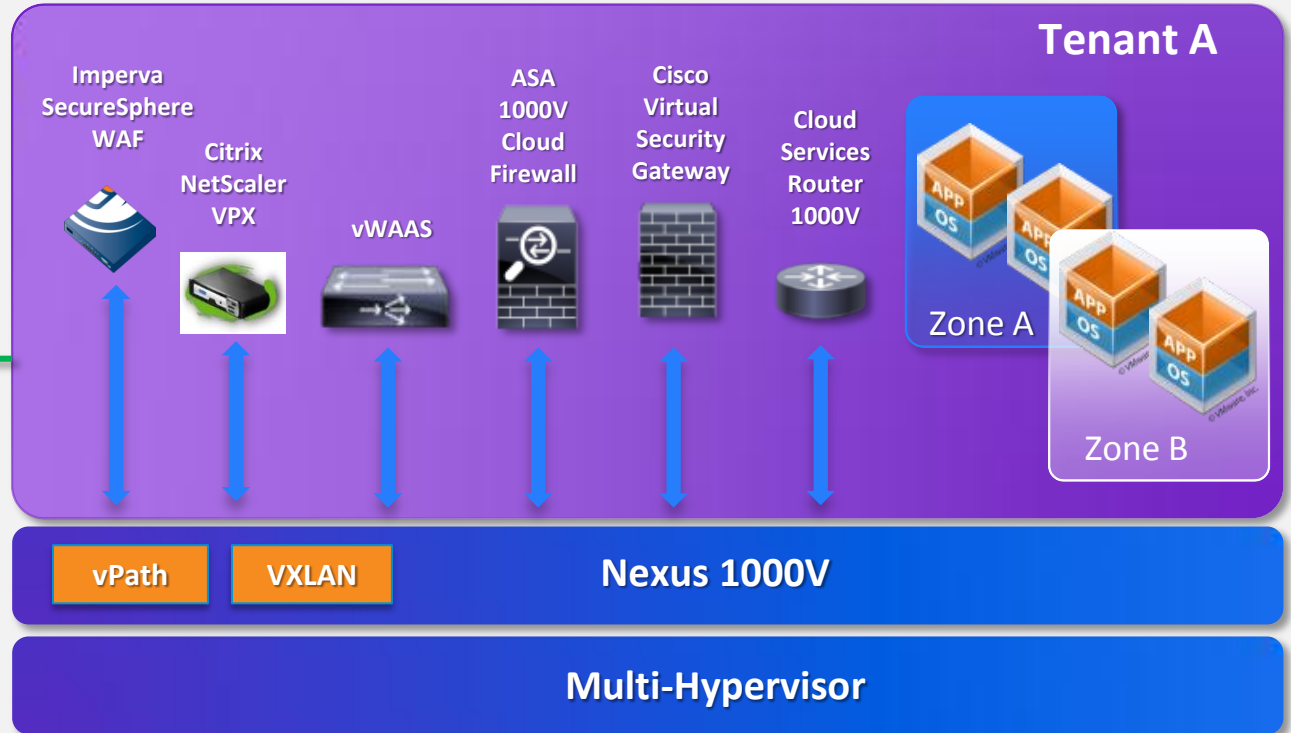
시스코의 VSN (Virtual Service Network) 아키텍처

클라우드 네트워크 서비스

가상화.클라우드 Data Center



물리적 인프라



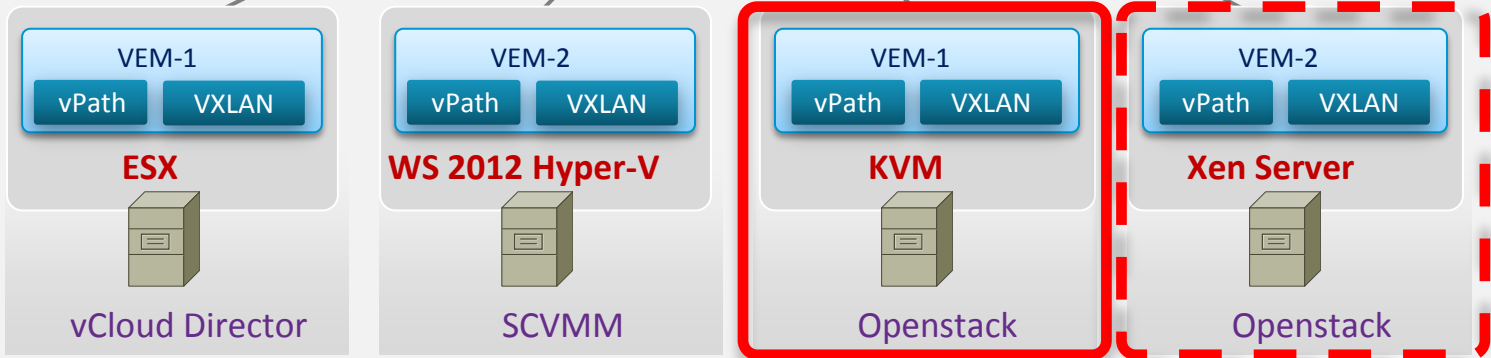
Nexus 1000V	VSG	ASA 1000V	vWAAS	CSR 1000V (Cloud Router)	Ecosystem Services
<ul style="list-style-type: none"> 분산형 스위치 NX-OS 기반 구성 	<ul style="list-style-type: none"> VM 기반 제어 Zone 기반 방화벽 역할 	<ul style="list-style-type: none"> Edge firewall, VPN Protocol Inspection 	<ul style="list-style-type: none"> WAN 최적화 Application traffic 가속 	<ul style="list-style-type: none"> WAN L3 gateway Routing & VPN 	<ul style="list-style-type: none"> Citrix NetScaler VPX virtual ADC Imperva Web App. Firewall
6000+ Customers	Shipping	Shipping	Shipping	Beta	Plan

시스코의 VSN (Virtual Service Network) 아키텍처



일관성 있는 기능 구현
 일관성 있는 네트워크 서비스
 일관성 있는 운영 모델

투자 보호 효과
 설치 및 운영시간 단축 효과
 위험요소 감소



시스코의 VSN (Virtual Service Network) 아키텍처

Nexus 1000V 무료 선언

무료 버전

CPU당 \$695

Nexus 1000V Essential 에디션

세계 최고의 가상 스위치 기술 제공

- 모든 L2 기능 제공
- Security, QoS 기능 제공
- VXLAN virtual overlay 기술 제공
- 관리 및 모니터링 기술 제공
- vPath 기반의 Virtual Service 제공

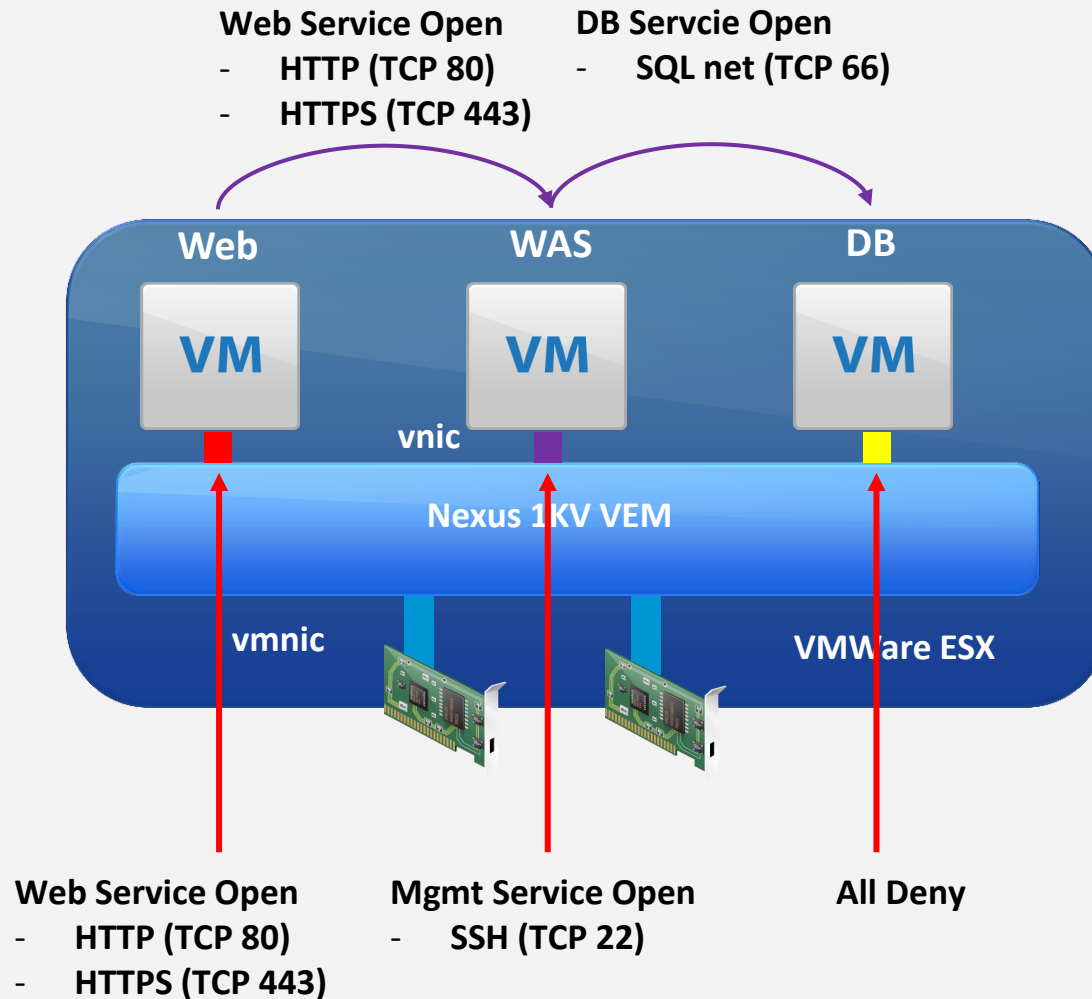
Nexus 1000V Advanced 에디션

Adds Cisco value-add features for DC and Cloud

- 제약 없는 모든 기술 제공
- VSG firewall 번들 제공
- Cisco TrustSec SGA 정책 제공
- 시스코 DC 향후 모든 기술 제공

업계 최초의 모든 하이퍼바이저 플랫폼에
무료 Nexus 1000V 기술 제공

왜 VSN (Virtual Service Network)이 필요한가?



시스코의 VSN (Virtual Service Network) 아키텍처

Virtual Security
Gateway (VSG)
ASA 1000V
CSR 1000V

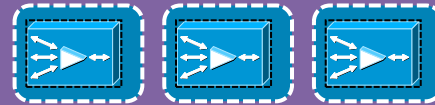


On Nexus 1000V

Virtual Network
Management Cent
er (VNMC)



Virtual WAAS



ESX ESXi Hypervisor
w/ Nexus 1000V

UCS /x86 Servers

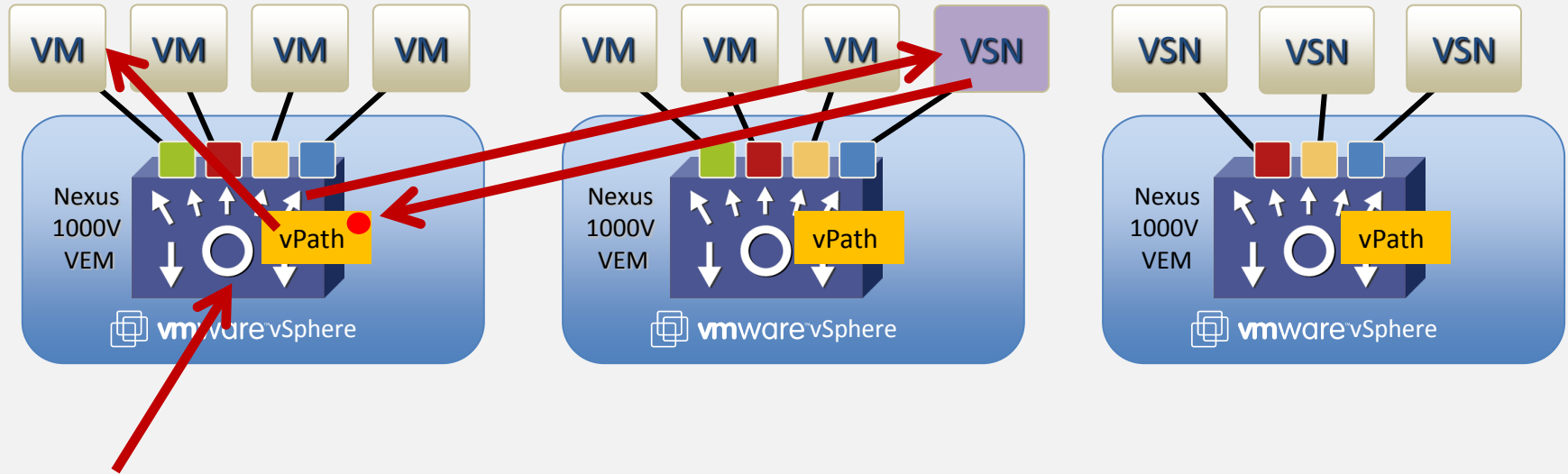


vPath

Nexus 1000V

시스코의 VSN (Virtual Service Network) 아키텍처

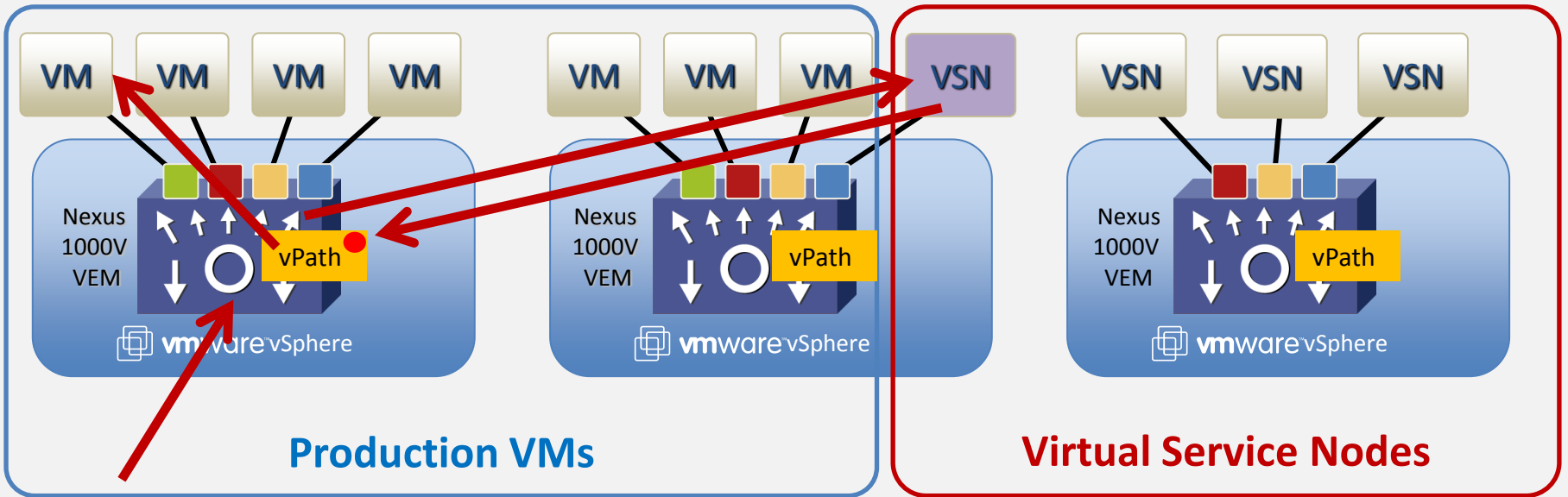
VSN Flow



**VSN(Virtual Service Node) 기반의
1st Flow**

시스코의 VSN (Virtual Service Network) 아키텍처

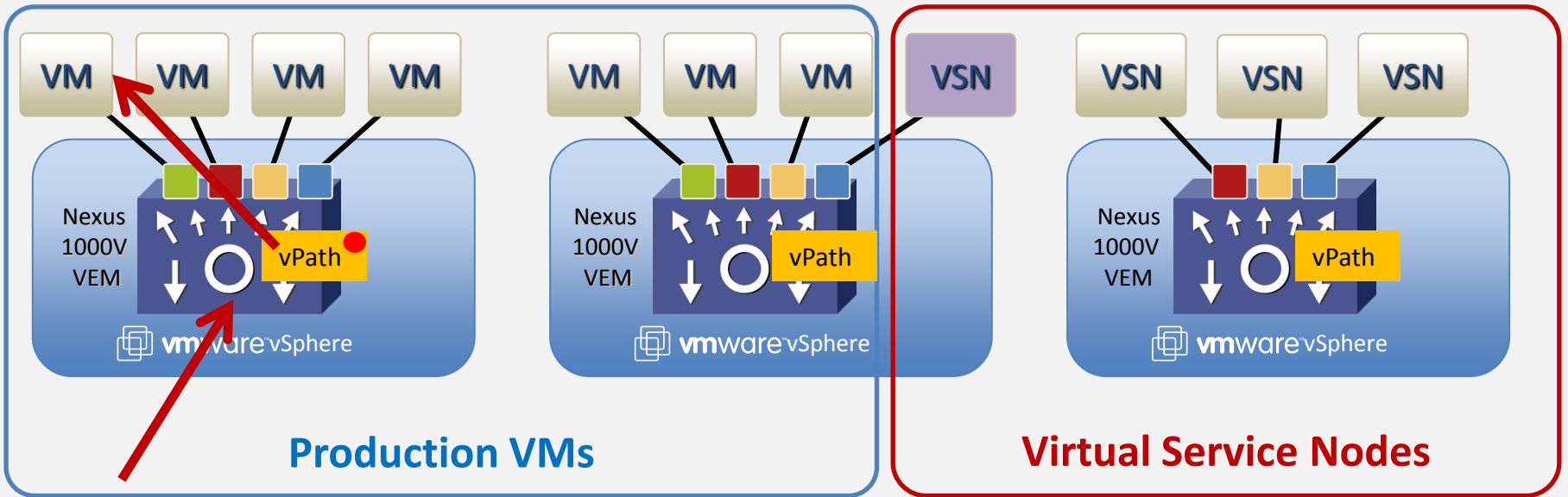
VSN Flow



**VSN (Virtual Service Node) 기반의
2nd Flow**

시스코의 VSN (Virtual Service Network) 아키텍처

VSN Flow



**VSN (Virtual Service Node) 기반의
2nd Flow**

시스코의 VSN (Virtual Service Network) 아키텍처

VSG 의 특징과 관리의 편의성

Virtual Security Gateway (VSG)



Context aware Security

VM 상태 인식 기반 보안 정책

Zone based Controls

Zone 기반의 제어

Dynamic, Agile

vMotion 기반의 보안 정책 이동성

Best-in-class Architecture

가상화 기반의 최상의 보안 기술

Virtual Network Management Center (VNMC)



Non-Disruptive Operations

최적의 가상화 운영 모델 제공

Policy Based Administration

Multi-tenancy 모델 구현

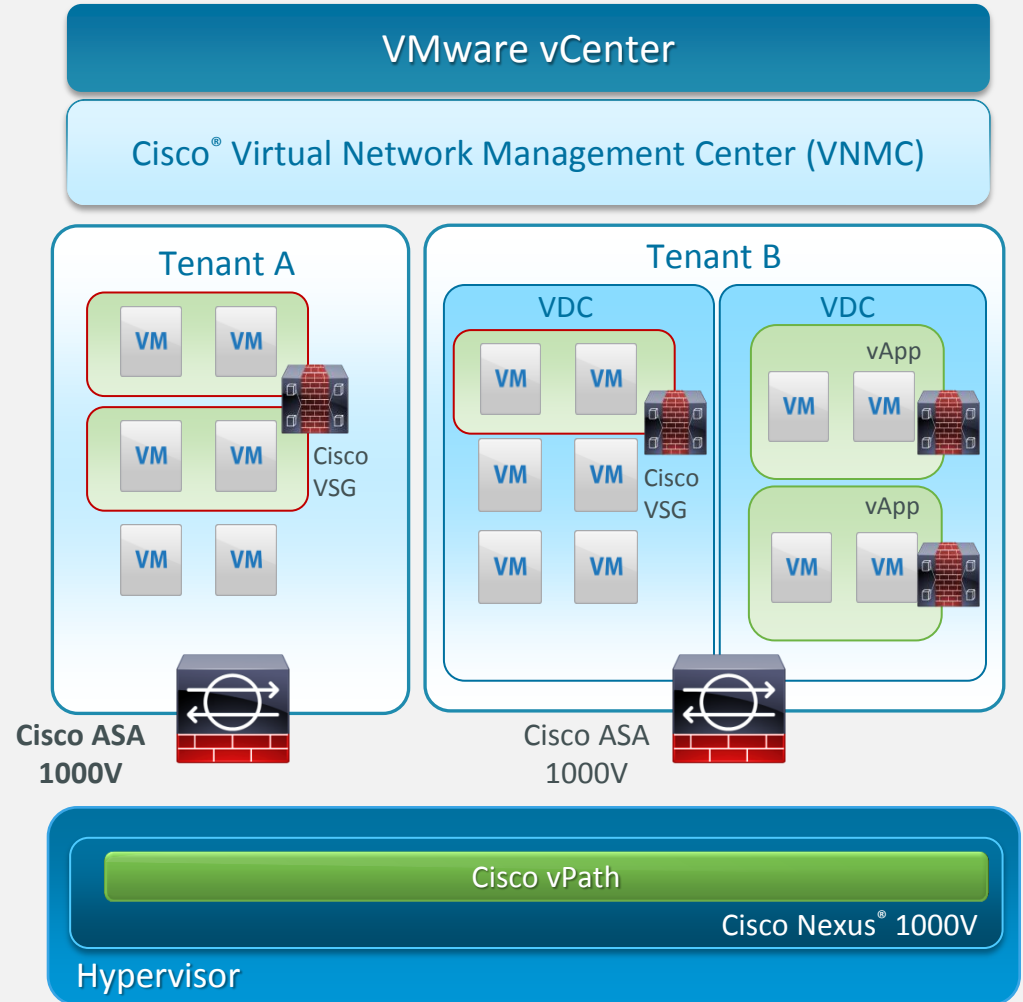
Designed for Automation

XML API 기반 보안 정책 적용

시스코의 VSN (Virtual Service Network) 아키텍처

ASA 를 가상화로 풀어내다.

- 검증된 시스코 보안 기술 적용:
일관성 있는 보안 운영 모델
- 협업화된 보안 구현 모델
 - intra-tenant secure zones : VSG
 - tenant edge controls : Cisco ASA 1000V
- 간편한 보안 구성 모델
 - Cisco Nexus® 1000V Switch 기반의 vPath 기술을 활용한 구현
- 확장성 높은 유연한 보안 구성
 - 데이터센터 내부 또는 데이터센터 간 Scale Out 형태의 구성시 보안 적용에 유리



Thank you