Virtualization System Security Service

Jacob Chen

Secure Virtualization: A New Paradigm

- **Virtualization is the most important solution being implemented in the Enterprise Data Center today.**

- **This creates the need for a ‘security for virtualization’ paradigm that protects virtual environments in ways beyond what is currently available to protect physical environments.**

<u>Gartner Group:</u>

Enterprises that do not leverage virtualization technologies will spend 25% more annually for hardware, software, security, labor, and space for their infrastructure.

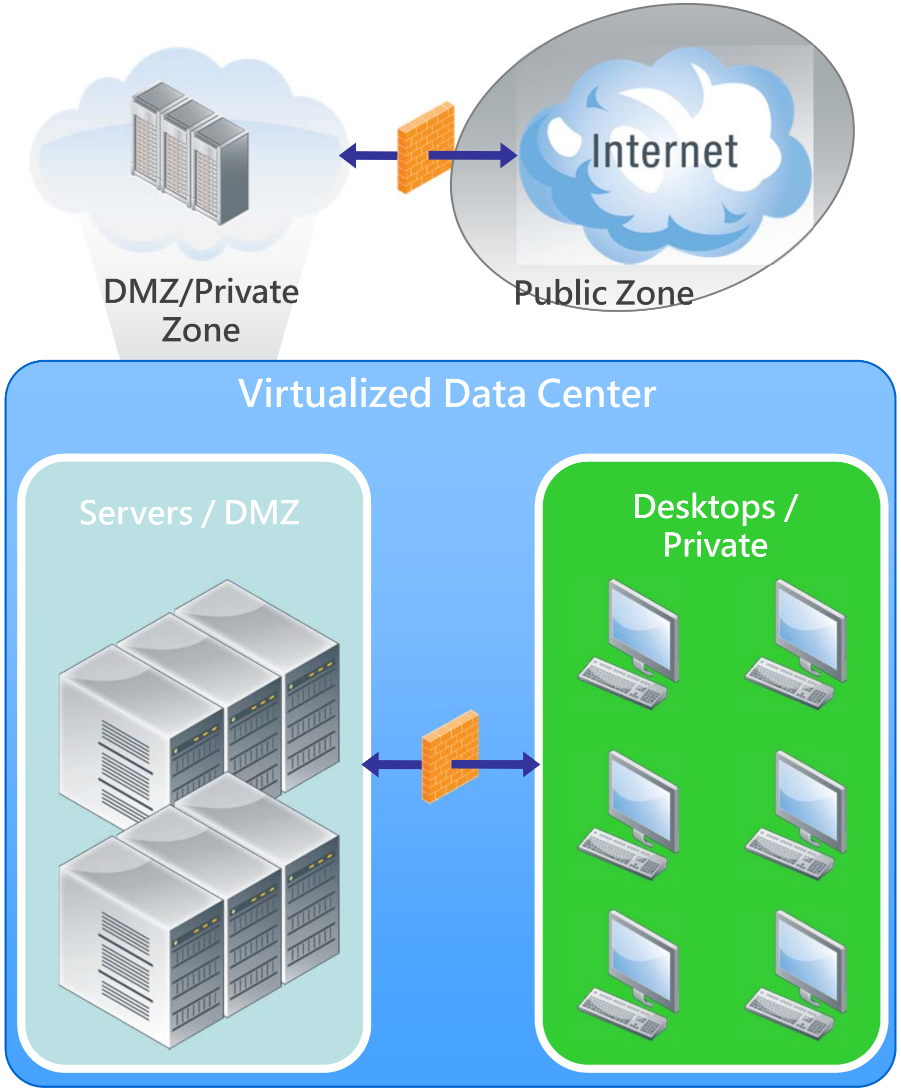
Virtualized Data Center Security

Logical Security Zones are used to isolate hosts with differing security requirements

- Servers
- Desktops

Primary security goal: separation of logical zones

- Virtual perimeters
- Firewalling between zones



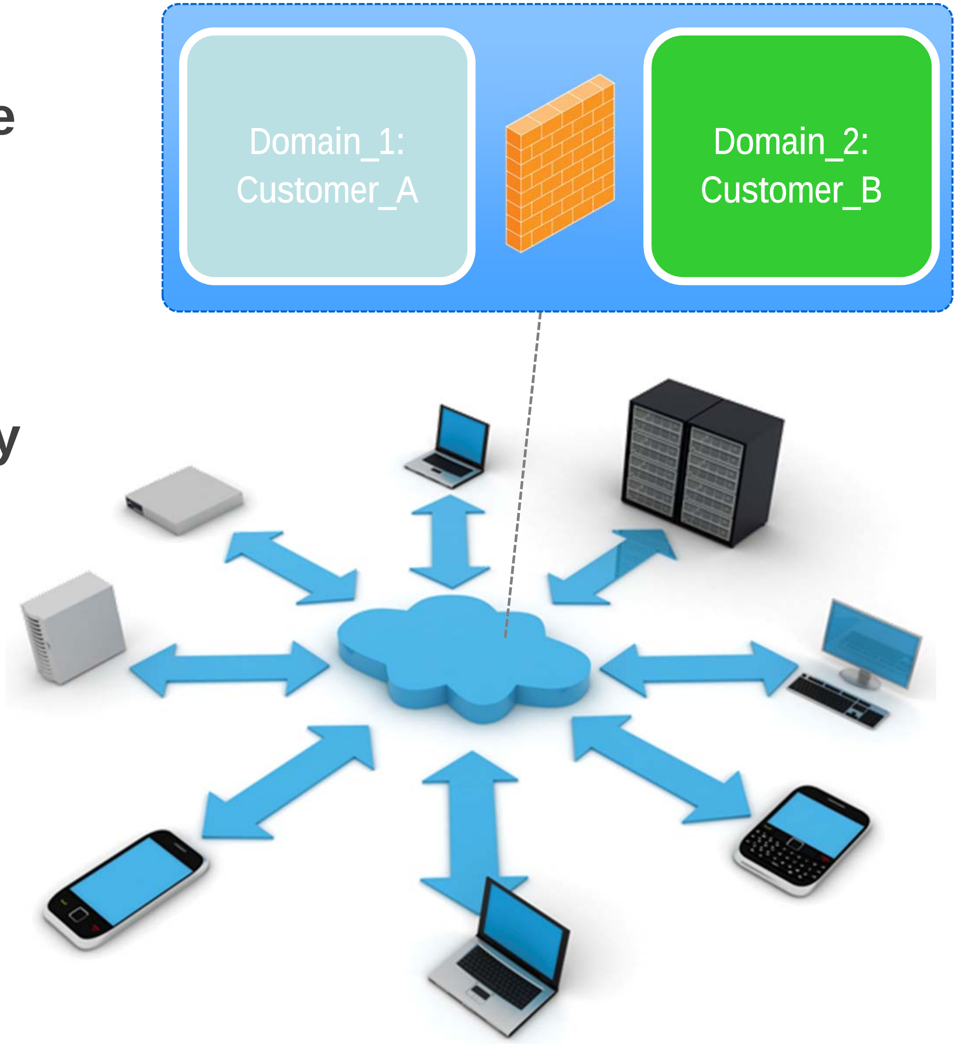
Virtualized Computing Security

Generally, security zones are more abstract but vary by cloud model

- Domains are a good model for security
- Maintaining confidentiality and integrity between domains is key

Some major security concerns

- High levels of risk exposure
- Loss of visibility
- Lack of security controls
- Maintaining compliance



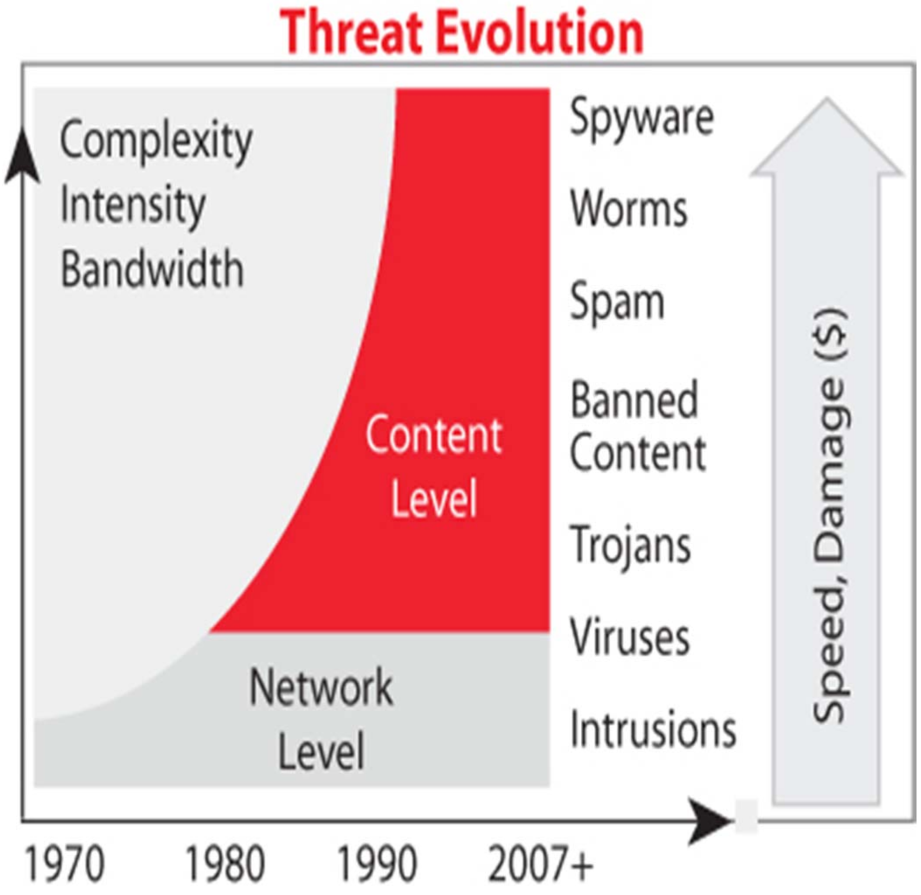
Security Threat Evolution

- **Multiple Threat Types**
  - Various Application Entry Points
  - Different Functions
  - Threat Payload Intent Varies
  - Broad Range of Propagation Techniques

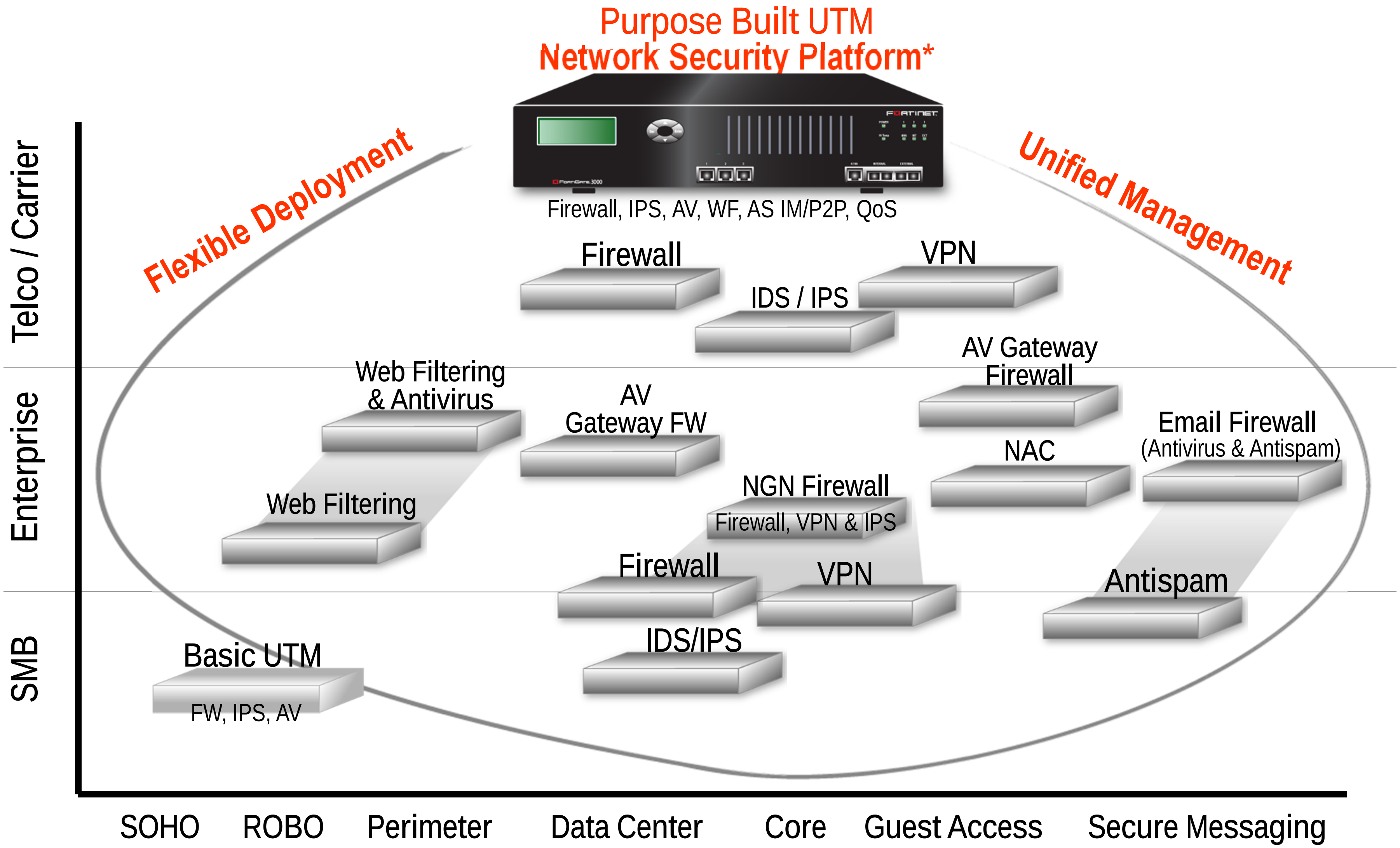
- **Content Level Threats**
  - Viruses & Spyware
  - Spam & Directory Harvest Attacks
  - Web Phishing

- **Network Level Threats**
  - Network Worms
  - DDOS/DOS
  - IP Packet Capture
  - Spoofing & Man-In-The-Middle

- **Crime ware is here!**
  - Intent of cyber threats are malicious
  - Hackers funded by organized crime



Purpose-Built UTM



* *Unified security exceeds sum of previous generation products*

Why Virtualization?

- Virtualization provides multiple instances of a software system on a single hardware platform
  - Allows server hardware to be shared by different applications
  - Provides separate management of individual application access
  - Reduces the amount of servers needed in data centers
  - Reduces network hardware and switch ports
  - Improves utilization of under-used resources
- Data Centers use virtual servers to save rack space, electricity, cooling, cabling and reduce staffing requirements.
- Virtual security systems are used to maximize the use of security and networking hardware systems in data centers.
- Virtual Domains can be used to front-end VMware servers
  - Different levels of security can be set for each VMware instance
  - Provides a complete security solution for VMware -- VMware currently has no security
- Virtual Domains can be used to provide custom levels of security for each customer in a multi-customer environment.

Virtualization Strategy

NTHU enables cloud computing providers and large enterprises to create secured virtual infrastructures.

Proven Success

Our virtualization technologies secure a wide range of public, private, and hybrid cloud infrastructures around the world.

Platform Choice

Hardware and virtual security options, working together, with a ‘single pane of glass’ management platform.

Fully Integrated

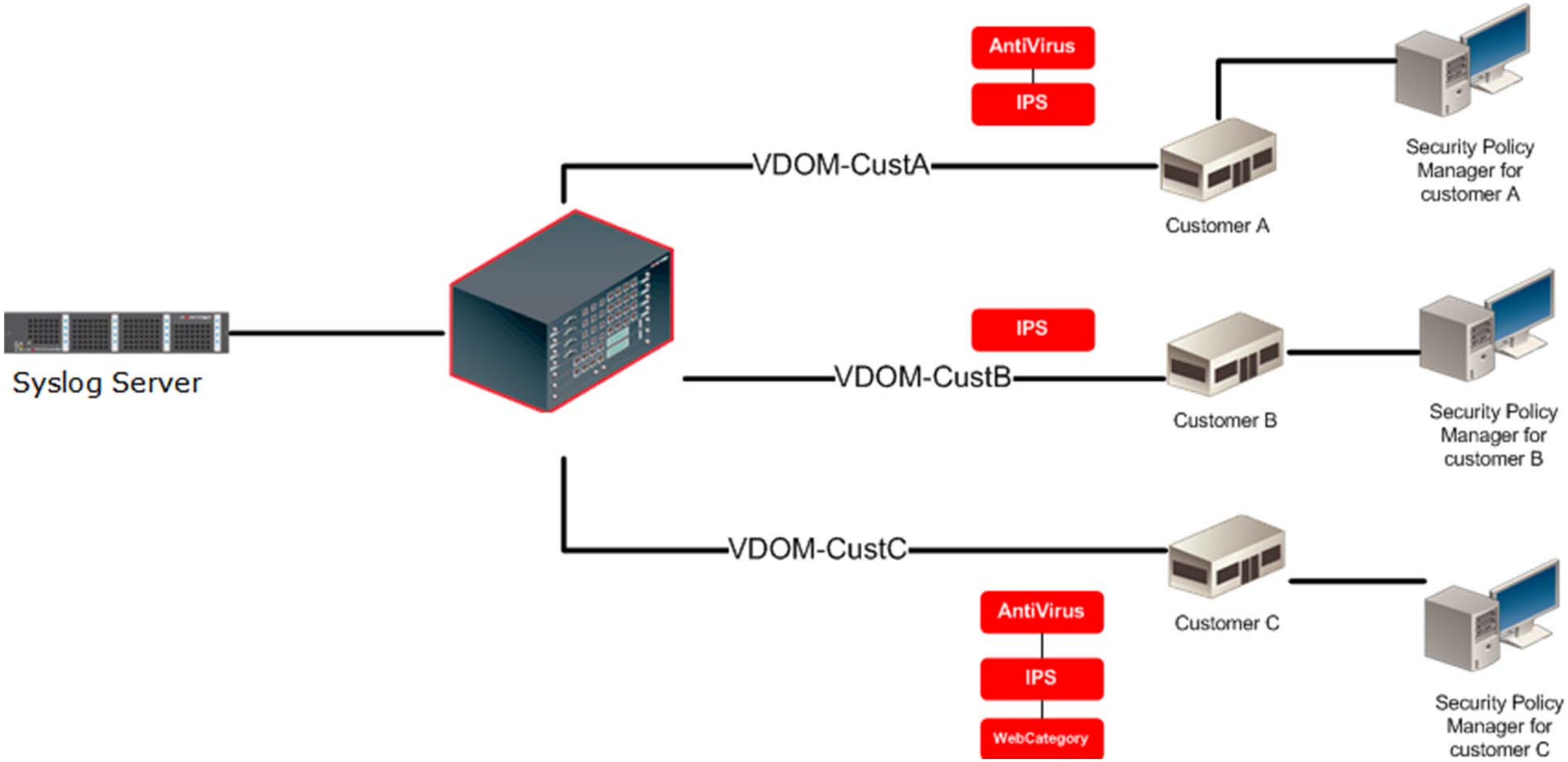
Our security and networking technologies are fully-owned and completely integrated for simplified licensing, deployment, and management.

What is a Virtual Domain?

- Virtual Domains (VDOMs) are containers for virtualized security devices
  - Allows security hardware to be shared by different organizations
  - Provides separate management of individual VDOMs
    - Customer A has their own management interface
    - Customer B has their own management interface
  - Allows a global admin to control privileges of VDOM administrators
  - Provides separate security zones, FW objects, routing tables, user groups, VPN configurations, logging to local disk, etc.
- MSSP/Service providers use VDOMs to separate customers traffic
- Enterprises use VDOMs to separate business units or departments
- VDOMs reduce the overall cost of security infrastructure
- All management, reporting, and logging flows from root domain
  - VDOM name tags are added to each log message.
  - Per VDOM reports are available from log server
  - We also supports Admin Domains (ADOMs) to prevent admins from accessing logs/reports outside of their domain.

Security VDOMs

Each VDOM contains its own virtual interfaces, route table, state table, application proxies, and IPS table instances.


AntiVirus
IPS
VDOM-CustA
Customer A
Security Policy Manager for customer A
Syslog Server
IPS
VDOM-CustB
Customer B
Security Policy Manager for customer B
VDOM-CustC
Customer C
AntiVirus
IPS
WebCategory
Security Policy Manager for customer C

100% Security Technology

Fully-owned and completely integrated security and networking technologies simplify licensing, deployment, and management.

Firewall

VPN

Antivirus

Intrusion
Preventio
n

WAN
Optimization

Antispam

Web Filter

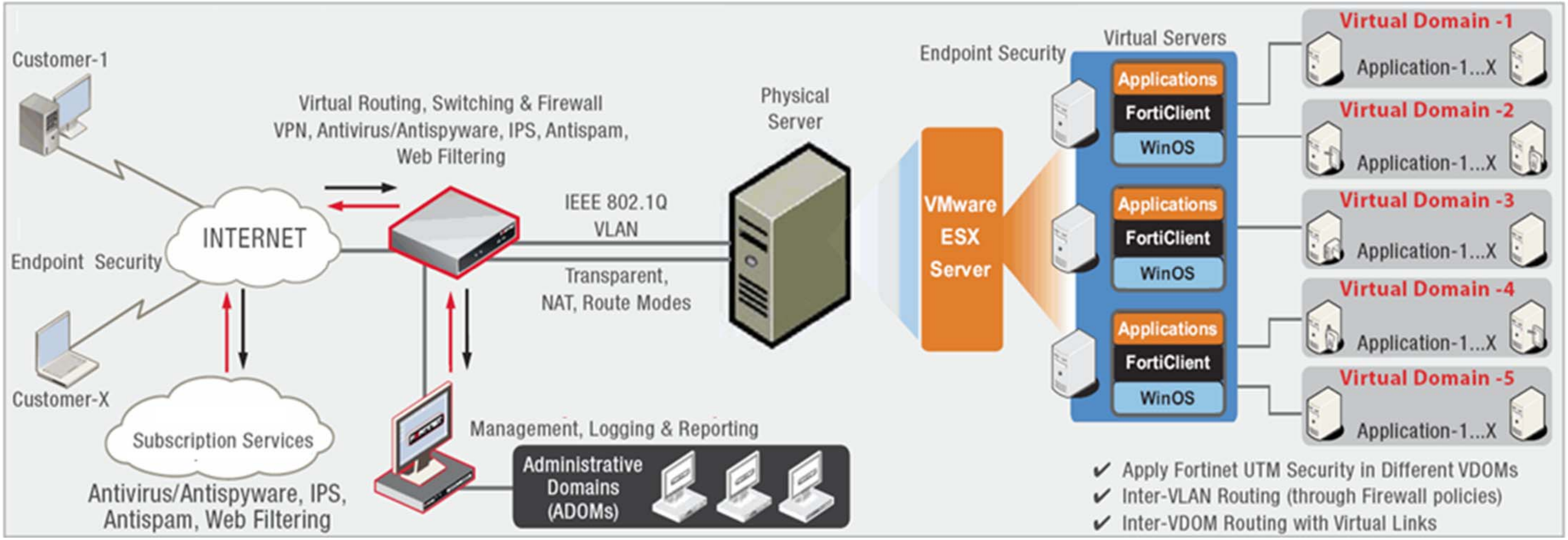
App
Control

Data Loss
Preventio
n

Vulnerability
Scan

No Per-User Licenses

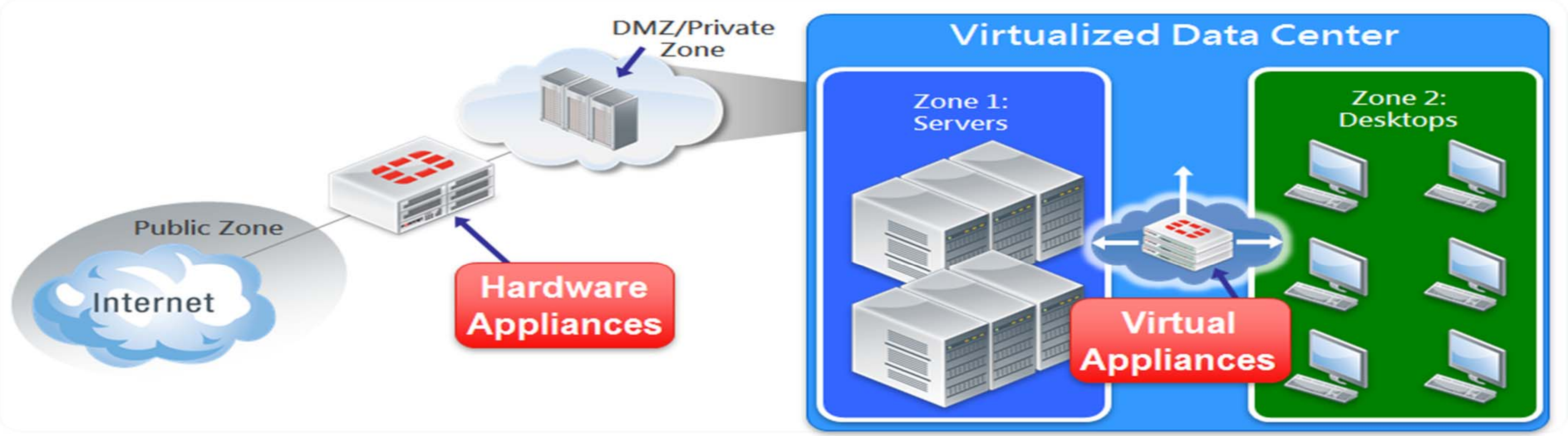
Joint Deployment Scenario – Data Center



- ✔ Apply Fortinet UTM Security in Different VDOMs
- ✔ Inter-VLAN Routing (through Firewall policies)
- ✔ Inter-VDOM Routing with Virtual Links

選擇計中虛擬主機的優點

- 在每一個Virtual Server的前端, 都會提供專屬的資安防護.
- 而每一個Virtual Firewall, 都能夠提供不同需求的資安服務, 例如: FW、IPS、Vulnerability Scan、AntiVirus、DoS 、…
- 中心已通過 ISMS資安認證, 以及全天24小時不中斷的備援服務, 各系所不需要再耗費經費與人員去維護硬體
- 研究人員應該要專心做專精的領域, 運算這部分就要讓雲端虛擬服務來做, 這樣也可以減少教授的負擔, 並且透過資源共享來降低成本
- 達到 "降低成本、提高可用性、增加管理彈性、長遠性"



Thank You!