

Security Models for Cloud

Kurtis E. Minder, CISSP

Introduction

Kurtis E. Minder, Technical Sales Professional

Companies:



Roles:

- Security Design Engineer
- Systems Engineer
- Sales Engineer
- Salesperson
- Business Development
- Global Account Manager

Actual work:

- Installation / Configuration
- Design
- Support
- Product development / POC
- Audit
- Penetration testing
- Sales / BD



CISSP Certification

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security CISSP
- Security Architecture and Design

The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.



Agenda

- Introductions
- Security Consolidation
- Cloud Security Models
 - Cloud Security
 - Security for Cloud Apps
- Who Pays this Guy?
- Q&A



Consolidate, *they* said.

- ✦ Gartner
- ✦ IDC
- ✦ Frost & Sullivan

- ✦ Point of Failure,
Multiple Consoles,
Troubleshooting
Difficulty, Licensing



U T M

- ✦ Unified Threat Management


- ✦ Fortinet Maintains the Lead
- ✦ Cisco and Juniper Follow

- ✦ Why UTM?

- ✦ Consolidated Approach
- ✦ Economic Benefits
- ✦ Architectural Benefits
- ✦ Security Benefits (Best of breed not best after all?) <-- Not Rhetorical



Case Study - UTM

- Massive Organization
 - Too Many Internet Connections
 - Too Many Devices
 - Too Many Vendors
 - Too Many Management Consoles
- 
- Carrier Partner Delivers Connectivity
 - Hosted Security in Wiring Center
 - Mutlitenant
 - Multi-discipline (UTM)
 - Customer Portal Interface

M S S



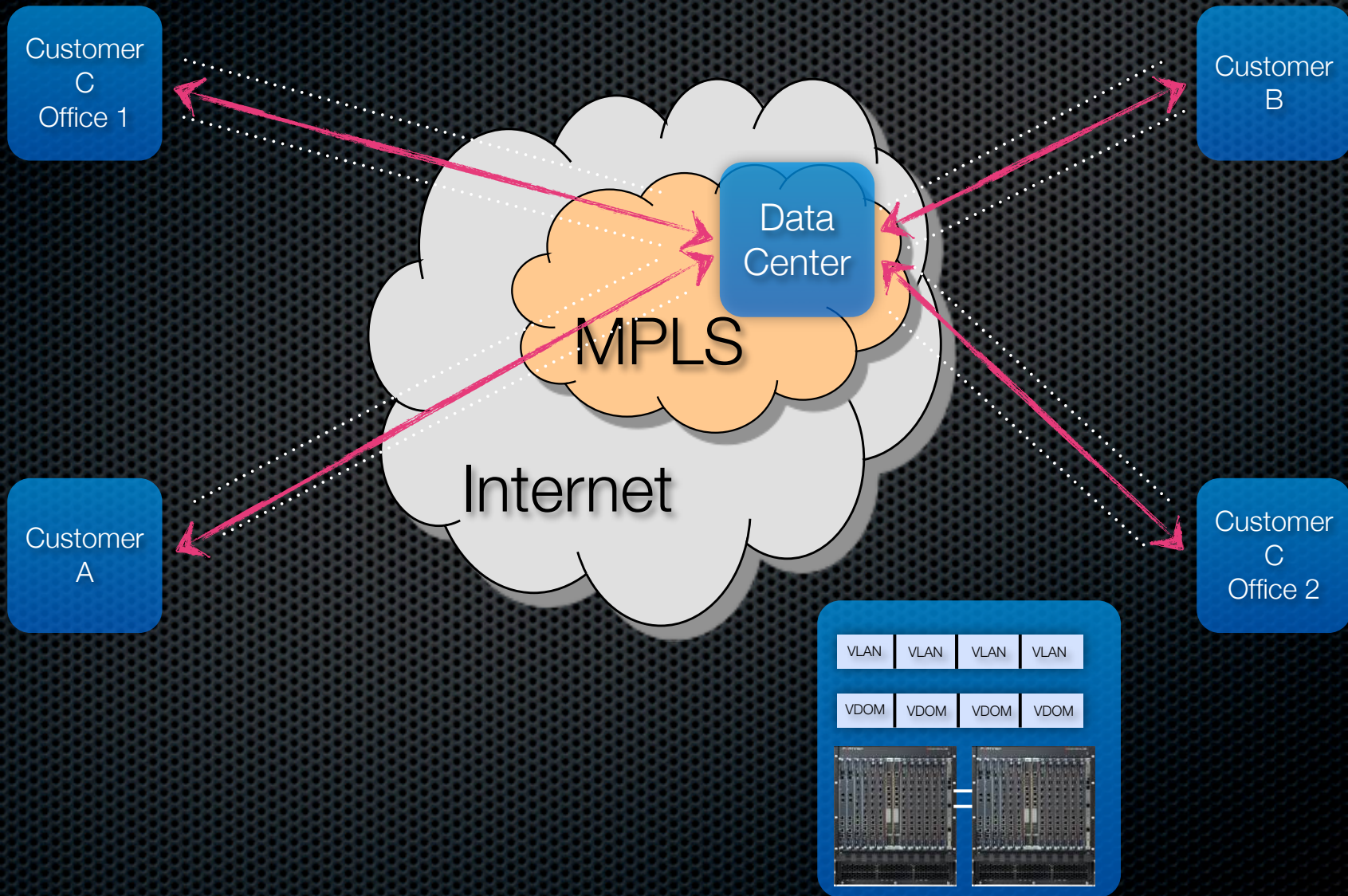
- ✦ Managed Security Services, Why?
 - ✦ Operational Benefits
 - ✦ No Capital Expenditure
 - ✦ Displaced Accountability
 - ✦ “Pure play” vs. Bundled Services / Utility Model
 - ✦ Cloud vs. CPE

Cloud

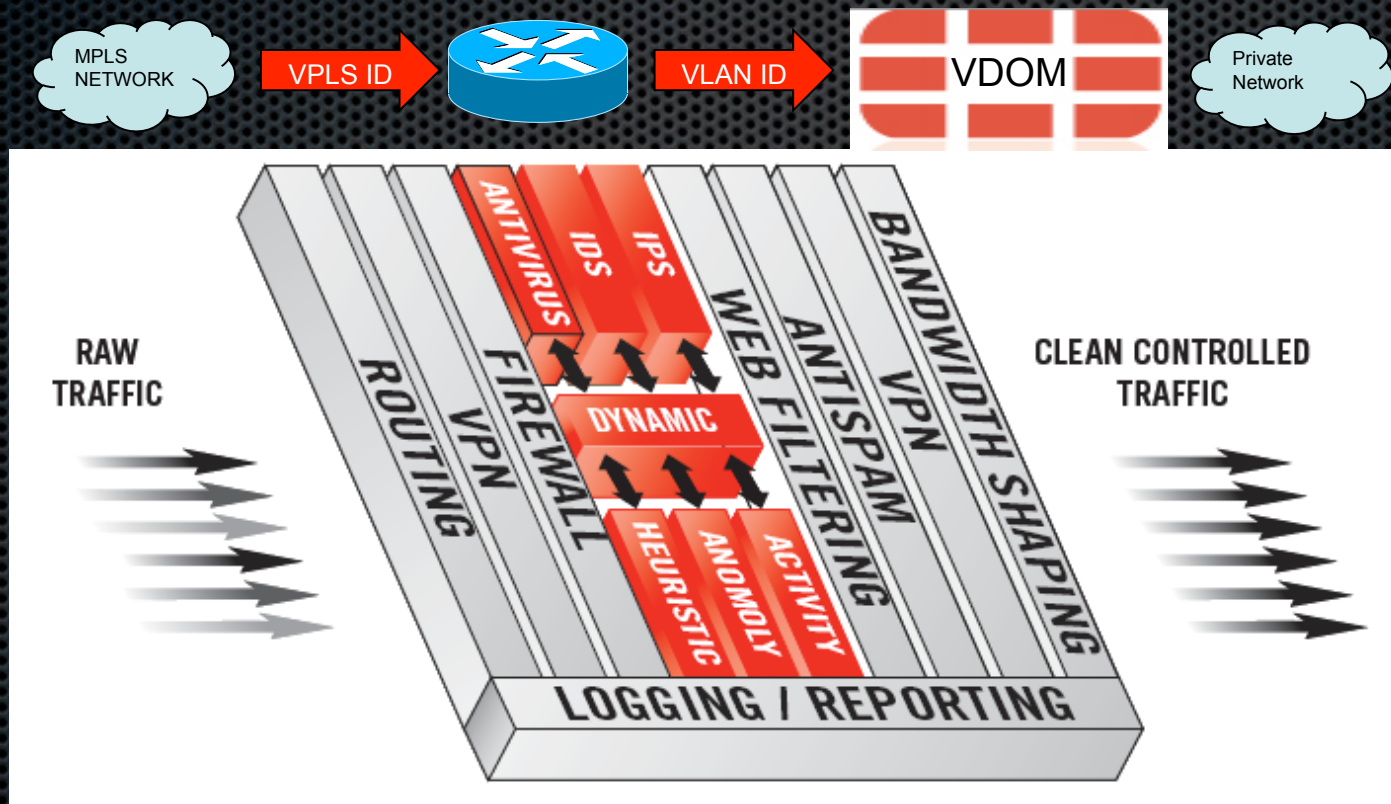
- Cloud Security, what does that mean?
 - “Clean Pipe” or Security Services as a Utility
 - Shared Services Model (Multi-tenancy)
 - Integrating with the carrier backbone
- Cloud Computing
 - SAAS, IAAS, PAAS need Security!
 - How to provision? Is it VM? Is it appliance?



Cloud Security Example



Cloud Security / Clean Pipe



Cloud Computing Offerings

- Infrastructure as a Service (Sometimes Hardware as a Service HAAS)
 - Outsourcing of equipment to SP - Examples are Storage, Processing, “Elastic Computing”
- Platform as a Service
 - Outsourcing of the computing platform to SP - Allows for custom development and flexibility (OS or web platform delivered as a service)
- Software as a Service
 - Complete application outsourced (WP, SF.com, etc.)

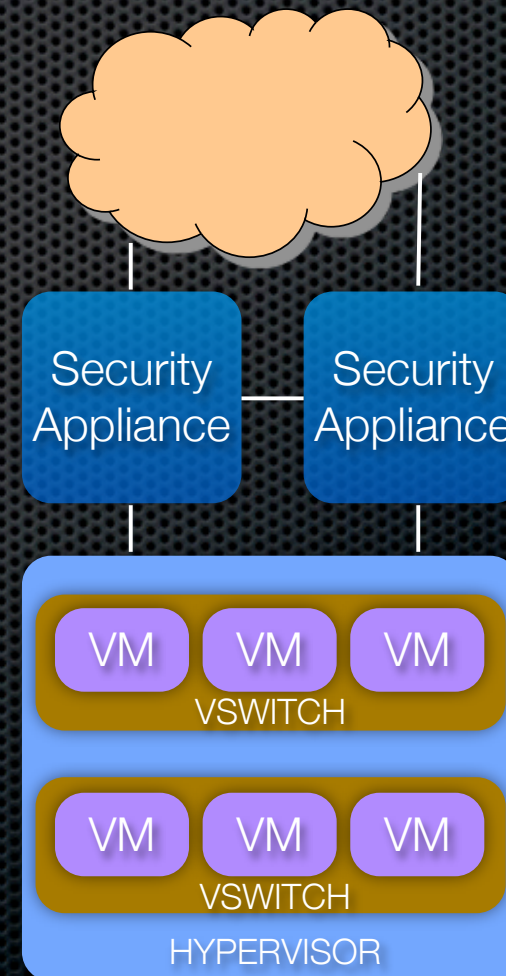
Securing Cloud Applications

- Most cloud applications are virtualized
- Hypervisor is a fundamental component
 - Hypervisor is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) cannot disrupt each other. *
- Three primary methods of securing cloud apps
 - Extra-Hypervisor
 - Intra-Hypervisor
 - Host

*thanks techtarget

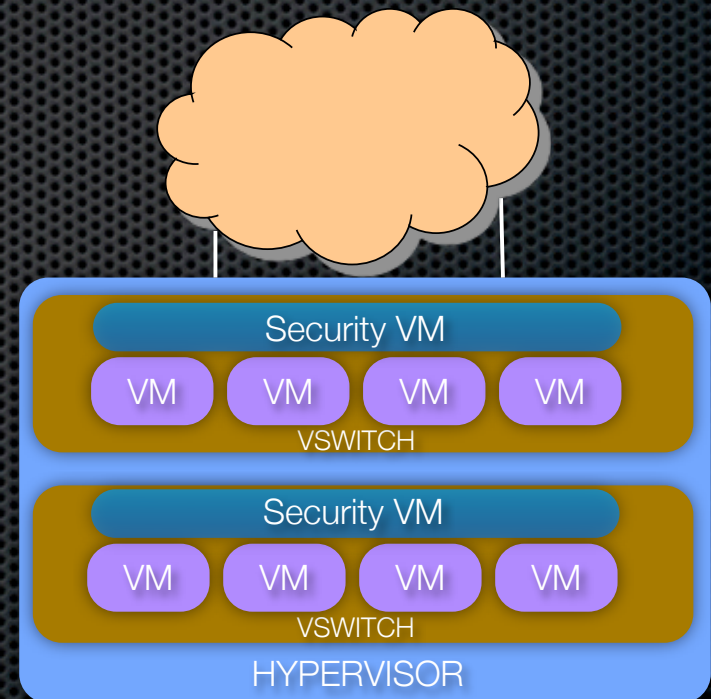
Extra-Hypervisor Security

- Outside the VM platform
- Typically an appliance
- Pros: Fast / Mature
- Cons: Lack of Visibility into VM space



Intra-Hypervisor Security

- VM based
- Typically leverages API for integration with the hypervisor
- Pros: Visibility to intra-VM communication
- Cons: Takes CPU from VM execution



The VM Security Problem

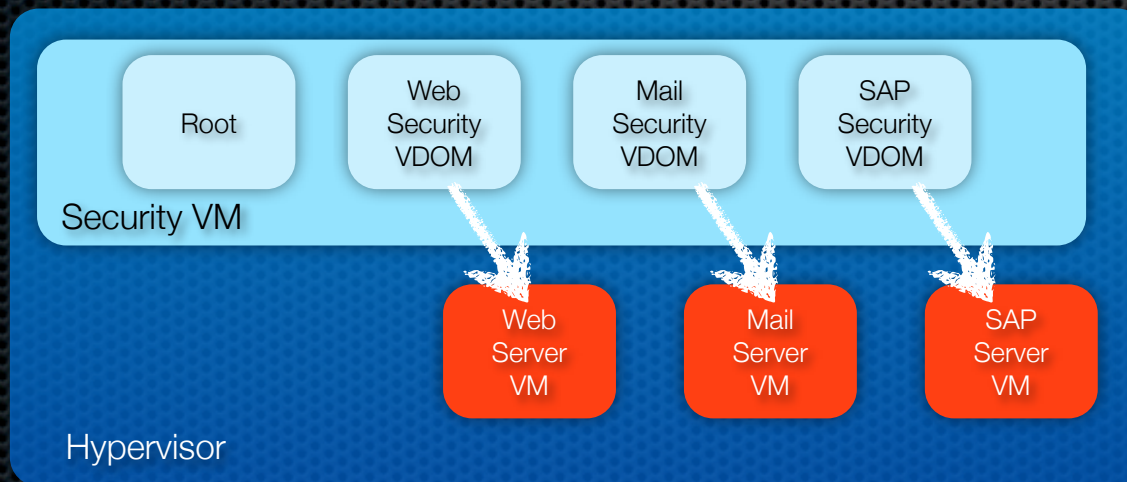
- ✦ VSwitch is not a switch
- ✦ VMWare has retracted some API options
- ✦ High Availability is more complicated
- ✦ Takes Resources from VM application operations
- ✦ *Easy* to create new applications!

Protected Provisioning

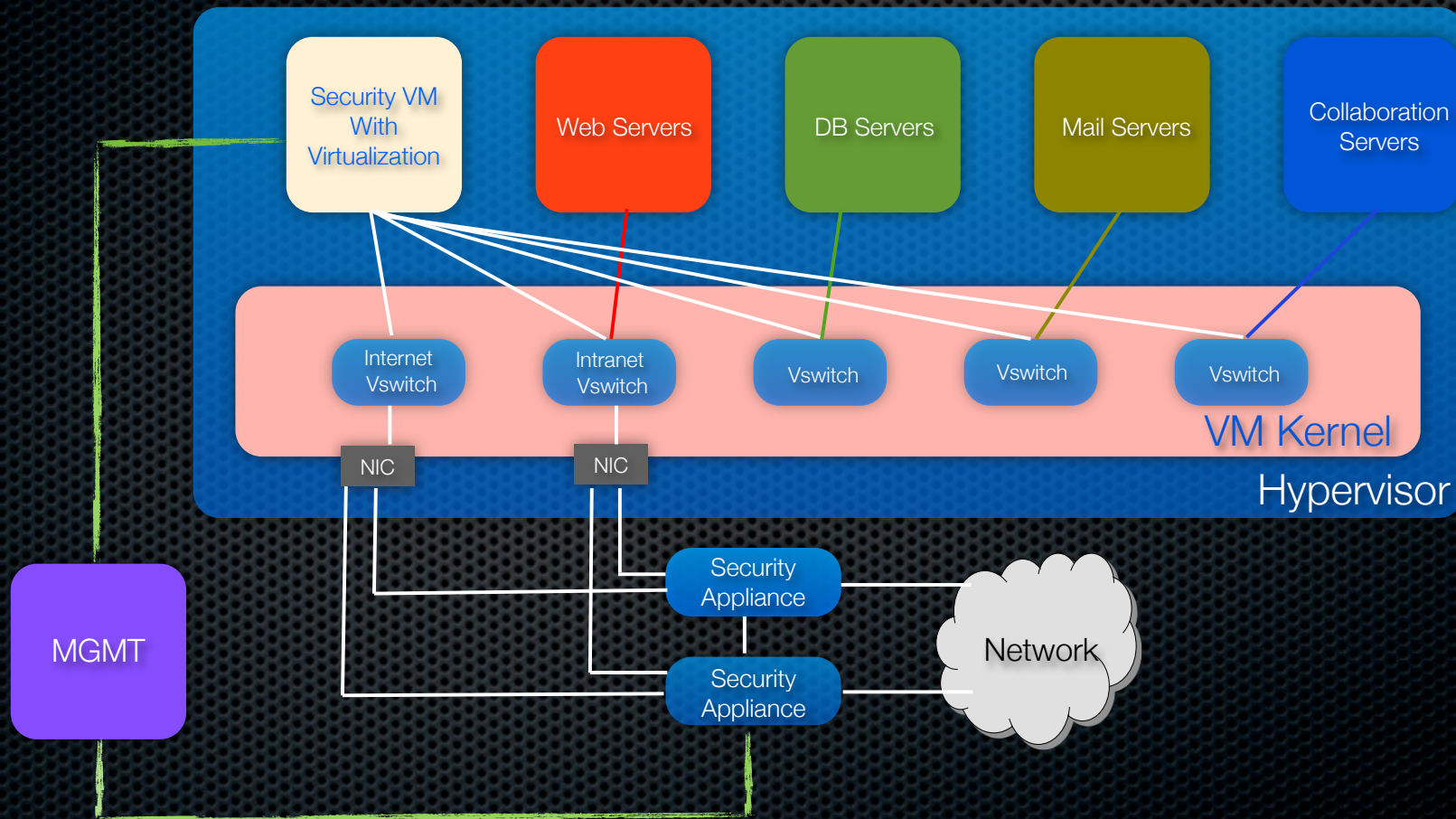
- ✦ VM security element is dynamically created based on policy.
- ✦ Application templates are pre-defined
- ✦ UTM Policy templates are pre-defined
 - ✦ Mail Server -> FW VM, IDP, AntiSpam
 - ✦ Web Server -> FW VM, WAF <- Automatic VA

The Wormhole

- ✦ Many security products have built in virtualization
- ✦ What happens when you virtualize them?
- ✦ Cool Stuff, welcome to the matrix.



Combined Architecture



Concluding

- ✦ Unified Threat Management / Consolidation a pervasive and persistent trend
- ✦ Managed Services / Utility and Cloud Security offers a viable alternative to self managed
- ✦ Evolution of physical to virtual driving security architecture in new directions
- ✦ Policy and Process must be automated to ensure proper compliance and protection for virtual assets

I Work @ FTNT



- ✦ Founded in 2000
- ✦ Nasdaq Listed FTNT
- ✦ ~1300 Employees
- ✦ Over 600k units shipped
- ✦ Over 100k customers
- ✦ 10 Years!



Thank You!

- Questions?