Securing the Virtualized Data Center With Next-Generation Firewalls

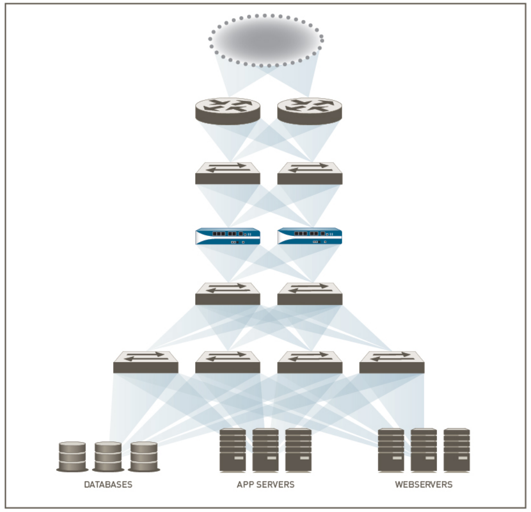
Stallion Otepää Seminar

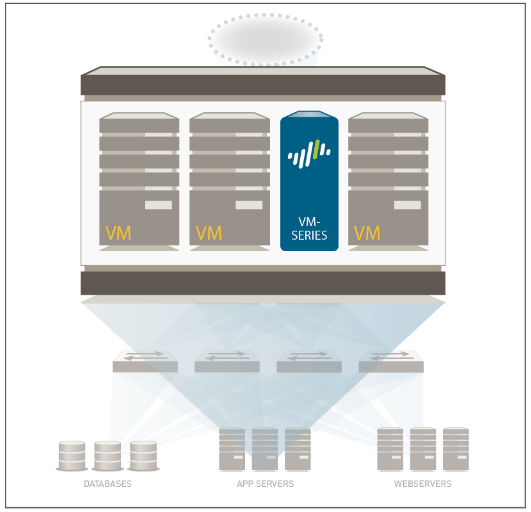
I

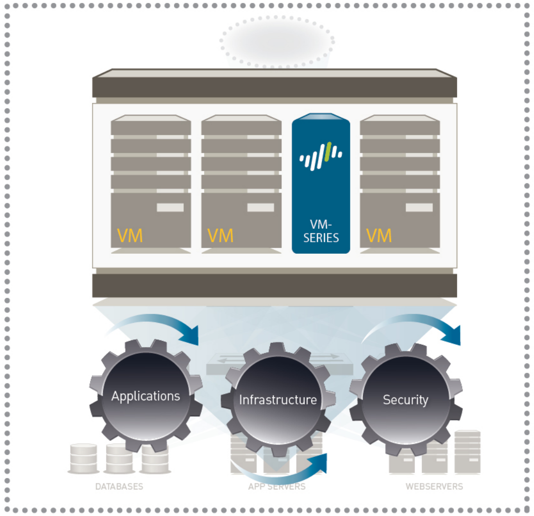
paloalto NETWORKS

the network security company™

Data Center Evolution







Traditional Data Center

- Dedicated application servers
- Server utilization=15%
- North–South traffic

Virtualized Data Center

- Multiple apps per server
- Higher operational efficiencies
- Improved server utilization

Cloud (Private/Public)

- IT as a "service"
- On-demand services
- Automation and orchestration

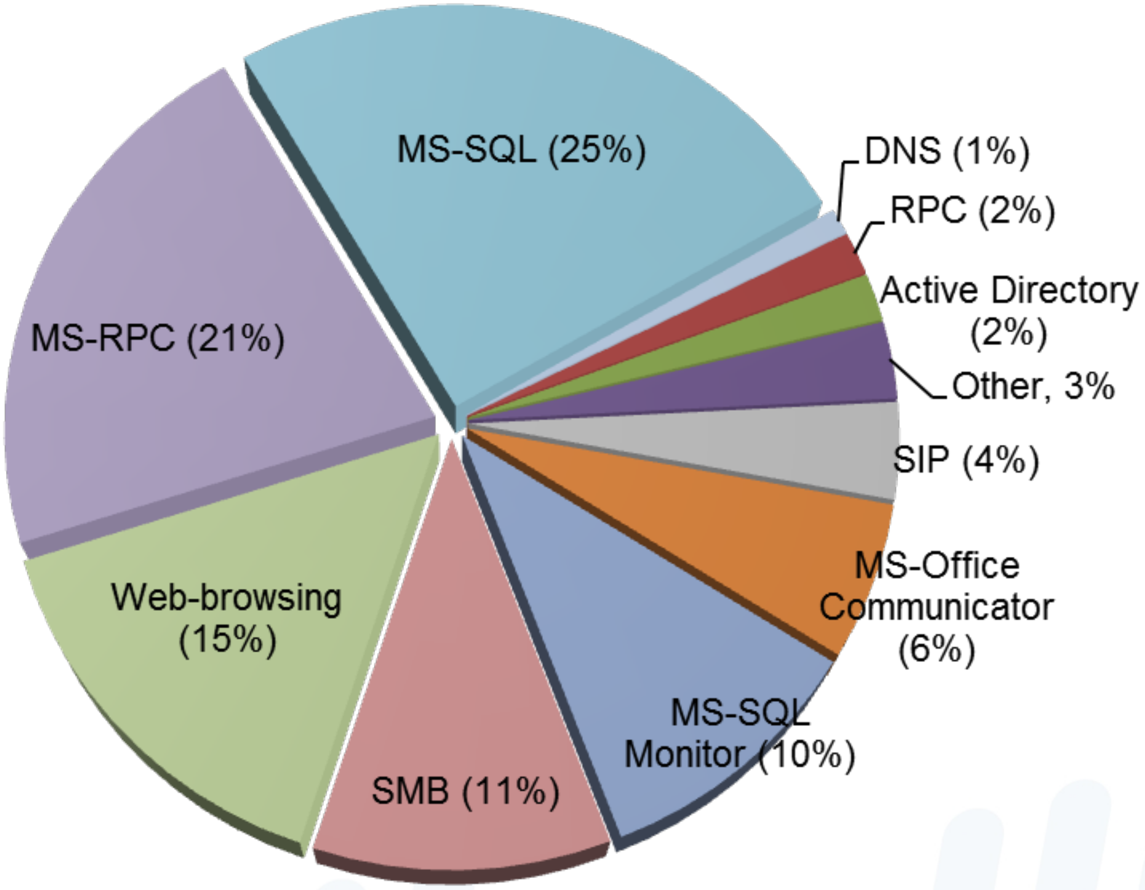
Dynamic, automated, "services-oriented"

Exploits Target High Value Assets

- 10 out of 1,395 applications

- 2,016 unique exploits and ~60M exploit logs observed

- 9 business critical applications account for 82% of the threat logs

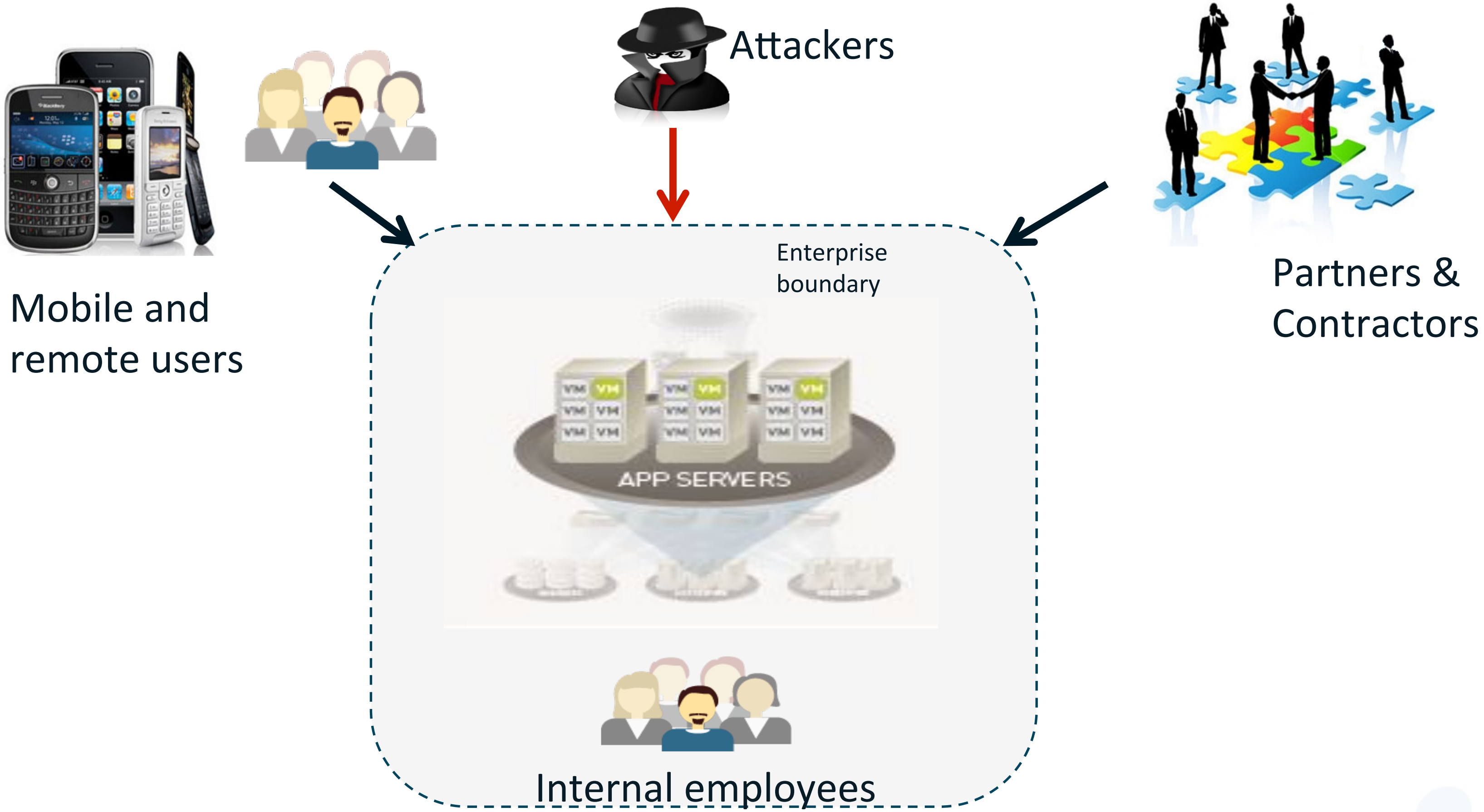


Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Security Hasn’t Kept Up with Rate Of Change

- **Configuration of security policies are manual and slow**
  - Weeks to provision security policies versus minutes for workloads
  - Security policies require manual and repetitive steps
- **Policies do not follow VM adds, moves, changes**
  - Policies are not tied to VM instantiation
  - Policies cannot track VM movement (server or data center)
- **Lack of visibility into the virtual infrastructure**
  - Segmentation of virtualized apps of different trust levels
  - Virtualized traffic may not flow outside of virtualized server (Sharepoint application communicating with SQL database)

But Your Existing Challenges Didn’t Go Away



Attackers

Mobile and remote users

Partners & Contractors

Enterprise boundary

Internal employees

Distributed Enterprise

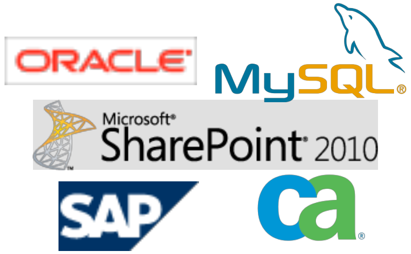
New Application Landscape

Modern Attacks

A New Paradigm for Security is Needed

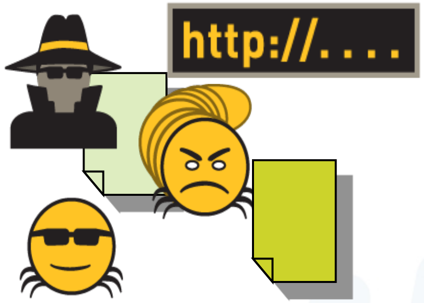
- **Deliver all the features that are table stakes:**
  - Safe app enablement, threat protection, flexible integration
- **Must become more dynamic**
  - Security policy must be there when VM is created
  - Security policy must follow VM movement
  - Security workflows must be automated//orchestrated so it doesn't slow down the data center
- **Consistent, centralized management**
  - Centralized management is critical
  - Must be consistent for all environments - physical, hybrid, mixed

Enabling Applications, Users and Content



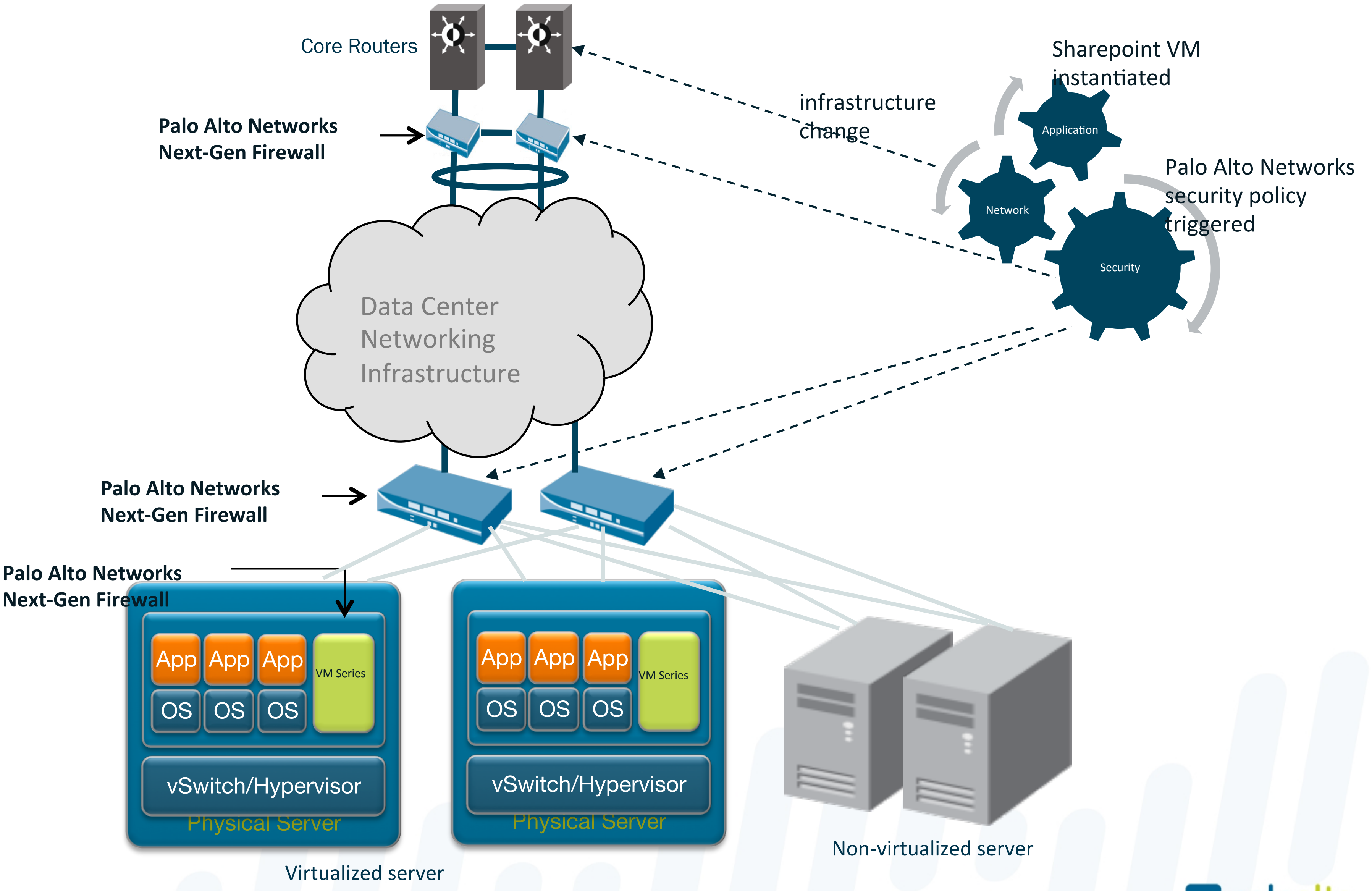
- **Applications:** Safe enablement begins with application classification by App-ID.

- **Users:** Tying users and devices, regardless of location, to applications with User-ID and GlobalProtect.



- **Content:** Scanning content and protecting against all threats – both known and unknown; with Content-ID and WildFire.

Virtualized Data Center and Cloud Deployments


Core Routers
Palo Alto Networks Next-Gen Firewall
infrastructure change
Sharepoint VM instantiated
Application
Network
Security
Palo Alto Networks security policy triggered
Data Center Networking Infrastructure
Palo Alto Networks Next-Gen Firewall
Palo Alto Networks Next-Gen Firewall
App
App
App
OS
OS
OS
VM Series
vSwitch/Hypervisor
Physical Server
App
App
App
OS
OS
OS
VM Series
vSwitch/Hypervisor
Physical Server
Virtualized server
Non-virtualized server

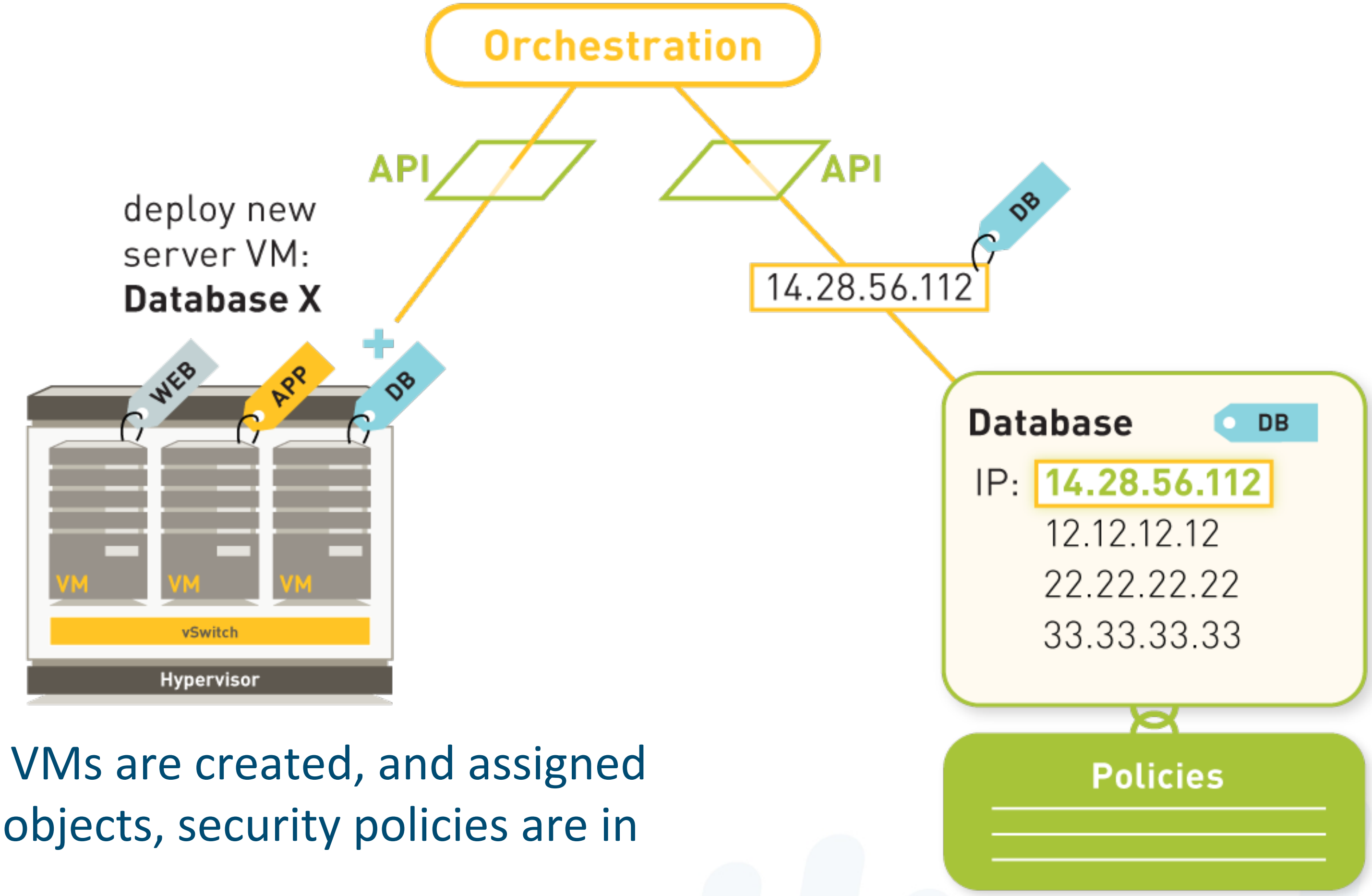
Introducing the VM-Series

Safe Application Enablement of Intra-Host Traffic

VM-100	VM-200	VM-300
50,000 sessions	100,000 sessions	250,000 sessions
250 rules	2,000 rules	5,000 rules
10 security zones	20 security zones	40 security zones

- Next-generation firewall in a virtual form factor
  - **Consistent features** as hardware-based next-generation firewall
  - Inspects and **safely enables intra-host communications** (East-West traffic)
  - **Tracks VM creation and movement** with dynamic address objects
- Initial support on VMware platform - ESXi 4.1 and ESXi 5.0
- Available in 3 models (VM-100, VM-200, VM-300), and supports 2, 4, 8 CPU cores
- Licensing by firewall capacity – Individual, Enterprise, Service-Provider

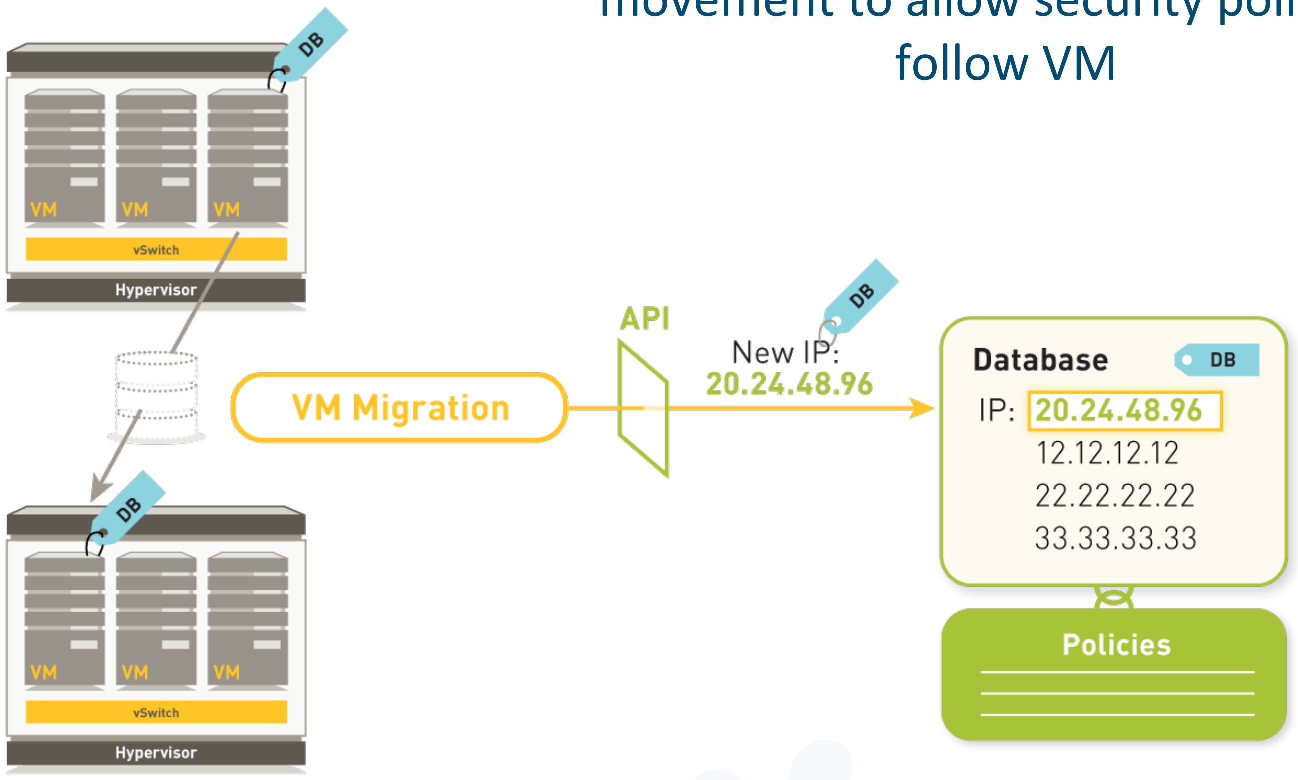
VM orchestration



When new VMs are created, and assigned to address objects, security policies are in place

VM Migration

Dynamic address objects tracks VM movement to allow security policy to follow VM



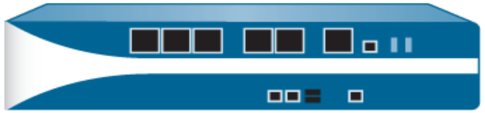
Automation and Orchestration via REST API

bmcsoftware

ca technologies

vmware

cloudstack open source cloud computing



Application/service/tenant
- Instantiation
- Provisioning
- Deprovisioning

Service state tracking

Policy Mapping

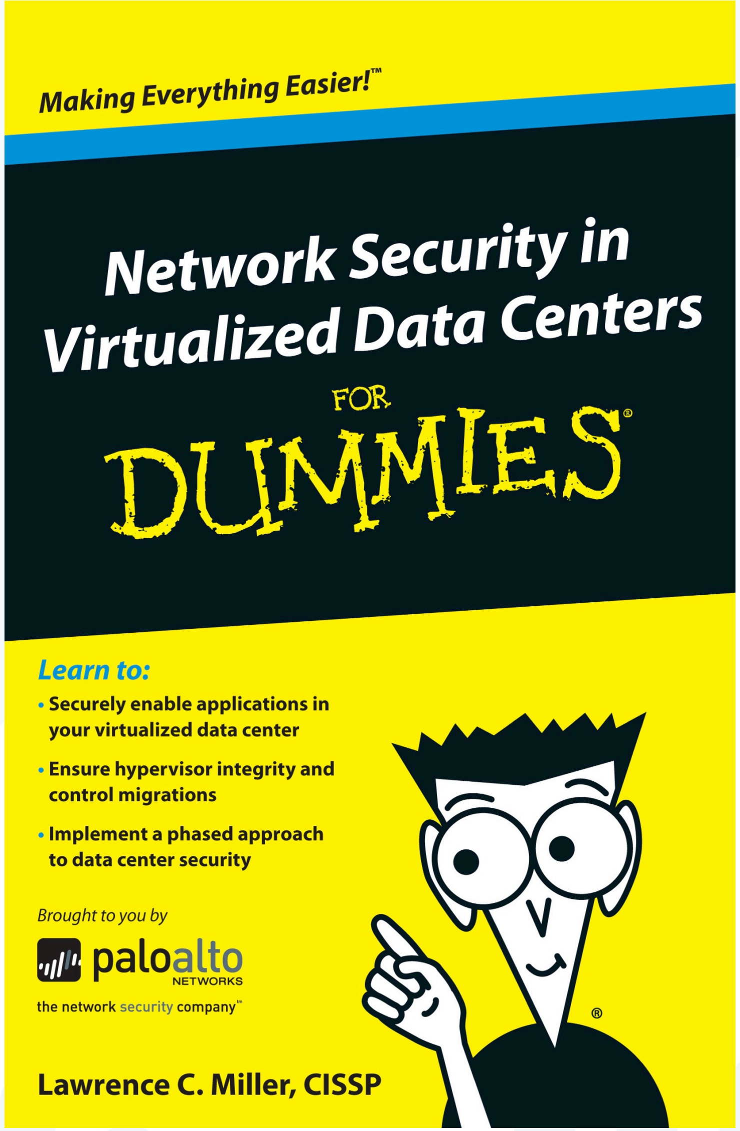
RESTful XML API over SSL

Device Configuration
ACC/Report data

Automated Compliance

Securing The Next-Gen Data Center Requires a Next-Generation Firewall

- Next-generation network security
  - Safely enables all applications in the datacenter
  - Protects against all datacenter threats without performance impact
  - Provides simplified integration into the infrastructure
  - Ties security policies to VM creation and movement
  - Security policies orchestrated in line with virtualized workloads
- Consistent management for virtualized or physical firewalls



Making Everything Easier!™

Network Security in Virtualized Data Centers FOR DUMMIES®

Learn to:

- Securely enable applications in your virtualized data center
- Ensure hypervisor integrity and control migrations
- Implement a phased approach to data center security

Brought to you by

paloalto NETWORKS

the network security company™

Lawrence C. Miller, CISSP

Questions

paloalto NETWORKS

the network security company™

paloalto
NETWORKS

the network security company™