the network security company™

Securing the Virtualized Data Center with Next-Generation Firewalls

November 2012

Table of Contents

Executive Summary

Virtualization is helping organizations utilize their data center hardware infrastructure more effectively, leading to reduction in costs, and improvements in operational efficiencies. Gartner[1] estimates that almost 50% of all x86 server workloads are virtualized today with this number expected to grow to 77% in 2015. Many organizations are also evolving their virtualization infrastructure to build their own automated, self-service, private cloud environments.

As organizations evolve from traditional data centers to virtualized and cloud computing environments, security architectures must support the changing set of requirements. This includes not only addressing fundamental tablestakes functionality such as safe application enablement, threat protection and flexible networking integration, but also new challenges brought on by the virtualized infrastructure, and the dynamic and automated nature of the virtualized environment. These include having visibility into virtual machine traffic that may not leave the virtual infrastructure, the ability to tie security policies to virtual machine instantiation and movement, and orchestration of security policies in lock step with application workflows.

This white paper describes the challenges of virtualized data center and cloud computing environments, and how to address them with next-generation firewalls.

Evolution Towards Virtualization and Cloud Computing

Today's IT organizations are increasingly tasked with doing more with less. In these challenging economic conditions, IT organizations are faced not only with shrinking budgets but are being asked to improve operational efficiencies and drive responsiveness for business processes. For many IT organizations, the adoption of technologies like virtualization and cloud computing provide many benefits from operational efficiencies to speed in application delivery.

Virtualization technology partitions a single physical server into virtual machines running multiple operating systems and applications. The hypervisor, a software layer that sits between the hardware and the "virtual" operating system and applications, is what allocates memory and processing resources to the "virtual" machines. Two types of virtualization are available – hypervisor virtualization and hosted virtualization. In hypervisor architectures, also known as bare metal or native virtualization, the hypervisor is the first layer of software running on the underlying hardware without a host operating system. In hosted virtualization, the hypervisor runs on top of the host operating system. This configuration supports the broadest range of hardware operating system including Windows, Linux or MacOS.

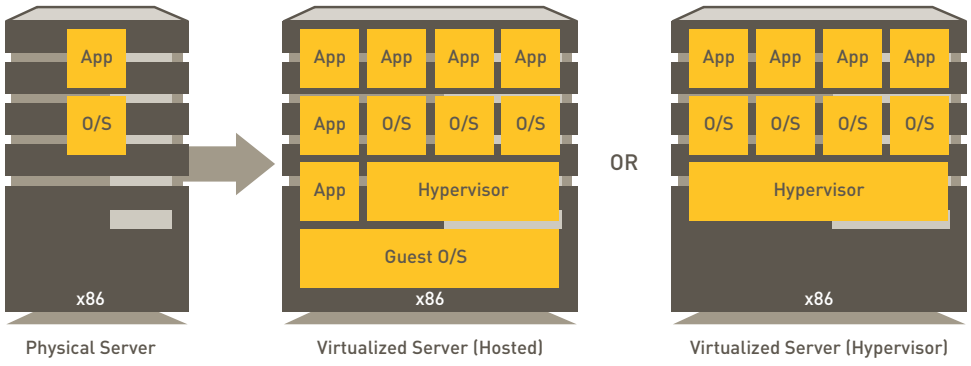

Figure 1: Virtualization Architectures

Figure 1 shows both architectures. Server virtualization typically utilizes hypervisor architectures while desktop virtualization uses hosted virtualization architectures. In this whitepaper, we will focus primarily on server virtualization and hypervisor architectures.

Why Server Virtualization?

Most data center virtualization initiatives begin with the consolidation of data centers running applications on dedicated, purpose-built servers into an optimized number of data centers with applications on standardized virtualized servers. Server virtualization improves operational efficiencies and lowers capital expenditure for organizations:

- **Optimizes existing hardware resources:** Instead of a "one server, one application" model, multiple virtual applications can be run on a single physical server. This means that organizations can leverage their existing hardware infrastructure by running more applications within the same system.
- **Reduces data center costs:** Reducing the server hardware "box" count not only reduces the physical infrastructure real-estate but also reduces data center related costs such as power, cooling and rack space.
- **Gain operational flexibility:** Through the dynamic nature of virtual machine provisioning, applications can be delivered quicker rather than the process of purchase, "rack/stack", cabling, O/S configuration. This helps improve the agility of the IT organization.
- **Maximizes efficiency of data center resources:** Because applications can experience asynchronous, or bursty demand loads, virtualization provides a more efficient way to address resource contention issues and maximize server utilization. It also provides a better way to deal with server maintenance and backup challenges. For example, IT staff can migrate virtual machines to other virtualized servers while performing hardware or software upgrades.

Why Cloud Computing?

Virtualization is often the first step in an organization's strategy to move towards automated, on-demand services. Cloud, unlike common misconceptions, is not a location but rather a pool of resources that can be rapidly provisioned. The U.S. National Institute of Standards and Technology (NIST) defines cloud computing in Special Publication (SP) 800-145 as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The business value of cloud computing is the ability to pool resources together to achieve economies of scale. This is true for private or public clouds. Instead of multiple organizations or groups within an organization independently building a data center infrastructure, pools of resources are aggregated and consolidated, and designed to be elastic enough to scale with organizational demand. This not only brings cost and operational benefits but technology benefits. Data and applications are easily accessed by users no matter where they reside, projects can scale easily, and consumption can be tracked effectively.

Virtualization is a critical part of this architecture, enabling applications to be delivered efficiently, and in a more dynamic manner. However, another critical aspect of cloud computing is software orchestration that enables disparate processes to be stitched together in a seamless manner, so that they can be automated, easily replicated and offered on an as-needed basis. The IT organizational model also needs to evolve towards a "services-centric", multi-tenant model, where consumption needs to be measured, and segmentation between multiple tenants needs to be provisioned.

Security Considerations in Securing the Journey to the Cloud

With virtualization and cloud technologies, the data center environment has evolved from rigid, fixed environments where applications run on dedicated servers towards dynamic, automated, orchestrated environments where pools of computing resources are available to support any application to be accessed anywhere, anytime, from any device.

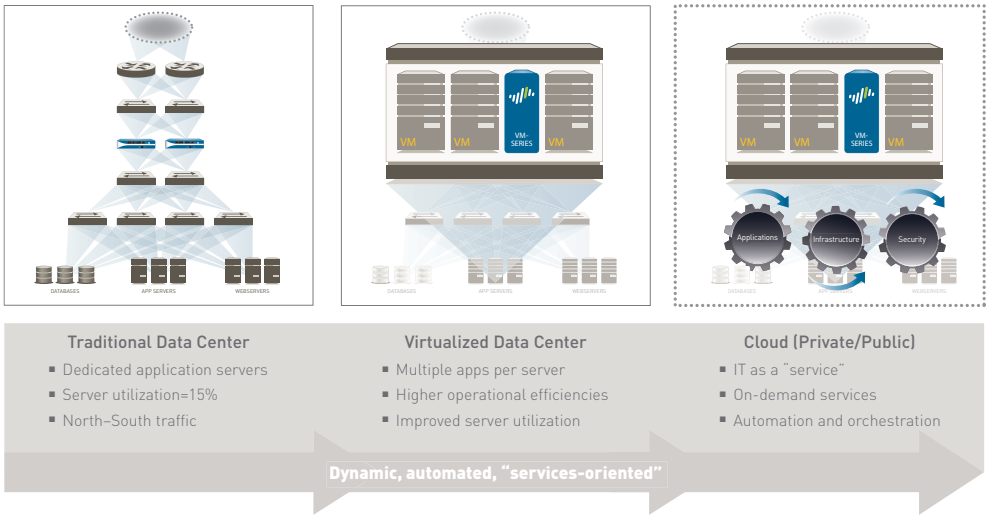

Figure 2: Evolution of data center architectures

Security is the biggest hurdle to embrace this new dynamic, automated, services-oriented architecture. The process to configure network security appliances today is excruciatingly painful and slow. Policy changes need to be approved, the appropriate firewalls need to be identified, and the relevant ports and protocols determined. While the creation of a virtual workload may take minutes, the security configuration for this workload may take weeks.

Security also cannot keep up with the dynamic nature of virtualization and cloud. Virtual machines can be highly dynamic, with frequent add, move and change operations. This complicates the ability to track security policies to virtual machine creation and movement so that requirements and regulatory compliance continue to be met. Virtualized computing environments also enable direct communication between virtual machines within a server. Intra-host communications may not be visible to network-based security appliances residing outside a virtual server. The routing of intra-host virtual machine traffic to external security appliances for inspection may not be ideal because of performance and latency requirements.

At the same time, the existing trends that have impacted the security landscape in the virtualized data center —changing application landscape, distributed enterprise, and modern threats—do not go away. The changing application landscape means that the identification, control and safe enablement of applications can no longer be accomplished via ports and protocols. The distributed enterprise of mobile users and extended enterprise, and the evolution of threats towards sophisticated, multi-vector, targeted attacks require user-based policies and a complete threat framework. In summary, next-generation firewalling capabilities to safely enable applications, protect against all known and unknown threats without performance impact, and integrate flexibly into the

data center continue to be critical, fundamental security requirements.

Therefore, security for the virtualized data center must exhibit the following characteristics:

1) **Deliver all the features that are table stakes:** These include safe application enablement, threat protection without impacting the performance of the data center, and flexible integration into the data center design. These features must be available within a virtualized firewall to secure intra-host communications or East-West traffic.

2) **Must become more dynamic:**
   - Security policies must be applied as soon as a virtual machine is created.
   - Security policies must follow virtual machine movement.
   - Security workflows must be automated and orchestrated so it doesn't slow down virtual workload provisioning.

3) **Centralized, consistent management:** Centralized management is critical, and must be consistent for all environments—physical, hybrid or mixed environments. The management configuration must provide one unified policy rule base for ease of configuration and complete visibility into the policies being enabled in the data center. In fact, Gartner[2] advocates that organizations "favor security vendors that span physical and virtual environments with a consistent policy management and enforcement framework."

Existing Security Solutions in the Data Center Do Not Deliver

Existing security solutions in the data center make their access control decisions based on ports and protocol. Many security solutions also bolt on application control and threat prevention features to their stateful inspection firewalls.

There are several problems with this approach. The lack of visibility into all traffic means that evasive applications, applications that use non-standard ports and threats that leverage the same behavior as applications may be missed. Security policies also become convoluted as you build and manage a firewall policy with source, destination, user, port and action, an application control policy with similar rules, in addition to other threat prevention rules. Policy gaps appear and grow because of the difficulty in managing and monitoring multiple appliances. A multiple policy rule base approach not only increases administrative overhead, but may increase business and security risks with policy gaps that may be hard to see. This multi-platform or multi-module approach also degrades data center performance as more and more features are enabled.

Finally, existing security solutions in the data center do not address the dynamic nature of the virtualized environment, and cannot track policies to virtual machine creation or movement.

Many virtualized security offerings are virtualized versions of port- and protocol-based security appliances, delivering the same inadequacies as their physical counterparts.

Palo Alto Networks™ Architecture for Virtualized Data Centers

Palo Alto Networks delivers a comprehensive approach to security for the virtualized data centers. The architecture addresses fundamental security challenges for the virtualized data center and supports the dynamic nature of virtualization and cloud.

	Physical Form Factor	Virtual Form Factor
Safe Application Enablement	▪ App-ID, User-ID, Content-ID, GlobalProtect, and WildFire	
Threat protection without performance implications.	▪ Separate management and data plane ▪ Single pass software architecture	
	▪ Multi-core hardware	
Flexible Integration	▪ Comprehensive networking foundation (routing, VLAN trunking, link aggregation) ▪ Integration at layer 1, 2, 3	
Cloud-readiness	▪ Multi-tenancy via virtual systems	▪ Multi-tenancy via virtual instances
	▪ Dynamic objects ties VM movement and creation to policy ▪ Cloud orchestration via REST API	
Centralized management, one integrated policy.	▪ Panorama with centralized provisioning and logging	

Figure 3: Palo Alto Networks Comprehensive Approach to Securing the Virtualized Data Center

Safe Application Enablement for Applications

Palo Alto Networks next-generation firewalls allow organizations to safely enable applications. This is achieved via next-generation firewall technologies—App-ID™, User-ID™, Content-ID™, GlobalProtect™, and WildFire™—that can identify all applications, enable them by user, application and content, and inspect all content for threats.

The next-generation firewall identifies all applications in the data center with App-ID regardless of ports, protocol, evasive tactic and encryption. Visibility into all traffic in the data center reduces the scope of attacks by controlling non-compliant use of applications, blocking rogue applications and distinguishing any unknown traffic. Differentiated access to data center applications by user/group leveraging User-ID and GlobalProtect supports secure anytime, anywhere access by employees, extended business partners and mobile users.

Finally, Content-ID and WildFire deliver a complete threat framework addressing known and unknown threats, from malware, exploits and spyware to targeted attacks. WildFire provides the ability to identify malicious behaviors in executable files by running them in a cloud sandbox and observing their behaviors. This enables Palo Alto Networks next-generation firewalls to identify malware quickly and accurately, even if the particular sample of malware has never been seen in the wild before. For Internet-facing data centers, denial-of-service features can control various types of traffic floods.

Safe application enablement features applied to security zones in the data center delivers meaningful segmentation, limits access, and delivers individual accountability to meet compliance mandates.

Threat Protection with Superior High-Performance Architecture

If an application hosted in a data center isn't available or responsive to users, an organization is often missing revenue opportunities—so network security controls, which all too often introduce delays and outages, are typically "streamlined." Network security performance therefore must go hand-in-hand with threat protection to ensure that as threat protection services are enabled, the performance of the data center is not affected.

The Palo Alto Networks single-pass software architecture offers superior performance compared to traditional approaches, including those found in a UTM or software blade approach. This is because of the unique architecture that processes functions in a single pass to reduce latency, allowing you to simplify your network security infrastructure and to eliminate the need for a variety of stand-alone and bolt-on security devices. Physical appliances combine the single-pass software architecture with parallel processing hardware architecture, with dedicated, specialized processing for networking, security, and content scanning so that the full suite of next-generation features can be enabled with high throughput and reliability.

Flexible Network Integration

Palo Alto Networks next-generation firewalls support more deployment options than any other device in the network security market. The next-generation firewalls provide deployments at L1, L2, L3, and tap modes (or a mixture of all on the same appliance) and couple that with powerful networking capabilities for integration (VLAN trunking, link aggregation) and high availability (separation of data and control planes, active/active and active/passive deployment options.) This accommodates any data center architecture, and the flexibility to add additional security controls without rearchitecting the network when the threat or application landscape changes.

Virtualization Security and Cloud-Ready Features

The virtualized next-generation firewalls feature a number of innovative features specifically designed to address the security challenges introduced by the virtualized environment, including the dynamic and automated nature of virtual machines:

- **Tying Policy to Virtual Machine Creation and Movement:** Virtual machines can be highly dynamic, with frequent add, move and change operations. The dynamic nature of virtualization introduces new security requirements for the virtual computing environment. Security policies, including the segmentation and compartmentalization of specific applications for compliance, must continue to be enforced in a virtual environment. This means the ability to keep the policies in sync with VM creation, and the ability to maintain policies with the mobility of virtual machines. Palo Alto Networks provides a feature called dynamic address objects that binds appropriate security policies to virtual machine instantiation and movement. This automates the process of keeping security policies in sync with virtual machines as they are created or moved.

- **Integration with Orchestration Software:** Data center environments typically automate the tasks and processes using workflows that help IT teams execute change with greater speed, quality, and consistency. Deployment of security capabilities can lag orchestration software provisioning for virtual environments, leading to security risks and considerable integration challenges. An automated way to provision network security in line with the pace of orchestration of the elements of the virtualized data center environment is needed.

  Palo Alto Networks offers a powerful XML management API that enables external cloud orchestration software to connect over an encrypted SSL link to manage and configure Palo Alto Networks firewalls. The exhaustive and fully-documented REST-based API allows configuration parameters to be seen, set and modified as needed. Turnkey service templating can be defined for cloud orchestration software so that the security features within the next-generation firewall become part of the data center workflow.

- **Hypervisor Security:** Finally, the security of the hypervisor, the virtualization layer between the operating system (O/S) and the hardware, is a new security challenge introduced only in a virtualized computing environment. Hypervisor attacks range from vulnerabilities that cause hypervisors to crash to complex "breakout" exploits that cause a guest VM system to escape and infiltrate its own host system. While the foundation of hypervisor security must start with hardened software, vulnerabilities associated with hypervisor can be addressed with the next-generation firewall.

Centralized Management

Centralized management for physical and virtualized next-generation firewalls is available with Panorama. Panorama is a centralized security management system that provides global control over a network of Palo Alto Networks next-generation firewalls. Using the same look and feel that the individual device management interface carries, Panorama eliminates any learning curve associated with switching from one mechanism to another.

Panorama allows administrators to control all aspects of the devices and/or virtual systems under management (security, NAT, QoS, policy based forwarding, decryption, application override, captive portal, and DoS protection). Using pre- and post-rules, Panorama administrators can enforce shared policies while allowing local policy flexibility. Rules in between the pre- and post-rules can be edited locally or by a Panorama administrator who has switched to the local firewall context. Software updates such as dynamic content updates (Applications, Threats, Antivirus, WildFire), and software licenses can also be managed centrally on Panorama. Panorama provides the ability to view logs and run reports across dynamic or locally queried data aggregated from managed devices.

Choice of Form Factor

Palo Alto Networks offers a choice of either virtualized or physical form factor to secure your virtualized data center. The choice of whether a physical or virtual network security appliance should be deployed in the data center depends on the specific issues to be addressed. Physical network security appliances are adequate if the same trust levels are maintained within a single server, for example, intra-host traffic can be forced off-box through a default security appliance for further inspection.

As organizations move towards pooled computing resources deploying applications of different trust levels, the visibility of intra-host communications can be provided only with virtual firewalls. In many data center scenarios, hybrid deployments of both physical and virtual appliances will exist, with physical firewalls being deployed for inter-server segmentation and virtualized firewalls for intra-server segmentation. However, because Palo Alto Networks next-generation firewalls support a single management interface to manage both physical and virtualized firewalls, and uses a single policy rule table for all next-generation functionality, operational and management complexities are reduced.

Palo Alto Networks VM-Series

The Palo Alto Networks VM-Series comprises three virtualized next-generation firewall models—VM-100, VM-200, and VM-300—supported on VMware ESXi 4.1 and ESXi 5.0 platforms. 2, 4 or 8 CPU cores on the virtualized server platforms can be assigned for next-generation firewall processing. Up to 1 Gbps firewall throughput with App-ID enabled can be supported with 4 CPU cores running. To ensure that management is accessible under periods of heavy traffic, the data plane and the control plane are separated. In addition, Palo Alto Network's single-pass software architecture offers a unique architecture that processes functions in a single pass to reduce latency.

The Palo Alto Networks VM-Series runs the PAN-OS security operating system, the same operating system on the physical firewalls, therefore supporting the same set of next-generation firewall capabilities.

Palo Alto Networks PA-5000 Series Firewall

The PA-5000 Series of next-generation firewalls is designed to secure data center environments where traffic demands dictate predictable firewall and threat prevention throughput. These high performance platforms are tailor-made to provide enterprise firewall protection at throughput speeds of up to 20 Gbps. The PA-5000 Series is powered by more than 40 processors distributed across four functional areas: networking, security, content inspection and management. Reliability and resiliency is delivered by active/active or active/passive high availability; physical separation of data and control plane; and redundant, hot swappable components. A 20 Gbps backplane smooths the pathway between dedicated processors, and the physical separation of data and control plane ensures that management access is always available, irrespective of the traffic load.

The PA-5000 Series comprises three models—the PA-5020, the PA-5050 and PA-5060—at 5 Gbps, 10 Gbps and 20 Gbps firewall throughput respectively, with App-ID enabled.

Secure Data Center Deployments

There are many flexible ways to deploy Palo Alto Networks next-generation firewalls in the virtualized data center. Physical firewalls can be used if all servers host applications of the same trust levels. Alternatively, in an environment with applications of mixed trust levels, the Palo Alto Networks VM-Series can be deployed within a virtualized server. A combination of physical and virtualized firewalls (not shown) may also be used—where physical firewalls provide segmentation between virtualized servers and virtualized firewalls deliver segmentation within the server.

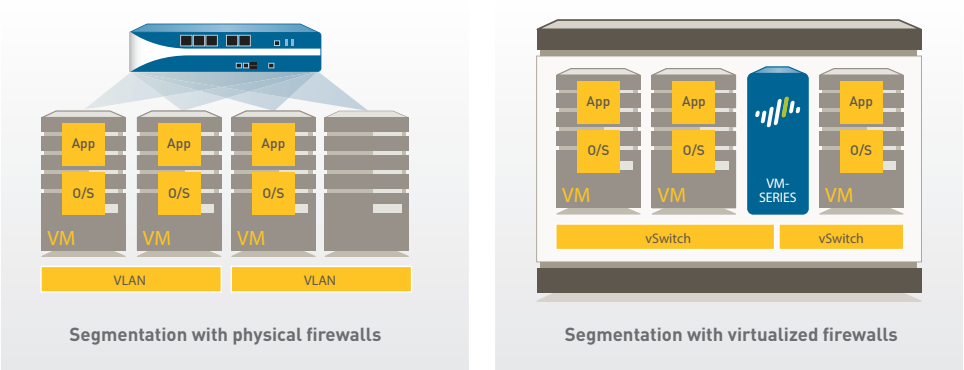

Figure 4: Next-Generation Firewall Deployments

Summary

Palo Alto Networks next-generation firewalls provide a security architecture that protects, scales and evolves with data center needs for physical, virtual and mixed-mode environments. The next-generation firewalls are designed to safely enable applications by user, application and content without compromising performance. In addition, the next-generation firewalls are designed to address key virtualization and cloud challenges from the inspection of intra-host communications, and tracking security policies to virtual machine creation and movement, to integration with orchestration software.

Footnotes:

1: Gartner Security and Risk Management Summit, Neil McDonald, June 2011

2: "Addressing the Most Common Security Risks in Data Center Virtualization Projects", January 2010

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com