Virtualization

Securing the Virtual World

White Paper

WatchGuard® Technologies, Inc.
Published: October 2011

Virtualization – Are You Secure?

There are counterclaims whether virtualized environments are fundamentally no less secure than physical ones, and that virtualization can actually enable better security.

With businesses always looking for ways to decrease costs, improve efficiencies and availability of IT resources, there has been a rapid adoption of virtualization technologies. Virtualization makes it easy to build and deploy new releases and put changes into production. Over the past decade or more, businesses of all sizes have leveraged virtualization to improve utilization and reduce costs. In addition, service providers have used virtualization to respond to customer demands and provide capabilities such as instant provisioning, as well as the ability to offer the isolation and manageability of dedicated hosting without reserving expensive hardware for each customer. Today, these capabilities are prerequisites to achieve the elasticity and flexibility of private and public clouds.

Advantages of Virtualization

The potential to lower IT costs by moving to a virtualized infrastructure can be significant. Virtualization allows you to run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of that one physical appliance across multiple environments. According to a CIO Research Survey, the top reasons customers move to virtual servers for their applications are:

- To cut costs via server consolidation (81 percent)
- To improve disaster recovery (DR) and backup plans (63 percent)
- To provision computing resources to end users more quickly (55 percent)
- To offer more flexibility to the business (53 percent)
- To provide competitive advantage (13 percent)

New Security Challenges

This adoption of virtualization raises the question — will security be harder or easier now? According to a report conducted by Applied Research,[1] some 2,100 of the top IT and security managers in 27 countries were surveyed about their opinions regarding this question. The results reflected a definite lack of consensus. The report showed that one-third of the group think virtualization and cloud computing make security "harder," while one-third said it was "more or less the same," and the remainder said it was "easier." The results seem to indicate that many are either in the process of defining policy for virtual environments, or have chosen to postpone that effort until a later date. Perhaps, as a result of this failure to tackle the security question when deploying virtualized servers, there are experts who believe that the majority of virtual deployments may be less secure than physical deployments. Neal MacDonald of Gartner Group has estimated that "60 percent of virtualized servers will be less secure than the physical servers they replace." MacDonald also identifies some of the most common security risks for data center virtualization projects:[2]

[1] *2010 State of Enterprise Security Survey – Global Data*, Applied Research, July, 2010
[2] *Addressing the Most Common Security Risks in Data Center Virtualization Projects*, Gartner, Inc., January 25, 2010

- Information security isn't initially involved in the virtualization projects
- A compromise of the virtualization layer could result in the compromise of all hosted workloads
- Workloads of different trust levels are consolidated onto a single physical server without sufficient separation. Adequate controls on administrative access to the hypervisor (Virtual Machine Monitor) layer and to administrative tools are lacking
- There is a potential loss of Separation of Duties (SOD) for network and security controls

Traditionally, network security has been designed as a 'one appliance, one application' model and designed with physical networking in mind. Firewalls and UTM appliances are leveraged in network designs based on the fundamental notions of:

- Perimeter enforcement – protecting the "inside" from the "outside" – with network architectures that are built on this separation
- All traffic flows over physical networks, so security can be implemented by interposing physical devices on the wire

With virtualization, these fundamental assumptions may not be true:

- Network architectures blur the definition of the "perimeter" with private resources spanning locations in arrangements leveraging VPNs
- An all-or-nothing, inside-vs.-outside approach does not take into account the need to protect
- Complicating matters, multiple organizations and applications within a business, and multiple businesses hosted by a service provider, can be on the same side of a physical perimeter
- Compliance and privacy requirements make it necessary to offer security and auditability between entities within the same virtual infrastructure
- Mobile users can easily bring malware into a shared infrastructure
- For service providers, the ability to offer full protection is even more critical when multiple customers are hosted on the same server farm – or even on the same server
- Physical appliances cannot offer in-line protection in a dynamic virtual infrastructure
- High-availability and live motion capabilities can mean that applications do not always run on the same physical servers
- Traffic can pass over virtual-only networks within a server, making it impossible to interpose a physical device

Tackling Security Challenges

Organizations need a clear choice to defend their networks, and that is where WatchGuard can help. WatchGuard eXtensible Threat Management (XTM) provides a number of layers of security to keep attacks out. WatchGuard's "Defense-in-Depth" with "Best-in-Class" Security defends against botnets, APTs, and other attacks, while keeping web browsers and organizations in control when using Web 2.O applications.

WatchGuard architecture consists of different security layers working cooperatively with one another to dynamically detect, block, and report on malicious traffic while passing benign traffic through as efficiently as possible. Each layer performs different security functions. Zero day protection is a consistent theme throughout the different layers — which means that WatchGuard protects businesses from new, unknown threats.

WatchGuard offers all this through a virtual appliance. XTMv next-generation security for virtual infrastructures delivers the same best-in-class, defense-in-depth protection offered by the WatchGuard XTM physical appliances. XTMv can protect both the perimeter and internal networks of virtual infrastructure. The following XTMv capabilities protect virtual assets:

- Powerful cloud-based URL reputation enabled defense service that protects web users from malicious web pages, while dramatically improving web throughput.
- Block unwanted email with 100% accuracy along with the viral payloads that spam often carries. Recognize spam regardless of the language, format, or content of the message – even image-based spam that other anti-spam products often miss.
- URL filtering service that blocks access to dangerous and inappropriate web sites in the workplace. It filters URLs on both HTTP and HTTPS to close the HTTPS loophole many other web filters leave wide open.
- Powerful signature-based protection at the gateway against known viruses, trojans, worms, spyware, and rogue ware.
- Scan all ports and protocols to block attacks that comply with standard protocols but carry malicious content, including buffer overflows, SQL injections, and remote file inclusions.
- Stay on top of the applications running on your network for tight security and high productivity and establish which applications can be used within your organization.

Why XTMv

One of the most critical aspects of securing virtualization is the ability to manage the environment. In particular, policies must be assigned by VM, zone, or both, rather than by the traditional location or network connection. The XTMv solution leverages proven management through the same interfaces as WatchGuard's award-winning XTM hardware appliances: a visual command line interface, an integrated web interface, or the centralized management capabilities of WatchGuard System Manager (WSM). A

WSM installation can manage a combination of XTM and XTMv appliances that enables visibility and control of this dynamic environment.

XTMv takes advantage of the performance characteristics of the virtual infrastructure and increases the opportunity for increased security, scalability, and flexibility. It supplies the same capabilities as the XTM hardware and is deployed as a vApp—a virtual machine conforming to the DMTF Open Virtualization Format (OVF) standard. It is supported on servers and networking equipment on the VMware vSphere Hardware Compatibility List.

XTMv supports rapid deployment and can be used to implement security policies not just on an inside-vs.-outside basis, but also between organizations or applications within the same infrastructure. XTMv provides fine-grained security policies for compliance and privacy within the organization and can be migrated within the virtual infrastructure, and protected using the high-availability capabilities of the virtual infrastructure, offering protection continuity even as the infrastructure changes dynamically. XTMv can easily be preconfigured and deployed along with the virtual machines that serve multi-component applications, making it easy to protect applications and their data by default. Policies can be defined not only at the intersection of physical networks, but between virtual-only networks within server farms or even on individual servers. Full threat prevention policies can be implemented at the physical perimeter and at the connection point for mobile and personal devices.

How XTMv Protects Businesses

The XTMv virtual appliance family can solve many different security, productivity, and compliance issues for organizations of all sizes — small, midsized and large offices. The datacenter edition capacity is limited only by the physical and virtual hardware on which it is deployed.

The virtual appliance is especially appropriate for managed security services providers (MSSPs), hosting providers, and larger IT organizations to separate traffic and policy enforcement at the perimeter because multiple instances of XTMv can run on a single vSphere hypervisor.

It manages traffic passing within the virtual infrastructure, and even across internal networks between virtual machines in the same cluster or even on the same server, thus it's appropriate for deployment to implement security policies between applications, user communities, or tenants. Even in small offices with a single server running consolidated workloads, an instance of XTMv can be run on the same server to protect the full server consolidation environment.

It is deployed as a virtual appliance without requiring specialized hardware so IT organizations can implement unified deployment processes in which the virtual machines constituting an application group and their own XTMv instance can be set-up in a single automated process.

Available in a wide range of bandwidth limits and resource capacities, **typical customer scenarios are:**

- Customer is looking to develop a more comprehensive acceptable use/security policy to protect virtual infrastructure
- Customer needs to satisfy internal or external auditors
- Customer is looking to update aging or failing security infrastructure

- Business is looking to cut operational expenses by leveraging existing virtual infrastructure
- IT organization or hosting/cloud provider wishes to supplement hardware appliances at the perimeter with virtual appliance based security between applications or users within the infrastructure

Target Companies

- Cloud/hosting/security service providers
- Retail/Hospitality companies with large virtualized HQ/Datacenter
- Large hospitals or health care campuses
- University campuses
- Investment banks, insurance companies, or other financial institutions
- Branch and remote offices with virtualization-based consolidated servers

Multiple Customers

One scenario in which WatchGuard XTMv virtual security appliances can go beyond the capabilities of physical devices is perimeter protection for multiple clients of service providers (whether hosting providers, cloud providers, or MSSPs offering "clean pipe" services through the provider's infrastructure). Multiple XTMv instances can be deployed on industry-standard servers at the perimeter or within the DMZ, and can be managed either via web interface (by the customer and/or the provider) or the multi-device WatchGuard System Manager.

(Note that, since industry-standard servers do not include special-purpose hardware for accelerating cryptography, providers that wish to deploy VPNs with high traffic requirements would probably choose to deploy a physical device – either an XTM hardware appliance or an SSL VPN appliance – in front of the XTMv instances to terminate multiple VPNs and deliver traffic to each XTMv instance.)

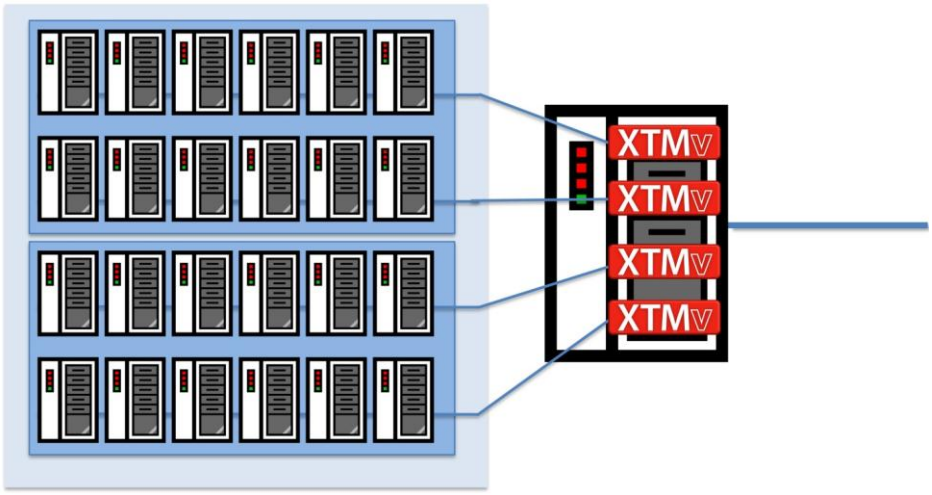

Figure 1. New Security Models for Virtual Worlds: Multiple Customers

Users and Apps

XTMv virtual appliances can also be used to simplify the deployment of services that are specific to user communities and applications, by defining and implementing security policies within the infrastructure, at the boundary between the users and/or applications and the rest of the organization. An XTM physical device at the perimeter can be used in a complementary fashion to protect from major external threats.

This approach yields three significant benefits to IT organizations and service providers:

- Instead of implementing large unified sets of security policies, those policies that are specific to protection of the application and its data, or of the user community, can be deployed in those XTMv instances. This selective configuration results in more efficient access and application control.
- With all virtual infrastructure traffic routed through XTMv instances, organizations and applications are protected not only from external threats, but also from internal unauthorized access, as well as from threats that could be carried into the infrastructure by mobile devices.
- Because XTMv virtual appliances can be cloned, relicensed, and rapidly put into operation, the deployment of an application-specific or user-community-specific instance can be automated in conjunction with deployment of the virtual machines that serve the users or applications.

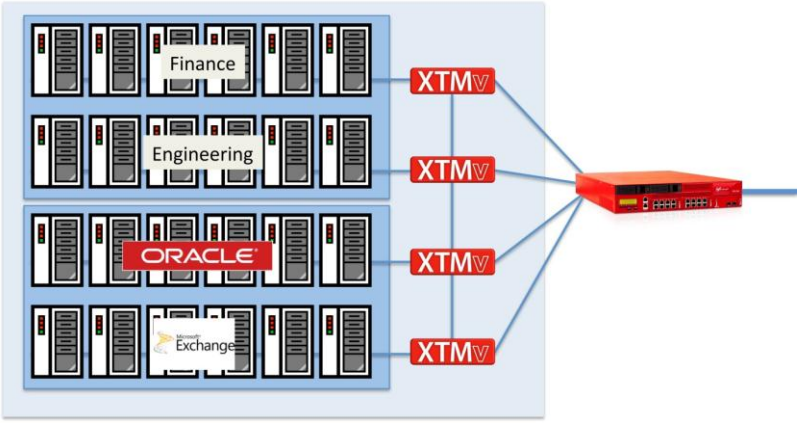

Figure 2. New Security Models for Virtual Worlds: Users and Apps

Summary

The effectiveness of WatchGuard's security solutions has been proven by providing mission-critical protection to thousands of businesses worldwide. The XTMv next-generation security for virtual infrastructures with its rich portfolio of individual security services, as well as the next-generation firewall (NGFW) and UTM service bundles, provides defense-in-depth to address the unique requirements of the most demanding environments. XTMv can also be configured with LiveSecurity, delivering software updates and technical support.

Find out more about the WatchGuard XTM family of network security appliances at www.watchguard.com, or contact your local reseller, or call WatchGuard directly at 1.800.734.9905 (U.S. Sales) or +1.206.613.0895 (International Sales).

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.