SONICWALL

EXECUTIVE BRIEF: 4 OBSTACLES TO ATTAINING PUBLIC/PRIVATE CLOUD SECURITY

Examining the security pitfalls threatening today's virtual environments

Abstract

Virtualization and cloud can cut costs and increase efficiency and operational agility, but faces ever-growing malware threats. IT must apply constrained budgets to protect public/private cloud environments against common security pitfalls, including:

- Blindness to inter-VM traffic
- Policy proliferation
- Virtual Sprawl
- Public cloud constraints

Business initiatives driving the move to virtualization

Facing rapidly-evolving markets, fierce competition and an accelerating business environment, organizations must protect market share as well as grow. More than ever, information technology plays a central role.

On the back end, IT is expected to keep pace with technology innovations, modernize the data centers and IT environment, and streamline IT services to position the organization for success. This includes designing, implementing and deploying new business-enabling applications, user productivity tools and services, and network architectures such private/public/hybrid cloud computing, network function virtualization (NFV) and mobility. Equally importantly, IT must also support and protect this dynamic network environment and mobile workforce on a flat, if not reduced, budget.

On the front end, IT must succeed at ensuring the company's web engagements, services and support are online 24x7x365. This involves keeping all the organization's web properties safe, undisrupted and in peak performance. IT seeks an affordable yet uncompromised security defense. This requires dynamic security that can prevent attacks while providing the analytics to protect and respond across the whole organization's physical

and virtual infrastructure. IT must insist upon uncompromised security, whether it is over wired/wireless or private/public cloud and from its central office to its remote campuses, branch offices, subsidiaries or partner environments.

The upside and downside of virtualization

For more than a decade, server virtualization has transformed the computing part of IT infrastructure from the physical world to the virtualization world. Virtualization remains prominent today, as it continues advancing and enriching the operational and economic benefits of the entire data center, cutting both OpEx and CapEx, allowing staff to focus on critical infrastructure.

Continuous advancements in virtualization tools and services, such as network function virtualization, are making it easy and fast for IT departments to develop and place virtualized workloads anywhere inside the virtual network (VN). Furthermore, virtualization gives IT greater network programmability and self-management capabilities, as well as the provisioning speed needed to run the data center with improved efficiency. This enables networking and application teams to tailor and deliver new services and instantly initiate, move, copy, clone, restore, or delete those services hosted on virtual machines at any time to meet their distinct data center operation needs. This increased level of operational agility and elasticity significantly lowers the cost of delivering application services to the entire enterprise.

But despite these many advantages, the flip side of using virtualization technology are the many security implications and concerns that IT must confront. (See Table 2, below.) Virtualization by its very nature adds many layers of infrastructure and operational complexity. Issues such as shared use of storage, routing devices, network segments and communication channels have proven to be vulnerable to cyber-attacks such as shared resource misuse attacks, cross-virtual-machine attacks, side-channel attacks and common network-based application and protocol vulnerabilities. These threats reach all parts of the virtual framework, including the hypervisor or virtual machine monitor (VMM), virtual machines (VMs), operating systems (OSs) in VMs, applications running on those OSs, and the virtual networking components of the virtualized environment. Improperly protecting the whole virtual environment could result in immeasurable harm to an organization.

Table 2 Relationships between vulnerabilities and threats in network virtualization environments

Threat categories		Vulnerabilities	Threats
Disclosure	Information Leakage	Lack of ARP table protection	ARP table poisoning
		Placement of firewall rules inside virtual nodes	Subversion of firewall rules
	Information Interception	Lack of ARP table protection	ARP table poisoning
		Transmission of data in predictable patterns	Traffic Analysis attacks
		Uncontrolled handling of multiple, sequential virtual network requests from a single entity	Inference and disclosure of sensitive topological information
		Unprotected exchange of routing information among virtual routers	Disclosure of sensitive routing information
	Introspection Exploitation	Uncontrolled Introspection	Data theft
Deception	Identity Fraud	Improper handling of identities:	
		- within individual networks	Injection of malicious messages with forged sources
		- among federated networks	Privilege escalation
		- during migration procedures	Abuse of node removal and re-addition in order to obtain new (clean) identities
	Loss of registry entries	Uncontrolled rollback operations	Loss of registry entries
	Replay attacks	Lack of unique message identifiers	Replay attacks
Disruption	Physical Resource Overloading	Uncontrolled resource allocation	Performance degradation
			Abusive resource consumption
		Uncontrolled handling of virtual network requests	Exhaustion of resources in specific parts of the infrastructure
		Lack of proactive or reactive recovery strategies	Denial of Service attacks
	Physical Resource Failure	Lack of proactive or reactive recovery strategies	Failure of virtual routers/networks
		Uncontrolled resource reallocation after failures	Overloading of remaining virtual routers after failures
Usurpation	Identity Fraud	Improper handling of identities and associated privileges	Privilege escalation
	Software Vulnerability Exploitation	Privilege escalation in Virtual Machine Monitors	Unauthorized control of physical routers

Source: "Virtual network security: threats, countermeasures, and challenges," Journal of Internet Services and Applications, Dec. 2015

Damages can include:

- Unauthorized takeover of virtual systems to execute malicious actions
- Unauthorized access to protected data assets
- Information theft
- Service disruption or degradation of part or entire virtual ecosystem

Virtualization is currently an active field of vulnerability and threat research in academia, bug bounty, ethical hacking and organized cyber-crime communities. New threats are discovered regularly. VENOM, CVE-2015-3456, is one such exploit that affects popular virtualization platforms such as Xen and KVM.

Hence, IT has reasons to be deeply concerned about its current security posture. Many organizations worry that current defenses system lacks the dynamic security controls and capabilities required to properly provide protection for virtual network infrastructures on a continuing basis. This makes ensuring operational uptime, service delivery and availability, and conformance to regulatory requirements very challenging for IT.

Practical scenario

To give a more practical perspective, let's examine a scenario where an organization's virtual environment exists in a physical firewall security architecture. Figure 1 (above right) describes the channel of communication flow from the application VM to the database VM on the VM host machine. The application could be a Microsoft SharePoint performing a read/write to a SQL database. In this scenario, IT must ensure application services are delivered safely.

Virtual environment with physical firewall

IT has two inspection approaches with existing legacy methods. One possible way is routing the VM to VM traffic through the virtual switch (vSwitch) northbound to the external switching fabric, and then to an external firewall which then returns the same channel southbound. Directing traffic this way takes many hops, and can cause problems like performance degradation, latency, packet loss, and security control concerns as defined above. The second approach is using a software-based firewall and running them as agents on each VM. This method faces similar challenges, with poor performance while adding management complexity as the volume of VMs increases.

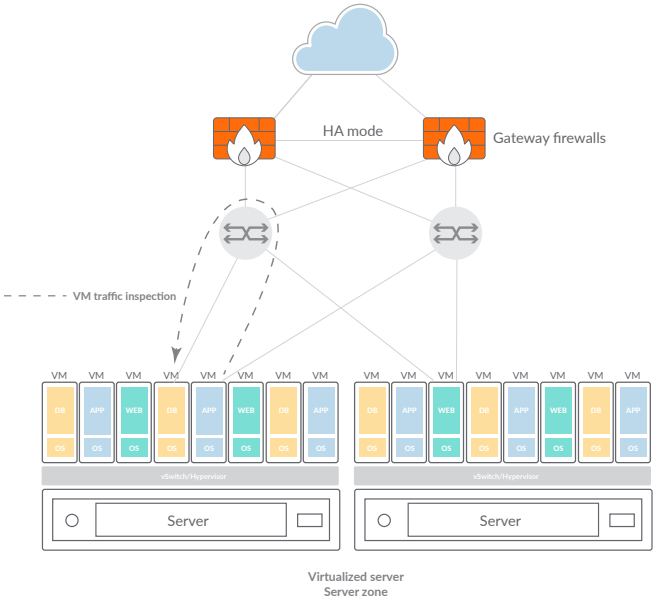

Figure 1: Virtual environment with physical firewall

When examining the security challenge of physical firewalls in a dynamic virtualized world, the common pitfalls IT will face are:

1. Blindness to traffic between virtual machines
2. Policy proliferation
3. Virtual sprawl
4. Public cloud environment

Blindness to traffic between virtual machines

When you have tens of VMs in a virtual system with communication going between them, a physical perimeter firewall may not see into lateral traffic, because the traffic may never traverse outside of that virtual server due to VM isolations or routing configurations. From a security perspective, this means monitoring for unusual events and anomalies in these scenarios becomes impossible.

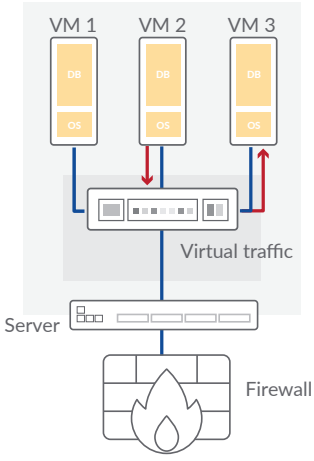

Figure 2: Inter-VM Traffic

SONICWALL®

Policy proliferation

When virtualized properties are created or moved, there are many complex networking configuration changes needed to steer those VMs' traffic to the physical firewall. This involves routing and NAT rules, ports and protocols that the application supports. Change management guidelines compel policy changes to flow through a manual and labor-intensive vetting, approving, auditing and testing workflow process before production roll-out. This is highly inefficient, operationally taxing and expensive because of all the people involved.

Moreover, with new rules compounding on top of the hundreds of other obscure rules that may have never been audited and cleared, security policies become convoluted and unmanageable. IT could begin seeing policy gaps appear and enlarge, threats missed, and/or performance drop.

Virtual sprawl

Virtual sprawl refers to a common problem where the number of virtual properties within an environment reach a point where it becomes far too difficult to track and control. When VMs get copied, cloned or moved (and in many instances, suspended and forgotten), it creates security risks, and leaves the environment open and vulnerable, as security policies and controls are disassociated. Hence, it's impractical to have a security rule fixed to a VM static IP address, considering the IP addresses of virtual machines often changes. This is a widespread issue, and hackers are actively exploiting vulnerabilities. Thus, a dynamic virtual environment requires dynamic security controls, with a tightly regulated and auditable change process to ensure VMs adhere to appropriate security and configuration policies.

Public cloud environment

Another problematic use case is where an organization's application services exist in the public cloud like Amazon Web Services (AWS) or Microsoft Azure. In a cloud environment, the organization's IT cannot put a physical firewall appliance into the provider's secured data center. These are extremely controlled facilities and, even if IT could place a physical device there, it simply cannot dictate the traffic pattern, so that the firewall would be in front of the organization's application traffic. In this case, the firewall must also be virtual, so IT might use software-defined networking (SDN) or manual configurations for traffic engineering to place the virtualized firewall in between its application services and the rest of the world, whether the path is internal or external to the data center.

Conclusion

Security is a key factor in any cost-benefit analysis of virtualization initiatives. Advantages in savings and efficiency must be weighed against potential damages due to growing threats and common pitfalls. IT needs to explore new solutions beyond legacy approaches and technologies that can effectively ensure virtualization security to succeed.

Learn more: Read our solution brief, "What to look for in a next-gen virtual firewall" and visit www.sonicwall.com/virtual-firewall.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com