

Securing the Virtualized Data Center

A Strategy for Private Cloud Security

Introduction

“As of mid-2011, at least 40% of x86 architecture workloads have been virtualized on servers; furthermore, the installed base is expected to grow five-fold from 2010 through 2015 (as both the number of workloads in the marketplace grow and as penetration grows to more than 75%).”

Virtualization of the data center provides IT departments with an attractive set of cost saving benefits including lower total cost of ownership, increased operational efficiencies and more flexible management capabilities. Virtualization also provides an equally impressive set of security challenges.

“Less than 20 percent of organizations using virtualization technology are adopting security tools to work in tandem with the software in order to decrease the risks that are inherent in a virtualized environment.”

Virtualized Data Centers (Private Clouds) have two fundamental differences from traditional data centers driving these challenges. The first difference is that the virtual data center relies on a hypervisor, which isolates the virtual machines (VMs) from the physical network. This creates a virtual network within the hypervisor that connects the server’s virtual machines and allows them to communicate without the traffic crossing the physical network. A consequence of this is that security threats are isolated from the traditional network security tools that provide visibility, control, threat detection, and automated response. Virtual machines residing on the same physical server can communicate across the virtual switch without having the traffic ever appear on the physical network where the security tools reside. The problem this creates is that if one virtual machine is compromised, a single insecure application can attack other virtual machines on the same physical server without being detected by the security tools on the physical network.

Benefits

- Move virtual machines between physical servers at will without impeding the enterprise’s security posture or requiring a time consuming manual process
- Ensure the visibility, threat detection and control of the virtual environment meets the same standard as the controls in the physical environment
- Gain the business agility promised by the virtualized environment

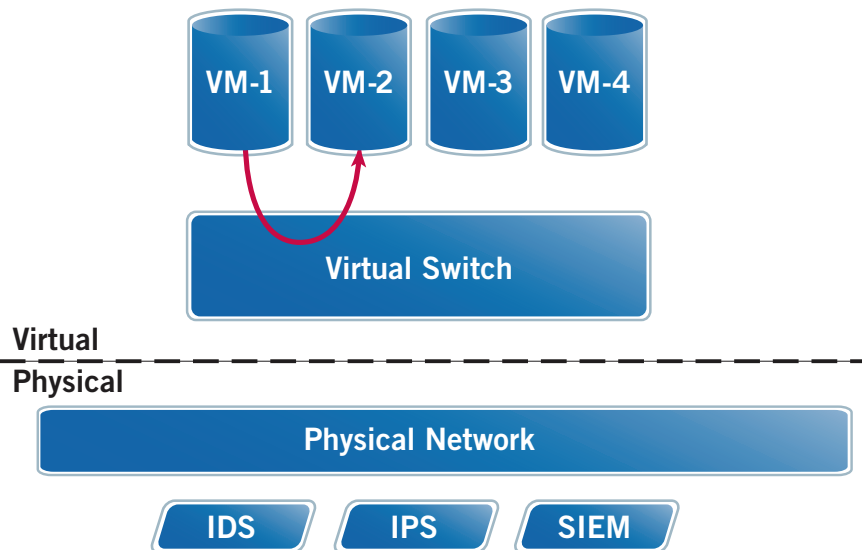


Figure 1 VM to VM Communications

¹ Bittman, Thomas, J, et.al “Magic Quadrant for x86 Server Virtualization Infrastructure,” Gartner Research Note G00213635, June 30, 2011

² Burke, John, Nemertes Research; Quoted in CSO.com; June 07 2011, Joan Goodchild, “Virtualized environments painfully insecure?”

The second difference between virtualized datacenters (Private Clouds) and traditional datacenters is the Private Cloud's combination of virtualization and automation. Virtual machines can be automatically moved between physical servers to provide high availability or load balancing.

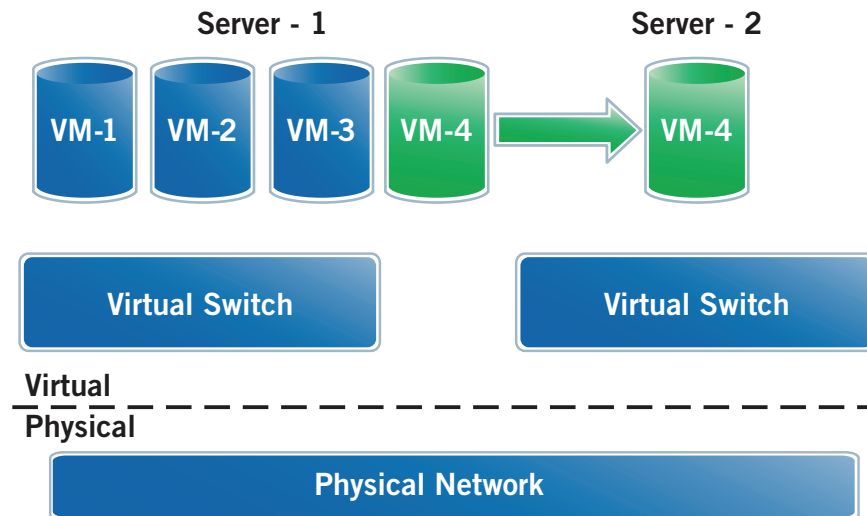


Figure 2 VM Automation

This automation means that to maintain the same security posture, network provisioning and security workflows must also be automated. Unfortunately many IT departments rely on time consuming and labor intensive manual workflows to provision and secure these virtual machines. This often means that the security and prioritization provisioning happen long after the virtual server has moved to a new physical server. Until the provisioning is complete the virtual server might be more vulnerable to attacks.

Securing the Virtualized Data Center

The fundamental best practices of providing visibility into network flows, enforcement of security and acceptable use policies, and threat detection and automated response that apply to the physical network also apply to the virtualized data center. Virtual servers require the same level of protection that a physical server receives: communications across the virtual network need to be inspected, flow data needs to be examined and the solution needs to be able to adapt to dynamic system mobility.

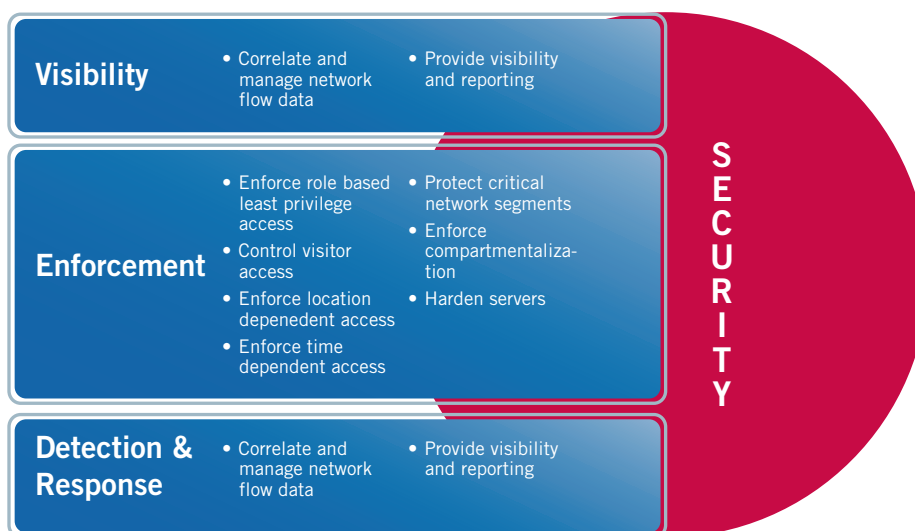


Figure 3 Security Best Practices

The challenge for enterprises is to find a set of tools that enable them to implement these best practices in the virtualized and automated environment of the virtualized data center. As Burke's research cited at the beginning of this paper shows, enterprises are struggling in this effort and leaving themselves open to increased risk.

The Enterasys solution

Enterasys provides a complete, end-to-end virtualization security solution that applies the experience of 28 years in network infrastructure and security to the new challenges of virtualization. The Enterasys solution for securing the virtualized data center consists of four components that can be deployed separately or in a fully integrated solution:

- Virtualized Host Intrusion Detection System (HIDS) sensor
- Virtualized Intrusion Detection System (IDS) sensor
- Virtualized Network Based Anomaly Detection (NBAD) flow sensor / SIEM
- Data Center Manager

When deployed together these four elements provide the visibility, enforcement, and threat detection required to secure the virtualized data center.

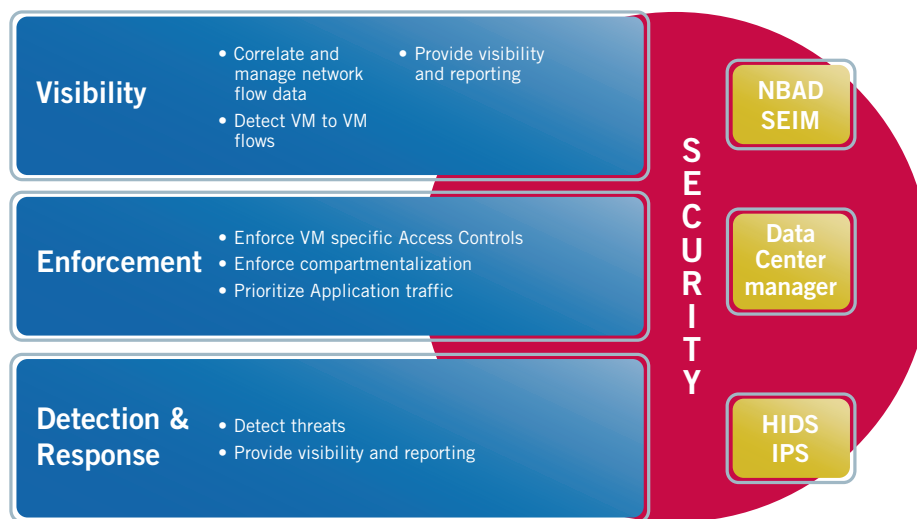


Figure 4 Enterasys Solution

Virtualized Host Intrusion Detection Sensor – Protecting the Virtual Server

Just like their physical counterparts virtual servers need protection from a variety of attacks. Enterasys virtualized host sensors are sophisticated security applications that detect attacks on virtual servers (VMs) in real time. Host intrusion detection is particularly valuable in environments where AES, SSL, IPsec, or other encryption schemes are deployed because the sensor analyzes the decrypted data. Enterasys virtualized host sensors monitor systems running today's most common operating systems for evidence of malicious or suspicious activity in real time. Host sensors use a variety of techniques to detect attacks and misuse, including analyzing the security event log, checking the integrity of critical configuration files, and checking for kernel level compromises. This hybrid approach helps organizations meet compliance requirements for servers as mandated by regulations including PCI, HIPAA and Sarbanes Oxley.

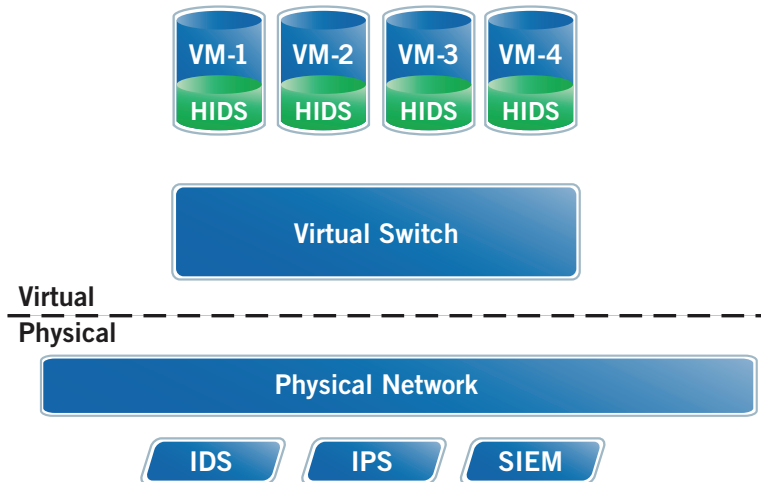


Figure 5 Virtualized HIDS

Enterasys host based sensors are unique for their broad platform support, including Microsoft® Windows, Solaris, Red Hat Enterprise Linux, HP-UX, Fedora Core, SUSE and AIX. The host sensors are supported on any supported O/S that is itself running on a virtual machine of a VMware ESX Server (version 3.0 or 4.0), AIX 5.3 and 6.1 running in logical partitions (LPARS), and on Solaris 10 running in logical domains (LDOMS) on supported platforms.

Enterasys host sensors provide maximum protection using the follow techniques to verify the integrity of the virtual server:

- Monitor file attributes such as file permission, owner, group, value, size increase, truncated and modification date
- Check file integrity to determine whether content of critical files was changed
- Continuously analyze log files using signature policies to detect attacks and/or compromises
- Monitor Windows event logs for misuse or attack
- Analyze Windows registry for attributes that should not be accessed and/or modified
- Perform TCP/UDP service detection for protection against backdoor services
- Monitor the kernel to detect suspicious privilege escalations and other signs of kernel-level compromises such as rootkits.

The host sensors support custom module development using Microsoft's .NET Framework. This allows users to leverage the power and flexibility of the .NET framework to customize Enterasys functionality to meet their needs.

Virtualized Intrusion Detection Sensor – Detecting the Threats

IDS systems deployed in the physical network cannot inspect VM to VM traffic that does not leave their physical server. This uninspected internal traffic represents a potentially serious threat vector. An infected virtual machine could compromise all of the other VMs residing on the physical server without anyone being aware of the attack. The compromise, having been allowed to escalate, increases the potential data loss and damages. Virtualizing the IDS sensor and attaching it to the virtual switch makes all internal (VM to VM) and external (VM to physical client) traffic available for inspection. Enterasys IDS virtual sensors can be deployed on VMware ESX™ servers. With these virtual machine options enterprises can deploy cost-efficient threat protection with the ability to monitor both the physical and virtual networks.

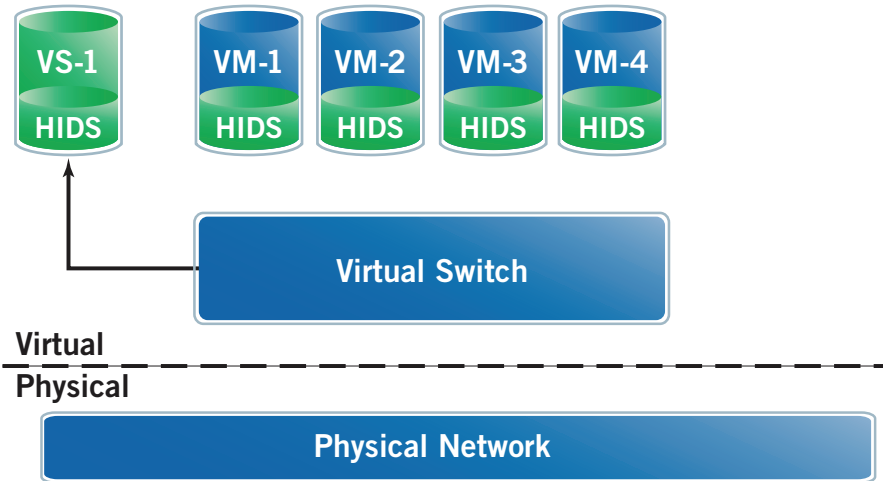


Figure 6 Virtualized IDS Sensor

The virtual IDS sensor is attached to a port on the virtual switch that is placed in promiscuous mode. In this mode all traffic seen on any port on the switch will be mirrored to the sensor for analysis.

The sensor ships with a comprehensive set of pre-installed signatures, VoIP protocol decoders for SIP, MGCP, and H.323 protocols, and features that provide advanced detection of malformed messages to help prevent DoS attacks. The sensor supports both IPv4 and IPv6 network protocols. Threat detection is accomplished using multi-method detection technologies that integrate vulnerability pattern matching, protocol analysis, and anomaly-based detection with specific support for VoIP environments. Application based event analysis is used to detect attacks against commonly targeted applications such as HTTP, RPC, and FTP.

The virtual sensors are centrally managed via the Enterprise Management Server (EMS). The EMS provides configuration management, status monitoring, live security updates, and a secure encrypted communications channel.

Virtualized Network Based Anomaly Detection (NBAD) Flow Sensor – Providing Visibility

Network and server administrators need to understand which clients and which applications are being used to access the information stored on both physical and virtual servers. External flow sensors can report on flows between the virtual servers and clients on the physical network, but to provide visibility into flows between virtual servers residing on the same physical server the flow sensor must be virtualized. The virtualized NBAD flow sensor provides the same visibility and functionality for the virtual network infrastructure that physical NBAD flow sensors provide for the physical network. The flow sensor connects to a port on the virtual switch that is placed in promiscuous mode so the sensor will see all data flows crossing the virtual switch. The sensor supports up to 10,000 flows per minute and can monitor three virtual interfaces with one additional switch designated as the management interface.

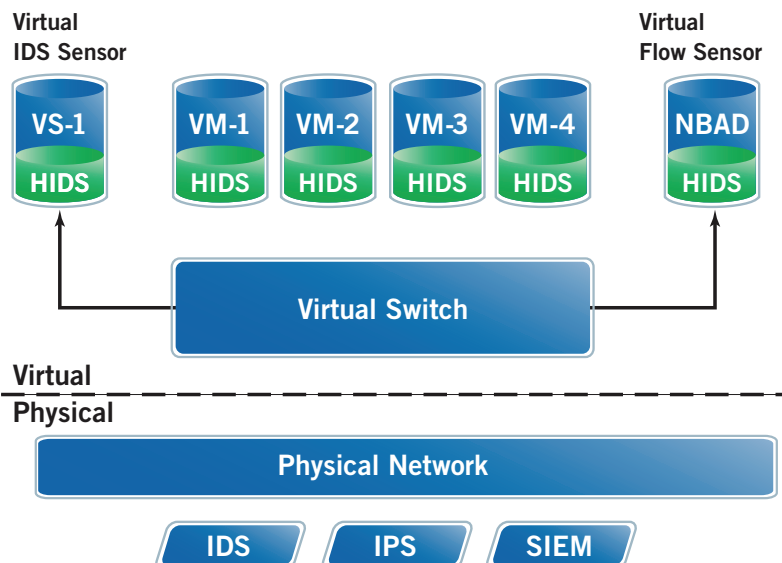


Figure 7 Virtualized Flow Sensor

The virtualized flow sensor collects flow data with application layer (layer seven) visibility. Flow data is collected and sent to the Security Information and Event Manager (SIEM) for analysis. The application layer visibility allows the SIEM to analyze and report on which applications are being used to access information on the servers. The SIEM correlates flow data from the physical and virtual environments and creates baselines of normal application flow patterns. If the flow patterns deviate from this baseline or reveal potential threats or vulnerabilities they are flagged and a security event is issued. Flows that represent threats or violations of policy are captured and reported for correlation and remediation.

Data Center Manager – Automating Security and Management Workflows

Virtual machine mobility refers to the automated process of moving a VM from one physical server to another to provide high availability, load balancing or disaster recovery. The physical network switches that connect the servers containing the virtual machines to the physical network provide access controls that protect the virtual machines and traffic prioritization rules for the applications accessing the virtual machines. Since each virtual machine will have different requirements they will each have a different set of provisioning rules. As long as a VM resides on a single physical server the network switch can be provisioned with the rules for that VM. If the VM is automatically moved to another physical server the network switch for the new physical server will have to be provisioned with the rules for the new VM. Relying on manual processes for this provisioning is labor intensive and the time lag between the movement of the VM and the provisioning of the physical switch represents a security threat to the VM. One of Enterasys Data Center Manager's features is the ability to automate the process of provisioning the network infrastructure to apply the correct access controls and traffic prioritizations for each virtual machine.

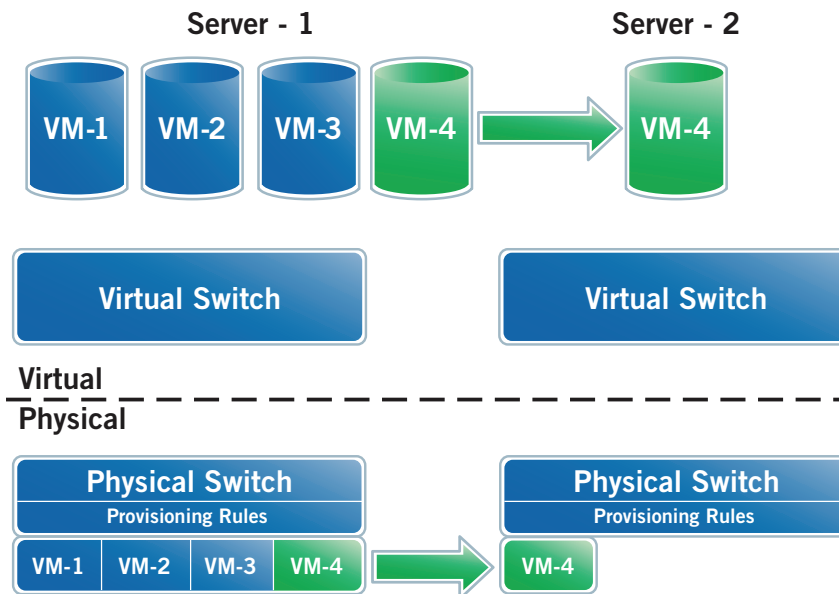


Figure 8 Data Center Manager

Data Center Manager ensures that the proper provisioning is automatically applied to each virtual machine. If the VM moves to another physical server, the VM's specific provisioning rules are automatically enforced by the new physical switch without requiring any manual intervention. Automating the provisioning workflows for the physical infrastructure reduces IT workload, improves virtual machine security, improves application delivery and satisfies compliance requirements.

In summary, Enterasys Data Center Manager provides:

- Automated unified physical-virtual network provisioning to improve efficiency in the virtualized data center
- Comprehensive virtual machine visibility to optimize resource use and decrease troubleshooting time
- Integrated workflow process to reduce IT workload and control VM sprawl
- Vendor agnostic technology support for a variety of virtualization platforms
- Simplified compliance addresses data center requirements through policy enforcement and traffic monitoring per virtual machine

Conclusion – Deploying a Secure Virtualized Data Center

Enterasys Networks provides a comprehensive set of integrated tools to help enterprises securely deploy virtualized data centers.

Flow sensors provide the visibility into the virtual environment that allows administrators to understand which external (physical) clients and applications are accessing information on the virtual servers. The visibility extends to detecting flow patterns that reveal potential threats or vulnerabilities and flows that represent violations of policy such as VM to VM traffic.

Intrusion Detection Sensors identify threats contained in traffic that crosses the virtual switch. Traffic from the physical network and from other VMs will be examined for potential threats. This inspection offers protection from an infected virtual server attempting to infect or compromise other virtual servers.

Host Intrusion Detection Sensors provide strong, multilayered protection for the virtual server. The host sensors use a variety of techniques to detect attacks and misuse, including analyzing the security event log, checking the integrity of critical configuration files, and checking for kernel level compromises.

Data Center Manager provides an extensive set of tools to automate the provisioning of the physical infrastructure to ensure that the proper controls and prioritizations are applied to each virtual server.

These tools can be deployed in concert or individually as required to meet specific enterprise requirements and priorities.

Enterasys data center solutions drive down operational costs through a combination of management automation across both physical and virtual environments and a robust and highly resilient distributed architecture. Built-in compliance controls and an open, standards-based approach for interoperability with existing data center solutions ensure a solid foundation for virtualization.

The Enterasys security tools provide a comprehensive solution for securing virtualized data centers, ensuring enterprises may confidently gain the maximum benefit from their data center virtualization efforts.

Additional resources:

- Enterasys Data Center Manager
- Enterasys IPS
- Enterasys SIEM

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

