

Sourcefire Virtual 3D Sensor™ and Sourcefire Virtual Defense Center™

Enhancing Protection for Physical and Virtual Environments

The Sourcefire Virtual 3D Sensor™ and Sourcefire Virtual Defense Center™ enable users to deploy Sourcefire's leading cybersecurity solutions within their virtual environments, increasing protection for both physical and virtual assets. These Sourcefire virtual appliances enable organizations to inspect traffic between virtual machines (VMs), while also making it easier to deploy and manage sensors at remote sites where resources may be limited. Now Sourcefire customers have the flexibility to select the physical or virtual solution that meets their specific infrastructure requirements.

APPLICATIONS FOR SOURCEFIRE VIRTUAL APPLIANCES

With the Virtual 3D Sensor and Virtual Defense Center (DC), Sourcefire is enabling customers to:

- **Secure virtualization** – Protecting virtual infrastructure from internal and external attacks with virtual security appliances
- **Virtualize security** – Leveraging cost- and energy-saving benefits of virtual security appliances to improve security efficiency

Securing Virtualization

Although organizations are deploying virtual infrastructure technologies for cost savings and operational efficiency gains, there are a number of risks associated with virtualization. These risks include VM sprawl (the propagation of VMs without adequate coordination or oversight), lack of separation of duties, lack of visibility into virtual network traffic, and hypervisor vulnerabilities. For more information on these virtualization risks, view the Sourcefire Technology Brief entitled "Strategies for Securing Virtualized Environments."

Of the aforementioned risks, one in particular is the increased number of security "blind spots" within the virtual environment. Since VM-to-VM traffic inside a physical server cannot be monitored by traditional security devices, this lack of visibility can make problem detection and resolution difficult. One example of why blind spots are concerning is the potential combination of different server zones. Some organizations are combining critical hosts and non-critical hosts on the same VMware ESX host for the sake of efficiency, but VM misconfiguration can cause these different server zones to accidentally be bridged together. The Payment Card Industry Data Security Standard (PCI DSS) recommends segmentation of critical hosts to protect critical data. By properly isolating and securing critical network segments that are virtual, an organization is also complying with PCI DSS.

Virtual hosts are just like physical hosts; they must be secured. Sourcefire Virtual 3D Sensors running Sourcefire IPS™ (Intrusion Prevention System) can detect attacks against and originating from VMs. Sourcefire RNA® (Real-time Network Awareness) installed on Virtual 3D Sensors can inventory VM attributes providing that the VMs are on the same network segment as the Virtual 3D Sensor. To combat VM sprawl, RNA identifies the manufacturer of both physical and virtual network interface cards (NICs), enabling customers to identify newly detected hosts as either physical or virtual machines. If the new host is a VM, then IT security can be alerted to audit the VM for compliance. The VM discovery process can also be automated by using compliance rules and white lists.

Sourcefire Virtual 3D Sensor and Virtual Defense Center Highlights

Benefits

- Leverage existing VMware investment
- Secure virtualization:
 - » Virtual environment visibility
 - » VM sprawl containment
 - » Assist with PCI DSS compliance
- Virtualize security:
 - » Cost, energy, & space savings
 - » Accelerated deployment
 - » For remote network areas without IT security resources
 - » Use when physical appliances are unable to be used or impractical
- Provide up to 500Mbps of IDS/IPS inspection
- Manage up to 25 physical and/or virtual 3D Sensors with Virtual DC
- Increase MSSP management effort efficiency

Virtualized Security Applications

- Remote network segments where local IT security resources may not exist (e.g., retail stores, remote offices)
- Stringent hardware restrictions for hostile environments (e.g., military ships, Humvees)
- Lengthy hardware certification requirements
- Space constraints – little rack space remains in the datacenter

Virtualizing Security

In contrast to securing virtualization, organizations can choose to virtualize security (i.e., use virtual security appliances) for cost and energy savings and to accelerate deployment. In addition, in cases where physical Sourcefire 3D[®] Sensor or Sourcefire Defense Center[®] appliances cannot be used or they are too impractical, an organization can deploy Sourcefire virtual security appliances to protect their environment.

Sourcefire Virtual 3D Sensor and Virtual Defense Center appliances can be used in organizations with:

- Remote network segments where local IT security resources may not exist (e.g., retail stores, remote offices)
- Stringent hardware restrictions for hostile environments (e.g., mobile vehicles, outdoor deployments)
- Lengthy hardware certification requirements
- Space constraints – little rack space remains in the datacenter
- Cloud computing services – deploy on demand

Sourcefire Virtual 3D Sensor

- Up to 500Mbps of inspection
- Identical 3D Sensor functionality
- Supports IDS/IPS, RNA, RUA, & NetFlow
- Recommended uses:
 - » Monitoring VM-to-VM traffic
 - » Small branch offices
 - » Remote locations
 - » Expanded RNA coverage
 - » Lab environments
- Performance will vary (dependent on hardware & VMs competing for resources)
- Supports VMware ESX/ESXi 4.0 platform

SOURCEFIRE VIRTUAL 3D SENSOR

The Sourcefire Virtual 3D Sensor enables customers to deploy the 3D System to far corners of their network where IT security resources do not exist and/or the deployment of physical 3D Sensors is impractical (e.g., retail locations, remote offices). It also provides the capability to inspect VM-to-VM communications while affording customers the opportunity to further exploit the cost- and energy-saving benefits that virtualization brings.

A single Virtual 3D Sensor is capable of inspecting up to 500Mbps of traffic and can run the same IDS/IPS, RNA, Sourcefire RUA[™] (Real-time User Awareness), and Sourcefire NetFlow Analysis capabilities that a physical 3D Sensor can. The Virtual 3D Sensor is compatible with VMware ESX and ESXi version 4.0. It requires at least 1 CPU core and 1GB of memory allocated to the sensor VM image.

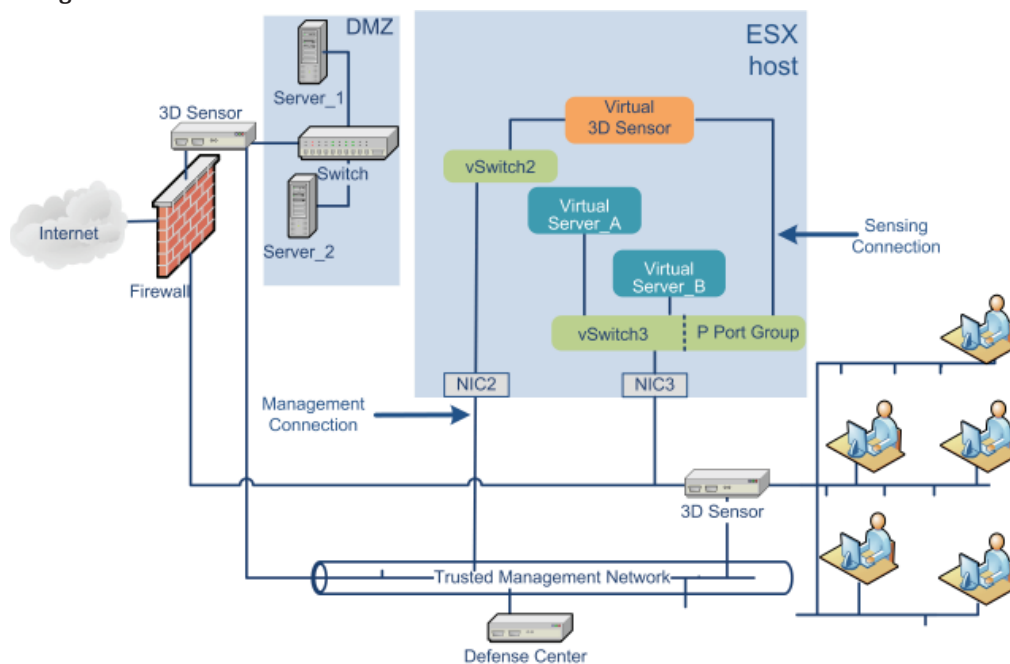


Figure 1. Sourcefire Virtual 3D Sensors can be deployed to areas of the network where IT security resources do not exist and/or deployment of physical 3D Sensors is impractical.

BENEFITS OF SOURCEFIRE VIRTUAL SECURITY APPLIANCES

The Sourcefire Virtual 3D Sensor and Virtual Defense Center appliances provide significant benefits to customers. Sourcefire virtual security appliances:

- Leverage existing investment in VMware virtualization technology
- Secure virtualization:
 - » Provide visibility into your virtual environments
 - » Help with VM sprawl containment
 - » Assist with PCI DSS compliance
- Virtualize security:
 - » Cost, energy, and space savings
 - » Accelerated deployment
 - » Use in remote network areas where IT security resources do not exist
 - » Use when physical appliances are unable to be used or are impractical
- Provide up to 500Mbps of IDS/IPS inspection
- Manage up to 25 physical and/or virtual 3D Sensors
- MSSPs can configure multiple Virtual Defense Centers to support multiple customers from a single VMware server, increasing management effort efficiency.

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

To learn more about the benefits of the Sourcefire Virtual 3D Sensor and Virtual Defense Center, visit us at www.sourcefire.com or contact Sourcefire or a Sourcefire reseller today.