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

Highest Visibility and Flexibility in Securing Virtual Networks

The Sourcefire Virtual 3D Sensor™ and Sourcefire Virtual Defense Center™, available on VMware and Xen platforms, enable users to deploy Sourcefire's leading cybersecurity solutions within their virtual environments, increasing protection for both physical and virtual assets. The Sourcefire® virtual appliances enable organizations to inspect traffic between virtual machines (VMs), while 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.

VIRTUALIZATION BENEFITS

Virtualization brings significant business benefits. It is capable of reducing costs, enabling rapid deployment, and improving system availability. Yet implementing virtualization introduces potential security risks. The process creates "blind spots" where there is greater potential for misconfiguration than in physical networks. Virtual infrastructure consolidates functions that other groups previously managed, such as networking or security, which further increases the risk for misconfiguration. Lastly, VMs quickly propagate without adequate coordination or oversight—a problem known as VM sprawl.

Sourcefire virtual appliances address the risks created by virtualization—blind spots, lack of separation of duties, and VM sprawl. The virtual appliances are the most dynamic and flexible means of securing the virtual network. They provide three main benefits:

- Reclaim the visibility you lose when virtualizing
- Virtual deployment is easier than physical deployment
- Get better prepared for PCI audits

RECLAIM THE VISIBILITY THAT IS LOST WHEN VIRTUALIZING

When deployed in physical hosts containing VMs, virtual sensors eliminate blind spots. Blind spots are especially problematic in virtual networks because any accidental change in topology or configuration will not be detected. The dynamic nature of virtual networks makes these accidental changes more likely. Figure 1 shows a Virtual 3D Sensor connected to two different virtual networks in the same host. The first network is for production traffic; the second network is for development traffic. Hosts on the development network contain source code and should not communicate with the production network.

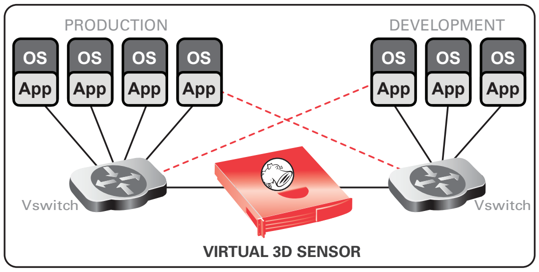

Figure 1. A Sourcefire Virtual 3D Sensor is monitoring different virtual networks in the same host.

Due to misconfiguration or inadvertent policy violation, these two networks have accidentally become connected (shown by the dotted lines). The Virtual 3D Sensor detects these type of changes, as well as any malicious traffic between the two networks.

Sourcefire Virtual Appliances Highlights

Benefits

- Reclaim the visibility you lose when virtualizing
- Virtual deployment is easier than physical deployment
- Get better prepared for PCI audits
- Provide up to 500Mbps of IDS/IPS inspection
- Manage up to 25 physical and/or virtual 3D Sensors with Virtual DC

Applications

- Protecting PCI-critical servers
- Small branch offices
- Remote locations (e.g., retail stores)
- Organizations with distributed IT security organizations
- Environments with hardware restrictions (e.g., mobile vehicles, military ships, outdoor deployments)
- Organizations with lengthy hardware certification requirements
- Environments with space constraints – little rack space remains in the data center
- Expanded Sourcefire RNA coverage
- Lab or training networks
- MSSP/Cloud Computing environments

VIRTUAL DEPLOYMENT IS EASIER THAN PHYSICAL DEPLOYMENT

Since virtual sensors are software-based and have no hardware components, they are easier to deploy and more flexible than physical sensors. However, physical sensors are still highly valuable for IDS or IPS deployments. The dedicated hardware generally provides high performance, which is required in multi-gigabit environments, such as a production data center. Physical sensors, however, have their own distinct requirements:

- Users must allocate power and rack space for them.
- Some environments have stringent hardware requirements, either because of required certification or hostile operating conditions. Physical sensors may not meet these requirements.
- Physical sensors must be shipped to their eventual location. Some international destinations have challenging customs requirements for hardware that incur significant costs or time.

Virtual sensors do not have these restrictions. They can be deployed immediately into existing hardware and start monitoring traffic right away. Because they can bypass restrictions imposed on physical hardware, virtual sensors can also monitor locations or network segments that may have been impossible to monitor before.

Another deployment advantage of Virtual 3D Sensors is that the same Sourcefire Defense Center® (DC) console can manage both physical and virtual 3D Sensors. Once a virtual sensor is added to a physical host, it can be registered to an existing DC and begin sending data right away. Users do not have to install a new management console or learn how to use a separate management application. Since the same DC is also managing the virtual sensors, the separation of duties remains intact. Security analysts can continue to manage the IDS/IPS deployment, whether virtual or physical.

GET BETTER PREPARED FOR PCI AUDITS

The current version of the Payment Card Industry Data Security Standard (PCI DSS) has no formal guidelines regarding virtualization. The existing PCI requirements, however, are still applicable in a virtual environment, especially if companies choose to combine virtual cardholder data environments (CDEs) with non-CDEs in the same physical host. Also, the PCI Special Interest Group (SIG) on virtualization is working on security guidance for virtual environments that may be added to the next version of the PCI standard, due in late September 2010.

It is important to maintain the same level of network segmentation and security among virtual systems as with physical systems. The Virtual 3D Sensor can monitor critical networks containing cardholder data or personally identifiable information (PII). This helps to meet PCI DSS Requirement 11.4, which requires use of IDSes/IPSes to monitor all traffic in the CDE.

Figure 2 illustrates how a Virtual 3D Sensor can monitor a CDE. Note that the CDE and non-CDE are provisioned on separate virtual switches and connected to separate physical network interfaces. Also, separate interfaces are used for critical functions, such as migrating VMs (vMotion), storing virtual images, and managing the virtual environments.

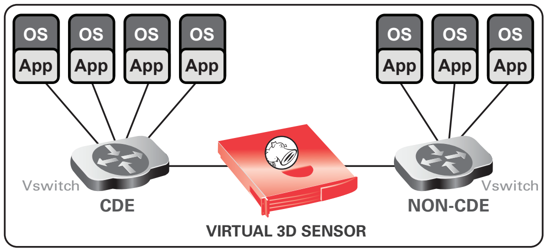

Figure 2. A Sourcefire Virtual 3D Sensor can monitor a CDE to help meet PCI DSS Requirement 11.4.

PCI DSS Requirement 6.3.2 requires that development, test, and production environments must be isolated from one another. The Virtual 3D Sensor helps to audit this requirement because the sensor can produce alerts if it sees any traffic between these networks.

SOURCEFIRE VIRTUAL 3D SENSOR

The Sourcefire Virtual 3D Sensor enables organizations to deploy the Sourcefire 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). The Virtual 3D Sensor can be deployed in passive or inline mode. Although primarily focused on monitoring traffic in virtual networks, Virtual 3D Sensors are flexible enough to monitor physical network traffic as well.

A single Virtual 3D Sensor is capable of inspecting up to 500Mbps of traffic and can run the same IDS/IPS, Sourcefire RNA® (Real-time Network Awareness), 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/ESXi 3.5/4.0 and Xen 3.3.2/3.4.2. It requires at least one CPU core and a minimum of 1GB of memory.

Sourcefire Virtual 3D Sensor

- Up to 500Mbps of inspection
- Identical 3D Sensor functionality–inline or passive deployment
- Supports IDS/IPS, RNA, RUA, and NetFlow Analysis
- Performance will vary (dependent on hardware and VMs competing for resources)
- Supports VMware ESX/ESXi 3.5/4.0 platforms and Xen 3.3.2/3.4.2 platforms

SOURCEFIRE VIRTUAL DEFENSE CENTER

Like the Virtual 3D Sensor, the Virtual Defense Center is also available as a VMware- or Xen-based virtual appliance. The Virtual Defense Center can manage any combination of up to 25 physical and/or virtual 3D Sensors, making it easier to manage sensors at remote sites. Customers can opt to monitor their Virtual 3D Sensors from the same physical DC they use to monitor their physical 3D Sensors.

Sourcefire Virtual Defense Center

- Identical Defense Center functionality (no Master Defense Center mode)
- Manages up to 25 physical and/or virtual 3D Sensors
- Performance will vary (dependent on hardware and VMs competing for resources)
- Supports VMware ESX/ESXi 3.5/4.0 platforms and Xen 3.3.2/3.4.2 platforms

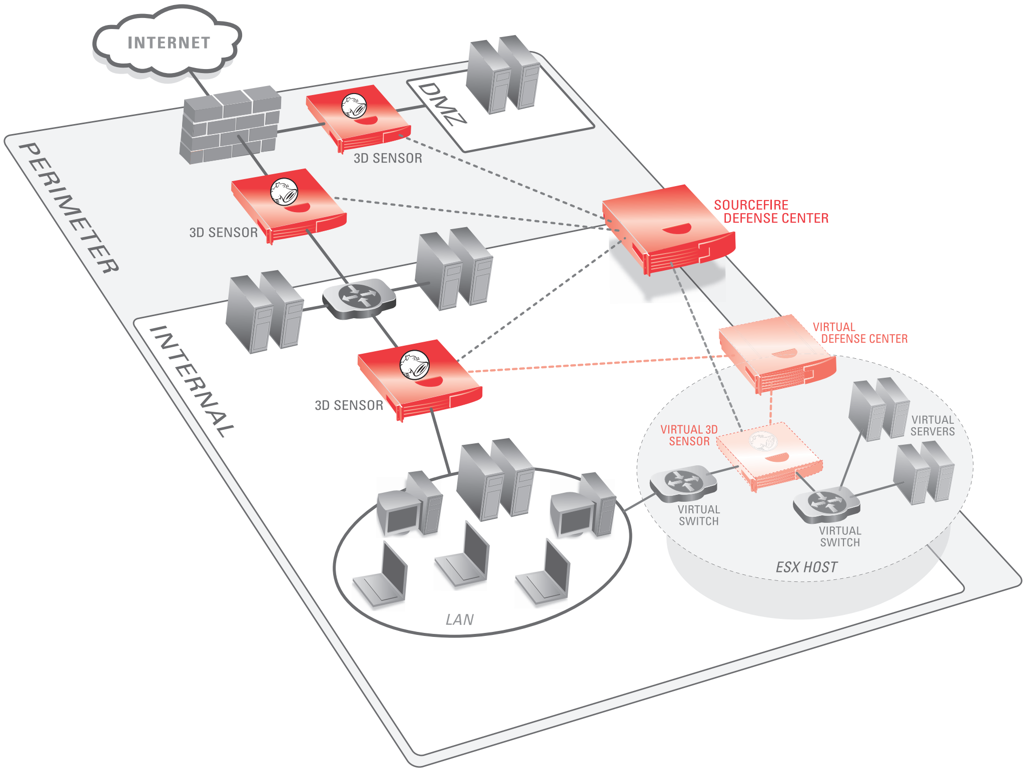

Figure 3. Sourcefire Defense Centers (physical and virtual) can manage up to 25 physical and/or virtual 3D Sensors. (Note: 3D Sensors cannot be monitored by more than one DC at a time.)

Managed Security Service Providers, or MSSPs, in particular, can benefit from a Virtual DC as they can leverage a single VMware or Xen server to host multiple Virtual DCs for multiple customer environments—without the inherent risk of intermixing security and/or compliance events from multiple customer environments while increasing the efficiency of management efforts.

The Virtual Defense Center is compatible with VMware ESX/ESXi 3.5/4.0 and Xen 3.3.2/3.4.2. It requires two CPU cores and a minimum of 2GB of memory.

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

Sourcefire virtual appliances increase protection for both physical and virtual assets. Sourcefire Virtual 3D Sensors, capable of inspecting up to 500Mbps of traffic, offer the most visibility and flexibility in securing your virtual network. Sourcefire Virtual Defense Center provides quicker and easier deployment. Smaller DCs can be deployed in remote locations, or multiple DCs can share the same physical host. The Virtual DC can manage any combination of up to 25 physical and/or virtual 3D Sensors, making it easier to manage sensors at remote sites.

Sourcefire virtual appliances offer three primary benefits:

- Reclaim the visibility you lose when virtualizing
- Virtual deployment is easier than physical deployment
- Get better prepared for PCI audits

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