Virtual Appliance™
Network monitoring gets cloud ready

Features & Benefits

» *Brings the unequalled real-time analysis and deep forensic power to a virtualized or cloud environment*

» *Hosted in a virtual server; reduces hardware footprint to support infrastructure scaling*

» *Eliminates network blind spots with proactive monitoring of traffic within a virtual server*

» *Helps generate a unified view of virtual and physical network environments*

» *Today's best solution for performance and security monitoring of virtualized environments, leading to reduced TCO*

» *Quick and easy centralized deployment, configuration and control*

» *Reduces power consumption leading to increased energy efficiency*

» *Heterogeneous Hypervisor Support (OpenStack, VMWare ESX/ESXi and vSphere, Oracle VM, KVM, etc.)*

The benefits associated with virtualization have led to the proliferation of virtual networks and the explosion of cloud computing. Both public clouds that share infrastructure, and private clouds that operate behind a firewall, present new security and performance problems, which have complicated the deployment of otherwise appealing new technologies. Total visibility into the virtual network infrastructure and cloud environments, in terms of availability and performance of virtual applications, is just as critical as insight into the physical network. Security risks are just as real, but more difficult to diagnose.

Solution

NIKSUN's Virtual Appliances are real-time data capture and analysis devices that reside within a virtual server. They glean insight into the performance and security of the cloud network by recording and analyzing all traffic directed to it, from either virtual or physical segments. Equipped with the uniquely powerful, award-winning NIKSUN® technology, these appliances bring the strengths of NIKSUN NetVCR® and NetDetector® – full packet capture and network performance analysis, and today's most advanced network forensic tool – into virtual and cloud environments. Data from distributed virtual appliances can now be aggregated and viewed on a central NetOmni™ console, not only for a unified view but also for more effective security and performance management.

Reduce Complexity

Virtual Appliances reduce the cost and complexity associated with adding physical hardware to the existing infrastructure. Out-of-the-box features reduce implementation time and costs so you're up and running fast. Appliances can be deployed across multiple virtual servers and within a private or public cloud for complete monitoring across the virtual infrastructure, providing a total view of the virtual world.

The deployment is a seamless process managed by the NIKSUN Virtual Controller. Users can easily deploy the software-only appliances through a simple point and click process.

Proactive Virtual Performance Monitoring

Virtual NetVCR™ continuously monitors virtual application traffic in real-time for proactive discovery of applications and services. Servers host a number of virtual applications within them, which typically communicate with each other. This generates a significant amount of network traffic which can tax service levels. Highly automated processes with high

service level expectations in terms of availability, data protection, and response turn around, are important for mission critical applications no matter if you are inside or outside cloud architecture. Virtual NetVCR quickly analyzes traffic characteristics and patterns within these environments to detect and immediately address any changes that may impact service levels. Performance analysis of virtual traffic is done via loss, latency, service and application response time, goodput, throughput and other similar metrics.

Virtual NetVCR provides a recording capacity of 1 Gbps per instance, so as your network grows, you can add as many instances as needed to seamlessly match the growth of your network.

Proactive Virtual Security Monitoring

Cloud or virtual servers face the same security hazards as physical servers. As traffic between virtual servers or within the cloud is isolated from the physical network, having an Intrusion Detection System residing within those environments is essential to counteract threats. The Virtual NetDetector™ monitors virtual network traffic for user-defined and threshold-based behaviors, while packets are analyzed and compared to preset signature and anomaly definitions. Incident alerts are linked to all packet information corresponding to an event occurrence. These alarms are available for further forensic investigation through an easy-to-use GUI that enables you to navigate anywhere with a single click. The NIKSUN Network Knowledge Warehouse (NKW) stores the indexed packets and provides the necessary data to reconstruct any incident and quickly analyze the traffic within the virtual network.

Unified View of All Network Traffic

While data from all distributed virtual appliances can be viewed on NIKSUN NetOmni™ for a complete picture of a virtualized enterprise environment, traffic from deployed appliances can also be pulled into NetOmni to present a unified view of all traffic across the virtual, LAN, WAN and MAN environments.
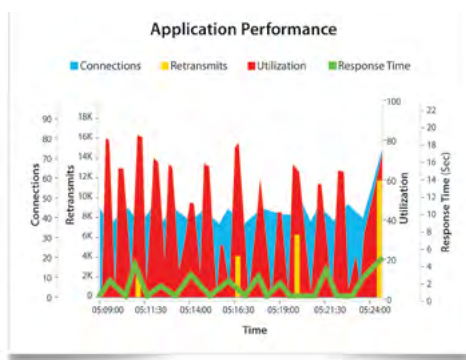
Real-time Traffic Analysis

As organizations move towards virtualization, as well as public and private cloud networks, NIKSUN's Virtual Appliances ensure visibility into both the existing physical, virtual and cloud infrastructure, providing a comprehensive platform that ensures the integrity of all facets of the network.

Technical Information

- » **Models**: Virtual NetVCR, Virtual NetDetector

- » **Database Size:** 8TB

- » **Recording Capacity:** 1 Gbps per instance*

- » **Scaleability:** unlimited instances for continuous growth and scaleability

- » **Hypervisor Support and Management:** OpenStack; VMWare ESX/ESXi 5.0 and vSphere 5.0; Oracle VM 3.3.1; KVM.

* Up to 8 vCPU cores per 1 Gbps instance

Interested in learning more?

For more information, please visit us online at *niksun.com*.