Case Study: Nielsen Mobile

Nielsen Mobile Gains Visibility Into Virtualized Server and Desktop Environments with Virtual Network Security Analyzer from Altor Networks

The Nielsen Mobile division of The Nielsen Company uses proprietary measurement technology and large-scale consumer panels to measure consumer behavior and attitudes about mobile phone services. Key elements assessed include signal quality, coverage and call metrics. Remote monitoring devices feed centralized servers, where vast amounts of data are analyzed and correlated into reports used by mobile carriers. Highlights of these reports are also syndicated for a wider audience.

The massive amounts of data collected by Nielsen Mobile, and the sophisticated algorithms required for analysis demanded substantial processing and storage resources. Nicholas Portolese, the company's senior manager of data center operations, turned to virtualization to address space constraints and power consumption. As early adopters of virtualization, the initial deployment of ten standalone servers with local storage were used for testing, development, quality assurance, and hosting offshore contractors' workstations. With the maturation of virtualization, Nielsen Mobile took another pioneering step and moved towards virtualization in their production environment. The data center currently houses 26 enterprise-class servers that are configured for high availability and dynamic resource scheduling, along with a number of standalone servers.

[Sidebar] **About Nielsen Mobile**

Nielsen Mobile is a service of The Nielsen Company and the world's largest provider of syndicated consumer research to the telecom and mobile media markets. The Nielsen Company is the world's leading provider of marketing information, audience measurement, and business media products and services. By delivering an unmatched combination of insights, market intelligence, advanced analytical tools, and integrated marketing solutions, Nielsen provides its many diverse clients with the most complete view of their consumers and their markets.

The Challenge

"Our data center experienced explosive growth, and along the way we lost visibility into and control over our virtualized resources," Portolese explains. The loss of visibility is the result of virtual networks that allow VMs to communicate with each other within the same physical servers, such that traffic never crosses onto the external physical network.

Portolese had several tools for analyzing physical network traffic, but had no ability to monitor or regulate virtual network traffic. He was unable to identify, for example, which protocols were passing through virtual switches. Nor could he match applications to the protocols being used. And when problems occurred, he lacked the means to isolate the root cause(s) quickly and accurately. "It was frustrating because we could see all the traffic flows in the physical network, but once traffic entered a virtual machine, we were totally blind as to how the virtual switch was operating," Portolese recalls.

Of particular concern to Portolese was the "security gap" that had opened up between traditional physical network security provisions and the virtualized server infrastructure. Physical firewalls, intrusion detection/prevention systems and VLANs are designed to defend static, mostly perimeter-based physical networks and are, therefore, ineffective at securing virtual switches or virtual traffic flows. In addition, Portolese was unable to take full advantage of advanced VM migration tools like VMotion owing to the complete lack of visibility into VLAN traffic among virtual machines.

For these reasons and others, traditional network analysis and security solutions are rendered virtually worthless in a virtualized environment. Portolese knew he needed to solve this problem before he could fully manage and secure his data center.

The Solution

"The vendors of virtualization software have yet to solve this problem, so I had to look elsewhere," says Portolese. After a thorough search of the market, Portolese found the Virtual Network Security Analyzer from Altor Networks. "I could tell right away it was exactly what was needed for our VMware environment."

Nielsen Mobile again became an early adopter of innovative new technology when Portolese installed VNSA agents on the company's ESX servers. The lightweight agents observe virtual switch traffic flows in real-time, communicating these observations to a centralized database with a dashboard for monitoring, analysis and historical tracking. Portolese appreciated VNSA's integration with existing VMware management systems so that he could correlate network, host and event information. With VNSA's ability to analyze virtual network traffic, Nielsen Mobile is now able to track and organize its virtual machines by network information, and create groups for different user communities and/or applications.

Portolese is initially using the VNSA to get real-time and historical visibility across the virtual infrastructure in the DMZ. "With increasing use of virtualization, we have started segregating our servers based on application. We have consolidated our outward-facing applications as a

cluster in the DMZ, and we need full visibility to proactively identify and protect against vulnerabilities in the name service, web service, unwanted broadcast, and unwanted protocols."

It is significant to note that Portolese was able to cost-justify the investment in the VNSA solution based solely on enhancing DMZ security. He explains: "IT is a cost center in most companies, and anything that does not enhance revenue these days can be difficult to justify. Eliminating a potentially serious vulnerability does get management's attention, however. Once managers understand that to get the cost-saving benefits of virtualization you really need a tool like this to maintain security, the decision then becomes a no-brainer."

The desktop virtualization project will enable Nielsen Mobile to get an even better return on its investment in VNSA by helping Portolese repurpose some older servers: "These servers work perfectly well, they're just no longer state-of-the-art in processing power. But they will be ideal in a separate cluster devoted to workstations, where viruses and worms, and unwanted broadcasts and peer-to-peer traffic would have created a show-stopper for this application without the Security Analyzer's ability to monitor all traffic."

After the DMZ project is complete, Portolese plans to use VNSA in another project which virtualizes desktop workstations where he will be able to audit workstation usage to comply with company policies.

The Results

Portolese found the Virtual Network Security Analyzer easy to use, and quickly realized both the power and potential of the product: "For the first time we are able to have complete insight into our virtual switch traffic, giving us both real-time and historical monitoring and analysis capabilities. This enables us to weed out, analyze and report on network bottlenecks caused by a number of sources, including unwanted protocols, and multicast and broadcast service announcements. It also enables us to optimize dynamic resource scheduling across our VMware environment, which is something we could not do before."

Early use of Altor's Security Analyzer revealed some interesting and surprising findings. For example, some nodes were using Microsoft's Windows update server instead of Nielsen Mobile's in-house update server, and some applications were using non-standard ports, also in violation of the company's strict security policy. Portolese even discovered that despite believing all unnecessary operating system functions had been disabled, such as multicast service advertising, many of these were still in fact active.

"With Altor's Security Analyzer we now have total visibility into and far greater control over our virtualized infrastructure," Portolese concludes. "Anyone with server or desktop virtualization really needs a tool like this to make fully-informed decisions about securing and optimizing available resources."

# # #