MARKET PULSE

Solving Critical Challenges of the Virtualized Data Center

Next-generation networking and security enable data center transformation.

A recent Network World survey, Next Generation Data Centers and Security, indicates that 62 percent of respondents are planning to or are engaged in data center upgrades. More than half are expecting to virtualize at least 40 percent of their servers this year, and one-third are targeting at least 60 percent of their servers. Already, roughly 50 percent of respondents either have deployed a portion of their infrastructure in a private cloud or have plans to do so within the next one to three years.

Yet as organizations progress on this virtualization and private cloud–computing journey, they are bumping up against a harsh reality inherent in virtualization: Applications are necessarily decoupled from the physical resources they use. This introduces new obstacles that can lead to traffic bottlenecks, inconsistent network policies, management blind spots and security loopholes.

To fully gain the benefits of greater business agility and cost efficiency that a highly virtualized, cloud environment provides, enterprises must adopt new network architectures and tightly integrated security models designed to overcome these obstacles.

"The ever-changing threat landscape … calls for the integration of best-in-class networking and security products," says Jon Oltsik, senior principal analyst at consultancy Enterprise Strategy Group (ESG). "In today's challenging and competitive business climate, enterprises must constantly keep a watchful eye across the entire network infrastructure to preempt a possible attack and be prepared to act if the unexpected occurs."

Brocade and McAfee have partnered to address the key network and security roadblocks that currently stand in the way of optimized data center virtualization. Together, they provide comprehensive services that enable businesses to take complete advantage of the benefits of virtualization and the cloud.

Barriers to Virtual Success

In many organizations, virtualization and cloud computing are seen as ways to meet the unrelenting pressure to reduce costs. IT has consolidated data centers and is deploying applications on virtual servers. In addition, as evidenced above, investments in private cloud computing are growing.

But as businesses move to the private cloud, they are finding server virtualization is severely limited by classic Ethernet designs and traditional network security controls. As data center virtualization scales, four critical tasks become increasingly cumbersome:

- Preventing traffic bottlenecks
- Reducing complexity of network policy and service level assurance
- Eliminating management blind spots that lead to outages
- Sealing up security loopholes to protect data

"Embracing virtualization technology may also mean challenging your traditional network and security design principles. The move to the virtual world usually means new best practices for network and security engineers," says Greg Brown, vice president of security at McAfee.

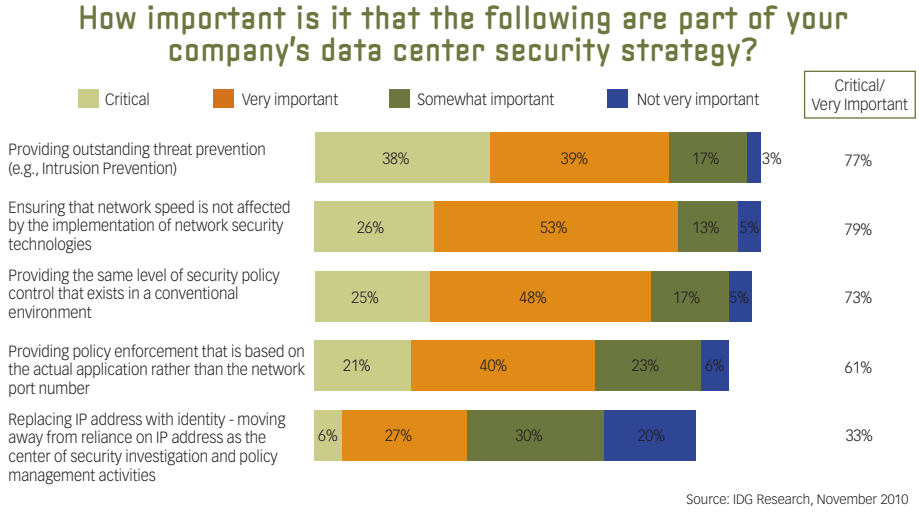
Classic Ethernet Traffic Bottlenecks

The survey shows that 54 percent of respondents are deploying 10 Gigabit Ethernet (GbE) throughout the data center. Yet despite this increased capacity, more than one-third of respondents say their most

NETWORKWORLD Custom Solutions Group

McAfee

BROCADE



Source: IDG Research, November 2010

pressing issues concerning virtualization are bandwidth and traffic engineering.

The problem lies in reliance on the Spanning Tree Protocol (STP) and multitier networks with inefficient handling of what is known as "east-west" traffic. Virtualization creates a lot of back-and-forth between servers and storage within the data center. This is counter to traditional static configuration of STP, which has the restriction of a single, active path and an expectation of north-south traffic flow. More than a quarter of survey respondents say they recognize that STP limits their company's ability to scale virtualization in the data center.

"The issue with STP is that it sets up a route through the network and effectively blocks certain ports," ESG's Oltsik says. "This is incredibly limiting as it prevents you from getting the bandwidth you need. This can result in timeouts and the retransmission of packets—not a good solution for applications that are latency-sensitive."

Policy Enforcement Complexity

Virtualized environments require additional orchestration in handling network policies. "With virtualization, an integral part of the network is now inside the virtualization software, and synching that with the rest of the network is a requirement," says Doug Ingraham, vice president of product management at Brocade.

The survey reveals that 40 percent of respondents consider movement of virtual machines (VMs) challenging as they introduce operational complexity. Typically, network policy configuration is tied to a physical port. With virtualization, virtual machines move across physical servers and, therefore, break static policy configurations.

"This could cause serious network and security problems. For instance, if a VLAN tag associated with a VM isn't communicated when a VM moves, you could have a VM that contains sensitive data open to the network," Oltsik says.

In addition, he says, it could allow risk-averse applications within proximity of risky applications. For businesses that fall under strict compliance rules, this is unacceptable. If policies are not applicable beyond the physical port, then this scenario can easily take place. Trying to map VM changes manually adds an unrealistic administrative burden to IT. If IT doesn't feel it is safe to move VMs around, then that could inhibit an organization's ability to get the most out of its virtual investment.

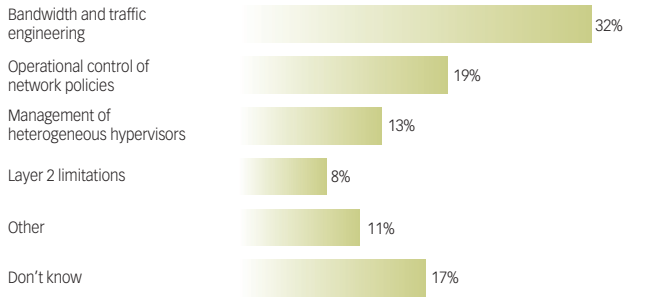
"You need an environment where, when virtualized traffic shows up on a port, its policy can be looked at and adhered to," Ingraham says.

Eliminate Management Blind Spots that Lead to Outages

Most IT teams would love to have unified security across virtual and physical environments. Instead, they are forced to patch together numerous solutions to try to get a glimpse of their security posture. The root of the problem is that many of today's security tools are based on IP address vs. identity. In fact, 61 percent of survey respondents who rate their data center as critical to the business say the use of identity vs. IP address is an essential tool for securing the data center. The lack of identity-based controls creates blind spots.

"In a dynamic, virtualized environment, the need to tie application and network activity back to specific individuals

Most Pressing Data Center Network Issue Created by Virtualization



Source: IDG Research, March 2011

and organizations is amplified," says McAfee's Brown. "The ease with which virtual infrastructure is created, modified, moved and accessed challenges conventional network security technologies."

With an identity-centric strategy, IT teams can follow users and applications across data center resources and track back at a granular level if an incident or threat occurs. Without this, IT has limited visibility when diagnosing problems.

Lack of Visibility and Security Loopholes

Finally, the virtualized data center is creating serious security loopholes that hackers could dive right through. It's not surprising then that more than 75 percent of survey respondents rate threat protection or intrusion prevention as a critical challenge for the next-generation data center. Yet half of these respondents are relying on the same security model for virtualization that they use for their physical environment. "A lot of enterprises are trying to make do with their physical security safeguards, but they really aren't conducive to the virtual world," Oltsik says.

The issue is that most security tools rely on physical trust boundaries, and those boundaries are broken by virtualization. Physical environment–focused security cannot demarcate between physical and virtual resources, and as such can't monitor VMs properly, protect boundaries, detect problems, or enforce policies.

Each of these issues puts barriers up to achieving the goals of virtualization and private cloud computing. IT must embrace a new security model that replaces physical trust boundaries with virtual ones. This will enable IT to provide seamless, secure user access to applications anywhere at any time.

The Brocade/McAfee Solution

Brocade and McAfee have partnered on a portfolio of offerings that seamlessly blend network innovations and security management to address the challenges of both physical and virtual environments. This unified approach eliminates bottlenecks, inconsistent network policies, management blind spots and security loopholes.

Brocade VDX 6720 Data Center Switches are specifically designed to improve network utilization, maximize application availability, increase scalability, and dramatically simplify network architecture in virtualized data centers. By leveraging Brocade Virtual Cluster Switching (VCS) technology, the Brocade VDX 6720 creates an Ethernet fabric at the edge, delivering large, flat Layer 2 networks built for "east-west" traffic and free of Spanning Tree Protocol. At the core, Brocade MLX Series routers deliver industry-leading 100GbE, 10GbE and 1GbE wire-speed density; rich IPv4, IPv6, Multi-VRF and MPLS; and advanced Layer 2 switching to provide cloud-optimized networks. The Brocade 1860 Fabric Adapter is a new class of adapter that meets all the connectivity needs of cloud-enabled data centers while providing unmatched performance, application-aware services, unified management, and reduced cost and complexity. It is the simplest, most flexible and most powerful server connectivity adapter designed to extend fabric services to virtual machines and applications in highly demanding virtualized environments.

Brocade also provides application-aware resource control that can monitor application demands and virtual server performance. When performance lags, Brocade's network intelligence detects this and triggers new virtual servers to come online, maintaining application service levels. Brocade's ADX family of application delivery controllers with integrated Application Resource Broker (ARB) software provides this network service to ensure application agility is efficiently maintained and performance remains at optimal levels.

McAfee Firewall Enterprise and McAfee Network Security Platform intrusion prevention system operate with

Brocade technologies to provide IT with a fully protected and unified platform for network and security that is high performance and always on.

"We're delivering to the virtual world the same world-class intrusion prevention, firewalling and access control that you have in the physical world," McAfee's Brown says. "The same appliance can protect both. Also, management interfaces are the same across both environments so users don't have to learn anything new."

In addition to offering consistent security management tools across physical and virtual environments, the joint solution delivers the protection, performance and identity-based security controls required for the virtual data center.

McAfee Network Security Platform has been validated in independent tests by NSS Labs to be over 95 percent effective in preventing network attacks, using a combination of protocol detection, network behavioral anomalies and reputation-based detections. The platform offers native 10GbE connectivity and even faster throughput performance to eliminate potential security bottlenecks within the data center.

Brocade and McAfee offerings feature an identity-based strategy that enables IT to automatically and properly apply policies across the physical, virtual and cloud environments. Such granularity speeds investigations and problem resolution as well as reporting. The ability to move security profiles with virtual machines and to know the identity of the host machine are critical to ensuring that compliance and other data-protection rules can be met. This information also helps to properly allocate resources and ensure quality of service.

Brocade uses sFlow for traffic monitoring and provides automated migration of Port Profiles for policy mobility. Combining Brocade's intelligence with McAfee Network Security Platform and McAfee Firewall Enterprise, administrators can construct trust boundaries and enforce dynamic policies that move with the VMs. Together, Brocade and McAfee eliminate the occurrence of inconsistent network policies, reduce vulnerabilities, and increase the ability to detect threats.

"Brocade and McAfee ensure that policies stay intact, even in a private cloud environment," Brocade's Ingraham says.

Integration between the network platform and the security platform is instrumental in eliminating management blind spots. The typical patchwork of network and security solutions has been replaced by a well-engineered unified infrastructure that communicates to identify and stop attackers. If McAfee generates a security event, Brocade's switches and routers can respond with automated actions, preventing widespread issues.

"There's no more swivel-chair management; you can easily see what's happening across systems," Brown says. Administrators can respond quickly with right clicks rather than having to call, email or trouble-ticket other IT personnel. "They can make instant, sound decisions," he says.

This tight collaboration also leads to the closure of security loopholes. Brocade and McAfee provide the visibility and policy enforcement necessary to ensure that VMs containing sensitive customer information are not jeopardized by VMs housing applications that may be experimental or not as well protected behavior such as cross-site scripting. "Now that you can see the virtual layer, you can apply common policies across your physical and virtual environments," Oltsik says.

Solid Solutions for Your Next-Generation Data Center

The Network World survey shows that enterprises are committed to virtualization and private cloud computing. But they need to ensure network and security issues will not thwart their success.

Brocade and McAfee provide an integrated solution portfolio of products that solve the critical challenges of the Virtualized Data Center. With Brocade and McAfee as strategic partners, businesses will be able to create a scalable, available, simple and secure virtual data center that is ready for private cloud computing.

For more information, please visit:

www.mcafee.com/brocade

www.mcafee.com/us/products/network-defense/index.aspx

www.brocade.com/McAfee

www.brocade.com/partnerships/technology-alliance-partners/technology-alliances/McAfee/resources.page