Secure virtual environments solution brief

The importance of application intelligence and control in virtual environments

Dell™ SonicWALL™ Next-Generation Firewalls with Application Intelligence, Control and Visualization plays a pivotal role in application efficiency, bandwidth utilization and Internet security in virtualized cloud environments.

Enterprises worldwide are speeding up their server virtualization. Running multiple applications and associated operating systems on a single physical device slashes the number of servers that enterprises need to purchase, deploy, house, operate, maintain, power, and cool, leading to substantial cost savings. The decoupling of workloads from underlying server hardware also delivers portability, thus meeting critical objectives for high availability, business continuity, and adaptability. Organizations are further realizing the benefits of fully dynamic virtualization by implementing the flexibility and scalability of hyperscale virtual server platforms and adding the elasticity to respond quickly to changes in virtual environments.

Frequently, organizations make the most of these dynamically scalable virtualized resources through deployment in private, public or combined cloud environments. By deploying virtualized services in the cloud, businesses can access highly scalable and responsive web applications and services without necessarily having to build and pay for underlying infrastructure. Because cloud computing usually entails the purchase of a service rather direct ownership of all the necessary bits and pieces, IT organizations also enjoy quicker startup times, better agility and investment protection (based on being able to terminate the relationship and change directions as needed), and need to only pay for what is used.

By shifting virtualized resources to the cloud, organizations place business-critical applications and sensitive data outside the corporate boundary. However, the available bandwidth needed to access these resources is undermined by the bandwidth consumed by the growing onslaught of Web 2.0, social media and streaming multimedia traffic—some legitimate, others non-productive and time wasting. For example, YouTube® traffic can reduce the available bandwidth required for business-critical applications. Latency-sensitive applications can suffer from degraded performance.

Traditional optimization solutions based on ports and protocols cannot address the problem. For example, trying to restrict web access (port 80) inherently counters the productivity and optimization benefits of deploying cloud based virtualized resources in the first place. Open access to the Internet is an incontrovertible fact, but controlling that access is central to a successful virtualization and cloud computing strategy. Failure to deploy an application control infrastructure puts your critical virtualized applications at the same priority level of time-wasting games and frivolous applications.

Moreover, virtualization in the cloud presents security issues. As more and more employees rely on web access to do their work, there is a greater likelihood for web-borne attacks, intrusions, spyware, botnets and other threats driven by a profit-driven malware economy. Unfortunately, traditional stateful packet inspection firewalls used in many organizations cannot solve the problem because they are not able to dig deeply into the payload to identify intrusions, viruses, spyware and other malware.

Next-Generation Firewalls with application intelligence, control and visualization

One of the most promising new security dynamics in the marketplace today are Next-Generation Firewalls (NGFW), such as the Dell SonicWALL E-Class Network Security Appliance (NSA) Series. Scanning every byte of every packet of all network traffic, Dell SonicWALL Next-Generation Firewalls provide complete application intelligence, control and visualization, regardless of port or protocol, by determining exactly what applications are being used and who is using them. This turns the traditional gateway firewall into something much more important: a productivity optimization tool. It does this by enabling organizations to define mission-critical applications, and then strategically prioritize access and bandwidth allocated to those applications and restrict access and bandwidth to inappropriate and non-productive applications.

Additionally, Next-Generation Firewalls also detect and eliminate malware, intrusions, data leakage and policy violations before they cause harm to a company's network or its users. By inspecting at the packet level in real time, without reassembling the packets, Dell SonicWALL Reassembly-Free Deep Packet Inspection® (RFDPI) technology provides high performance and low latency security.

Application intelligence, control and visualization helps IT address the challenges of virtualized computing in two distinct ways. First, it provides detailed visibility and control of associated traffic based on the specific applications and services being used and, optionally, based on who is using them and when they are being used. Therefore, critical traffic between a business and a virtualized infrastructure that utilizes port 80 or port 443 can be distinguished from ordinary web-bound traffic carrying less critical information because Next-Generation Firewalls identify the specific web applications and users and match corporate IT policy to the flows. Access control and threat inspection policies can thus be set and enforced on a highly granular basis, instead of having to treat all traffic the same. Second, it provides IT with a means to mitigate potential performance issues. The ability to discern which specific applications comprise a given traffic stream, combined with built-in QoS and bandwidth enforcement capabilities, enables IT departments to reserve bandwidth for essential applications, and prioritize their treatment relative to less critical services. In addition, comprehensive reporting capabilities support ongoing monitoring and tuning, thus ensuring that associated rules remain aligned with actual conditions and shifting usage patterns.

Using application intelligence and control, administrators can create bandwidth management policies based on logical pre-defined categories (such as social media or gaming), individual applications, or even users and groups. As new applications are created, new signatures can be pushed to the firewalls and the appropriate policies automatically updated without IT spending time and effort to update rules and application objects. In addition, administrators can use granular application-based policy to restrict or block the transfer of specific files and documents, prioritize or throttle bandwidth and deny access to internal or external web sites.

In virtual environments, bandwidth management can be extremely critical, especially in situations where applications transfer massive databases between virtual servers. Mission-critical applications need bandwidth prioritization while non-critical applications like social media and gaming need to be bandwidth throttled or completely blocked. However, even if an administrator has created a rule to optimize the network, how do they know it has actually worked? Administrators must visualize application traffic to properly control ingress and egress bandwidth and network use, and to adjust network policy based on critical observations. Administrators can then quickly modify application rules to conform to network policy. In addition, the same data can be sent to an analyzer for off-box monitoring, troubleshooting and analysis of historical network activity.

Targeted security solutions for virtual environments

The virtual server hypervisor is not only a conduit through which all of the applications riding on top can be compromised, but it is also becoming a bigger target for hackers as virtualization grows in popularity. Placing a Dell SonicWALL Next-Generation Firewall in front of the organization's virtual server farms is an ideal solution in this case. In contrast to narrowly focused stateful inspection firewalls, Dell SonicWALL Next-Generation Firewalls can provide robust protection against the broadest spectrum of threats to hypervisors and virtual machines by integrating real-time gateway intrusion prevention, anti-malware, and anti-spyware.

Virtual switching capabilities allow administrators to re-create portions of their network within a single physical host. The problem this introduces, however, is how to enforce security policies on the traffic flowing between different virtual machines on the same server. Routing all inter-VM communications through a Dell SonicWALL Next-Generation Firewall can enforce all access control policies and thoroughly scrub associated traffic for embedded threats.

Another capability common to server virtualization is live migration, a feature that allows dynamic re-location of workloads from one physical server to another (e.g., so that scheduled maintenance can be performed without interrupting operations). The challenge this presents is that conventional security devices are unable to properly protect associated workloads (at least not without operator intervention) due to their dependence on network-layer attributes for enforcing policies. Dell SonicWALL Application Intelligence and Control is not dependent on network-centric details such as IP address, directional orientation, and other characteristics of the physical or logical environment. Application Intelligence and Control is equally capable of enforcing policies and inspecting communications traffic for threats based on higher-layer attributes, such as the specific applications and services being used, who is using them, and when. This gives Dell SonicWALL Next-Generation Firewalls a high level of granularity and resilience in terms of being able to account for and fully protect dynamically shifting workloads.

Ultimately, organizations cannot gain the full benefits of virtual application deployments unless the applications are secure and have the bandwidth to function optimally. IT needs to focus ensuring the viability of mission-critical applications and restrict the flow of nonproductive and dangerous application traffic. Dell SonicWALL Next-Generation Firewalls with Application Intelligence, Control and Visualization help organizations get the most from their virtualization investments.