DELL SonicWALL

Next-Generation Firewalls: Critical to SMB Network Security

Next-Generation Firewalls provide dramatic improvements in protection versus traditional firewalls,

particularly in dealing with today's more sophisticated and rapidly changing threat landscape. In fact, if your organization is still using traditional firewalls to protect against malicious threats, you could actually be increasing your security risks rather than alleviating them. Traditional firewalls may give you a false sense of protection when, in reality, they are lacking critical features and functionality.

TechTarget® Custom Media

TABLE OF CONTENTS

That’s why small and midsize businesses need to deploy a Next-Generation Firewall (NGFW) as an integral part of their overall security strategies. NGFW and a Unified Threat Management platform can bolster your protection against the constantly evolving threat environment.

It is also important to understand that not all NGFWs are created equal. In choosing a solution, make sure you are not sacrificing throughput and productivity for security. An NGFW should be able to provide:

- **Advanced Threat Protection:** This should include Deep Packet Inspection (DPI) of the entire packet payload for intrusion prevention, malware detection, gateway antivirus, traffic analytics, application control and Secure Sockets Layer (SSL) decryption.

- **No Trade-off Between Performance and Protection:** Network traffic should be inspected with minimal latency for optimal throughput and maximum application performance while ensuring comprehensive security. Solutions from Dell SonicWALL, for example, improve performance dramatically by enabling DPI without buffering or packet reassembly.

- **Maximum Productivity Through Granular Application Control:** An NGFW should provide application intelligence and control, real-time bandwidth and application visualization so administrators can manage applications to deliver maximum user productivity as well as massive scalability.

The need for next-generation firewalls

Cybercriminals are constantly adjusting their targets to attack our greatest vulnerabilities. These days, the web is far and away the target of choice. According to one report, approximately 85% of all malware comes from the web, with more than 30,000 web sites infected every single day.[1] What’s more, cybercriminals are increasingly going after soft targets, such as social networks, where users may be less circumspect in their behaviors. Attackers are also targeting mobile devices such as smartphones and tablets, since security safeguards are less likely to be in place, and the bring-your-own-device (BYOD) trend may make it easier to infiltrate corporate networks or obtain confidential documents.

[1] Security Threat Report 2102, Sophos

Attacks on SMBs are also increasing, as smaller companies are perceived to lack sophisticated security solutions such as NGFWs. For example, since early 2010, 40% of attacks have been aimed at SMBs, versus 28% against large enterprises.[2] Unfortunately, the perception of security weaknesses is based on reality, as more than 80% of SMBs in a recent survey said they have no cybersecurity plan. [3]

In addition, cybercriminals are taking advantage of weaknesses in traditional firewall technology. Traditional firewalls work with a simple classification of network traffic based on which port or protocol it uses. For example, most web traffic is identified as TCP traffic coming through port 80. While the port and protocol meet the firewall's restrictions and thus qualify as acceptable HTTP traffic, no information is available to the firewall about the specific applications or data payload associated with the traffic. The increased use of web-based services also allows the application content utilizing open ports to be more varied and thus more vulnerable to malicious programs. Because traditional firewalls do not inspect the traffic payload, they are unable to distinguish good traffic from bad traffic.

NGFWs, on the other hand, provide traditional firewall protection such as packet filtering, network address translation (NAT) and stateful packet inspection (SPI), as well as a more advanced security platform based on granular traffic inspection to allow intelligent enforcement of security policies based on variables such as user credentials or application actions. Integrated intrusion prevention and application control allow for inspection and policy enforcement, even on SSL-encrypted traffic. Finally, an NGFW allows applications and services coming into the network to be viewed, providing a context for application bandwidth management and optimization, while enabling advanced analytics reporting and security.

Research firm Gartner lists these minimum NGFW requirements:

- Nondisruptive in-line bump-in-the-wire configuration
- Standard first-generation firewall capabilities, such as NAT and SPI and virtual private networking
- Integrated signature-based intrusion prevention system engine
- Application awareness, full-stack visibility and granular control
- Capability to incorporate information from outside the firewall, such as directory-based policy, blacklists and whitelists

[2] SMB Threat Awareness Poll, Symantec, November 2011

[3] New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity: Majority Have No Policies or Contingency Plans, National Cyber Security Alliance, October 2012

- Upgrade path to include future information feeds and security threats
- SSL decryption for identifying undesirable encrypted applications

What to look for in an NGFW

As noted, the key in selecting an NGFW is to make sure you are getting maximum protection without sacrificing performance. The real measure of security and performance is DPI throughput and effectiveness. Unfortunately, many firewall vendors have adopted the same malware-inspection approach used by traditional desktop antivirus solutions: buffer downloaded files, then inspect the malware.

This flawed methodology introduces significant latency, which can lead to major problems. First off, latency slows down application performance and, with the growing use of software as a service, remote desktop virtualization, collaborative software and mobile devices, any degradation in performance can cripple key applications. This could negatively impact revenue opportunities, profitability and business operations. Furthermore, introducing latency into the equation results in additional security risks, since temporary memory storage can limit protection to a maximum file size.

Dell SonicWALL has taken an innovative approach to maximizing threat protection and performance through its patented Reassembly-Free Deep Packet Inspection (RFDPI) engine. Unlike other DPI methods, RFDPI is not hindered by having to store traffic in memory before inspection. As documented in independent benchmark testing, this leads to significant performance advantages versus competitive solutions. [4]

Dell SonicWALL solutions deliver on the three fundamental requirements of NGFWs – advanced threat protection, maximum performance and granular application control – in the following ways:

DPI for Maximum Performance: The patented Dell SonicWALL RFDPI engine uses a combination of complex pattern matching, heuristics, correlation, advanced real-time decision methodologies and data normalization to maintain extremely high performance, low latency and high efficiency regardless of file size. Performance of Dell SonicWALL NGFWs is also bolstered through the use of a multi-core hardware architecture, enabling

[4] Dell SonicWALL SuperMassive E10800 is rated the highest in overall protection by NSS Labs; E10800 wins Network World's Clear Choice performance test; ISCA Labs confirms E-Class NSA Series are the first available firewalls to receive enterprise firewall certification and meet all NGFW evaluation requirements; Dell SonicWALL Next-Gen Firewalls Secure Networks, Prevail as Top-Rated Products in Independent Lab Tests, September 6, 2012

each CPU to process a portion of network packets simultaneously in parallel with other CPUs, making optimum use of available processor cycles. This combination offers efficient, high-performance solutions for packet, content and security processing while at the same time delivering massive scalability.

Advanced Threat Protection: In addition to all traditional firewall threat protection, RFDPI allows Dell SonicWALL NGFWs to extend protection to block malware. Most competitive solutions can scan only six protocols, which provides a false sense of security. Malicious traffic transmitted through any other protocol is not subject to inspection. Working at both the network and application layers, the RFDPI engine examines all downloaded, emailed and compressed files. Dell SonicWALL NGFWs scan every packet on all ports and all protocols every time. Beyond that, Dell SonicWALL offers intelligent malware detection technology that can dig deeper for elements in the flow that may contain harmful code.

Application Intelligence and Control: The RFDPI engine enables the NGFW to identify and control applications, regardless of the port or protocol. This provides granular control and real-time visualization of applications to examine traffic, bandwidth utilization and security threats. With this type of granular control, organizations can guarantee bandwidth prioritization and address security threats in real time. Administrators can restrict or block the transfer of specific files and documents, prioritize or throttle bandwidth and deny access to internal or external web sites. Application intelligence and control addresses a key challenge for IT professionals, particularly with the growth of high-bandwidth and high-collaboration applications, such as streaming video, social media, gaming and cloud-based services. These applications can introduce new security threats, while also draining precious bandwidth that should be prioritized for mission-critical applications. Dell SonicWALL Application Intelligence is a tightly integrated feature of Dell SonicWALL NGFWs.

To address the security needs of SMBs, Dell SonicWALL offers NGFW security through its Network Security Appliance series of integrated solutions and the Unified Threat Management platform, combining multiple security features and multiple layers of protection into a single platform to protect against attacks, viruses, Trojans, spyware and other malicious threats.

Conclusion

The threat landscape is changing rapidly. And it is also intensifying: With new types of malware, cybercriminals have become increasingly sophisticated and coordinated in their attacks. They are out to exploit every vulnerability, and if your organization is not taking advantage of the advanced protection offered by NGFWs, then you are at increased risk of a successful attack.

Deploying a security solution that incorporates an NGFW can provide the protection you need, but it is important to deploy the right solution. Independent tests have confirmed that NGFW solutions from Dell SonicWALL are delivering industry-leading threat protection and performance, while enabling best-of-breed features and functions such as intrusion prevention, SSL decryption, and application intelligence and control. Now is the time to explore Next-Generation Firewalls from Dell SonicWALL.