

Why Performance Matters Solution Brief

NETWORK SECURITY

Nine Things to Expect from a Next-Generation Firewall

Why Performance Matters

Today's corporate networks are under increasing pressure to support growing quantities and types of traffic—and thwart the associated threats. Regardless of your company size, you need to reconsider the firewall securing your data and applications. After all, Web 2.0, streaming video, and hosted, cloud-based, and peer-to-peer (P2P) applications all expose your company to potential infiltrations, data loss, and downtime. In addition to introducing security threats, these applications drain bandwidth and productivity, and compete with mission-critical applications. To complicate matters, the convergence of voice and video in today's corporate environments heightens the need for a high-performance security solution that does not impact the quality of time-sensitive media.

You need a solution that handles both inbound and outbound traffic flows—one that delivers the velocity and security to ensure a productive work environment. The answer is a holistic approach to network protection offered by a next-generation Unified Threat Management (UTM) firewall.

Traditional Firewalls Fall Short

Traditional legacy firewalls rely upon stateful packet inspection, which falls short when it comes to ensuring protection of critical information and resources in today's work environment. First, they only protect against inbound traffic—yet outbound traffic can be the launch pad attackers use to infiltrate your network. Next, only firewalls equipped with anti-virus gateway capabilities can protect against harmful Internet traffic, such as viruses and spyware. Finally, traditional firewall products offer no protection against harmful traffic crossing the LAN and limited protection against wireless traffic. In fact, they cannot efficiently handle internal LAN and mobile traffic without slowing down the network.

Consider a 150-person business that routinely exchanges large electronic files with its partners, uses time-sensitive Voice over IP (VoIP) and broadband video, and plans to adopt Web 2.0 applications. A traditional firewall cannot handle this company's requirements without negatively impacting network throughput. As a result, voice and video quality will be degraded and employee productivity will suffer.

The Need for Next-Generation, High-Performance Firewalls

Some companies question the need for a high-performance firewall—such as one that can transfer 1.7 GB per second—when they are connected to the Internet via a 100 MB pipe. But in today's business environments, high-performance is a necessity. Here's why.

Deep Packet Inspection (DPI) is the new standard and with good reason—it scans every item in a packet unlike stateful packet inspection that inspects only a sample of the packet's contents. However, unless your firewall can handle high throughput, DPI scanning will bring your network to a screeching halt—or at least make it very sluggish. On top of that, corporate networks are becoming more complex, comprising multiple LAN segments. With important data and applications traversing those segments, firewalls need to scan all parts of the network—and that requires top performance.

To date, companies have tolerated the performance slowdowns associated with traditional firewall processing. After all, it may take longer to process or transmit data, but it doesn't impact the quality of work being done. However, all of that changes in today's converged networks. Because voice and video are time-sensitive, any delays in firewall or network performance can degrade quality. Furthermore, traditional firewalls and earlier UTM solutions are unable to ensure the secure transmission of voice and video, because they lack DPI technology. Clearly you want a firewall capable of addressing all of these issues.

"Customers that have deployed SonicWALL's UTM solutions have seen a significant decrease in losses due to the prevention of viruses, spyware and other malicious activity. In addition, they have seen increases in productivity due to the additional content management features. The new DPI engine has resulted in a tremendous improvement in performance. It has allowed our customers greater flexibility in deciding how and where it is deployed while maintaining their budget objectives."

Mike Johnson, Cerdant

Unified Threat Management is the New Standard

In the face of today's complex network challenges, your company needs a security solution that can support all application and data requirements, including converged networks. UTM is the latest approach to security—one that offers the necessary level of protection against today's risks while ensuring the highest levels of productivity and application quality. Fortunately, you can benefit from unified threat management by leveraging SonicWALL next-generation firewall appliances.

"The SonicWall NSA E7500 is a breeze to configure, an excellent performer, and the truest unified threat manager (UTM) we tested, blocking an impressive 96 percent of the attacks we threw at it."

Infoworld 5/27/09 review

Nine Things to Expect from SonicWALL's Next-Generation Firewall

- 1. Unified Threat Management**
Delivers a secure, converged solution that enables significantly higher performance to improve network security and productivity
- 2. Site-to-site VPN convergence (voice, video, data)**
Unites separate offices, expands tele-worker capabilities, and terminates VPN tunnels for remote locations and VPN phones
- 3. Remote VPN (IP Sec and SSL VPN)**
Provides mobile users with access to all office services, controls access to resources via user and groups, and maintains security through DPI
- 4. Uninterrupted, high-quality voice and video**
Enables administrators to prioritize voice and video over other less time-sensitive traffic
- 5. Specified traffic restrictions**
Scans files/documents for keywords and specified content
- 6. Control and elimination of non-essential traffic**
Regulates mail attachments and file transfers; manages bandwidth to restrict streaming video/ music, Web 2.0, and P2P applications; applies restrictions to applications, groups, or on a per-user basis; blocks access to specified Web sites
- 7. LAN traffic protection**
Inspects and cleans every packet of encrypted traffic crossing the LAN from content-based threats such as viruses and malware
- 8. Granular log controls to track all network activity**
Allows network administrators to track network utilization, monitor security activity, and view Web usage
- 9. Future-proofed network**
Adapts and responds to emerging threats as new applications and data traverse your network

Conclusion

Because SonicWALL® offers a family of network security appliances—from entry-level to enterprise-class—companies of all sizes can protect multiple areas of their business with a single investment. Integrated anti-virus, anti-spyware, intrusion prevention protection, and application control are delivered at gigabit speeds, which helps safeguard against all application-layer and content-based attacks without compromising performance. By consolidating threat management, you gain a central point of management, avoid training employees on multiple products, and realize lower total cost of ownership. Plus, with no software to install, your administrators won't need to wrestle with the complexities of operating systems. Perhaps most important, you'll extract greater value from the data, voice, and video applications your employees rely upon on a daily basis.

"I've looked into other solutions with similar functionality such as Cisco, and they are all far more expensive. SonicWALL gives me the performance I need and more money left in my budget."

Jesse McKneely,
Director of Infrastructure and Project Management,
Birmingham-Southern College

