The Advantages of a Multi-core Architecture in Network Security Appliances

SonicWALL Network Security Appliance (NSA) technology greatly exceeds the security and performance of traditional network security solutions by conducting comprehensive Unified Threat Management (UTM) and real-time Deep Packet Inspection over a breakthrough multi-core processor architecture.

CONTENTS

SONICWALL

ABSTRACT

Network security has become increasingly complex. Network communications no longer rely simply on store-and-forward applications like email, but have expanded to include real-time collaboration tools, Web 2.0 applications, instant messenger (IM) and peer-to-peer applications, Voice over IP (VoIP), streaming media and telepresence conferencing, each presenting conduits for potential attack. The complexity of securing today's networks demands a Unified Threat Management (UTM) approach.

To be truly effective, UTM requires deep packet inspection (DPI) in real time. Sophisticated malicious attacks can penetrate traditional stateful packet inspection products. To maintain acceptable network performance, traditional solutions focus on scanning only the packet headers, missing threats hidden within the data portion of packets. Ideally, network security solutions need to be capable of fully inspecting the entirety of every packet in real time for all current internal and external threats. This real-time full-packet DPI capability, pioneered and developed by SonicWALL®, is known as Reassembly-free Deep Packet Inspection™ (RFDPI).

The performance of the underlying architecture is crucial for accomplishing real-time DPI without significantly impairing throughput. Yet traditional single-processor and ASIC solutions cannot keep up with evolving complex attacks in real time from both inside and outside the network perimeter due to the increased inspection demands required.

A multi-core architecture is the best platform for delivering UTM with real-time DPI. Compared with general purpose and ASIC processors, multi-core technology offers higher performance, scalability, and energy efficiency than other network security platforms available today. The flexibility, economy and power of multi-core processors in conjunction with reassembly-free DPI, form the bedrock of the high-performance network security industry.

Emerging Trends in Network Security Technology

Facing evermore complex network environments—and a corresponding array of malicious threats—network security is increasingly dependent upon a unified threat management approach incorporating real-time deep packet inspection. These technologies, however, demand an underlying platform—such as a multi-core processor architecture—that can handle their security functionality without negatively impacting network throughput and corporate productivity.

Unified Threat Management (UTM)

Unified Threat Management (UTM) has become a de facto requirement in protecting modern networks. Traditional point solutions simply no longer provide sufficient, timely and unified protection against today's complex threats. These malicious attacks take advantage of an increasingly complex business networking environment that can often include unregulated Internet access, and peer-to-peer, IM and multimedia applications. This complexity inherently increases potential avenues for spyware, malicious mobile code, key loggers, VoIP attacks, phishing, fraudulent Web sites and blended threats (e.g., Recent Storm Worms) that combine virus and worm technologies in extremely elusive multifaceted attacks. Complexity also undermines IT control over the network, often resulting in decreased bandwidth, lower productivity, and corporate liability associated with inappropriate or illegal traffic.

Traditional point solutions, which have been installed to solve some of the threat and productivity issues, are difficult to deploy, manage and update, increasing operating complexity and overhead costs. Instead, organizations today demand an integrated approach to network security and productivity that combines the management of traditionally disparate point technologies.

Unified Threat Management (UTM) represents the established trend in the evolution of the traditional firewall into a product that not only guards against intrusion, but performs content filtering, data leakage protection, intrusion detection and anti-malware duties typically handled by multiple systems.

UTM Using Reassembly-free Deep Packet Inspection

Traditional solutions using stateful packet inspection technology only audit approximately 2% of the traffic that moves through the firewall. In contrast, UTM solutions that enable Deep Packet Inspection (DPI) are designed to audit 100% of externally- and internally-originating traffic. However, not all DPI methodologies are created equal.

Reassembly-free Deep Packet Inspection (RFDPI), pioneered and developed by SonicWALL, can handle the scanning of unlimited files sizes and an unlimited number of connections on the network in real time. RFDPI technology has been designed and fine-tuned for multi-core hardware, enabling intelligent inspection at extremely high speed, resulting in significantly greater scalability and performance than other DPI methods.

Unlike all other DPI methods, RFDPI is not bound by the requirement to halt and store traffic in memory. (Often, this limitation requires administrators to either pass traffic unchecked when under excessive load, or block all traffic, even legitimate business communication.) Also, unlike other DPI methods, RFDPI does not limit the size of file that any one user can download, nor does it limit the number of users that can be protected at one time. This makes RFDPI architecture the most scalable in the industry and the most powerful solution for enabling real-time UTM.
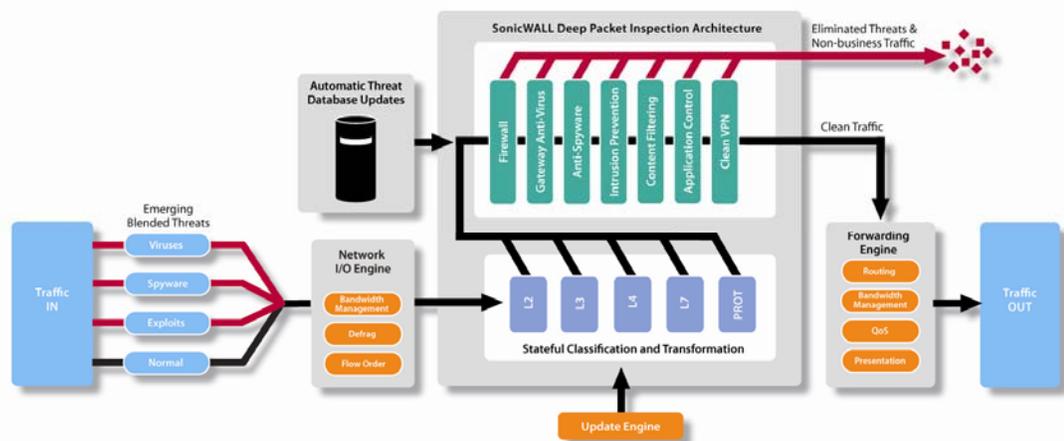

Figure 1. Reassembly-free Deep Packet Inspection in a Unified Threat Management System

Comparing Network Security Architecture

Security vendors developing next-generation security appliances have taken multiple approaches in underlying hardware design. SonicWALL has chosen a multi-core processor architecture. Other vendors have chosen general purpose processors and separate security co-processors. Still others have chosen to design and build ASIC (Application-Specific Integrated Circuits) platforms. The following section explores the inherent limitations within general purpose and ASIC approaches and contrasts these limitations against the overwhelming benefits of multi-core technology.

Limitations of general purpose processors

General purpose processors rely on a single processing CPU for handling all functions. They do not provide any type of security acceleration, and usually require additional third-party security co-processors for the necessary security acceleration. Since a general purpose processor runs at a higher clock speed and requires additional co-processors, it consumes more power during general operation. Additionally, general purpose processor solutions are limited by bus speeds between the general purpose processor and security co-processor. General purpose processors also can be comparatively limited in memory bandwidth, resulting in slower packet processing. Overall, general purpose single processor designs offer a less-than-ideal hardware platform for UTM inspection.

Limitations of ASIC processors

While ASIC platforms have a place in high speed packet forwarding, they have inherent design challenges and limitations when used in network security appliances. One particularly significant challenge is the inherent limitation in a vendor's ability to field upgrade the ASIC micro code to deal with the evolving security landscape. With ASIC solutions, the lack of available microcode space may prevent the vendor from adding new functionality required to deal with changing protocols, upgraded standards or bugs. This limits ASIC-based security appliances as there is no guarantee the appliance can be upgraded to deal with customer's future networking needs.

Benefits of multi-core processors

Multi-core processors have many advantages over a general purpose and ASIC processor in supporting UTM appliances. These advantages include lower power consumption, onboard security co-processors and increased memory bandwidth necessary to increase throughput. SonicWALL's multi-core platforms integrate hardware acceleration and automation into a wide range of packet processing and application-specific functions. SonicWALL's SonicOS firmware leverages these hardware features to deliver significant performance advantages over conducting these same functions using software alone.

Compared with general purpose processors, the multi-core processors used in SonicWALL next-generation security appliances provide additional security co-processing per core, allowing each individual core to perform any additional security acceleration on-chip. By integrated security co-processors in its multi-core platform, SonicWALL has developed a high-performance solution that significantly decreases latency in security co-processing. Furthermore, the SonicWALL multi-core architecture is not limited by bus speeds, since all security acceleration is done on-chip. Anticipating future iterations, the extendable SonicWALL multi-core platform is designed for easy expansion to apply even more cores-per-chip, more chips-per-board, and more boards-per-chassis.
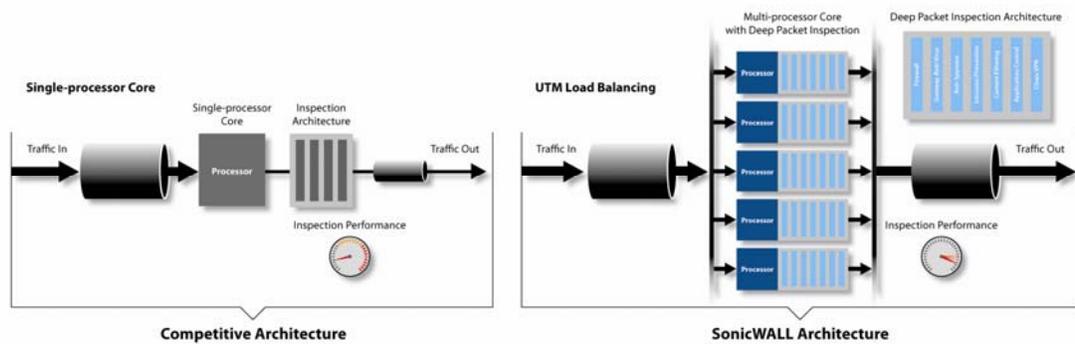

Figure 2. Multi-core processing versus single-core.

To increase network packet processing performance, SonicWALL designed its multi-core processor with greater memory bandwidth than a general purpose processor. This increased memory bandwidth provides a faster packet processing platform, since more memory resources are available per packet. With a general purpose processor, the bandwidth is limited to 86 GB/s, while multi-core processors have in excess of 100 GB/s of memory bandwidth available.

The design and implementation of multi-core processors also demonstrate high efficiency. For example, in SonicWALL multi-core appliances, this efficient and optimized implementation translates into low power and small silicon area consumption. As a result, these processors integrate a significant amount of application specific hardware acceleration and allow up to 16 cores onto a single processor, offering the highest performance as measured by a broad range of real-world applications and benchmarks. Multi-core processor technology has allowed SonicWALL to develop enhanced network security appliances that consume roughly 30% less power than comparable solutions built using a general purpose processor and security co-processors, while providing similar network scanning speeds. SonicWALL multi-core processor appliances apply up to 16 cores (and are designed to extend to accommodate even more cores in future iterations) providing high-performance parallel packet processing, with integrated security co-processors running at a lower clock speed while consuming less power during normal operation.

And unlike ASIC solutions, SonicWALL's multi-core security appliances are fully field upgradeable, and thereby able to keep ahead of evolving security threats while providing new security and protocols as adopted or modified by industry consortiums.

Conclusion

To meet the security demands of today's networks, SonicWALL applies Unified Threat Management using real-time Reassembly-free Deep Packet Inspection. This comprehensive level of UTM requires the utmost performance from its underlying hardware architecture. When compared to general purpose processor and ASIC approaches, the multi-core processor architecture of SonicWALL Network Security Appliance (NSA) solutions are conclusively superior.

The fundamental rationale behind a multi-core architecture is to maximize application performance and scalability while minimizing power consumption and development complexity. Multi-core architectures combine application specific hardware acceleration with high performance multi-core processor architecture techniques. This optimal combination offers high performance and efficient solutions for packet, content and security processing. When compared to alternative architectures, multi-core architectures offer much greater efficiency in terms of low power consumption and minimized development complexity. Unnecessary overhead and complexity is removed.

With a compelling combination of innovative technology, high performance, cost-effectiveness and reliability, SonicWALL has emerged as the worldwide leader in Unified Threat Management, helping organizations defend against network attacks, improve productivity and efficiency, simplify administration through a single management interface and lower the total cost of network security ownership.