

Accelerating Unified Threat Management
with Specialized Hardware

White
Paper



Multi-Threat Security Solutions

FORTINET®

Introduction

The "security versus performance" dilemma has been alleviated by advancements in unified threat management architecture. Many IT professionals implementing network security once found, however, that placing more security controls within the network typically led to a network performance impact. The primary issue with network-based security was intensive computational overhead associated with implementing content-based security measures. This issue was further compounded as the industry began the shift toward a consolidated network security solution combining multiple security features within a single platform, commonly known as a Unified Threat Management (UTM) platform. Due to this history, many enterprises have been reluctant to adopt UTM platforms over concerns of the impact it will have on network performance.

The performance concerns, while once quite valid, are today largely resolved through the use of specialized hardware which accelerates security technologies. As security technology evolves, platforms utilizing specialized hardware have broken through the performance barrier, bringing the benefits of consolidated network security to enterprises of all sizes and in deployment locations never thought possible. The goal of this white paper is to demonstrate why UTM platforms must use specialized hardware to keep pace with security infrastructure consolidation and ever increasing speeds of enterprise networks.

The Evolution of Networking Technologies

Routers and Firewalls

In order to explore the evolution of UTM technology and the specialized hardware used to enable enterprise adoption, it is first necessary to draw a parallel with other network technologies. In particular, it is important to understand how specialized hardware has fueled adoption to a broader range of customers. Consider the evolution of networks and how network routers, called gateways at inception, were originally general purpose computers running software that handled the identification and forwarding of packets of data to their next destination on the network. This technology was essential for many network designs, but was typically a bottleneck in the flow of data between applications. Today, however, it is a different story with network routers being specialized devices which rely on customized processors and Application Specific Integrated Circuits (ASIC) to deliver high-performance traffic forwarding between networks and applications. The move from general purpose computers to specialized hardware in the network routing industry was driven largely by performance requirements (Metz, 1998, p.15) and once implemented, helped to fuel the adoption to a wider range of customers and applications. Figure 1, below, demonstrates the evolution path of network routers from general purpose computers with routing software to specialized devices.

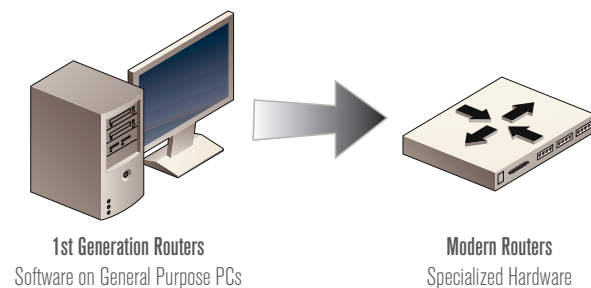


Figure 1: Evolution of Routers to Specialized Hardware

We can also draw a parallel with firewalls, which followed a similar pattern, but added a layer of evolution. Firewall technology itself evolved from network router technology, and at inception was little more than a network router with packet filtering capabilities. The technology matured from basic packet filtering to a more complex control technology which included stateful packet inspection and finally to full application layer inspection devices (IEEE, 1997). Firewalls, like network routers, were implemented first in software and evolved to hardware with increasing network speeds, but their evolution was also driven by the integration of another technology.

Around the year 2000, a technology designed to connect remote networks securely via the Internet was gaining acceptance: Virtual Private Networks (VPN) (Gleeson et al., 2000). The integration of firewalls and VPN technology was a natural fit, as enterprises typically deployed both at the network perimeter. In the end, falling prices for high-speed Internet access and VPN technology, with its complex cryptography, drove the need for the acceleration capabilities that specialized hardware is designed to provide. An illustration of the evolution of firewalls is shown in Figure 2 below.

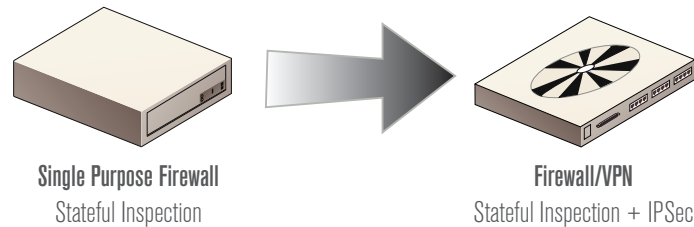


Figure 2: Evolution of Firewall technology with Integrated VPN Capabilities

With both network routers and firewall/VPN devices, history has demonstrated that evolution to specialized devices realizes performance and functionality increases. It should come as no surprise, then, that it is essential that UTM technology evolves along a similar path.

The Evolution of UTM Platforms

UTM platforms, also called "Next Generation Firewalls", expand on traditional firewalls to incorporate additional complementary security technologies. UTM platforms are defined by International Data Corporation (IDC) to minimally include firewall, VPN, intrusion prevention and antivirus features. Since the introduction of UTM platforms, there have been two approaches to their architecture — license the technologies needed to complete the platform, or build the technology in house.

As illustrated in Figure 3 (page 4), the first design attempted to link the best-of-breed products and were introduced by security vendors who approached the design of a UTM platform with a core competency in a single security technology. Some vendors, for example, were experts in firewall technology, while others were experts in intrusion prevention technology. These vendors augmented their product by partnering with complimentary technology providers who were considered to be leaders in their respective security technology. Some UTM products provided management interfaces which united the suite of disparate technologies with a goal to simplify management of these products, while others required separate management interfaces for the various security technologies that ran on a common hardware platform.

The second design approach was a uniform architecture approach that involved the construction of a system from the ground up to provide each security function natively. This approach was the more difficult of the two architectures to implement. In order to be accepted by the market, each security function had to meet the standards established by standalone security products. However, the core functions provided by UTM platforms—firewall, intrusion prevention and antivirus—had matured since the onset of the UTM era, so building competent security functions was both possible and cost effective. This design approach also had the advantage that the management interface was naturally unified because the platform incorporated multiple security technologies from inception.

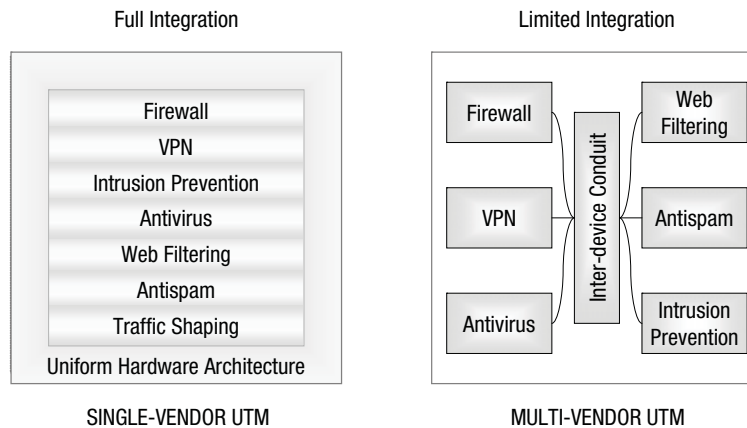


Figure 3: Different approaches to UTM architecture

Shortly after the first UTM platforms arrived on the market, IT professionals discovered that the Achilles' heel of the platforms was performance. Vendors who had built UTM platforms through best-of-breed partnerships were left with little room to scale their solution for higher speed networks. This was so because their ability to optimize the platform was limited by restricted access to other vendors' source code. For vendors who had built UTM platforms using the closed architecture approach, the fruits of their additional work in building a single vendor product began to pay dividends in flexibility. By owning the source code for the security technologies, there were a host of opportunities to address performance issues. One optimization was to eliminate redundant processing by ensuring that traffic was disassembled and re-assembled as few times as possible on its trip through the device.

The most significant performance contribution, however, proved to result from hardware acceleration of the security inspection process. As with routers and firewalls, ASIC technology was proven to improve throughput. Hardware engineers discovered that by adding security-specific ASIC processors and extending hardware optimizations through to the application layer of the Open Systems Interconnection (OSI) Reference Model, UTM platforms could realize exponential performance gains.

As UTM platforms expanded their functionality to include other technologies such as antispam and web filtering, the performance issue only compounded. UTM platforms with multi-vendor technologies were not able to take full advantage of hardware acceleration and thus were reluctant to add additional features to an already resource-starved system. UTM platforms from a single vendor who had taken advantage of software and hardware integration, however, were not bound by this limitation. The single vendor solutions have and continue to scale into larger networks and more comprehensive UTM solutions.

Building the High-Performance UTM

While there are many components in a UTM appliance, there are three major components to high-performance UTM systems: specialized hardware, specialized software and evolving security content. Through intelligent integration, each component contributes to the effective security and scalable performance provided by a UTM solution.

Specialized Hardware

Two major types of specialized UTM co-processing hardware contribute to performance scalability—content processors and network processors. These processors work in conjunction with the general purpose processor. The general purpose processor works in concert with the other specialized processors similarly to the way that the brain works with the spine and peripheral nervous system to perform system activities.

Content Processors

Processors that are specifically engineered to perform high-speed comparisons of objects to known threat patterns held in memory are called *content processors*. Objects can be many things, such as a network packet or a compressed file archive. These processors are highly adapted for protocol recognition and parsing, allowing them to quickly assemble data streams and inspect them for suspicious patterns or content. As shown in Figure 4, content processors are not placed to directly receive traffic, and generally process objects looking for threats when instructed to by the general purpose processor, instead of functioning autonomously.

Content processors can accelerate antivirus, intrusion prevention and other application level security technologies, especially comparing objects to known threats. Many people have the misconception that ASIC technology implements static security that cannot adapt to new threats. But content processors implement only scanning logic in hardware, and are not used to store threat pattern data, which continue to be stored by memory. Therefore, updates for evolving threats remain as simple as an update to a software-only solution.

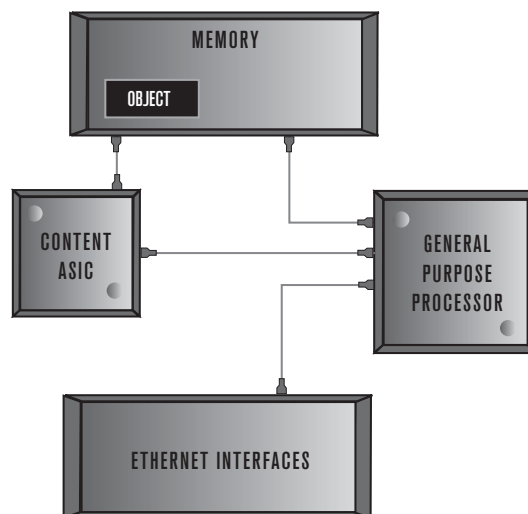


Figure 4: High-Level Architecture of a UTM System with an onboard Content Processor

Moreover, content processors can also contain cryptographic engines that relieve the general purpose processor from the high intensity calculations that take place during encrypted communications. Virtual Private Network (VPN) setup and key maintenance are particularly taxing on a system, making them ideal candidates for hardware acceleration.

Network Processors

Hardware designs that are engineered to perform high-speed processing of network flows are called *network processors*. This type of processors typically are placed inline between the general purpose processor and network ports, directly receiving traffic and performing some functions automatically. The processing work accomplished by network processors reduces the load placed on other system components. Figure 5 (page 6) illustrates the position of the network processor within the architecture. Network processors handle much of the maintenance tasks associated with packet-based communication, general TCP processing, encryption/decryption, and network address translation (NAT).

A new generation of network processors can also perform security inspection and take action, if necessary, to modify traffic flows. Network processors can very quickly defragment packets. Network processors are able to accelerate the reassembly of fragmented packets which are a naturally occurring condition on the network, but this fragmentation condition is a technique often used by attackers in an attempt to evade legacy security systems. The latest generation of network processors can be programmed with the current firewall and IPS policy, filtering traffic, detecting protocol anomalies and expediting delivery of latency-sensitive traffic at the interface level—without burdening the rest of the system. In the case where traffic bypasses other portions of the system, the network processor first downloads session processing instructions from the general purpose processor, then processes packets mostly autonomously, remitting only necessary state information. By communicating the

state information and not the actual packets, general purpose processor congestion is alleviated and performance improves dramatically.

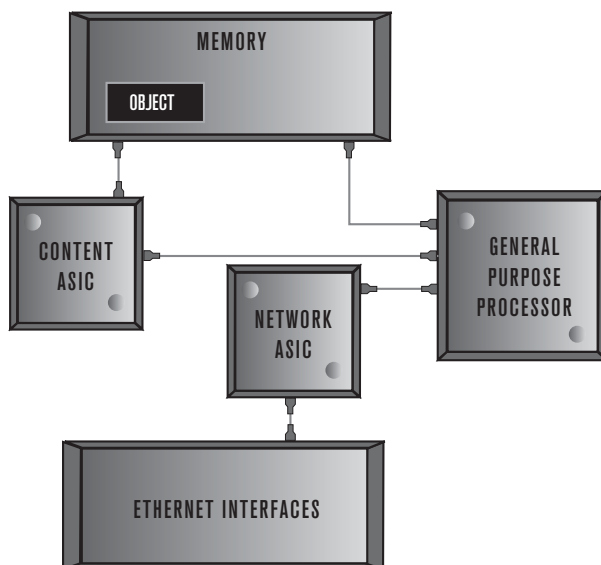


Figure 5: High-Level Architecture of a UTM System with an onboard Network Processor and Content Processor

Advanced network processors which have embedded security functions have been able to perform firewall security at line rate, processing traffic at gigabit speeds using any packet size with very low network latency. The processors can produce similar results with IPSec VPN traffic. These levels of performance are critical as networks are upgraded to take advantage of increasingly faster local area and wide area network standards, such as 10-Gigabit Ethernet and beyond.

Specialized Software

As discussed earlier, completely integrating performance-enhancing hardware with security software requires specialized programming. This typically requires the ability to modify the source code, an uncommon reality with most multi-vendor UTM products. The lack of integration in this type of design typically requires that every task run on the Central Processing Unit (CPU), eliminating the possibility of multi-processor distributed computing. Even if portions could be accelerated with hardware, it's unlikely that a third-party security vendor will modify their software to benefit the UTM manufacturer. To make matters worse, the combination of multiple technologies means that there is a high probability that redundant operations related to packet or flow processing are also occurring, further impeding performance.

Single-vendor solutions can depend on a reliable "order of events" to always occur and thus are able to prevent this type of redundant, inefficient processing. For example, if the firewall function maintains the state of connections, there is no need to repeat this state maintenance within the IPS function. More importantly, however, is that single-vendor solutions can take advantage of specialized hardware in the system. By offloading intensive content inspection tasks to co-processing hardware, the general purpose processor can scale in performance more efficiently, allowing more security functions to co-exist on a single system.

Evolving Security Content

If there is only one constant in network security, it is that threats to networked assets are constantly evolving. In order to keep up, a diverse pool of threat intelligence must be developed and maintained. And when building a highly integrated UTM solution, it is beneficial to be the guardian of the resulting security content that is incorporated onto the system. By being the sole director of security content, common "overlap" can be avoided between technologies; ensuring that the best tool in the UTM portfolio is enabled to mitigate threats as early as possible in the threat's life cycle. Performance can also be an additional benefit, as the security research and development team has intimate knowledge of the hardware's capabilities. Often the team will write the security content in a manner that makes the most efficient use of the system resources, leveraging hardware acceleration whenever possible. A security benefit of in-house security research is that researchers can collaborate across security disciplines, deciding where the earliest point of threat mitigation is possible. All of these points ultimately translate to increased security effectiveness in a single vendor, hardware accelerated UTM solution.

Summary

As demonstrated in this white paper, as performance demands continue to increase, UTM devices must become increasingly specialized hardware appliances. As other devices such as routers and firewalls have evolved into specialized hardware devices, UTM solutions have evolved along a similar path and high-performance enterprise UTM devices today should employ hardware acceleration to expedite the content inspection process. In fact, hardware acceleration is now a requirement for maintaining continuity and removing security as the network bottleneck. Single-vendor UTM solutions employing ASIC-based processing hardware are now able to accommodate high-speed networks, such as internal network segments, and are able to secure and process traffic as close to line rate as possible. Finally, in order to achieve the most benefit and offer the highest levels of security effectiveness and efficiency, complete integration of specialized hardware with the software and security content is required. The result of the complete integration of specialized hardware, fully integrated software, and original security content is a solution that *truly* unifies threat management while providing the highest levels of performance and protection possible.

References

Metz, C. (1998). IP Routers: New Tool for Gigabit Networking. *IEEE Internet Computing*, 2(6), 14-18.

IEEE (1997). Firewalls: An Expert Roundtable. *IEEE Software*, 14(5), 60-66.

Gleeson, B., Lin, A., Heinanen, J., Armitage, G., Malis, A. (2000). A Framework for IP Based Virtual Private Networks. Networking Working Group. Retrieved April 23, 2008, from <http://www.ietf.org/rfc/rfc2764.txt>

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management security systems, which are used by enterprises and service providers worldwide to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection, including: firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispam — designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office solutions to high-performance chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in seven programs by ICSA Labs (Firewall, Antivirus, IPSec, SSL, Network IPS, Antispyware and Antispam). Fortinet is privately held and based in Sunnyvale, California.

FORTINET

1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com

©2008 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, FortiReporter and the "Forti" family of marks are trademarks or registered trademarks of the Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600. Although Fortinet has attempted to provide accurate information in these materials, Fortinet assumes no legal responsibility for the accuracy or completeness of the information. Please note that no Fortinet statements herein constitute or contain any guarantee, warranty or legally binding representation. All materials contained in this publication are subject to change without notice, and Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

WPR138-0608-R1