

Accelerating UTM with Specialized Hardware

Summary

Tighter security requirements and ever-faster enterprise networks are placing extraordinary demands on UTM platforms. Resource-hungry security functions such as content-based inspection can slow system performance and decrease throughput, resulting in high network latency and traffic bottlenecks. Developers of multi-vendor UTM platforms have struggled to keep pace in today's network environments as difficulties associated with the licensing and integration of disparate technologies have slowed innovation. Alternatively, developers of single-vendor UTM platforms have designed hardware-accelerated platforms which leverage specialized ASICs to offload and process demanding security tasks. This white paper provides a brief overview of the evolution of UTM platforms and explains why corporate IT departments are deploying specialized hardware to keep pace with new security threats and ever-faster enterprise networks.

Introduction.....	3
The Evolution of Networking Technologies.....	3
Routers and Firewalls.....	3
The Evolution of UTM Platforms.....	4
Building a High-Performance UTM Solution.....	5
Specialized Hardware.....	5
<i>Content Processors</i>	5
<i>Network Processors</i>	6
<i>System-on-a-chip Processors</i>	8
Specialized Software.....	8
Evolving Security Content.....	8
Conclusion.....	9
About Fortinet.....	9
About FortiOS.....	9

Introduction

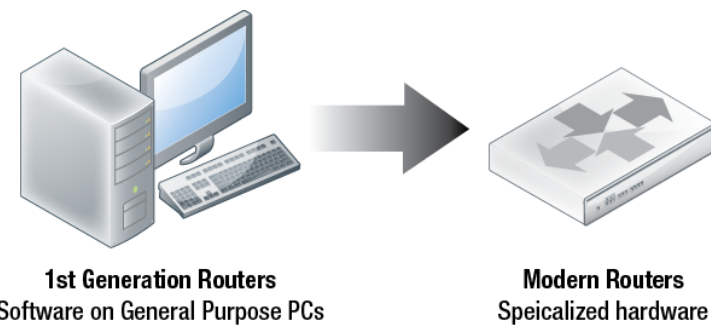
First generation unified threat management (UTM) devices suffered from performance limitations due to the fact that they were implemented on platforms not specifically designed for security purposes. The resulting network bottlenecks forced security administrators to make compromises between network security and network performance. Understandably, these tradeoffs made some enterprises reluctant to explore the benefits of migrating security functionality to UTM platforms.

Today's advanced circuit designs and processor technologies have resolved performance concerns. Application specific integrated circuits (ASICs) and system-on-a-chip (SoC) processors have been incorporated into hardware designs to accelerate demanding security functions. Hardware-accelerated UTM platforms are delivering the benefits of consolidated network security to enterprises of all sizes, including small/branch offices, global corporations, large data centers and global telecommunications carriers. This white paper provides a brief overview of the evolution of UTM platforms and explains why corporate IT departments are now deploying a new generation of very high performance, very low latency UTM platforms built with specialized hardware.

The Evolution of Networking Technologies

Routers and Firewalls

Before exploring the evolution of UTM technology and its specialized hardware, it is helpful to review the development of other networking technologies. In particular, it is important to understand how specialized hardware has fuelled the adoption of modern networking technology. Network routers, initially called gateways, were typically general purpose computers running network routing software. Routers receive and identify data packets, then forward them to their next destination on the network. This technology is essential for many network designs, but historically created a bottleneck in the flow of data between applications. Today, network routers have evolved into highly specialized devices, relying on customized



processors and ASICs 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 primarily by performance requirements¹. After the resolution of the bottleneck problem, a wide range of customers adopted routers to solve a broad range of problems.

Firewalls evolved in a similar fashion, but required an extra step. At its inception, firewall technology was little more than a network router with some packet filtering capability. As it evolved, the technology matured from

Figure 1: Evolution of Routers to Specialized Hardware

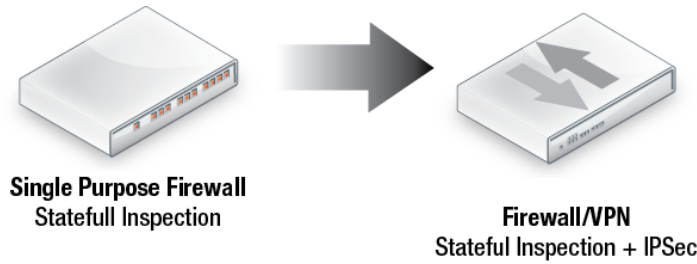
basic packet filtering into more intelligent stateful packet inspection, and finally into full application layer inspection devices². Firewalls, like network routers, were implemented initially as software running on general purpose computers, later requiring specialized hardware platforms as network speeds increased and more security functions were added in response to new threats.

By the year 2000, new networking technology known as virtual private networks, or VPNs, were enjoying increased acceptance³. VPNs enable the creation of a secure connection between separate networks over the Internet. The integration of firewalls and VPNs was a natural fit, as enterprises typically deployed both technologies at the network perimeter. Inevitably, cheaper high-speed Internet access, growth in the number of remote users and increased processing demands created a new bottleneck at the network perimeter. The need for additional throughput acceleration using specialized hardware again became apparent.

¹ Metz, C. (1998). IP Routers: New Tool for Gigabit Networking. IEEE Internet Computing, 2(6), 14-18.

² IEEE (1997). Firewalls: An Expert Roundtable. IEEE Software, 14(5), 60-66.

³ 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>



First with network routers and then with firewall/VPN appliances, history has demonstrated that specialized hardware platforms have become a necessary milestone in the cycle of evolution for network devices. Therefore it should come as no surprise that UTM appliances have evolved along a similar path.

Figure 2: Evolution of Firewall Technology with Integrated VPN Capabilities

The Evolution of UTM Platforms

UTM platforms expand on traditional firewalls to incorporate additional complementary security technologies. Market research and analysis firm International Data Corporation (IDC) defines UTM platforms as including a firewall, VPN technology, intrusion prevention and antivirus security features. Security vendors have generally taken two different approaches to developing UTM platforms:

- 1) License or acquire missing technologies from third parties to complete their UTM platform.
- 2) Build the required UTM technology in-house.

As illustrated in Figure 3 on the following page, many initial UTM designs were based on the first approach with third-party technology clustered around a core competency. For example, some vendors were experts in firewall technology, while others specialized in developing intrusion prevention systems. These “multi-vendor” developers added new security features to their UTM platforms by partnering with other best-of-breed technology providers. This approach enabled fast, low-cost platform design. Unfortunately, customers were forced to use separate management interfaces for each non-native security technology. In an effort to paper over some of the gaps between the different technologies, some multi-vendor developers offered “unified” management interfaces.

Vendors following the second design approach of building all technologies in-house were able to develop uniform security architectures from the ground up, seamlessly integrating the required technologies to provide all required security functions natively from the UTM platform. Similarly, since all security technologies were integrated from design inception, the management interface was also unified. The major drawback of the single-vendor approach was the R&D investment required to develop all of the security technologies in-house, and bring innovative technology to market across the spectrum of UTM services. Single-vendor platforms had a high bar to reach as each native security function had to meet the standards previously established by best-of-breed standalone security products.

As first generation UTM platforms arrived on the market, IT professionals identified performance as their Achilles' heel. As additional security functions were added and network speeds increased, the performance of UTM devices decreased to unacceptable levels. Multi-vendor developers who had built UTM platforms through best-of-breed partnerships soon realized that restrictions limiting access to third-party source code also restricted their ability to efficiently scale their solutions to meet new performance demands. Meanwhile, designers at single-vendor UTM developers were able to modify their source code and optimize their platforms quickly to address performance issues and new security threats.

For example, the elimination of redundant processing associated with the disassembly and re-assembly of network traffic allowed single-vendor UTM platforms to realize significant gains in throughput. The most significant performance contribution, however, was achieved through hardware acceleration of the inspection process itself. As done earlier with routers and firewalls, customized ASICs were developed to target and accelerate the most demanding security functions. Single-vendor hardware engineers soon discovered that their UTM platforms could realize exponential gains in performance, simply by adding ASICs to their designs and extending hardware optimization to the application layer of the Open Systems Interconnection (OSI) Reference Model.

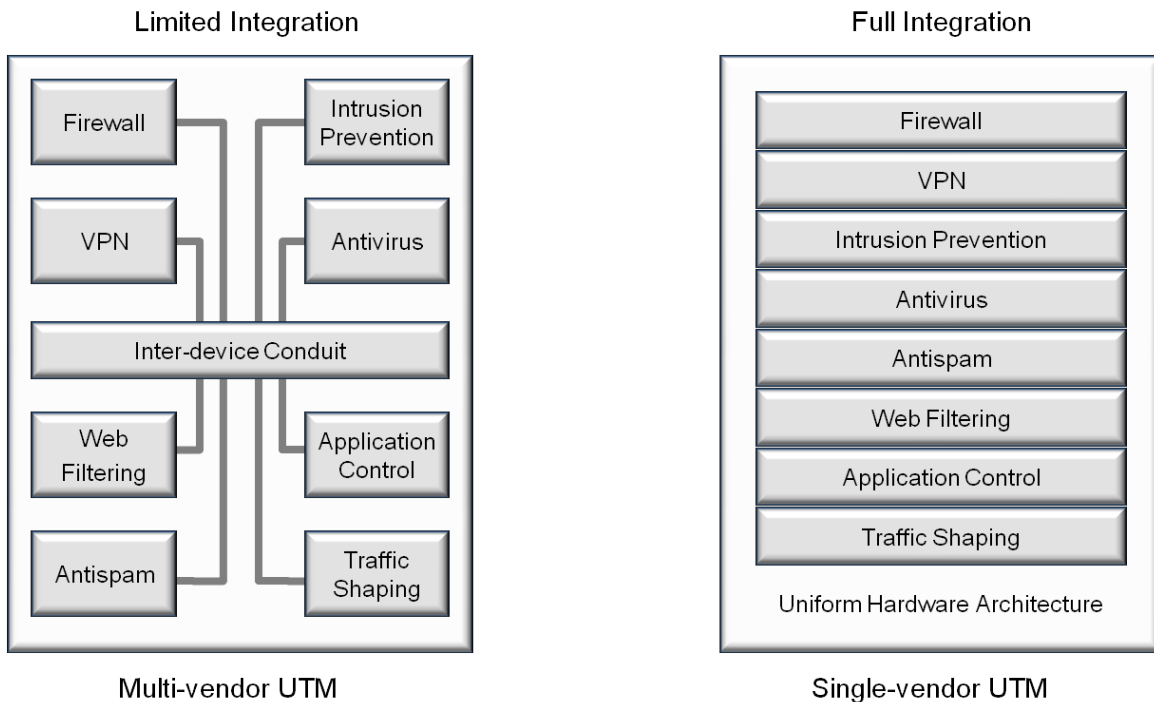


Figure 3: Different Approaches used in Developing UTM Architectures

As new threats forced vendors to add security functions such as antispam and web filtering to their UTM platforms, performance limitations again came to the fore. Unable to take full advantage of hardware acceleration, vendors selling multi-party UTM solutions were reluctant to add more features to their already resource-starved platforms. Again, vendors who had developed their UTM platforms in-house quickly optimized their solutions through software changes and hardware acceleration. Today, single-vendor UTM solutions are being deployed into the largest and fastest networks around the world, delivering both the high performance and best-of-breed protection required by the world's most successful companies.

Building a High-Performance UTM Solution

A high-performance UTM solution has three major components: specialized hardware, specialized software and evolving security functionality. Through intelligent integration, each component contributes to the security, performance, stability and scalability provided by the resulting UTM platform. In this section we provide a brief overview of the design approach used by Fortinet®, the leading provider of UTM solutions.

Specialized Hardware

Three major types of specialized ASICs contribute to the performance and scalability of Fortinet UTM systems; Content Processors, Network Processors and Security Processors. These specialized FortiASIC™ chips work in unison with a general purpose central processing unit (CPU); similar to the way the human brain works with the spinal and peripheral nervous system to accomplish tasks.

Content Processors

FortiASIC Content Processors are purpose-built to perform high-speed, on-the-fly comparisons between suspect objects, such as network packets or compressed files, and known threat patterns held in memory. Content Processors are optimized for protocol recognition and parsing, enabling quick assembly of data streams for security inspection. As shown in Figure 4, Content Processors do not receive traffic directly from the network and only examine suspect objects when so instructed by the general purpose CPU.

Content Processors accelerate tasks requiring comparison of objects to known threats, especially antivirus, intrusion prevention and other application-level security functions. Many people have the misconception that ASIC technology implements static security that cannot adapt to new threats. But FortiASIC Content Processors only implement scanning logic in hardware and are not used to store threat pattern data, which is stored in memory. Therefore, applying a threat update to a single-vendor hardware-accelerated solution is just as fast and simple as applying a threat update to a software-only multi-vendor solution running on a generic hardware platform.

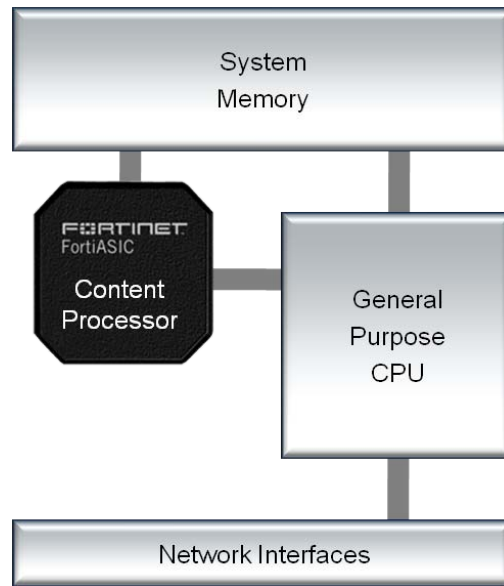


Figure 4: High-Level Architecture of a UTM System with an onboard Content Processor

Moreover, FortiASIC Content Processors include cryptographic engines that can offload repetitive calculations from the general purpose CPU, such as the encryption/decryption processing required for VPN communications. Additional resource-intensive tasks, such as VPN connection setup and key maintenance can also be offloaded, making Content Processors an ideal multi-purpose solution for hardware acceleration.

Network Processors

FortiASIC Network Processors are optimized to process network traffic flows at high-speed. They reduce the load on other system components by taking on many of the packet-based communications maintenance tasks such as general TCP processing, network address translation and some encryption/decryption tasks. Network Processors defragment packets very quickly for inspection and can take immediate action to modify traffic flows. These advanced processors improve security by accelerating the reassembly of fragmented packets which occur naturally on networks. Fragmented packets can be exploited by attackers to evade legacy security systems.

Network Processors can also be programmed with firewall and IPS policies to filter traffic, detect protocol anomalies and expedite delivery of latency-sensitive traffic at the interface level. Since they perform most of their functions automatically, they can receive traffic directly from the network and are typically placed in-line between a general purpose CPU and the network ports. Figure 5 illustrates how Network Processors offload traffic from the interface. Network Processors enable Fortinet appliances to deliver switch-like low latency and support millions of connections per second, regardless of packet size.

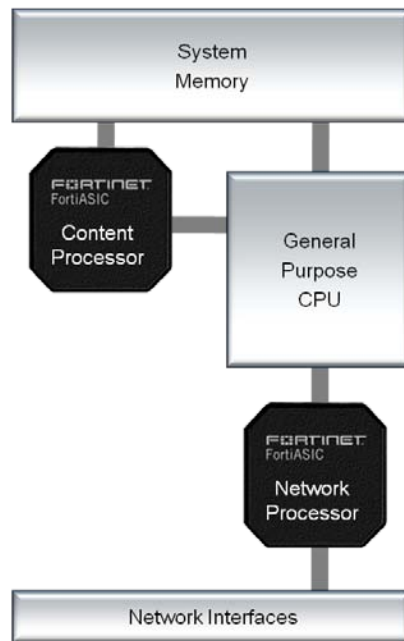


Figure 5: High-Level Architecture of a UTM System with Content and Network Processors

Security Processors

FortiASIC Security Processors accelerate flow-based inspection technologies including antivirus, application control, intrusion prevention and data loss prevention. They can be placed at the network interface area or at the system level in the UTM architecture. In situations where traffic bypasses other parts of the UTM system, the Security Processor can download session processing instructions from the CPU and process entire packets autonomously. The Security Processor returns only state information to the CPU, freeing CPU cycles for other tasks. This co-processing arrangement can deliver dramatic improvements in system performance. Figure 6 shows how Security Processors can be placed in the UTM system architecture to focus on different tasks.

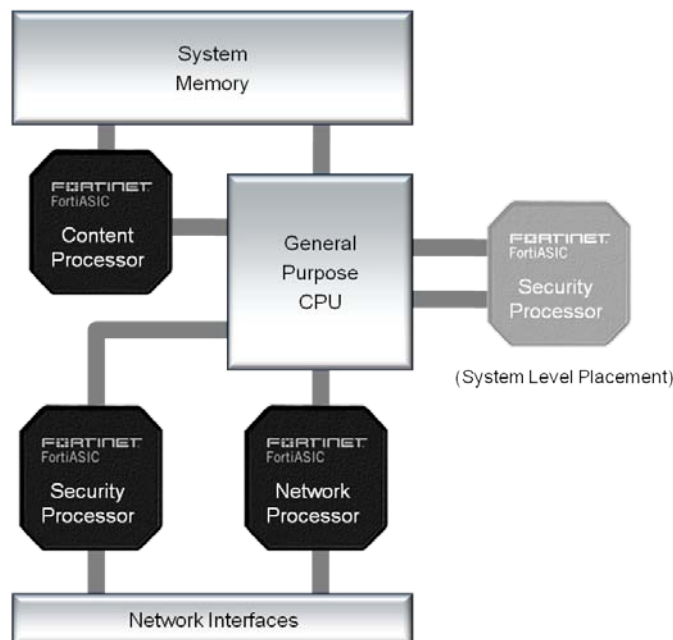


Figure 6: High-Level Architecture of a UTM System with Content, Network and Security Processors

FortiASIC designs and technology have improved at a rapid pace, enabling very low latency processing of packets of any size. Fortinet UTM appliances can now deliver network firewall security at near line-rate gigabit speeds. In addition, FortiASICs have been shown to dramatically increase IPSec VPN traffic flows. These performance breakthroughs are proving critical as IT managers upgrade their networks to take advantage of new 10-Gigabit and even 100-Gigabit Ethernet standards.

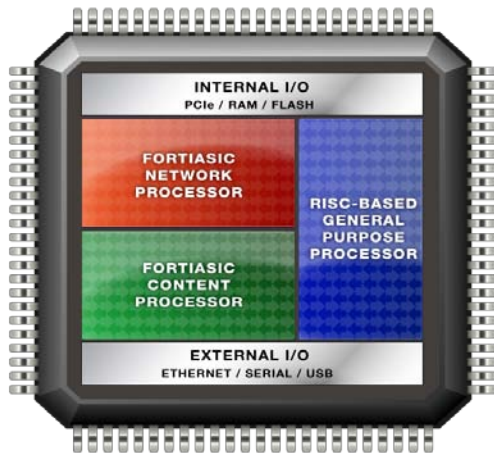


Figure 7: FortiASIC System-on-a-chip Processor

System-on-a-chip Processors

For additional simplification and consolidation of processing power, Fortinet created a system-on-a-chip (SoC) processor that combines specialized ASIC processors and general purpose CPUs on a single chip. The FortiASIC-SoC was designed for use in the FortiGate UTM platform.

As shown in Figure 7, the FortiASIC-SoC integrates a FortiASIC Network Processor, a FortiASIC Content Processor, a general purpose CPU, on-board memory, and some input/output functionality. Frequently, IT departments do not have the budgets available to deploy full UTM security capabilities at small branch offices. The FortiASIC SoC is an important development because it enables deployment of enterprise-class network security in environments where it was not previously economical.

Specialized Software

As discussed earlier, the proper integration of performance-enhancing hardware and security software requires specialized programming. Restricted by licensing agreements, manufacturers of multi-vendor UTM products are typically forced to run all security-related tasks on a general purpose CPU, entirely bypassing the benefits associated with multi-processor distributed computing. Even if portions of security functions could be accelerated with hardware, it's unlikely that a third-party security vendor will modify their software to benefit the UTM vendor. To make matters worse, the resulting combination of multiple technologies increases the probability of redundant packet and flow processing, further slowing UTM system performance.

Alternatively, single-vendor solutions enjoy a reliable "order of events" which allows planning ahead to avoid redundant or inefficient processing of packet flows. For example, if the firewall function is able to store and retrieve the state of all connections, there is no need to repeat this state maintenance within the IPS function. Most importantly, software developed for single-vendor UTM solutions can leverage specialized hardware to offload demanding security tasks. This allows more efficient scaling of the UTM platform and permits more security functions to co-exist.

Fortinet developed its security-hardened FortiOS™ operating system to take full advantage of the hardware acceleration capabilities provided by the FortiASIC line of custom processors. This purpose-built operating system enables FortiGate consolidated security appliances to deliver maximum performance and protection for high-speed networks, while delivering the most comprehensive suite of IPv6-ready security and networking services available within a single device.

Evolving Security Content

If there is one constant in network security, it is the relentless evolution of security threats. In order to keep pace, security vendors must be able to develop and maintain a diverse pool of threat intelligence. When building a tightly integrated UTM solution, it is beneficial to be the guardian of the resulting security content that is incorporated into the system. Manufacturers of single-vendor UTM solutions can design their systems to avoid processing "overlap", ensuring the fastest throughput and most efficient threat mitigation. Performance benefits realised with specialized hardware can be substantial, as compute-intensive tasks can be handled by custom-built ASICs and SoCs. In addition, when security technologies are developed in-house, threat researchers can collaborate across disciplines delivering the most efficient threat identification and mitigation. Developing UTM solutions in a single-vendor environment can result in platforms that deliver superior network performance and security effectiveness.

Conclusion

As demands on the performance of security solutions have increased along with network speeds, UTM platforms have evolved into highly specialized hardware appliances. Their evolution has followed a path similar to other networking devices such as network routers and firewalls. Hardware acceleration of security functionality is now required to maintain network throughput and traffic integrity. Single-vendor UTM solutions employing ASIC-based processing hardware can now process traffic at near line-rate network speeds, satisfying the ever-higher performance demands made by today's high-speed networks. Finally, in order to achieve the maximum benefit and offer the highest levels of security effectiveness and efficiency, intelligent integration of specialized hardware with software and security content is required. Single-vendor UTM solutions deliver truly consolidated threat management, while providing the highest levels of security and performance possible for today's enterprises and service providers. The days of trading performance for security are now a thing of the past.

About Fortinet

Fortinet delivers unified threat management and specialized security solutions that block today's sophisticated threats. Our consolidated architecture enables our customers to deploy fully integrated security technologies in a single device, delivering increased performance, improved protection, and reduced costs. Purpose-built hardware and software provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. Our customers rely on Fortinet to protect their constantly evolving networks in every industry and region in the world. They deploy a robust defense-in-depth strategy that improves their security posture, simplifies their security infrastructure, and reduces their overall cost of ownership. For additional information, please visit Fortinet at: <http://www.fortinet.com>.

About FortiOS

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of FortiGate multi-threat security platforms. FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC™ content and network processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS helps you stop the latest, most sophisticated, and dynamic threats facing your network today with expert threat intelligence delivered via FortiGuard® Security Subscription Services.

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with return and replace hardware support or 24x7 Comprehensive Support with advanced hardware replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and a 90-day limited software warranty.

FORTINET

GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE

Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated
300 Beach Road #20-01
The Concourse, Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015



Copyright © 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.