



Real-Time Network Security Systems Run In-Line

AdvancedTCA®-based platform harnesses Portwell* and Intel® for faster time-to-market, lower development costs and optimum performance

Summary

The modular approach to system development is rapidly gaining acceptance in the highly competitive telecom industry. It enables developers, platform providers (also known as ODMs) and OEMs to build systems on a common architecture, saving development time and resources by leveraging the design work of others.

Fortinet* recently employed the modular approach to build three new real-time network security systems for Internet Service Providers (ISPs) and telecommunications companies (telcos). Fortinet's solutions follow the new AdvancedTCA (ATCA™) specification to deliver the performance required by the telecom segment along with the modular design strategy that speeds development.

With Fortinet's award-winning experience in the security segment, company engineers were able to employ a modular platform strategy—by using the ATCA specification along with the design expertise of Portwell, Intel and others—to deliver three new products quickly and efficiently. As a result, the FortiGate*-5020, FortiGate*-5050, and FortiGate*-5140 antivirus firewalls are believed to be the first ATCA-based, in-line security systems to reach the marketplace.

This case study looks more closely at Fortinet's success and the pivotal roles played by Portwell* and Intel in the delivery of their new high-performance, in-line security system.

Moving Network Security in Line

Traditional network security solutions based on stateful inspection firewalls leave networks vulnerable to content-based attacks—like viruses, worms, spyware and spam—that travel through email and Web protocols. Recent virus outbreaks demonstrate that security solutions must continually adapt to changing threats. ISPs and telcos urgently need to deliver advanced security services to their Internet and email customers to protect them from the increasing number and complexity of content-based attacks.

While a number of security solutions are available for deployment at the enterprise edge, few can scale to handle the performance requirements of ISPs, telcos, etc. or the core networks of the largest enterprises. In particular, solutions based on standard computing architectures are inadequate to handle significant amounts of traffic with the kind of content analysis required to detect viruses, worms and other complex attacks.

According to Fortinet, today's content-based attacks must be addressed deeper inside the network via security systems that sit in-line at the core, screening all traffic. Such systems require very high, carrier-grade performance so they can effectively protect the network without degrading performance. Ideally, in-line security systems are easily adaptable to changing conditions.

Fortinet recognized the need for scalable, flexible security solutions that can sit inside the network core. So with expertise in Internet security gateways for enterprise environments, Fortinet planned to extend their award-winning product line to telecommunications carriers. The challenge lay in the engineering: how to quickly and cost-effectively deliver a carrier-grade system with built-in scalability and upgradeability to handle ever-increasing bandwidth requirements?

Strategic Design Decisions

Extending their successful design to meet the needs of carriers required all-new engineering. Fortinet's unique software, the custom-built ASIC that accelerated the security services, the backplane chassis and system boards—everything needed additional development engineering. What's more, Fortinet's target customers showed interest in solutions based on the new ATCA specification because of the flexibility enabled by the modular approach.

Fortinet understood that success depended on finding ways to focus the bulk of its development effort on those aspects of the system that were most unique and differentiated. To that end, company engineers made several important design decisions that enabled them to deliver their advanced in-line security system well ahead of other vendor solutions:

- Adopt the modular platform approach to system development
- Utilize the standardized platform architecture of the carrier-grade AdvancedTCA specification (See related sidebar: "The Promise of ATCA")
- Tap into the design expertise of third party ODMs (Portwell and others) for providing board-level design
- Focus company resources on the development of the advanced security-accelerating ASIC and the security software that provide unique value to customers
- Rely on standards-based components to ensure ease of development, easy integration, and interoperability

Three "Firsts"

Fortinet's design decisions significantly reduced the amount of development work required for the company's new carrier-grade security systems. In fact, these strategies enabled Fortinet to deliver one of the telecom industry's first ATCA™-based security solutions—not just one, but three of them.

The FortiGate-5020, FortiGate-5050, and FortiGate-5140 systems are designed for deployment in both the network edge and core to screen traffic in real-time. Offering carrier-grade performance in combination with Fortinet's security expertise, the new integrated security platforms offer maximum protection against the content-based attacks that are most common today. In fact, Fortinet's three new ATCA-based systems are the only available solutions that can

The Promise of ATCA™

The ATCA specification for carrier-grade telecom systems delivers high availability, high performance, lower costs and faster time-to-market. It provides a standardized platform architecture that can be used to deliver any number of services—including security—allowing for optimum scalability and versatility over time. The telecom industry has embraced this new specification wholeheartedly, especially for the flexibility enabled by the platform's modular approach.

ATCA addresses the performance needs of next-generation communications equipment. The architecture is optimized around connectivity requirements of signaling and media gateways, while also providing headroom for higher performance computing elements. The scalable backplane of the ATCA specification supports a variety of standard and proprietary interfaces, robust system management, and superior power and cooling capabilities.

Such robust performance in a standardized platform offers tremendous versatility for telecom solutions. Developers all start with the same basic architecture and a head-start in application design. Despite the complexity of new communications solutions, ATCA simplifies the development process significantly. The standardized platform design of ATCA allows developers to focus resources on their unique hardware and software by leveraging a common, carrier-grade approach to providing basic system infrastructure such as backplanes, power, boards, and cooling.

detect and eliminate viruses, worms and other content-based threats without reducing network performance—even for real-time applications like Web browsing.

In building these products, Fortinet called upon the design expertise of Portwell, Intel and others, as well as its own highly experienced team of engineers. Fortinet wrote the award-winning FortiOS* software, and is also the developer of the overall antivirus firewall system. Fortinet also built the custom FortiASIC* Content Processor chip that provides acceleration for the advanced security functions (antivirus, IDP, VPN, and firewall). Portwell worked with Fortinet to incorporate the FortiASIC chip into to the design of the ATCA-based system board known as the FortiGate*-5001.

Why Portwell?

Fortinet tapped the ODM design expertise of Portwell for development of the system board. “The ODM model makes good economic sense,” explains Richard Hanke, Fortinet’s vice president of product management. “We can leverage the expertise and skill of the industry’s top specialty design engineers to speed our time-to-market and focus our efforts on what makes our product different from the competition.”

By using Portwell, Fortinet engineers had more time to spend on the development of the custom ASIC and the security software that make the new antivirus firewalls unique. With several years building solutions in the security segment for Intel and leading OEMs, Portwell had the right level of expertise necessary to deliver the final board quickly and easily.

What’s more, Portwell’s membership in the Intel® Communications Alliance gave them an advantage in working with the new ATCA specification. “We had direct access to many of the engineers inside Intel who helped develop the specification. They gave us design tips and helped us understand the nuances of the design, which really made a difference in our ability to produce the first ATCA-based security board for Fortinet,” explains Kin Tse Hong, VP of Engineering for Portwell.

Why Intel?

Both Fortinet and Portwell engineers specified Intel components for the system board. Intel’s standards-based, high-performance processing helped simplify design efforts and ensured compatibility with the ATCA platform. Because Intel processing components are compatible with multiple stan-

dard interfaces, it is quite simple to design and port them to the Fortinet solution.

In the three new Fortinet FortiGate antivirus firewalls, the Portwell-developed board incorporated two low-voltage Intel® Xeon™ processors, the Intel® E7501 chipset, and the Intel® 82546EB Dual Port Gigabit Ethernet Controller. This combination of components achieves the greatest overall level of performance.

Fortinet currently has a total of 13 platforms in production. Using Intel components, Fortinet can develop a single instruction set that works across all platforms, minimizing individual development on each of those systems.

The Intel Communications Alliance is another reason Portwell and Fortinet favor Intel. Members of the Alliance gain early access to Intel’s product designs so that new product development work can be done in parallel. What’s more, the Alliance provides members with access to expertise within the ecosystem, allowing them to work together to solve unique industry challenges more quickly and efficiently than they would be able to do separately.

Feature-Rich, Real-Time Security for ISPs and Telcos

The FortiGate*-5000 Series of antivirus firewalls offer unprecedented security, performance, scalability, and reliability that meet the stringent demands of large enterprises, carriers and MSPs, including Managed Security Service Providers (MSSPs). Deployable at the network core and edge, these chassis-based systems consist of three models—the FortiGate-5020 (two slot), the FortiGate-5050 (five slot), and the FortiGate-5140 (14 slot).

Each FortiGate-5000 blade can deliver 4 Gbps of performance—enabling the delivery of 50 GB of performance on a single 14-blade, FortiGate-5140 system. Each system has four gigabit Small Form-Factor pluggable (SFP) ports and four tri-speed gigabit Ethernet ports. FortiGate-5000 systems can be deployed in multi-chassis configurations with the ability to maintain full operation even with multiple power supply, fan, blade, and link failures. For service providers, MSSPs and large enterprises, the FortiGate-5000 has virtual domains and can create up to 250 antivirus firewalls from a single FortiGate blade.

“The ATCA chassis standard gives us the versatility to scale our solution to meet the needs of ISPs and telcos quickly and efficiently. Once the development work was done on the 2-slot version, we didn’t need to do much additional development to bring out the 5-slot and 14-slot versions,” continues Hanke. “By using the standardized ATCA chassis and back-plane design, we saved about half the usual development time and also reduced our development costs.”

The Benefits

When Fortinet’s three new service provider antivirus firewalls began shipping, they were believed to be the first ATCA-based security products available to both the enterprise and service provider segments. Fortinet’s quick time-to-market—in half the usual development time—can be traced to a combination of sound strategic decisions:

- Adopting the modular platform approach to product development
- Use of design expertise by third parties like Portwell for the basic, modular boards and components

For More Information:

Fortinet*
www.fortinet.com

Portwell*
www.portwell.com.tw

Intel® Xeon™ Processors
<http://developer.intel.com/design/xeon>

Intel® E7501 Chipset
<http://developer.intel.com/design/chipsets/E7501>

Intel® 82546EB Dual Port Dual Port Gigabit Ethernet Controller
<http://www.intel.com/design/network/products/lan/controllers/82546EB.htm>

- Choosing high-performance, standards-based ingredients, like the ATCA specification and Intel processors

Portwell believes all of its OEM customers will see a significant overall cost reduction by adopting the modular strategy. “Standards-based architecture cuts a lot of time and effort from the design of new solutions,” explains Kin Tse Hong. “Our proven quality and performance, along with standards-based products from Portwell and Intel, can help our OEM customers enter new markets quite easily. Fortinet’s success is a case in point.”

Conclusion

Fortinet wisely chose the modular strategy to deliver its new firewall and credits the expertise of its development partners for helping to meet its aggressive time-to-market goals. “Working with partners to develop our FortiGate-5000 series has been a win-win situation,” says Hanke. “It makes a lot of sense for industry experts to collaborate on new solutions for the benefit of the customer.”



A community of communications and embedded developers and solution providers

Find out more about a business solution that is right for your company by contacting your Intel representative, or visit the Intel® Business/Enterprise Web site at intel.com/business or its industry solutions specific sites at intel.com/business/bss/industry/.



Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life-sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.

Information regarding third party products is provided solely for educational purposes. Intel is not responsible for the performance or support of third party products and does not make any representations or warranties whatsoever regarding quality, reliability, functionality, or compatibility of these devices or products.

Copyright © 2004 Intel Corporation. All rights reserved. ATCA is a trademark of the PCI Industrial Computers Manufacturers Group.

Intel, the Intel logo, and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others. 1004/QUA/ET/PDF



302031-001US