Unified Threat Management (UTM) Security Appliances

Omar Cruz, Donald Shin

Introduction

Today's business networks are under attack, invaded by hackers and competitors attempting to cause mayhem and gain access to private information. Network security threats are real and growing. With an estimated $40 billion (USD)* of data loss per year, service providers and end users are becoming painfully aware of the consequences of unsecured networks and databases.\(^1\) Over the last several years, networking equipment OEMs have had to reverse the traditional debate on platform security features. Rather than debating which systems require security, the discussion has changed: What type of security features does this system need, and how do I implement them as effectively and efficiently as possible?

The technology required to defend against these attacks is increasing in complexity and evolving at a rapid rate. End-point software patches alone do not deploy quickly enough through the enterprise to forestall the most serious attempts to do damage, therefore network antivirus software is used to counter serious threats quickly. Most enterprises deploy security devices behind legacy routers to detect and stop malicious traffic before it reaches servers and desktops. Some of the most common network security devices include:

- Firewall/virtual private network (VPN) appliance—a combination of firewall and IPsec-based VPN gateway
- Intrusion detection and prevention systems (IDS/IPS)
- Content filter for viruses and spam
- Potpourri of software stacks and products, making maintenance difficult
- Unified threat management (UTM) or integrated services router (ISR)

Determining which solutions will best serve the needs of the enterprise requires a close examination of how today's numerous solutions will be integrated in the future.

Effectiveness, cost, ease of implementation and a variety of other considerations must be factored into the equation, along with the need to get integrated products to market quickly.

Challenges Faced by Network Equipment Vendors

Some of the key challenges that network equipment vendors face while designing a security appliance are:

- Complex networks need comprehensive security solutions: Threats are rising, so the need for a UTM solution—including firewall, IPS, Anti-X and secure VPN and fine-grained access control to prevent attacks, ensure data confidentiality, prevent viruses and stop spam—is essential.
- Due to ever-increasing complexity and performance and security needs, network equipment vendors need multicore (two to eight cores) processors with performance ranging from 1 to 2 GHz to meet enormous computing demands.
- Complex multicore silicon needs highly optimized and tuned software solutions in short time frames for faster time to market.

Key Benefits of Using Power Architecture® in Security Appliances

Freescale's Power Architecture based UTM appliance solution has been adopted by leading original design manufacturers (ODMs) who offer commercial off-the-shelf appliances. Freescale's hardware and ODM partner ecosystem is intended to deliver extended support to Freescale's customers in hardware engineering, turnkey manufacturing and fulfillment and pre-built hardware manufacturing, among other services and products. Off-the-shelf UTM appliances from major ODMs are FCC, UL and CE certified and ready to ship, enabling customers to focus on differentiated value-added services and leveraging the performance offered by multicore processors. Freescale's solution provides customers with access to low-power, high-performance multicore processors that deliver improved margins with minimal integration and developments costs.

Accelerate Time to Revenue

Decrease time to market with fully integrated security and networking functionality that allows you to simply develop with no impact to schedule. Accelerate time to revenue by reaching new markets faster.

Bend the Cost/Performance Curve

Achieve multiple performance enhancements by leveraging Freescale's solutions-centric approach at price.

---

levels similar to current-generation appliances. With the help of its ecosystem partners, Freescale can provide customized solutions to suit the needs of individual customers.

Create an Extensive UTM Appliance Roadmap

Freescale’s Power Architecture processors running VortiQa software showcase scalable performance at industry-leading performance-to-power ratios. Freescale provides a broad range of scalable UTM platforms from cost-effective to high-performance systems. Uniform architecture simplifies software development costs and meets both low- and high-end solution requirements to help fill out a whole customer portfolio (Figure 1).

One example is the cost-effective P2041 processor (Figure 2) that brings advanced levels of multicore performance to SMB network security applications. The P2041 processor integrates a quad-core processor with hypervisor privilege mode for new value-added services that can be realized with virtualization.

The P2041 processor also integrates hardware acceleration for data path packet processing with Freescale’s Data Path Acceleration Architecture (DPAA), which includes:
- Queue and buffer management (BMAN, QMAN)
- Packet classification (FMAN)
- Crypto engine (SEC)
- Deep packet inspection through pattern matching engine (PME)
- 10 Gb networking

Freescale Power Architecture Solutions for Security Appliances

Freescale and its ecosystem partners have teamed up to provide comprehensive solutions to the UTM security appliance market. The IDC definition of UTM appliance includes firewall, IPsec, VPN, intrusion prevention system (IPS) and gateway antivirus functions. Going forward, more applications are being added to UTM appliances such as SSL, VPN and VoIP security.
Table 1: UTM Security Appliance Solutions—Portfolio

<table>
<thead>
<tr>
<th>ODM UTM Appliance</th>
<th>ODM</th>
<th>Freescale Processor</th>
<th>Cores</th>
<th>Core Frequency</th>
<th>Application Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPX6-187</td>
<td>Curtiss-Wright</td>
<td>P4080</td>
<td>8</td>
<td>1.5 GHz</td>
<td>Embedded, military and aerospace security</td>
</tr>
<tr>
<td>NCP-7560</td>
<td>Advantech</td>
<td>P4080</td>
<td>8</td>
<td>1.5 GHz</td>
<td>High-end enterprise and service provider systems</td>
</tr>
<tr>
<td>Niagara 710</td>
<td>Interface Masters</td>
<td>P4080</td>
<td>8</td>
<td>1.3 GHz</td>
<td>Enterprise and data center</td>
</tr>
<tr>
<td>MR-630</td>
<td>Lanner</td>
<td>P2040/41</td>
<td>4</td>
<td>1.5 GHz</td>
<td>Small to mid Enterprises</td>
</tr>
<tr>
<td>SifoWorks™ 8572E</td>
<td>O2 Security</td>
<td>MPC8572E</td>
<td>2</td>
<td>1.2 GHz</td>
<td>Mid-enterprise IPS-based deployments</td>
</tr>
<tr>
<td>CAK-2000</td>
<td>Portwell</td>
<td>P2020E</td>
<td>2</td>
<td>1–1.2 GHz</td>
<td>Mid-enterprise low-power systems</td>
</tr>
<tr>
<td>MR-610</td>
<td>Lanner</td>
<td>P1020</td>
<td>2</td>
<td>800 MHz</td>
<td>Branch office and small business</td>
</tr>
<tr>
<td>AP1020</td>
<td>Senao</td>
<td>P1020</td>
<td>2</td>
<td>800 MHz</td>
<td>Branch office and small business</td>
</tr>
<tr>
<td>SCB-2615</td>
<td>Aewin</td>
<td>P1024</td>
<td>2</td>
<td>533 MHz</td>
<td>Branch office and small business</td>
</tr>
<tr>
<td>SCB-3220</td>
<td>Aewin</td>
<td>P1010</td>
<td>1</td>
<td>800 MHz</td>
<td>Branch office and small business</td>
</tr>
<tr>
<td>MR-350</td>
<td>Lanner</td>
<td>P1020</td>
<td>2</td>
<td>800 MHz</td>
<td>Branch office and small business</td>
</tr>
</tbody>
</table>

Table 2: Freescale Reference Designs for UTM Solutions

<table>
<thead>
<tr>
<th>Freescale Reference Designs</th>
<th>Freescale Processor</th>
<th>Network Ports</th>
<th>Performance</th>
<th>Application Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>P4080PCIe</td>
<td>P4080</td>
<td>2x 10 GbE</td>
<td>20 Gb Firewall</td>
<td>Enterprise and data center</td>
</tr>
<tr>
<td>P2041RDB-PA</td>
<td>P2041</td>
<td>5 GbE</td>
<td>5 Gb Firewall</td>
<td>Mid-enterprise low-power systems</td>
</tr>
<tr>
<td>P2020 UTM</td>
<td>P2020</td>
<td>5x GbE</td>
<td>4 Gb Firewall</td>
<td>Branch office and small business</td>
</tr>
<tr>
<td>P1020 UTM</td>
<td>P1020</td>
<td>3x GbE</td>
<td>2 Gb Firewall</td>
<td>Branch office and small business</td>
</tr>
</tbody>
</table>

Table 1 lists the UTM security solution portfolio offered by ODMs using different QorIQ processors for specific application areas. Table 2 lists the available Freescale reference designs that can meet the broad spectrum of demand for UTM security applications, providing solutions from branch offices and small business to the enterprise data center.

One example of an optimized appliance targeting branch office solutions is Aewin’s SCB-2615 (Figure 3). This system implements a micro 6 port GbE appliance based on the dual-core P1024/15 processor, creating an all-in-one solution that includes UTM processing bandwidth for both wired and wireless office networking in an ultra-cost-effective micro platform.
Freescale’s Solution-Centric Approach with Complete Ecosystem Support

Freescale’s security appliance program enables us to deliver a solution-centric approach (Figure 4) by bringing together four elements needed for the development of a complete UTM security appliance.

- With over 20 years of expertise in embedded communications processing, Freescale’s QorIQ and PowerQUICC processors provide a coherent migration path from single core to multiple core while simultaneously meeting performance needs (with P5 platform scaling up to 2 GHz) and providing low-power, cost-effective solutions. These features make them the ideal processors for UTM appliances.

- VortiQa software products developed through world-class, in-house expertise are optimized to take complete advantage of Freescale’s QorIQ communications platform and PowerQUICC processor silicon.

- An expanded and extended ecosystem of partners can help you to deliver innovative and comprehensive solutions in specific vertical markets. For example, Freescale’s partners can work with you to integrate legacy applications, switching infrastructure, VoIP, video and other convergence applications, as well as several business applications.

- Developer support includes Linux® OS, build tools and CodeWarrior build tools through Freescale’s expanded partner ecosystem.

One of the key requirements of the UTM market is that UTM platforms need to show performance while maintaining low bill of materials (BOM). Freescale’s solution brings together its proven QorIQ and PowerQUICC processor families and VortiQa software, optimized for performance delivered with the help of Freescale’s ODM partners for the best performance at the lowest power levels—thus providing the most cost-effective BOM solution.
How Do Freescale and VortiQa Software Address the Needs of UTM Market?

VortiQa solutions speed development by providing fully integrated, architecturally compatible application software that eliminates or greatly reduces the time needed for these tasks. VortiQa software is optimized to take full advantage of Freescale’s QorIQ processor technology, including PME, security accelerator, IPSec, data path acceleration and other features, thereby boosting performance in embedded systems. The following sections detail features and functions of QorIQ and VortiQa solutions.

Stateful Packet Inspection Firewall and NAT
VortiQa software contains a powerful stateful packet inspection firewall that defends against a wide range of attacks, such as IP address spoofing, distributed denial of service (DDoS), syn-floods, re-assembly and fragmentation. Comprehensive and fine-grained policy enforcement is supported along with NAT and application layer gateways (ALGs).

IPSec Virtual Private Network (VPN)
The IPSec VPN allows seamless and secure connectivity between remote and central sites using VPN. It supports IKEv1 and IKEv2 for automatic key negotiation and remote user access. In addition, VortiQa software IPsec VPN includes native support for Freescale security acceleration engines.

Common Utilities and Basic Networking Functions
Common utilities and basic networking functions include support for several network protocols for LAN and WAN connectivity. They also provide management engines for comprehensive configuration, logging and monitoring.

Intrusion Prevention Common Utilities and Basic Networking Functions
Integrated IPS detects and prevents real attacks using protocol/traffic anomaly and signature-based rules. IPS uses an application-aware architecture that substantially reduces false positives. VortiQa software’s IPS signature database contains thousands of signatures for malicious attacks and is updated regularly. The IPS includes native support for Freescale’s PME technology.
Quality of Service (QoS) and Traffic Management
Extensive traffic management capability helps to ensure QoS of traffic passing through the network. It limits the bandwidth for lower priority traffic generated by network file transfer applications and shapes traffic according to bandwidth and queuing policies.

Configuration Management Interfaces
VortiQa software contains a built-in optimized web server with easy-to-use GUI and a command line interface for management of network gateway functions. A log generation function can direct logs to external syslog servers and send logs as emails.

Antivirus/Antispam Detection and Prevention (AntiX)
Integrated antivirus and antispam capabilities can scan network data, including email messages, for known malware and viruses and protect systems from attacks. VortiQa software’s AntiX feature includes native support for Freescale’s PME technology.

High Availability
VortiQa software provides high availability and load sharing support for its security services to help ensure no loss of network connectivity.

Virtual Security Gateway
Virtual security gateway (VGA) functionality allows the creation of fully enabled virtual gateways that can support multiple gateways within a single device.

Conclusion
Freescale is providing flexibility and choice for vertical networking markets with a solution-based approach that combines VortiQa software with QorIQ platforms, PowerQUICC processors and joint collaborations with a range of well-respected industry partners. The recent addition of several top independent software vendors, original design manufacturers and systems integrators to Freescale’s broad community of third-party partners further extends the availability of solutions based on Freescale silicon.
Information in this document is provided solely to enable system and software implementers to use Freescale Semiconductor products. There are no express or implied copyright license granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Freescale Semiconductor reserves the right to make changes without further notice to any products herein. Freescale Semiconductor makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters which may be provided in Freescale Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including “Typicals” must be validated for each customer application by customer’s technical experts. Freescale Semiconductor does not convey any license under its patent rights nor the rights of others. Freescale Semiconductor products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Freescale Semiconductor product could create a situation where personal injury or death may occur. Should Buyer purchase or use Freescale Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify and hold Freescale Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Freescale Semiconductor was negligent regarding the design or manufacture of the part.