IP Services

Freescale Network Security Solutions

freescale.com/networking

freescale semiconductor

Overview

Today's business networks are under attack and being invaded by hackers and competitors attempting to cause mayhem and gain access to private information. The technology required to defend against these attacks is increasing in complexity and evolving at a rapid rate. Wireless and Voice-over-Internet Protocol (VoIP) telecommunications networks are vulnerable to the same security risks, driving security features to be incorporated as an integral part of the telecommunication infrastructure equipment to provide a safe networking environment. 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 is used to quickly counter serious threats.

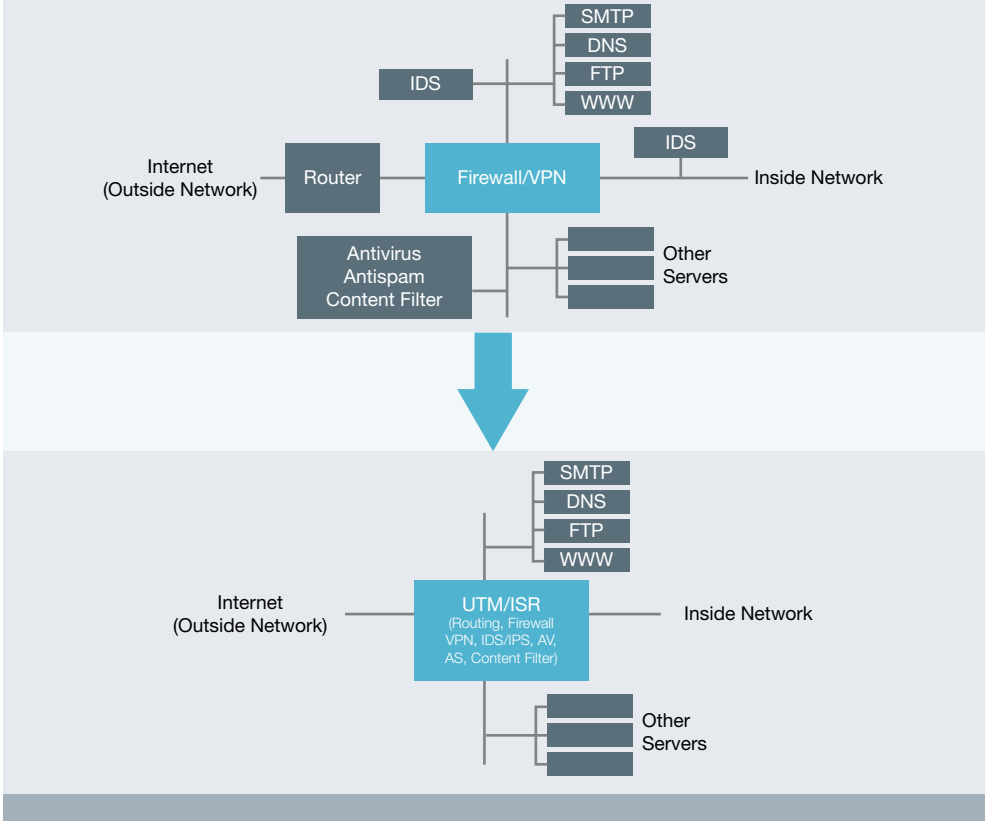
Most enterprises deploy security devices behind their legacy routers to detect and stop malicious traffic before it reaches their servers and desktops. Some of the most common network security devices include:

- 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
- Universal threat management (UTM) or integrated services router (ISR)

Determining which solutions will best serve the needs of the enterprise requires a close examination of the future integration of the numerous solutions being implemented today. 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.

Freescale, a leading provider of integrated communications processors, has several products that are ideal engines for integrated network security equipment—from small office/home office (SOHO) and small-medium business (SMB) to large enterprise and telecommunications infrastructure deployment. Freescale's products, combined with an extensive ecosystem of third-party development partners, offer solutions and reference platforms that original equipment manufacturers (OEM) can leverage to accelerate their time to market.

Network Security Appliances



Firewall/Virtual Private Network Appliance

A firewall/VPN is deployed at the edge of an enterprise network as a defense device used to limit traffic between external and internal networks based on certain policies. The firewall policies are configured using rules such as blocking certain IP addresses or ports. The VPN gateway enables SMB and enterprise users to ensure private and secure communications via the public Internet, using encryption and a tunneling protocol.

PowerQUICC™ communications processors and host processors, built on Power Architecture™ technology, are currently being used in a variety of firewall/VPN hardware platforms. The MPC82xx and MPC83xx PowerQUICC processor families are ideal solutions for SMB deployments which require moderate performance. The MPC74xx, MPC86xx and MPC85xx processor families meet the needs of high-performance enterprise deployments.

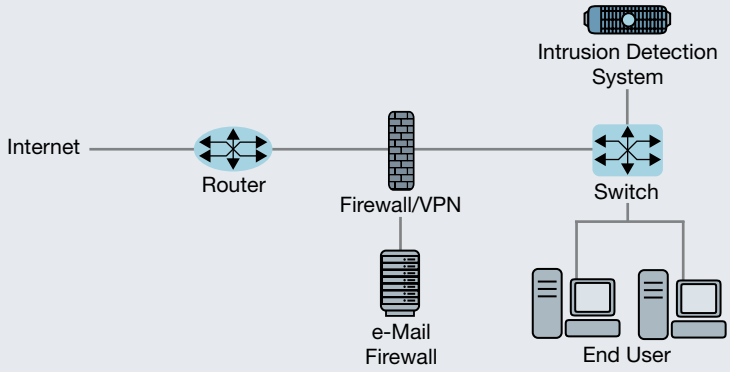
Intrusion Detection/ Prevention System

An IDS identifies potential attacks within the network traffic by monitoring and identifying malicious traffic and generating alarms for each threat. The IDS watches the traffic within the network, looking for protocol and traffic anomalies, known signatures and other identifiers of malicious traffic. Intrusion prevention systems operate within the data stream and can act on security threats to thwart attacks by stopping malicious traffic that may be present.

Antivirus, Antispam and Content Filter

These systems detect and stop viruses, spam and undesirable content in files and other objects carried via Web, e-mail, file transfer and other protocols. Most network systems today implement these functions with network antivirus and content filtering software only, but as bandwidth requirements increase, the processing needs for this functionality start to increase exponentially.

Universal Threat Management/IP Services Router



Universal Threat Management/ Integrated Services Router

Today's network security implementations are very complex and involve discrete FW/VPN and IPS/IDS systems. The content filtering/ antivirus functionality is usually implemented on the server in software. From an enterprise user perspective, the current multisystem solution is an expensive and complex implementation to manage. In an effort to address this issue, network equipment vendors are combining multiple networking and security functions including routing, firewall, VPN, IDS/IPS and antivirus in a single device. These appliances are known as ISR or UTM systems.

Design Challenges

The key design challenge for networking and network security vendors is to be able to deliver a reliable and exciting family of products with a wide range of performance from SOHO to large enterprise deployments. Their engineering challenge is to be able to deliver industry-leading performance and continuously evolve, adapt and upgrade their products' ability to detect high-speed, upper-layer attacks that are exponentially growing in sophistication. Furthermore, vendors are under pressure to be able to deliver these features in a cost-effective and timely manner.

Ideal Processor Engines

The PowerQUICC and Power Architecture families of processors from Freescale are ideal engines for network security equipment. These processors have been engineered to maximize embedded application performance by delivering the highest processing capability in an embedded power envelope. Freescale's platforms are among the first processor platforms to integrate hardware security acceleration, enabling OEMs developing FW/VPN and security appliances to offload compute-intensive security processing and deliver increased levels of system performance and services, while achieving significant cost savings and design simplification.

Freescale's software-compatible processor platforms offer a variety of performance ranges from SOHO and SMB to large enterprise and telecommunications infrastructure deployment. Customers developing SMB security solutions can take advantage of the integration and cost/power optimized solutions that the MPC83xx platforms offer. The MPC83xx platform of products includes an e300 core coupled with System-on-Chip (SoC) integration of Gigabit Ethernet and multiple PCI interfaces operating at less than 4 watts. The security engine allows customers to accelerate IPsec/SSL by offloading the cryptographic processing and freeing up CPU cycles for other protocol processing and system tasks.

For enterprise solutions, Freescale offers a fully integrated, high-performance solution with the MPC85xx platform. For high-performance ASIC designs, customers can use the MPC74xx/MPC86xx platforms. The MPC85xx product family includes single/dual e500 cores coupled with SoC integration of multiple Gigabit Ethernet and PCI interfaces, along with hardware accelerators for cryptographic, Regex pattern matching, decompression and table lookup operations, enabling Gigabit performance and beyond.

Freescale continues to invest in its processor platforms to offer high-performance cores and hardware accelerators for packet and content processing, enabling OEMs to deliver equipment with line-rate network content security performance.

Freescale has a broad ecosystem of third-party development partners in the network security arena that enable OEMs to accelerate their time to market.

VPN/FW Gateway HW/SW

Firewall Solutions from Freescale

Deployment	Processor	Hardware Platform	Software	Availability
Enterprise	MPC74xx, MPC8641, MPC8641D	OEM proprietary; typically Power Architecture™ processor acting as control processor working in conjunction with ASICs	OEM Proprietary	N/A
SMB	MPC8541E, MPC8555E	Freescale MPC8555 Configurable Development System	Aricent Enhanced Security Solution www.futsoft.com/ess.htm	Now
SMB	MPC8349E	Freescale's MPC8349E mITX Reference Board	Jungo www.jungo.com/openrg/opensmb.html	Now
SOHO	MPC8272	Freescale QUICCStart MPC8248 Evaluation System	Kenati www.kenati.com/products_NPgateway.html	Now

Intrusion Detection/Prevention System

The following table shows known implementations and tests using Freescale processors

Deployment	Processor	Hardware Platform	Software	Availability
Enterprise	MPC74xx, MPC8641, MPC8641D	OEM Proprietary	OEM Proprietary	N/A
Enterprise	MPC8572E	Freescale MPC8572E Pattern Matcher Enablement System (MPC8548 + FPGA)	Open Source Application www.snort.org	Pattern Matcher Enablement system available to select customers now
SMB	MPC8555E, MPC8541E	Freescale MPC8555 Configurable Development System	Open Source Application www.snort.org	Now

Antivirus, Antispam and Content Filter

The following table shows known implementations and tests using Freescale processors

Deployment	Processor	Hardware Platform	Software	Availability
Enterprise	MPC8572E	Freescale MPC8572E Pattern Matcher Enablement System (MPC8548 + FPGA)	Kaspersky Lab SafeStream virus signatures www.kaspersky.com	Pattern Matcher Enablement system available to select customers now
Enterprise, SMB	MPC8555E, MPC8541E	Freescale MPC8555CDS Configurable Development System	Open Source Application www.clamav.net	Now

Universal Threat Management/Integrated Services Router

The following table shows Freescale solutions for UTM/ISR applications

Deployment	Processor	Hardware Platform	Software	Availability
Enterprise	MPC74xx, MPC8641, MPC8641D	OEM proprietary; typically a Power Architecture™ processsor acting as a control processor working in conjunction with ASICs	OEM proprietary	N/A
SMB	MPC8555E, MPC8541E	Freescale MPC8555 Configurable Development System	Intoto www.intoto.com	Now
SOHO	MPC8272	Freescale MPC8272 Application Development System	Jungo www.jungo.com/openrg/openrg.html	Now

Infrastructure

The following table shows software-hardware combinations that have been tested to function well together. These combinations are suitable for telecommunications network infrastructure equipment, or to provide high part baseline stacks for OEMs to add the software.

Deployment	Processor	Software	Availability
Crypto Toolkit	PowerQUICC™ I and PowerQUICC II with SEC 1.x PowerQUICC II Pro and PowerQUICC III with SEC2.x	Certicom www.certicom.com	Now
IPsec	PowerQUICC I and PowerQUICC II with SEC 1.x PowerQUICC III with SEC2.x	Arabella www.arabellasw.com	Now
IPsec	PowerQUICC I and PowerQUICC II with SEC 1.x PowerQUICC III with SEC2.x	Kenati www.kenati.com/products_NPgateway.html	Now
IPsec, SSL/TLS	PowerQUICC II Pro and PowerQUICC III with SEC2.x	Mocana www.mocana.com	Now
IPsec	PowerQUICC I and PowerQUICC II with SEC 1.x	QNX Software Systems, www.qnx.com	Now
IPsec	PowerQUICC I and PowerQUICC II with SEC 1.x PowerQUICC II Pro and PowerQUICC III with SEC2.x	Wind River, www.wrs.com	Now

Third-Party Support

Arabella

Arabella provides Secure Linux® and expedited fast path (EFP) microcode solutions for PowerQUICC processors from Freescale. Arabella Secure Linux features include IPsec, NAT, firewall and SSH. The innovative EFP products can increase the systems-level throughput of a PowerQUICC-based design by up to 10 times with no hardware changes. EFP features include point-to-point protocol (PPP), bridging, triple-play services, routing and NAT.

Certicom

Certicom Corp. protects the value of your content, software and devices with government-approved security. Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the undisputed leader in ECC, Certicom's security offerings enable developers to quickly and easily address the requirements of markets such as government communications, smart devices, service providers and enterprise software.

Aricent Enhanced Security Solution

The Aricent Enhanced Security Solution is a pre-integrated router solution that enables equipment manufacturers to quickly build a secure VPN router. Combining VPN (IPSec/PPTP/L2TP) capability, an industry certified stateful firewall, NAT routing, intrusion detection and content filtering, the Aricent ESS is an all-in-one solution for branch offices and enterprise VPN router manufacturers.

Intoto

Intoto is a leading provider of integrated security, wireless and voice software platforms to networking and communications OEMs. Intoto's software solutions are used extensively in many high-volume and top-tier networking products such as security appliances, broadband gateways, IADs/integrated communication platforms, routers and edge appliances.

Jungo

The Jungo OpenRG™ is a complete and integrated software platform for the development of network devices in the digital home and small office. It allows the rapid development of the following:

- Multiservice residential gateways
- Home/SOHO routers
- Wireless access points
- Cable/DSL routers

The Jungo OpenSMB™ is a complete and integrated software platform for the development of advanced SMB networking devices. It allows the rapid development of the following:

- Business firewall/VPN routers
- Wireless APs
- Converged voice/data gateways
- Security appliances

Kaspersky Lab

Kaspersky Lab develops, produces and distributes secure content management solutions that protect customers from IT threats. Kaspersky Lab's products protect both home users and corporate networks from viruses, spyware, adware, Trojans, worms, hackers and spam. For many years now, the company has waged a battle against malicious programs, and in doing so has gained unique knowledge and skills that have resulted in Kaspersky Lab becoming a technology leader and acknowledged expert in the development of secure content management solutions. Today, Kaspersky Lab's products protect more than 200 million users worldwide and its technology is licensed by leading security vendors globally.

Kenati

The Kenati NP Gateway platform is a fully functional software platform for a SOHO or SMB gateway device. The platform is ideal for OEMs and contract manufacturers (CM) that are looking for an out-of-the-box gateway platform which does not require any development effort on their end. The look and feel of the platform can be easily customized. For original design manufacturers (ODM) that wish to build upon or integrate with the existing platform, the source code version of NP Gateway is shipped with a development kit.

Mocana

Mocana provides complete, standards-based, RFC-compliant embedded security solutions for embedded systems. They are approximately 1/10 the footprint of some alternatives and are ideally suited to voice, video and data devices and applications. Protocols include:

- Embedded IPsec/IKE
- Embedded SSL Server
- Embedded SSH Client
- Embedded SSL Client
- Embedded SSH Server
- Embedded RADIUS Client

Open Source Applications

Snort® is an open source network intrusion prevention and detection system utilizing a rule-driven language which combines the benefits of signature, protocol and anomaly-based inspection methods. With millions of downloads to date, Snort is the most widely deployed intrusion detection and prevention technology worldwide and has become the de facto standard for the industry.

Clam AntiVirus is a GPL antivirus toolkit for UNIX®. The main purpose of this software is the integration with mail servers (attachment scanning). The package provides a flexible and scalable multithreaded daemon, a command line scanner and a tool for automatic updating via Internet. The programs are based on a shared library distributed with the Clam AntiVirus package, which you can use with your own software. Most importantly, the virus database is kept up to date.

QNX Software Systems

QNX Software Systems' comprehensive suite of pre-integrated protocol stacks supports IKE, RADIUS, SSH and SSL, as well as other advanced security features. Running on the QNX Neutrino® RTOS, these security protocols leverage the powerful security engine on selected PowerQUICC processors from Freescale to deliver highly optimized encryption and authentication for next-generation network elements.

Wind River

Wind River platform solutions tightly integrate an Eclipse-based development suite with a choice of VxWorks or Wind River Linux operating systems, a rich set of advanced networking and security technologies (TCP/IP v4/v6, IPsec, IKEv1/v2, SSH, SSL, Cryptography Libraries, Cryptography offload, firewall, NAT, RADIUS, WPA/WPA2 supplicant, MIPv4/v6) optimized for resource constrained devices, worldwide customer support and professional services to enhance your team's capabilities. Wind River platforms are validated on a wide selection of Freescale board support packages. Integration of Wind River platforms with Freescale's silicon reduces effort, cost and risk, while improving quality and reliability throughout the device life cycle, from board bring-up to managing deployed product.

Learn More: For more information about Freescale products
please visit www.freescale.com

// DOCNUMBER: BRNTWKSECSOLTN // REV 3

BUILT ON Power™

freescale semiconductor