

White Paper

# Designing UTM

## with the PowerQUICC® III MPC8572E

---



## Overview

---

Freescale's PowerQUICC® families of processors have long established themselves as the premier communications processors in the market, widely used in numerous networking and network security devices. The MPC8572E, the first PowerQUICC III processor with an integrated pattern matcher, is specially designed to satisfy the additional requirement of high-performance networking equipment to be application-aware. It is well-suited to power the increasingly popular Universal Threat Management (UTM) systems with a conglomerate of functions including routing, firewall, IPSec VPN, anti-virus, anti-spam and content filtering. This white paper describes how high-performance, cost-effective UTM equipment can be designed with the MPC8572E.

# Contents

---

1	Rising Popularity of UTM.....	4
1.1	Key Reasons for UTM's Success .....	4
1.2	Functionalities of UTM.....	4
1.3	Security Deployment in Branch Offices.....	5
2	Design Challenges .....	6
2.1	Router and Firewall Datapath .....	6
2.2	IPSec VPN Datapath.....	6
2.3	Application Content Processing in IDS/IPS, Anti-Virus, Anti-Spam and Content Filter.....	6
2.4	System Design Issues.....	7
3	MPC8572E PowerQUICC III Processor Overview .....	7
4	Designing UTM with the MPC8572E .....	9
4.1	Additional Policy Elements in UTM.....	9
4.2	Flow-Based UTM Operations .....	10
4.2.1	Basic ACL-Like Policies.....	10
4.2.2	Enhanced Content Policies.....	10
4.2.3	Summary UTM Processing .....	10
4.3	Dual-Core Usage Model for UTM Operations .....	11
4.3.1	Control Path.....	11
4.3.2	Packet Data Path.....	12
4.3.3	Content Data Path .....	12
4.3.4	IPSEC VPN Control and Data Paths.....	12
4.4	Performance Advantages of the MPC8572E in Content Data Path.....	13
4.5	Accuracy Advantages of the MPC8572E in Content Data Path .....	13
4.5.1	Regex.....	13
4.5.2	Stateful Rule.....	13
4.5.3	Sets and Subsets.....	14
4.5.4	Matching Across Packet Boundaries.....	14
4.5.5	Performance Minimally Dependent on the Number of Signatures.....	14
4.6	Performance Advantages of the MPC8572E in Packet Data Path.....	14
4.6.1	Packet I/O .....	14
4.6.2	Packet Processing .....	14
4.6.3	Traffic Management .....	14
4.7	Hardware Platform Design with the MPC8572E.....	15
4.7.1	Cost Advantages.....	15
5	Summary.....	15

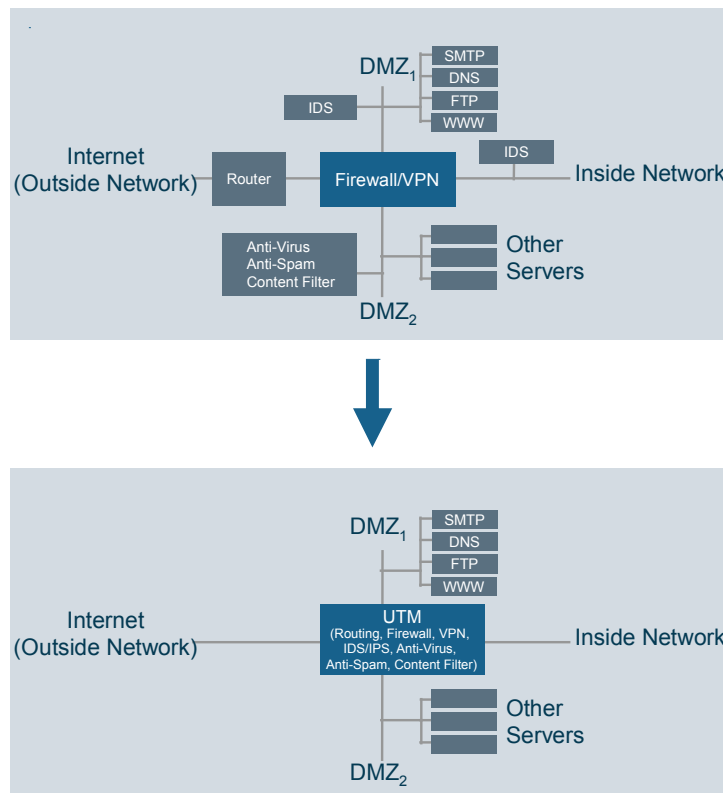
# 1 Rising Popularity of UTM

Universal Threat Management (UTM), also known as Integrated Services Router (ISR) and Secure Services Gateway (SSG), is rapidly becoming the single most important network security device in many enterprises, particularly in small- and mid-sized offices.

## 1.1 Key Reasons for UTM's Success

By integrating the functionalities previously found in multiple security and networking devices, the UTM enables the same level of network security at much lower capital and operating costs—there are fewer devices to purchase and to maintain. The “before and after” scenarios shown in the diagram below illustrates the compelling value proposition of deploying UTM.

Figure 1: Trend Towards UTM



## 1.2 Functionalities of UTM

The UTM integrates functionalities found previously in multiple devices. But why were so many networking and security devices deployed in the first place?

The first device facing the open Internet is the router to provide networking functions.

Behind the router is the firewall/VPN security gateway which has been the only critical piece of network security equipment for some time. The main purpose of the firewall is to stop unwanted traffic from entering or leaving the internal enterprise network. The purpose of the IPSec VPN is to provide secure communication between two sites through the open Internet.

But the industry now recognizes that some 90 percent of attacks in recent years have exploited application vulnerabilities<sup>1</sup>. The traditional stateful inspection firewall, based largely on matching packet header information against Access Control Lists (ACLs), is ineffective to fend off such attacks. Therefore, many enterprises also deploy Intrusion Detection Systems (IDS) to monitor traffic in vital network segments—the IDS is able to detect application layer attacks. But detection alone is insufficient—it is also important to terminate the attack upon detection. The trend is to evolve the IDS into an Intrusion Prevention System (IPS) which takes detection to the next level and stops the detected attacks, including application attacks.

To have greater protection against virus, spam and undesirable content from propagating into or out of the enterprise network, application-specific anti-virus, anti-spam and content filtering devices are also deployed.

Hence, in addition to servers and client PCs, a security-conscious enterprise would deploy equipment that provides the following functionalities in a typical office:

- Routing
- Stateful Inspection Firewall
- IPSec VPN
- IDS/IPS
- Anti-virus
- Anti-spam
- Content filter

And the UTM integrates most, if not all of these functions.

### 1.3 Security Deployment in Branch Offices

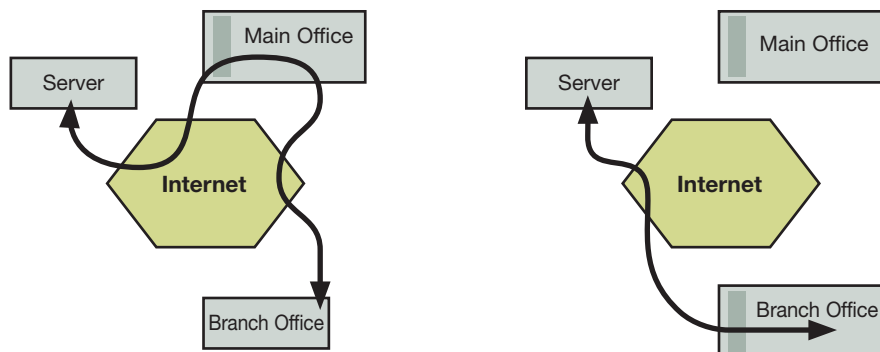
While UTM is definitely getting increasingly popular, some may still question its use in branch offices—the deployment of firewall, IDS/IPS, anti-virus, anti-spam and content filtering functions in branch offices is not quite universal yet.

Today, some enterprises deploy network security equipment at the central site only. This approach has the advantage of relatively simple management of (centralized) security. On the other hand, this approach pays a penalty in terms of poor performance and inefficient bandwidth utilization—Internet-bound traffic from a branch office is first backhauled to the headquarter, typically in an IPSec tunnel, examined by the security equipment deployed there, and if checked out to be clean, allowed to travel to the Internet.

It has been reported that “by 2009, half of branch offices will have direct Internet connections as opposed to routing Internet traffic from branch offices over the WAN and onto the Internet from a headquarters site. That is up from 10 percent today<sup>2</sup>.”

To have high application performance, Internet traffic destined for the branch office should be allowed to enter from the Internet directly, without going through headquarter. In this case, however, security protection needs to be deployed at the branch office as well. Please see figure 2 below.

**Figure 2: Branch Office Internet Connectivity and Traffic Flow**



<sup>1</sup> Symantec Internet Security Threat Report, Trends for July 05–December 05, Volume IX, March 2006

<sup>2</sup> [www.networkworld.com/news/2006/020606-juniperssg-side.html](http://www.networkworld.com/news/2006/020606-juniperssg-side.html)

Furthermore, network security professionals are increasingly taking the view that perimeter defense alone—stopping bad traffic as it enters the Enterprise network from the open Internet—is inadequate. The use of portable PCs and wireless access increase the probability of “attacks from within.” To prevent the spread of worms or viruses from both outside and inside, network security devices should be deployed within the enterprise network. Security at the branch office provides protection from internal attacks.

Hence, to achieve higher performance for Internet traffic at the branch office and to protect against attacks from within, deployment of security functions and UTM at branch offices will further increase.

## 2 Design Challenges

---

In essence, the UTM performs a conglomeration of divergent networking and security functions previously provided in different specialized devices, each optimized for a specific function. The key challenge of building a world-class UTM system is to design a platform that can perform all the divergent functions simultaneously and at high-speed. To be competitive, the platform has to be cost-effective and designed within a short time interval.

To have a better appreciation of the design challenges, let's take a look at the processing requirements of a few key functions in the UTM.

### 2.1 Router and Firewall Datapath

Router and firewall datapaths are relatively simple: the challenge is speed, speed and speed! Designers put a lot of effort into minimizing the number of instructions in the datapath in order to achieve high performance. Below are some datapath operations that can potentially consume a large number of CPU cycles:

- Servicing (high rate of) packet I/O interrupts
- Checksum verification/calculation in Rx and Tx frames
- Looking up large table(s) to determine what is to be done with a received packet
- Optionally provide Quality-of-Service (QoS) control

In addition to minimizing the number of CPU cycles in the datapath, the designer must make sure that bus and memory bandwidth is not the bottleneck for data movement in high-throughput networking applications.

### 2.2 IPSec VPN Datapath

The challenges associated with high-speed router and firewall datapath are also applicable to the IPSec datapath. In addition, the highly CPU-intensive crypto operation is required.

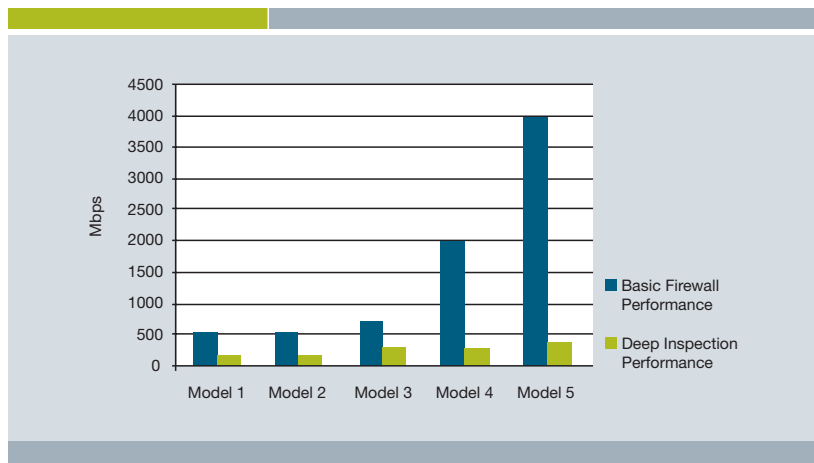
A coprocessor may be used to offload and accelerate crypto operations. A coprocessor that can perform all the crypto operations required in the datapath in a single path and will incur less overhead. The designer should also make sure that the communications path between the rest of the system and the crypto coprocessor is efficient to achieve high performance.

### 2.3 Application Content Processing in IDS/IPS, Anti-Virus, Anti-Spam and Content Filter

Processing application content in packet flows presents a very different set of challenges. Compared with processing essentially fixed location packet header information as in router, firewall and IPSec datapath, processing application content is considerably more complex.

The graph in figure 3 shows that using software to process application content as represented as “Deep Inspection” leads to very unsatisfactory performance.

**Figure 3: Firewall Performance: Basic vs. “Deep Inspection”**



To implement such complex functions as application content processing, the processor must have general-purpose CPU core(s) with standard ISA.

To attain any degree performance, there must be adequate CPU cycles available provided by one or more high-frequency CPU cores.

A large cache is typically needed to enable efficient utilization of CPU cycles, especially dealing with a large number of flows.

For equipment requiring high-performance application content processing, the brute-force method of providing more CPU cycles may not be the best solution—a good hardware pattern matcher can do the job faster and with lower power dissipation. In choosing the pattern matcher, one should be cognizant of the fact that simple string match hardware is not adequate for complex content processing—the pattern matcher should have powerful Regular Expression (Regex) or even more powerful capabilities.

## 2.4 System Design Issues

To be able to find processing elements that can perform the UTM operations at high speed is a very good start, but not quite the end of the story. The system designer must make sure that various functional blocks can operate efficiently together in a pipeline to achieve high throughput and low latency.

To be competitive, the platform must be cost-effective and help enable a short development cycle. Plus, it must operate within a tight power budget in the embedded environment.

A well-designed, low-powered SoC integrated with the right processing and I/O elements will go a long way towards a simple, elegant, cost-effective system design.

## 3 MPC8572E PowerQUICC III Processor Overview

The MPC8572E is a new PowerQUICC III processor purposely built to meet the requirements of high-performance application-aware networking and content security. It is based on the highly successful PowerQUICC System-on-Chip (SoC) platform, well-proven in traditional networking and enhanced with further integration of new hardware, optimized to process application content at high speeds.

The MPC8572E consists of dual e500 cores built on Power Architecture™ technology, achieving clock speeds from 1.2 GHz to 1.5 GHz. The CPU cores, each with 32 KB I-Cache and 32 KB D-Cache, share 1024 KB of integrated L2 cache. For memory, the MPC8572E includes two integrated 64-bit DDR2/DDR3 SDRAM controllers.

To further speed up processing, while keeping power dissipation down, the MPC8572E integrates powerful engines: a security engine that accelerates crypto operations in IPSec and SSL/TLS, a pattern-matching engine to handle regular expression matching, a deflate engine to manage file decompression, and two table lookup units (TLU) that manage complex table searches and header inspections.

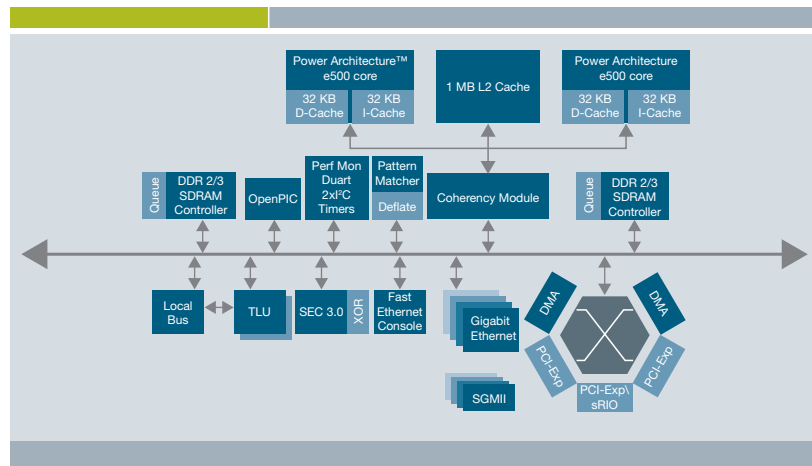
The MPC8572E offers a combination of network interfaces, including four integrated enhanced Triple-Speed Ethernet controllers (eTSEC). These controllers accelerate packet I/O by offloading checksum calculation. They also provide QoS support with eight Rx and eight Tx hardware queues to accelerate traffic management.

For high-speed connectivity to other devices, the MPC8572E supports PCI Express®, Serial RapidIO® and DMA interfaces.

All major processing and I/O elements are integrated into the MPC8572E with a highly optimized internal interconnect architecture to ensure high bandwidth, low latency and efficient pipeline operation, balancing processing performance with I/O system throughput.

Based on Freescale's 90 nm silicon-on-insulator (SOI) copper interconnect process technology, the MPC8572E is designed to deliver higher performance with lower power dissipation.

**Figure 4: MPC8572E PowerQUICC® III Block Diagram**



The Pattern Matcher is the key contributor to the MPC8572E's ability to process packet content at high speed for application-aware networking and content security applications.

The Pattern Matcher is an integrated hardware block inside the MPC8572E with the following capabilities:

- High-performance, feature-rich hardware pattern matching of compressed and uncompressed data
  - Patterns expressed in regex with significant capabilities beyond that provided by the regex language
  - Stateful Rule—correlates multiple pattern matches and maintains state between matches
- Improvements over other pattern matching technologies:
  - No pattern “explosion” to support “wildcarding” or case-insensitivity
  - Fast compilation of pattern database
  - Fast incremental additions to pattern database
  - Live pattern database update
  - Patterns stored in main DDR DRAM, not SRAM or FCRAM
- On-chip hash tables for low system memory utilization, removing need for costly low-latency memory technologies
- Pattern matching across data “work units” (e.g. can match patterns split across TCP segments)

## 4 Designing UTM with the MPC8572E

A white paper has previously been written on designing Firewall/VPN with the MPC8572E<sup>3</sup>. In this white paper, we are going to focus more on the additional functionalities found in the UTM.

### 4.1 Addition Policy Elements in UTM

The basic firewall supports essentially ACL-like policies. The UTM, in addition, supports content security policies.

Let's first look at an HTTP example.

A simple, ACL-like policy supported by the basic firewall looks like:

*"Allow traffic from the Outside Network to the WWW server in DMZ1 if the protocol is TCP and the destination port number is 80."*

A more sophisticated policy supported by the UTM, based on the basic policy above but further enhanced to invoke IDS/IPS function, looks like:

*"Allow traffic from the Outside Network to the WWW server in DMZ1 if the protocol is TCP and the destination port number is 80; and check traffic for intrusion using client-to-server HTTP signatures."*

Next, let's look at an SMTP example.

Below is the simple, ACL-like policy supported by the basic firewall:

*"Allow traffic from the Outside Network to the SMTP server in DMZ1 if the protocol is TCP and the destination port number is 25."*

An enhanced policy supported by the UTM based on the one above, invoking anti-virus function may look like:

*"Allow traffic from the Outside Network to the SMTP server in DMZ1 if the protocol is TCP and the destination port number is 25; and check the traffic for viruses."*

From the two sets of examples, we observe that simple ACL-like policies and sophisticated content security policies can share the same structure, the latter with additional scrutiny on the content further defined:

*<action, source, destination, service, optional content security ops>*

Note that basic policies essentially deal with packet header information of source, destination, service (= protocol + port#) only, while sophisticated policies have to process content in addition.

<sup>3</sup> Designing Firewall/VPN with the PowerQUICC® III MPC8572E

## 4.2 Flow-Based UTM Operations

### 4.2.1 Basic ACL-Like Policies

Typically, a flow-based packet processing approach is used in high-performance network security equipment like the basic firewall. The operation can be separated into:

- Control path
- Data path

Alternatively, the approach can be described as “first packet” and “subsequent packet” processing.

The control path is performed at the beginning of a flow, i.e. when a new packet is received and there is no flow table entry matching the characteristics of the packet. The key steps are:

- Classify the flow itself and its child flows (as in FTP, SIP, etc.)
- Consult policy table to determine how the flows are to be processed, e.g., allowed, denied, “tunnel”, apply suitable QoS, keep statistics, etc.
- For each flow, add an entry to the flow table stating how subsequent packets in the flow are to be processed, including the packet at hand

The data path is as follows:

- Receive packet
- Look up entry in a potentially very large flow table
- Process according to the “recipe” in entry, e.g. forward, NAT, apply QoS, collect statistics
- Transmit packet

We note that for simple policies, the datapath involves processing based on packet header only.

### 4.2.2 Enhanced Content policies

In essence, the control or “first packet processing” path is the same as that for basic ACL-like policies. The difference is in the data path. The application protocol and content of the packet flows need to be processed to make sure that they are safe. Depending on the policy, one or more content security functions like IDS/IPS, anti-virus, anti-spam and content filter are applied to the packet content.

### 4.2.3 Summary UTM Processing

In view of the fact that the UTM has two very different types of datapaths, we’ll use the following terminology to describe UTM operations in the rest of this paper:

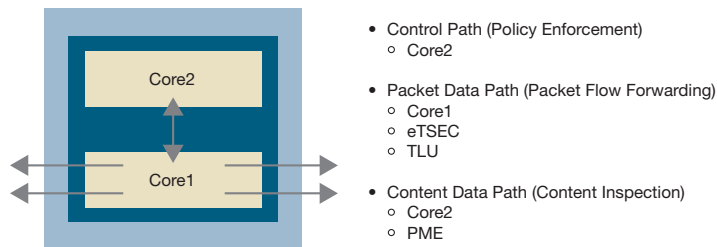
1. Control path
2. Packet data path
3. Content data path

We recognize that the control or “first packet processing” path may or may not be carried in a separate “control” connection.

### 4.3 Dual-Core Usage Model for UTM Operations

The dual-core MPC8572E can be used in the Symmetric Multi-Processing (SMP) or the Asymmetric Multi-Processing (AMP) mode. This white paper describes how UTM operations can be implemented in the AMP mode.

Figure 5



In essence,

- Core2, working in conjunction with the Pattern Matcher, is used for the CPU-intensive application protocol and content processing, including matching suitable parts of the packet flow payload against intrusion, spam and virus signatures.
- Core1, working in conjunction with eTSECs and TLUs, is used for the packet data path, such as packet I/O, forwarding, controlling QoS and updating statistics.

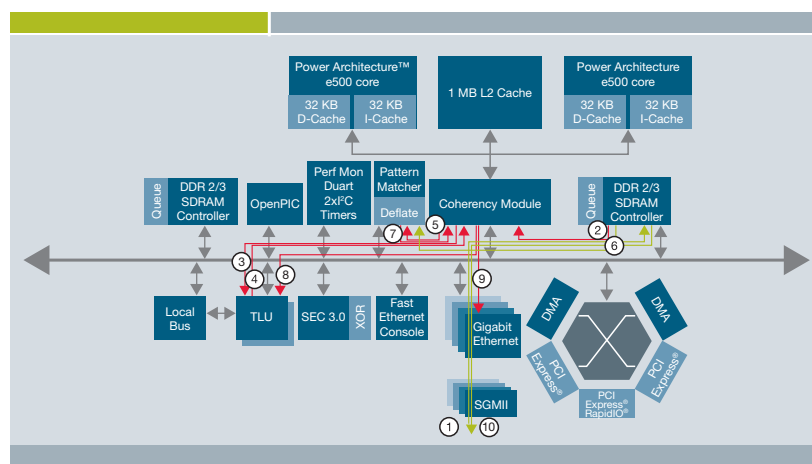
#### 4.3.1 Control Path

The control or “first packet processing” path is shown in more detail in figure 6:

1. Ethernet controller puts received packet into appropriate queue in memory and informs Core1
2. Core1 extracts 5-tuple key from the packet header
3. Core1 writes key to TLU to lookup flow table
4. Core1 reads back lookup (negative) result and informs Core2
5. Core2 analyzes packet payload, instructs Pattern Matcher to scan payload against application protocol signatures
6. Pattern Matcher reads data from memory and scans for patterns
7. Pattern Matcher informs Core2 of scan result
8. Core2 adds flow table entry in TLU and informs Core1
9. Core1 process packet as per recipe and instructs Ethernet port to transmit
10. Data retrieved from memory and transmitted, apply QoS as required

While the control path is relatively complex, it affects mainly the latency of the first or first few packets.

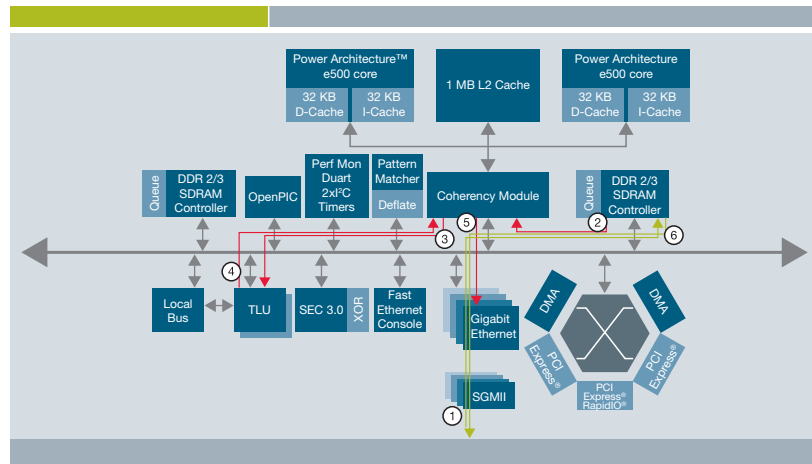
Figure 6: UTM Control Path on MPC8572E



### 4.3.2 Packet Data Path

In more detail, the packet data path is shown in figure 7:

Figure 7: UTM Packet Data Path on MPC8572E



1. Ethernet controller puts received packet into appropriate queue in memory and interrupts Core1
2. Core1 extracts 5-tuple key from the packet header
3. Core1 writes key to TLU to lookup flow table
4. Core1 reads back (positive) results of the lookup and retrieves additional flow entry data from memory if required, and processes packet as per “recipe” in flow table
5. Core1 instructs appropriate Ethernet controller to transmit packet
6. Ethernet controller transmits packet, applying QoS as required

### 4.3.3 Content Data Path

The diagram depicting the content data path looks similar to that of the control path shown earlier (figure 6). The individual operations are as below:

1. Ethernet controller puts received packet into appropriate queue in memory and informs Core1
2. Core1 extracts 5-tuple key from the packet header
3. Core1 writes key to TLU to lookup flow table
4. Core1 reads back (positive) results of the lookup and retrieves additional flow entry data from memory if required, and informs Core2
5. Core2 process application protocol and content as per recipe, and instructs Pattern Matcher to scan payload against intrusion, spam, virus and other signatures
6. Pattern Matcher reads data from memory and scans for patterns
7. Pattern Matcher informs Core2 of scan result
8. Core2 informs Core1
9. Core1 packetizes content as required and instructs Ethernet port to transmit
10. Data retrieved from memory and transmitted, apply QoS as required

### 4.3.4 IPSEC VPN Control and Data Paths

The UTM also supports IPSEC VPN. Descriptions of how the MPC8572E can be used to support IKE and IPSec can be found in a previous paper.<sup>3</sup> In essence, the crypto security block is used to accelerate the crypto operations in both IKE and IPSec.

<sup>3</sup> Designing Firewall/VPN with the PowerQUICC® III MPC8572E

## 4.4 Performance Advantages of the MPC8572E in Content Data Path

A powerful e500 core, working in conjunction with the hardware Pattern Matcher, is used in the content data path that matches packet payload against intrusion, virus, spam and other application signatures. This highly CPU-intensive operation is offloaded and accelerated by the hardware Pattern Matcher. The interaction between the e500 core and the Pattern Matcher is very efficient via descriptors in L2 cache. As a result, the content data path is greatly accelerated.

## 4.5 Accuracy Advantages of the MPC8572E in Content Data Path

The built-in Pattern Matcher that offloads and accelerates matching of a packet payload against application signatures has a number of features and operational characteristics that are conducive to accuracy, leading to higher security:

- Regex
- Stateful rule
- Sets and subsets
- Matching across packet boundaries
- Performance minimally dependent on the number of signatures

### 4.5.1 Regex

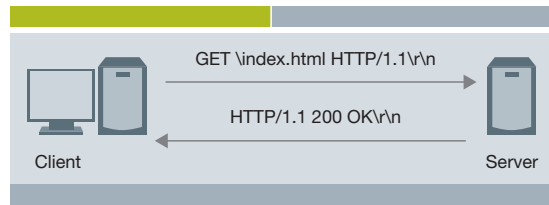
The Regex Compiler associated with the MPC8572E's Pattern Matcher supports a major subset of the Practical Extraction and Report Language (PERL) regular expression syntax as well as capabilities beyond that provided by PERL. The Pattern Matcher can match thousands of Regexes in parallel at multi-Gbps speed.

This means that the signature designer has a very powerful tool at his or her disposal to design sophisticated signatures to achieve high accuracy without worrying about performance.

### 4.5.2 Stateful Rule

The Pattern Matcher's Stateful Rule capability can be used to track application protocols and create the context for stateful pattern matching to achieve high accuracy.

**Figure 8: Typical HTTP Request-Response Exchange**



As a first step, the signature designer can create a very accurate signature using Regex based on the request or the response. To take a step further, the designer can build an even more accurate signature based on the protocol request-response exchange itself as well as the regexes representative of the request and the response.

A simplified example is illustrated below:

1. Define regex signatures of HTTP request and response

```
http_request /^get|post\s.+?http\d\d$/im
```

```
http_response /^http/1\d\s2\d\d.+$im
```

2. Define Stateful Rule matching the protocol exchange

```
STATEFUL_RULE: HTTP_Recognizer
  RESET_STATE:
    EVENT "http_request"
      next_state AWAIT_response
  STATE AWAIT_response:
    EVENT "http_response"
      # report HTTP traffic observed
      report {0x00000001}
      next_state RESET_STATE
```

### 4.5.3 Sets and Subsets

The Pattern Matcher supports signature sets and subsets. This feature can be used to create the context for stateful pattern matching to achieve high accuracy.

For example, while the UTM supports IDS/IPS, anti-virus and anti-spam functions, matching packet payload against all signatures regardless of context leads to more false positives and is therefore not a good idea. While in the context of detecting intrusion, only intrusion signatures should be compared. To go one step further in terms of granularity, if the flow in question is a client to server HTTP connection, only the set of intrusion signatures related to client to server HTTP should be used. The Pattern Matcher enables such context sensitive matching to be performed.

### 4.5.4 Matching Across Packet Boundaries

Application messages do not necessarily follow packet boundaries. For accurate signature-based detection, matching across packet boundaries is required. This capability is supported in the MPC8572E's Pattern Matcher.

### 4.5.5 Performance Minimally Dependent on the Number of Signatures

A UTM with low pattern matching performance, such as one implemented with software, puts the IT manager in an awkward position to choose between security or speed:

- Configuring relatively few signatures to achieve higher performance at the risk of lowering the coverage of detection, or
- Configuring the complete set of signatures to detect all the known problems but suffer from lower performance as a result

To solve this problem, the throughput performance of MPC8572E's integrated Pattern Matcher is minimally affected by the number of patterns configured.

## 4.6 Performance Advantages of the MPC8572E in Packet Data Path

### 4.6.1 Packet I/O

The UTM is a networking device. As such, it should not bottleneck network traffic, the first requirement of which is to simply have the ability to receive and transmit packets at a high rate. The overhead in servicing a high rate of transmit and receive interrupts is high and can significantly slow down the performance of the device. The integrated Ethernet controller is able to coalesce interrupts, thereby reducing the interrupt servicing overhead and improve performance.

In a networking device where the I/O rate is high, memory access speed in addition to the availability of CPU cycles can have a significant impact on system performance. The integrated Ethernet controller on the MPC8572E stashes received packet headers in L2 cache while writing to memory. As a result, the e500 CPU core accesses data with reduced latency. In fact, the transmit and receive buffer descriptors can be locked in the L2 cache for fast access by the Ethernet controller and the e500 core.

### 4.6.2 Packet Processing

A powerful e500 CPU core with clock speeds up to 1.5 GHz is dedicated to provide the CPU cycles (and flexibility) required for packet-layer processing. Furthermore, the following operations are offloaded from the CPU core:

- IP and TCP checksum calculations to the Ethernet controller
- Flow table lookup to the TLU

Checksum calculations are required for every packet received. Offloading this calculation results in less software execution and higher performance.

Searching for an existing entry in a potentially very large flow table is performed every time a packet is received. This operation can be offloaded to the built-in TLU on the MPC8572E.

### 4.6.3 Traffic Management

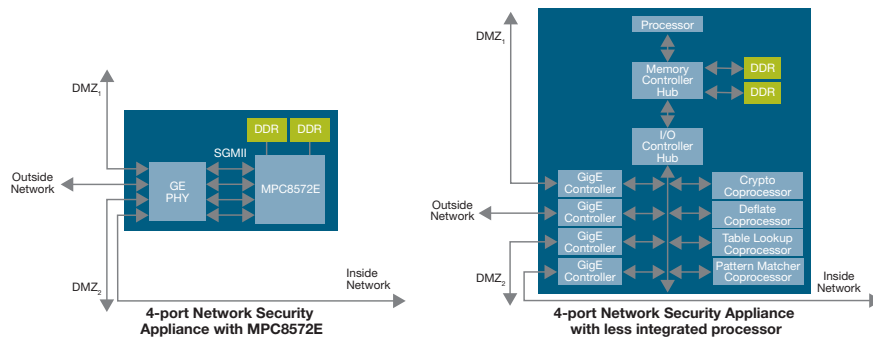
Some traffic management functions can be accelerated and offloaded to the integrated Ethernet controllers. The eTSECs have built-in QoS support for eight Rx and eight Tx hardware queues. The transmit scheduling can be set to strict priority or modified weighted round robin.

## 4.7 Hardware Platform Design with the MPC8572E

In essence, the UTM essentially receives packets, processes the packet's header and the application content in the packet payload, and transmits the packet.

Figure 9 below shows two simplified block diagrams of a 4-port network appliance, one implemented with the MPC8572E and the other with a less integrated processor.

**Figure 9: 4-Port Networking Appliance Implementation**



### 4.7.1 Cost Advantages

The very simple system design—a direct result of the exceptional integration in the MPC8572E—can help enable significantly lower system cost and shorter time to market. There is no separate memory controller hub, I/O controller hub, Gigabit Ethernet controllers, table lookup coprocessor and pattern matcher coprocessor to complicate the design and add to the cost. Specific to the Pattern Matcher, there is also no separate expensive low latency memory—the MPC8572E's built-in Pattern Matcher does not need it for high performance, unlike other pattern matching engines on the market.

## 5 Summary

Freescale's PowerQUICC family of processors has a long legacy and an established reputation as the premier family of communications processors in the market. They are widely used in a variety of networking devices including switches, routers and network security devices. The MPC8572E, the first PowerQUICC III processor with an integrated Pattern Matcher, is specially designed to satisfy the additional requirement of high-performance networking and network security devices such as the UTM to process application content at high speed.

The MPC8572E's dual e500 cores provide CPU cycles and flexibility to execute the software for packet data plane and content data plane operations. The performance of the MPC8572E is further enhanced by the integrated hardware blocks that off-load and accelerate CPU-intensive operations with low power dissipation:

- TLU: manages various table lookup operations widely used in packet forwarding and security
- eTSEC: allows traffic management and checksum calculation of sent and received packets
- SEC: enables crypto operations in IKE and IPSec
- Deflate: provides decompression
- Pattern Matcher: matches packet payload against signatures of intrusion, virus, spam and undesirable content in general

The built-in Pattern Matcher, with its features and operational characteristics, is particularly conducive to providing high performance and accuracy simultaneously in UTM content data plane:

- Regex allows the creation of sophisticated signatures that are fingerprints of various forms of undesirable content
- Stateful rule enables even more accurate signatures by tracking application protocol exchange
- Set and subsets enable only relevant portion of the total signature be used in a context-sensitive manner
- Matching patterns across packet boundaries to increase accuracy by matching application messages that span packet boundaries
- Performance minimally dependent on number of signatures enables the IT manager to configure the complete set of signatures to provide fine-grain granularity and accuracy without worrying about degradation of performance

The MPC8572E processor, with all major processing and I/O elements included, helps enable a very simple, elegant system design, with low system cost and a shortened design cycle. Contributing further to cost-effectiveness is the Pattern Matcher's use of DRAM instead of expensive low latency SRAM or FCRAM. As a result, OEMs can count on using the MPC8572E to deliver highly competitive UTM products to the market.

## How to Reach Us:

### Home Page:

[www.freescale.com](http://www.freescale.com)

### Power Architecture Information:

[www.freescale.com/powerarchitecture](http://www.freescale.com/powerarchitecture)

### e-mail:

[support@freescale.com](mailto:support@freescale.com)

### USA/Europe or Locations Not Listed:

Freescale Semiconductor  
Technical Information Center, CH370  
1300 N. Alma School Road  
Chandler, Arizona 85224  
1-800-521-6274  
480-768-2130  
[support@freescale.com](mailto:support@freescale.com)

### Europe, Middle East, and Africa:

Freescale Halbleiter Deutschland GmbH  
Technical Information Center  
Schatzbogen 7  
81829 Muenchen, Germany  
+44 1296 380 456 (English)  
+46 8 52200080 (English)  
+49 89 92103 559 (German)  
+33 1 69 35 48 48 (French)  
[support@freescale.com](mailto:support@freescale.com)

### Japan:

Freescale Semiconductor Japan Ltd.  
Headquarters  
ARCO Tower 15F  
1-8-1, Shimo-Meguro, Meguro-ku,  
Tokyo 153-0064, Japan  
0120 191014  
+81 3 5437 9125  
[support.japan@freescale.com](mailto:support.japan@freescale.com)

### Asia/Pacific:

Freescale Semiconductor Hong Kong Ltd.  
Technical Information Center  
2 Dai King Street  
Tai Po Industrial Estate,  
Tai Po, N.T., Hong Kong  
+800 2666 8080  
[support.asia@freescale.com](mailto:support.asia@freescale.com)

### For Literature Requests Only:

Freescale Semiconductor  
Literature Distribution Center  
P.O. Box 5405  
Denver, Colorado 80217  
1-800-441-2447  
303-675-2140  
Fax: 303-675-2150  
[LDCForFreescaleSemiconductor@hibbertgroup.com](mailto:LDCForFreescaleSemiconductor@hibbertgroup.com)

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.