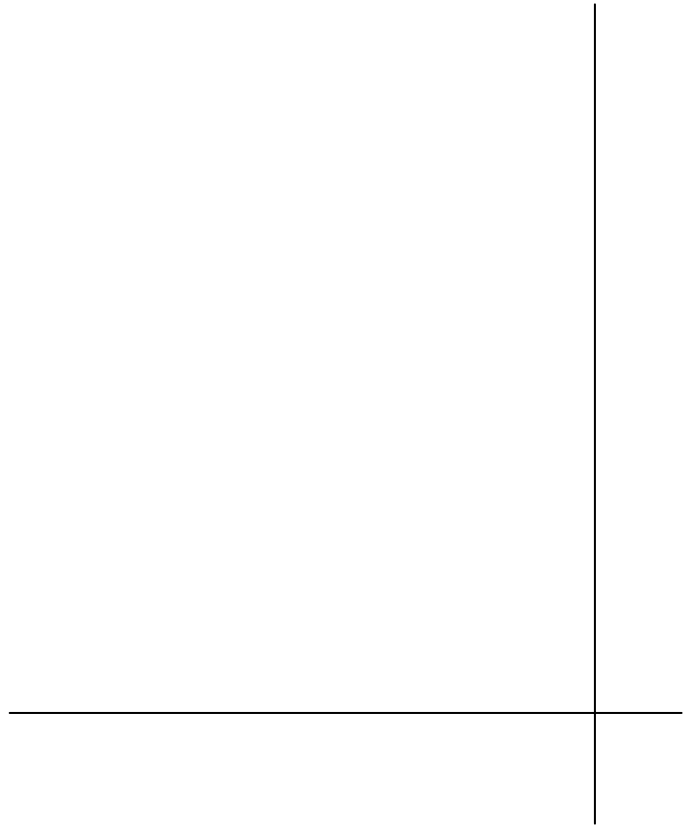




# **The T9000 Family of Content Processor ASICs**

***Accelerated Network Security on an ASIC***

*A Tarari Whitepaper*



**Table of Contents**

Overview .....3

Background.....4

    Device Manufacturers – Chasing the Value-Add .....4

    Content Processors – More Work in Smaller Packages.....5

    Tarari Content Processor ASICs .....6

Network Security – The Defense Never Rests .....7

    The Threat Landscape .....7

    New Dangers .....8

Meeting the Threats with the Tarari T9000 Family .....9

    Built for Content Inspection .....9

T9000 Features ..... 13

T9000 Family ..... 14

T9000 Architecture..... 15

    Functional Description..... 15

T9000 Applications and Benefits..... 17

    With Communication Processors ..... 17

    Combined Software-Hardware Solutions ..... 21

    More Resources from Tarari ..... 23

Conclusion ..... 23

## Overview

As network security has evolved, more of the security functions traditionally executed on application servers (packet inspection, validation, content-based routing) have moved to devices in the network infrastructure itself, and the market compels the designers of these devices to offer an expanded level of network protection in a smaller package with greater efficiency and, of course, a lower price. The expanding role of XML and Web services, with their attendant vulnerabilities, offers the next big security challenge.

Original design manufacturers (ODMs), original equipment manufacturers (OEMs) and network device architects continually evaluate technologies and components in search of high-performance security without traffic bottlenecks in order to drive higher profits by converting security challenges into market opportunities. The market has evolved to span the range of software alone, dedicated appliances, processor boards, and now finally to “Accelerated Network Security on an ASIC,” with the greatest potential for more ODM/OEM revenue.

**Tarari’s T9000 Content Processor ASICs represent the most comprehensive family of acceleration chips, providing multi-gigabit hardware acceleration for anti-spam, anti-virus, intrusion detection (IDS), compliance, XML application processing and security, cryptography and compression/decompression. The T9000 series provides drop-in compatibility with any existing Tarari acceleration solutions, and is already the most commercially advantageous choice of several leading networking, switch and UTM appliance ODMs/OEMs.**

This paper explores how the T9000 family delivers incremental value in network devices through security implementation and application processing, including XML/Web services application processing. Its

### Key Messages

- Designers of network security devices require solutions that can keep up with increasing traffic, proliferating threats and continual diversification of protocols, without performance penalties.
- Tarari’s T9000 Family of Content Processor ASICs offers these designers the greatest commercial potential by combining the breadth of an appliance, the performance of a chip and the flexibility of Tarari’s content processing engine in the optimal network security component.
- Network security and XML application processing are growing closer and will soon be inseparable. In fact, XML application processing represents a significant advance and a significant differentiator for device vendors in the current generation of network technology.

objective is to explain how devices built around the T9000 family provide the broadest, deepest range of security and processing for traditional network functions and XML with substantial business benefits.

## **Background**

### ***Device Manufacturers – Chasing the Value-Add***

Network equipment vendors are constantly trying to add more value to their platforms to satisfy customers and boost profits. The compelling technology-need, of course, is driven by traffic, network growth, and the spiraling dependence on moving data, and the resulting opportunity is for vendors to meet that need and deliver real value. These vendors are finding more and more opportunity for value expansion (new markets, better profit margins, competitive advantage) in the increasingly important area of network security.

Consider the evolution of traffic management in network equipment, driven by the expanding reach and versatility of the network and the need for more bandwidth. First, hubs were broadcast devices, taking packets in and forwarding them to all points downstream. Next, equipment vendors saw the chance to add value by forwarding packets to only the destination IP address, thereby reducing wasted bandwidth, and the switch came to market. Then came VLANs, which allowed a single switch to behave like multiple, virtual switches, connecting devices on different segments. Manufacturers will continue to find new ways to add value for their customers and profit for themselves in higher performance and added features.

There are two key areas in which vendors will add value in the current generation of network devices: securing network traffic as the vendors and customers have long known it; and extending network security

value to application processing, especially for XML/Web services applications.

XML application processing represents a significant advance and a significant differentiator for device vendors in the coming generation of network technology.

### ***Content Processors – More Work in Smaller Packages***

The evolution, proliferation and variety of network threats have increased the security demands on network devices. Meeting these threats year upon year means that these devices must examine a wide variety of traffic (e-mail, HTTP, XML) on several levels (headers, payload, messages) against increasing numbers of patterns (viruses, intrusions, attacks, spam), yet meet users' expectations of acceptable rates of throughput.

As designers of network devices have seen, these security demands are extremely compute-intensive in that the most common algorithms for addressing security threats – regular expression processing, DES (Data Encryption Standard), encoding/decoding – require high numbers of processor cycles per byte of data processed. Inspecting more bytes of data naturally consumes more cycles, which leads to bottlenecks: performance bottlenecks on the CPU and traffic bottlenecks throughout the network.

### ***Approaches to Acceleration***

Most methods of accelerating security focus on offloading the work from the CPU to other, more efficient resources, as described below.

	Performance	Flexibility	Price/ Performance Ratio	Small Form Factor
Software on Host CPU	◆◆	◆◆◆◆	◆◆	◆◆◆◆◆
Dedicated Network Appliance	◆◆◆	◆◆◆◆	◆◆◆	◆
Reconfigurable Logic in Silicon	◆◆◆	◆◆◆◆◆	◆◆◆	◆◆◆
Content Processor ASIC	◆◆◆◆◆	◆◆◆◆◆	◆◆◆◆◆	◆◆◆◆

**Table 1 - Approaches to Acceleration**

- Software acceleration running on the host CPU is a flexible, quick fix, but its power-to-performance ratio does not scale to fit the ever increasing cost pressures faced by large-scale switch manufacturers.
- Dedicated network appliances are flexible, but their footprint is large, making it impractical for organizations to deploy them at every potentially vulnerable port on the network.
- Reconfigurable logic in silicon offers similar flexibility and performance, though its cost is better suited to dynamic, high-end devices than to low-end, commodity devices.
- Dedicated content processor boards such as Tarari’s RAX (Random Access XML) and RegEx (Regular Expression) Content Processors deliver high performance and high flexibility, targeted at devices with a PCI slot.
- Content Processor ASICs embody the best of all categories – especially price/performance ratio - with the greatest commercial advantage over time and production volume.

***Tarari Content Processor ASICs***

These approaches have evolved, then, into Tarari’s T9000 Content Processor ASICs, which combine chip-caliber performance, the flexibility

of nine different on-board security acceleration algorithms and the interface to dozens more, high efficiency of manufacture, and the small form factor required for board-level integration as a component.

In the same way that each step in the evolution of traffic management devices (hubs, switches, VLANs) was marked by a new chip, Tarari's T9000 is the chip that marks the evolution in devices to the twin value-add of network security and application processing.

## **Network Security – The Defense Never Rests**

### ***The Threat Landscape***

Here is a summary of common threats against which security appliances must defend the network:

- Intrusions - The adverse effects of intrusions are well known: loss of network bandwidth because of saturation with bad packets, compromise of sensitive information such as passwords and consumer data, and loss of time and resources amounting to billions of dollars in widespread intrusions.
- Viruses - The threat-landscape here is a function of platform and application, with viruses spreading close behind the growth of devices (mobile phones, handheld computers, smartphones), transports (Bluetooth, MMS) and applications (Internet Relay Chat, instant messaging).
- Spam – As unsolicited, bulk e-mail continues to increase in volume, the level of annoyance and lost productivity rises. While the nature and effects of other threats are more vague to end-users, unfiltered spam makes it all the way through to the inbox, revealing network vulnerability at its most conspicuous.

- Threats have evolved from viruses and exploits to encompass spam, privacy and even compliance.
- With Web services and XML comes a parallel set of threats and exploits beyond the scope and protection of traditional network security solutions.

- XML Attacks – Vulnerabilities in XML have given rise to the category of security known as XML Threat Management (XTM). XTM defends applications against parsing attacks such as XML Denial of Service (XDoS) due to poorly encoded messages, oversized payloads and massively nested data.

### ***New Dangers***

The foregoing list points not only to traditional, network-based threats, but also to emerging ones.

The migration to Web services applications has led to growth in XML traffic, with accompanying growth in network threats. In fact, many of the traditional gaps that network security technology had begun to plug (viruses, spam, DoS) have now become exploitable again through XML and Web services. As the adoption of XML and Web services continues to grow, such vulnerabilities will become better known, to the point where concerns for traditional network security and XML security will no longer be separate.

Furthermore, emerging business drivers like data privacy, transaction monitoring and regulatory compliance are becoming urgent enough to seem like threats. Because the territory is relatively uncharted and the swath of regulation so wide, companies are scrambling to respond – much as they have done in the face of network threats – to the dual challenge of multi-billion-dollar spends<sup>1</sup> and uncertainty in the selection and deployment of security tools.

OEMs, ODMs and Independent Software Vendors (ISVs) counter these threats with a wide range of solutions, from low-end software on a

---

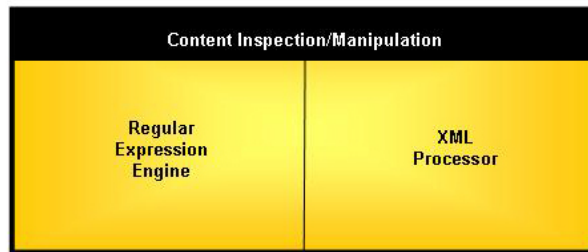
<sup>1</sup>AMR Research, “Spending in an Age of Compliance,” by John Hagerty and Fenella Scott, 2005.

general-purpose CPU to carrier-class security appliances. The Tarari T9000 Family of Content Processing ASICs is ideally suited to any of the solutions in this range.

## Meeting the Threats with the Tarari T9000 Family

### *Built for Content Inspection*

At the heart of the T9000 are two key engines, as described in Figure 1:



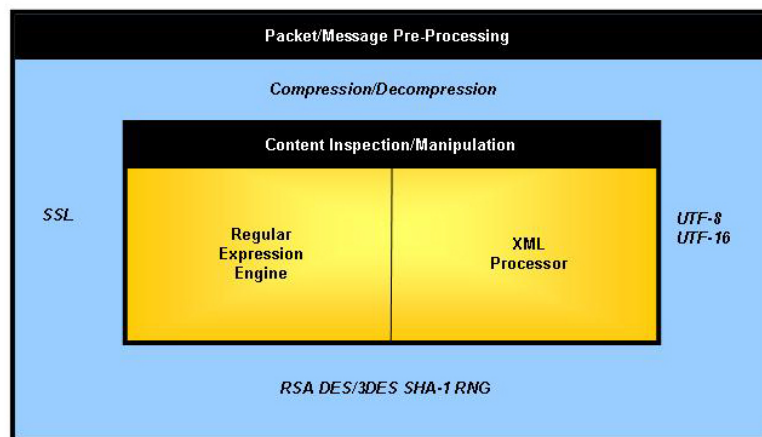
**Figure 1 - Silicon Components, Content Inspection**

The Tarari T9000 embodies an entire library of intellectual property designed to inspect, evaluate and manipulate content in packets and messages. The core technologies behind this library are the Regular Expression (RegEx) Engines and the XML Grammar Processors.

- The **RegEx Engine**, comprising single or dual regular expression cores, is designed for simultaneous evaluation of up to 50,000 POSIX 1003.2-formatted regular expressions total, at up to 3.2 Gbps overall throughput. With support for nested hierarchical start conditions, macros, comprehensive/longest match modes, and complete/short/bit vector match result options, the engine is ideal for HTTP and MIME parsing, content routing and application content filtering.

- The **XML Processor**, comprising two agents, provides data stream parsing/tokenization and stateful grammar analysis for decomposing and processing XML application protocol grammars. Its microcode-programmable engine allows for field updates as XML grammar and constructs evolve. Two independent execution threads process at 1.25 Gbps each, for up to 2.5 Gbps of overall throughput.

The T9000 next capitalizes on these high-performance, dedicated engines to do the heavy lifting of pre-processing packets and messages, as depicted in Figure 2:



**Figure 2 - Packet/Message Pre-Processing**

This pre-processing paves the way to optimized versions of several of the most CPU-intensive algorithms used in scanning, parsing and filtering data:

- The **Compression and Decompression Agents** support the underlying algorithms (as outlined in RFC 1951) used in popular lossless data compression tools such as zlib, zip, gzip, PKzip and WinZip. The Compressor, which implements the deflate algorithm, can absorb uncompressed input data at up to 1 Gbps. The Decompressor, which implements the inflate algorithm, can output decompressed data at up to 4 Gbps.

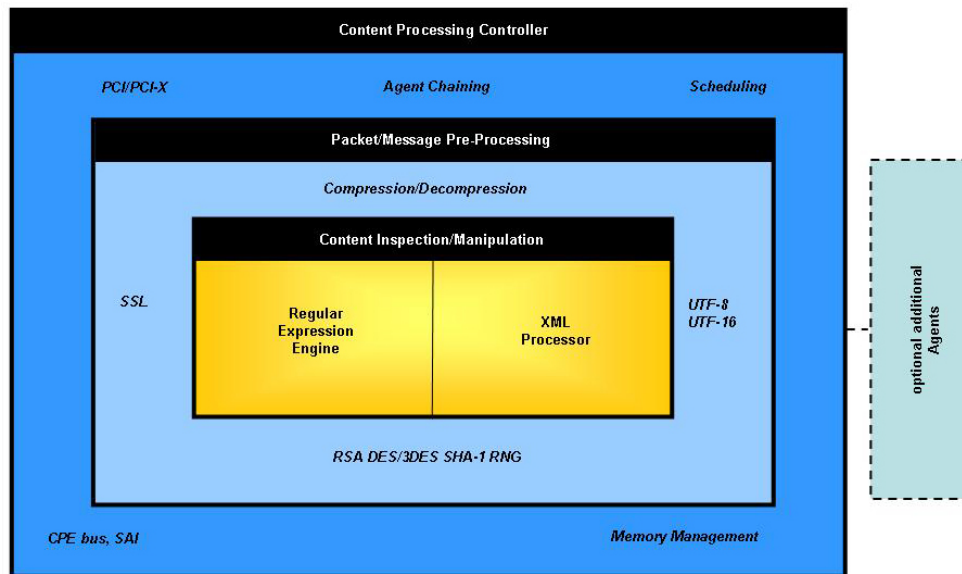
- The **Character Conversion Agent** provides rapid conversion of UTF 8 characters to UTF 16 characters to support Grammar Processing at up to 1 Gbps.
- The **RSA Agents** provide modular exponentiation of input files of any bit-length between 16 and 2048, in increments of 16 bits. These agents can be used to accelerate the Rivest-Shamir-Adleman (RSA) public-key cryptographic algorithm. RSA is widely used in modern cryptographic protocols, especially for the purpose of securely exchanging keys for faster bulk-encryption algorithms, which is its function in SSL. The RSA agents can collectively perform modular exponentiation calculations at 2000 Tps (transactions per second).
- The **Encryption/Decryption Agents** perform bulk-data, symmetric key encryption and decryption conforming to the Data Encryption Standard (DES) at 1 Gbps. The algorithm uses at least one 56-bit key in DES mode and three keys in triple-DES mode. The agent supports ECB (Electronic Codebook) and CBC (Cipher Block Chaining) variants of both single and triple-DES modes.
- The **Secure Hash Generator (SHA-1) Agent** condenses a file of arbitrary size into a 20-byte message digest or hash, according to the Secure Hash Standard, FIPS PUB 180-1. The SHA-1 Agent computes hashes on input data at rates of up to 1 Gbps.
- The **Random Number Generator Agent** uses hardware to synthesize truly random numbers at up to 1 Gbps for seeding cryptographic keys or any other application requiring large, random integer numbers. An external input is provided for accumulating entropy to help further seed the generator.

**The  Advantage**  
The Acceleration Company

On-board agents for:

- Compression/Decompression
- Character Conversion
- RSA
- Encryption/Decryption
- Secure Hash Generation (SHA-1)
- Random Number Generation

Finally, the T9000 wraps these engines and agents in the Content Processing Controller (CPC), which provides the interface for them to work with the outside world, as shown in Figure 3:



**Figure 3 - Content Processing Controller**

The CPC handles PCI/PCI-X interface, agent chaining, scheduling and memory management. Most important, the CPC provides access to the Content Processing Engine (CPE) bus and additional off-chip resources. This means that the T9000 can control up to two external CPEs with as many as 64 content processing agents to accommodate:

- thousands of additional regular expressions or rules
- additional custom agents
- higher throughput

The ability of the T9000 to control off-chip agents is what allows for in-field, real-time programming changes to meet the needs of network security and application processing. This combination is unique in the realm of acceleration: The Tarari T9000 delivers the arsenal of basic tools required to combat the most prevalent threats to network and XML security with the *price/performance ratio of an ASIC*, while

accommodating an upgrade path with the *flexibility of reconfigurable logic*.

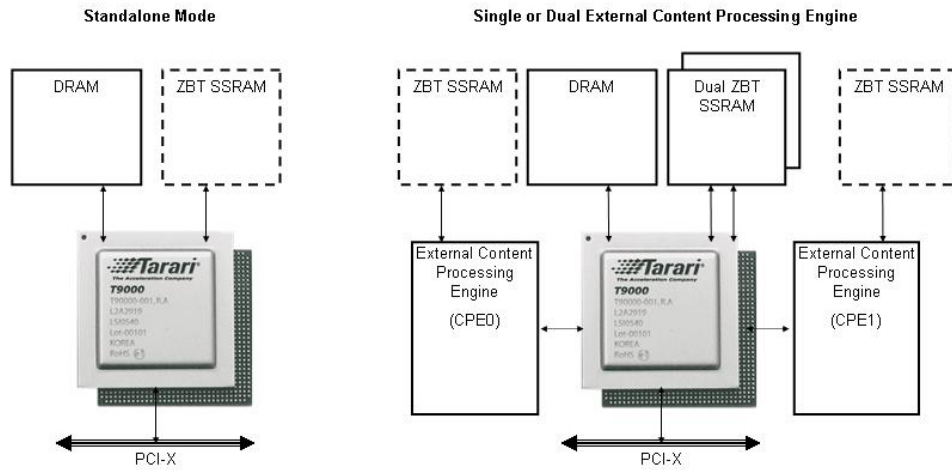
### **T9000 Features**

The T9000 ties together the functionality of these agents with a set of advanced, on-chip features representing the power and breadth of technology normally contained in at least four separate chips with independent functions.

- DRAM controller - Eliminates redundant, in-out data transfers. This allows the T9000 to operate on the same dataset through multiple agents and loops on the chip, without the need to send the dataset back to the system.
- Autonomous agent load balancing – Minimizes processing interrupts and leverages all resources on the ASIC automatically.
- Agent chaining – Allows on-chip processing of multiple tasks in a series without host intervention.
- Support for external FPGA logic – Offers complete infrastructure to configure and leverage multiple vendors’ off-chip resources (e.g., FPGAs) as CPEs, paving the way for upgrade and expansion (more agents, new standards, additional processors). External agent logic behaves identically to the internal agents (access to load balancing, DRAM, management, API, etc.).

#### **The Advantage** The Acceleration Company

- Tarari’s T9000 outstrips “baked-in” ASIC solutions by allowing access to expandable, flexible, off-chip resources.
- On-chip agents deliver the range of network security functions normally available in four separate chips.
- T9000 combines the business benefits of an ASIC with the engineering benefits of reconfigurable logic.



**Figure 4 - External Logic**

- API compatibility – Provides a single interface to other Tarari product families (software, coprocessor board, ASIC) and solution footprints (entry-level device to network appliance), reducing engineering costs.
- PCI-X host interface – Applies to a broad range of host processing solutions.

**T9000 Family**

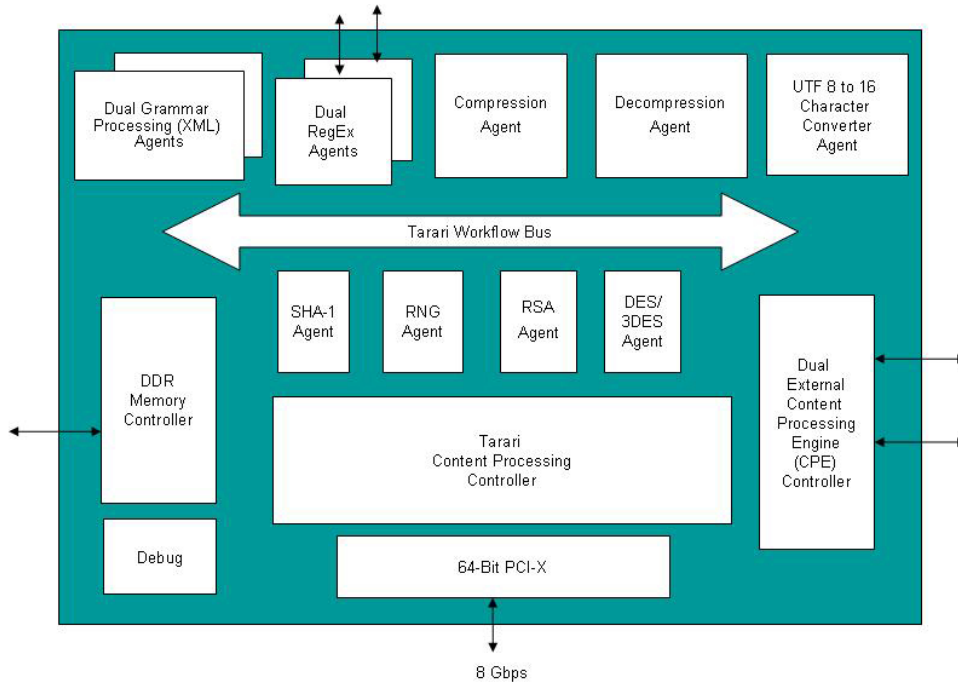
Tarari has anticipated market needs and created a family of ASICs based on performance and application, each endowed with cryptographic and compression/decompression agents, and full CPC functionality:

Network Security	XML App Processing	Network Security plus XML App Processing
<b>CPA9213</b> 3.2 Gbps RegEx	<b>CPA9221</b> 2.5 Gbps RAX	<b>CPA9790</b> 4-6 Gbps RegEx 3-5 Gbps XML Dual CPE Type1
<b>CPA9113</b> 1.6 Gbps RegEx	<b>CPA9121</b> 1.2 Gbps RAX	<b>CPA9590</b> 3.2 Gbps RegEx 2.5 Gbps XML

**T9000 Architecture**

As a highly integrated processor, the T9000 relies on a set of independent agents, each of which performs a specialized function. These agents are bound together by the Tarari Workflow Bus, a DDR Memory Controller and a PCI-X system interface that includes a sophisticated DMA engine.

**Functional Description**



**Figure 5 - T9000 Simplified Block Diagram**

**64-Bit PCI-X System Interface**

The PCI-X System Interface consists of a Target Interface and a DMA Controller. The Target Interface is accessed by the host bridge to perform initialization, configuration and diagnostics on the T9000. The DMA engine is used during system operation to coordinate the movement of data and job control information between host memory and the T9000.

### *DMA Controller*

To improve efficiency, the T9000 becomes a PCI-initiator (master) to write and read bursts of data to and from the Host-Bridge (target). The DMA engine is controlled by descriptors stored in host memory. When kicked off, the DMA engine fetches as many valid descriptors as it can and then begins processing them in order. Each descriptor points either to a data file in main memory to be fetched and transferred to the DDR SDRAM connected to the T9000, or it points to a file in the DDR SDRAM that is to be transferred to host memory.

### *DDR Memory Controller*

The Memory Controller allows the T9000 to be connected to a variety of DDR-1 SDRAM devices that support different speeds, latencies and form factors. The interface is optimized to connect directly to PC2100, PC2700 and PC3200 200 pin SODIMMs. It is also possible to connect directly to individual on-board DDR SDRAM devices. The device can physically address up to 8 GB, with a recommended minimum of 256 MB.

### *Tarari Workflow Bus*

The Tarari Workflow Bus performs two fundamental functions by:

1. Arbitrating for access to the DDR SDRAM between agents and the DMA controller;
2. Distributing the memory read return data and inter-agent communication commands to their proper destinations (DMA or agents).

### *Dual External CPE Controller*

The T9000 connects to external agents in the optional Content Processing Engines (CPEs) through a high-speed interconnect called the Content Processor Interface (CPI) bus. The T9000 has two CPI buses, used to connect to agent sets located in the two external CPEs. It gives each of these external agents the same access to T9000 resources that

the internal agents have. Each CPI bus consists of two unidirectional, source-synchronous Double Data Rate (DDR) buses. Each half of the bus is 38 bits wide and can transfer data at up to 10.6 Gbps in each direction, or 21.2 Gbps total (full-duplex bus).

**Regular Expression Agent SSRAM Interfaces**

The external SSRAM (Synchronous Static Random Access Memory) interfaces are needed whenever the Regular Expression Pattern Matcher agents are to be used. Each interface can use either 36 or 72 MB of Zero Bus Turnaround (ZBT), No Bus Latency (NoBL) or No Turnaround (NtRAM), pipelined SSRAM devices.

**T9000 Applications and Benefits**

Described in this section are typical models for integration of the T9000 in network security and XML processing, designed for a wide variety of applications, along with benefits realized from integration:

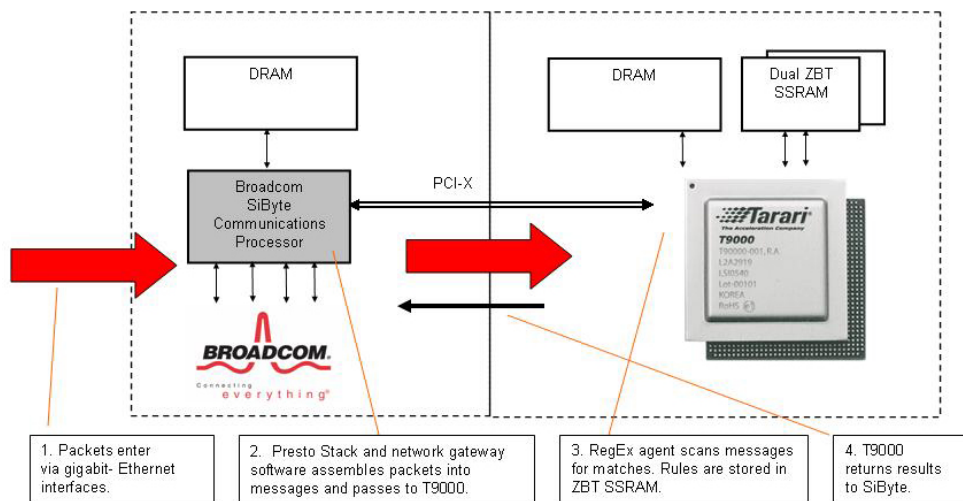
Intrusion Prevention	Anti-virus	Anti-spam
Anti-Spam for SMS/Text Messaging	Instant Messaging Filtering	Compliance
Security Event Management	XML Security	Content-based routing
Publish/Subscribe	XML Parsing Offload	XML Firewalls
Content Compression	VOIP	Content filtering
Mobile filtering	Real-time reporting	Ad Hoc Reporting/ Datamart

**With Communication Processors**

The T9000 is designed to run alongside industry-leading communication processors such as Intel, Broadcom Corporation’s SiByte™, Raza Microelectronics’ XLR™, Freescale Semiconductor’s PowerQUICC™, and other x86, MIPS, ARM, or PowerPC-based communication processors. It also supports general-purpose processors such as the Intel® x86. Tarari provides the software stack for direct integration with these chips in appliances and gateways.

### Tarari-Broadcom Integration

As depicted in Figure 6, Broadcom's SiByte communications processor lives at an optimal point in the network for integration with the T9000. In this reference design, the SiByte terminates the transport protocol, assembles messages and passes them across the PCI-X bus to the T9000 for deep content inspection against security rules stored in ZBT SSRAM. The T9000 hands the results back to the SiByte, which handles the message accordingly.



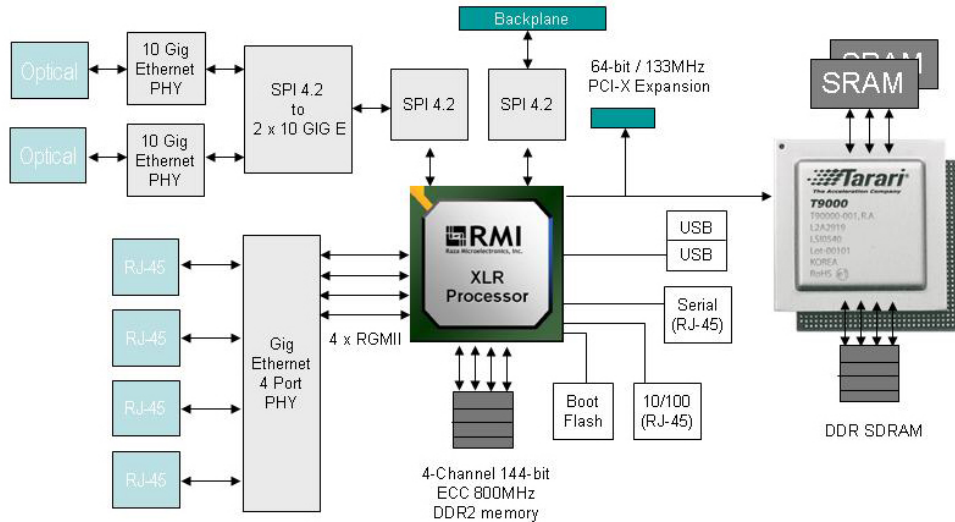
**Figure 6 - T9000 and SiByte**

In tandem with the SiByte's high-performance, high-function integration and low power consumption, the T9000 adds valuable offload at the gateway, to keep compute-intensive security operations from ever reaching the CPU.

**Benefit:** In-process, application-specific acceleration means higher profit margin and value-add to SiByte solution.

### Tarari-RMI Integration

Figure 7 depicts the integration of the T9000 with the XLR processor from Raza Microelectronics Inc. (RMI).



**Figure 7 - T9000 and XLR**

The XLR family of thread processors enables such solutions as security (firewall, VPN, anti-virus, intrusion detection and prevention), Web services, virtualized storage, load balancing, server offload and intelligent routing and switching. At the heart of these solutions are the same drivers as those behind the T9000 – content-awareness and application intelligence – so the Tarari-RMI fit in network appliances is ideal.

In this reference design the T9000 offloads and accelerates network security and Web services operations directly from the XLR processor, freeing cycles for traffic processing. The T9000’s memory controller provides memory access interface and memory management logic for off-chip Synchronous Dynamic Random Access Memory (SDRAM).

**Benefit:** No need to modify XLR processor to handle additional operations, because T9000 handles them.

*Conventional Server Integration*

The T9000 can also be integrated to motherboards with Intel-based x86 processors like Pentium Mobile or Xeon, connected by the Southbridge

PCI-X interface. OEMs can deliver this Tarari-accelerated solution as a conventional server platform, commonly adopted as network security appliances.

**Benefit:** Longer useful life of low-cost x86 processors, which offload security functions to T9000.

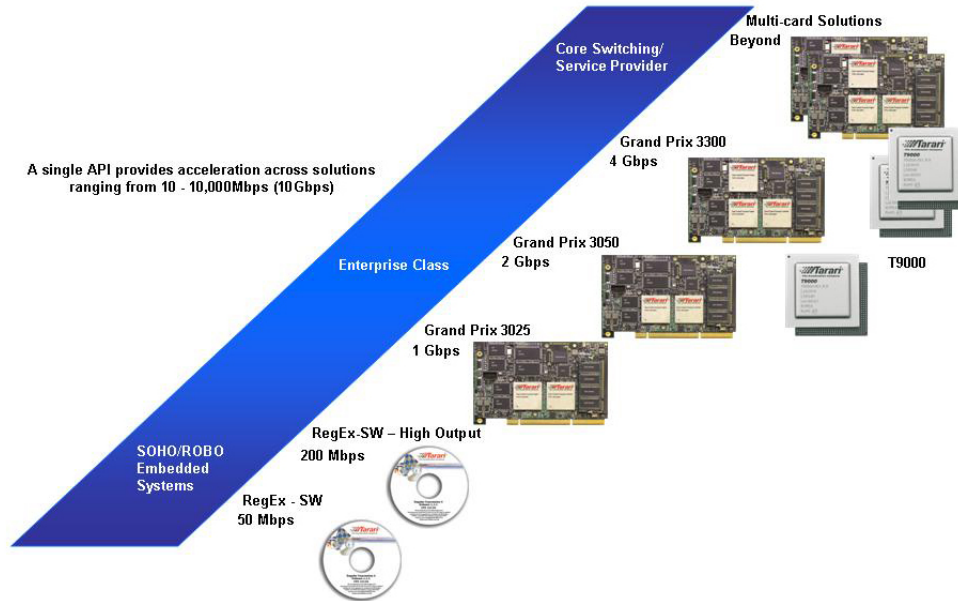
*Scalable from 10Mbps to 10Gbps with a Single API*

Tarari's family of acceleration products comprises not only the T9000 ASIC, but also software libraries and Content Processor boards, allowing the close fit between Tarari and RMI to scale from entry-level devices to high-end appliances (Figure 8).

- SOHO/ROBO embedded systems – Low price-points, stiff competition and soft performance requirements call for the 8-thread XLR processors, with security accelerated by Tarari's software.
- Enterprise-class devices – Mid-range platforms call for 16-thread XLR processors, accelerated by Tarari's Content Processor boards or T9000 ASIC.
- Core switching and service provider appliances – Carrier-class equipment calls for 32-thread XLR processors, with T9000 ASICs and multiple Content Processor boards for access to extensive off-chip resources.

**The Tarari Advantage**  
The Acceleration Difference

- Tarari lowers engineering costs by providing a single code line and API on which to develop a broad range of solutions.
- Vendors can take their existing technology and easily enter new markets at high, middle and low ends.
- This scalability benefits development around Tarari's entire family: software, content processor boards and ASICs.



**Figure 8 - Scaling with Tarari**

Finally, this entire scale of solutions for network security and XML application processing is accessible through a single API.

**Benefit:** Single code base and development effort for all platforms from 10Mbps to 10Gbps.

***Combined Software-Hardware Solutions***

Another opportunity for ODMs to add value lies in bundling security software with the hardware platforms described above. In this model, depicted in Figure 9, communication processors handle incoming packets and offload security tasks to recognized software applications (anti-virus, anti-spam, intrusion prevention/firewall) accelerated by the T9000.

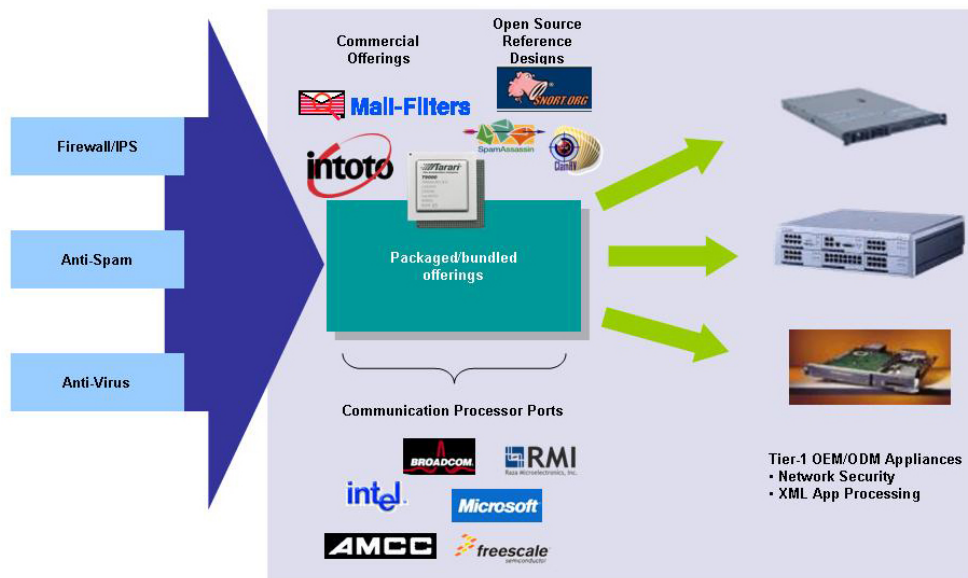
Tarari has already built relationships with OEM software providers and tested a number of commercial security applications:

- Intoto’s IntruPro IPS – a fully integrated, NSS-approved intrusion prevention software suite

**The  Advantage**

- Tarari’s integration with existing security software means shorter time to market for OEMs/ODMs.
- Commercially proven network security software offers strong product differentiation against open-source solutions.

- MailFilters.com's Anti-Spam – an extremely high-speed, small-footprint solution for appliance vendors and embedded environments
- Kaspersky Lab's Anti-Virus - multi-tier detection, flexible settings, regular updates and versatile administration tools for effective protection against spam



**Figure 9 - Packaged/Bundled Offerings**

Because Tarari has already done the integration work with these applications, they are immediately marketable by OEMs in these bundles for use in tier-1 appliances performing network security. These bundled, value-added products give channel partners a strong market differentiator by offering features not available from other sellers in the same channel.

This offering is an updated model with precedent in the evolution of personal computing. Microsoft and Intel demonstrated a strongly symbiotic relationship in their respective development of software and hardware as they worked towards a platform that interoperated and served specific business needs in the enterprise. Similarly, Tarari and its

OEM software providers offer the comprehensive network security/XML application processing platform that will be of greatest impact in tomorrow's security appliances. In the rapidly evolving world of network security, this type of relationship between Tarari and its OEM software providers gives vendors a seamless, comprehensive implementation of software and hardware and compelling added value.

### **More Resources from Tarari**

Tarari has developed its own security software for XML application processing, optimized for Tarari hardware and software:

- XSLT (eXtensible Stylesheet Language Transformation) – optimized for Web services and transactional XML processing, delivering performance gains of 60 to 3500% over most widely used XSLT software engines
- XDoS (XML Denial of Service) Detection - defense against XML-borne attacks (e.g., recursive payload, element/attribute name size, jumbo payload, etc.) and support for XML-specific security standards (e.g., well-formedness, SOAP validation) at network speeds
- Schema Validation – high-level message verification with pre-compiled, cached grammars to protect against schemas imported from unauthorized locations

Tarari also offers a full range of reference materials, technical collateral, reference designs and prototype circuit diagrams for use in building platforms around the T9000. These materials represent Tarari's several generations of intellectual property and experience in acceleration technology.

### **Conclusion**

Tarari is the fast lane to the new value and revenue opportunity of combined, wire-speed security for traditional IP traffic and XML application processing. By providing the broadest functionality in a

#### **The Advantage**

- Tarari's applications support the intertwined needs of traditional network security and XML application processing.
- The T9000 opens up opportunities for XML security revenue to vendors of traditional security devices.

single ASIC, the T9000 fulfills an as yet unaddressed market need and enables OEMs to adopt proven technology in a reduced form factor and cost of goods sold. Vendors benefit from broader and deeper revenue opportunities, and customers benefit from greater security with no performance penalty.

## Legal Information

Tarari is a trademark or registered trademark of Tarari, Inc. or its subsidiaries in the United States and other countries.

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

Copyright © 2002-2007 Tarari, Inc. All rights reserved.

\* Other names and brands may be claimed as the property of others.

\*\* Performance tests and ratings are measured using specific computer systems and/or components, and reflect the approximate performance of Tarari products as measured by those tests. Any difference in system hardware or software design or configuration can affect actual performance. Buyers should consult other sources of information to evaluate the performance of components they are considering purchasing. For more information on performance tests, and on the performance of Tarari products, contact us as indicated below.

# The T9000 Family of Content Processor ASICs

*Accelerated Network Security on an ASIC*

*A Tarari Whitepaper*

Additional information: [info@tarari.com](mailto:info@tarari.com)

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

Telephone: (858) 385-5131

Tarari, Inc.

10908 Technology Place

San Diego, CA 92127-1874

USA

