Tarari®
The Acceleration Company

Accelerating the Unified Threat Management Platform

Broad, Deep Network Protection at Wire-Speed

A Tarari Whitepaper

Table of Contents

Overview

With looming threats from all quarters, enterprises rely heavily on three core technologies for network security:

- intrusion prevention
- anti-virus
- anti-spam

Although no self-preserving organization would operate its network without any of these solutions, maintaining them individually has become burdensome. The proliferation of items to manage adds almost as much complexity as the original security problems.

The market has evolved towards Unified Threat Management (UTM)[1], in which a single appliance embodies these core security technologies. Hosted in a single network device, rather than in separate ones, the UTM appliance reduces the number of items to manage while maintaining resilient security.

Combining core security technologies in one device, however, creates a performance problem. Processing a constant stream of packets and inspecting them deeply for such different types of malicious content is very compute-intensive. It can also be resource-

Key Messages

- The variety in network threats calls for a diverse set of defenses.
- Maintaining these defenses has become a burden on network administrators, who want unified threat management (UTM) – multiple defenses in a single appliance.
- Combining in a single appliance the content processing work demanded by such diverse defenses results in a performance penalty.
- Tarari’s Regular Expression Content Processor (RegEx-CP) provides the acceleration, processor offload and scalability needed to make the UTM a viable player in network security, whether in 10Mbps, low-end devices or in carrier-class network appliances.

[1] Term coined by Charles Kolodgy in the IDC Research report “Worldwide Threat Management Security Appliances 2004-2008 Forecast; The Rise of the Unified Threat Management Security Appliance,” (#31840) September, 2004

intensive, requiring high-end hardware. Only dedicated acceleration inside the UTM appliance can remove the trade-off between security and performance.

The Tarari Regular Expression Content Processor (RegEx-CP) is the ideal complement to the UTM solution. RegEx-CP accelerates the compute-intensive evaluation of inbound packets on the network and offloads the resource-intensive heavy lifting from the host processor. For OEMs and vendors of UTM hardware, Tarari's RegEx-CP scales from entry-level embedded devices to carrier-class, multi-gigabit appliances.

This paper describes a reference model of a UTM appliance comprising intrusion prevention, anti-virus and anti-spam, accelerated by Tarari.

The UTM Appliance - Background

Evolution

Several computing-generations ago, "sneaker-net" was the greatest threat and network security was little more than a matter of running widely available anti-virus software to keep desktop machines safe from floppy-borne viruses. As commercial use of the Internet grew, it became necessary to deploy a firewall to defend the network from unwelcome intrusions. Later came unsolicited, bulk e-mail, which soon had network administrators deploying anti-spam products to keep it from bogging down traffic and needlessly filling users' inboxes.

The threats have evolved separately, and while all are equally dangerous, no single solution suffices to combat them equally. Device manufacturers have offered separate products as software, hardware and software-on-hardware, and users have implemented them in "layers": an appliance for intrusion prevention, a device for anti-spam, a server for anti-virus, and so on.

The network administrators charged with running this equipment now find it burdensome. With each new layer of security comes a new layer of administrative complexity - vendor relationships, service contracts, power requirements, cooling needs, software upgrades, operating system patches - and the resulting patchwork quilt of security devices weighs on the network as much as it helps to defend it.

Administrators would prefer to view security holistically. They want to see core security technologies converging in fewer devices - preferably one device - moving further into the network infrastructure. Threats come from different sources, take different forms and cause different kinds of trouble, yet still end up in the same place, and so technology and the market have shifted beyond server-centric security in the network to unified threat management (UTM).

Market Outlook

Growth in the market segment since 2003 has come to outpace that of traditional security solutions. In 2004 the segment grew by over 200%, exceeding $300M in revenue. The market for integrated security devices including UTMs has been estimated at $3.3 billion by 2009.[2]

There has also been growth in the number of vendors entering the market: In 2003 there were seven named vendors and in 2004, twelve vendors, with prospects for doubling by 2006.[2] The UTM market is extremely competitive.

The concept of one appliance with multiple security technologies is very popular with small- and medium-size vendors, and larger customers who have many branch and remote facilities.

Form Factor

The goal of the UTM platform is to protect the entire range of networks, whether in global enterprises or in small-office-home-office/remote-office-branch-office (SOHO/ROBO) organizations. Each of the core security technologies is readily available in solutions that protect all the way up and down the scale; however, most device manufacturers invest in developing a solution for only a limited market segment (e.g., intrusion prevention appliance for the enterprise, embedded firewall in a SOHO device).

[2] “Integrated Security Appliances: SMBs Fuel Explosive Growth,” In-Stat, (#IN0501820LN) February 2005

The prohibitive cost of developing and testing a UTM solution that suits all form factors restricts the markets which a vendor can profitably enter and results in few vendors being able to reach the entire range of networks.

The UTM Appliance - Components

UTM appliances deliver the core technologies of network security in a single box, with network-based security updates. By definition, not all of the capabilities in the appliance need be utilized, but the functions must exist inherently in the appliance, and the individual components cannot be separated.[3]

This reference model of a UTM appliance includes intrusion prevention, anti-virus and anti-spam.

Intrusion Prevention

An organization's first line of defense against the onslaught of network attacks is its intrusion prevention system (IPS). A robust, properly configured, frequently updated IPS can shield a network from the most destructive attacks perpetrated by today's and tomorrow's hackers, whether inside or outside the network.

The most common types of intrusion are:

- Reconnaissance intrusions, in which a hacker is probing for vulnerabilities by using ping sweeps, DNS zone transfers, email reconnaissance, TCP/UDP scans, and indexing of public web servers for CGI holes.
- Exploits, which take advantage of software features and bugs to gain unauthorized access to the system, send large amounts of data to known buffer-overrun holes, check login accounts by guessing passwords and spoof packets to cause multiple replies to a host from a single packet.
- Denial-of-service (DoS) attacks, aimed at disrupting the services in a system by crashing services, overloading the CPU or network links, or filling a disk to capacity.

[3] IDC, September, 2004

The adverse effects of these intrusions are well known: loss of network bandwidth because of saturation with bad packets, compromise of sensitive information such as passwords and consumer data, misinformation due to tampered Web sites, and loss of time and resources amounting to billions of dollars in widespread intrusions.

> The value of the intrusion prevention system lies in its ability to process the content of each packet against thousands of patterns defined by signature rules.

Market Requirements

The market's desire for network safety from intrusion means:

- keeping the network free from rogue packets and harmful traffic
- ensuring that good packets are not discarded with the bad ones
- dealing with security in a way that does not materially impact network throughput
- allowing for easy maintenance and administration

Product Requirements

Ironclad intrusion prevention can be as simple as unplugging the right cable, but the downside of zero-throughput is unacceptably steep. To meet market needs, then, a product must:

- accurately identify an intrusion through rigorous pattern-matching algorithms
- analyze potential intrusions deeply enough to keep false-positives to a minimum
- adapt quickly to the ever changing threat-landscape
- preserve network throughput

At the center of all of its various features and strengths, the value of the intrusion prevention system lies in its ability to process the content of each packet against thousands of patterns defined by signature rules. Executing this evaluation step quickly and accurately is a key market requirement.

Anti-Virus

More familiar to the user, though just as annoying to the administrator, is the network-borne virus. "Virus" is a generic term, covering many different types of malware – classic viruses, Internet and email worms, Trojans, backdoors, hacker utilities, joke programs, misinformation-ware – that circulate amid otherwise innocent traffic.

The threat-landscape 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). In 2003, Sobig.F spread via email messages generated by stealing addresses from victims' computers and propagated so rapidly that at one point, one out of every 17 email messages traveling through the internet was a copy of Sobig.F. Estimates of worldwide damage from attacks in 2003, including clean-up and lost productivity, were on the order of $82 billion.[4]

Again, the value of an anti-virus solution in the UTM platform depends heavily on how quickly it is able to process content, match patterns and calculate checksums to protect the network from viruses.

Market Requirements

Whether sweeping through enterprises around the globe or frustrating individual home users, viruses remain a persistent threat which security software must identify and eliminate. Key market requirements are:

- quick, accurate identification of viruses
- prompt inoculation/removal of infected files
- frequent updates to virus profiles
- low impact on normal user/administrator tasks

Product Requirements

To meet the challenge of combating an ever-growing number of viruses, security software vendors must:

- offer solutions all along the path from the desktop to the edge of the network

[4] Computer security firm mi2g, cited in "The Enemy Within," Clive Thompson, The Guardian, February 2004

- develop a scanning engine that accurately and quickly compares virus signatures to file content
- ensure that the heuristic analysis used to supplement pattern-matching does not slow scanning
- update virus signatures in immediate response to emerging threats
- build in the capacity for automatic update/upgrade of virus signatures

Again, the value of an anti-virus solution in the UTM platform depends heavily on how quickly it is able to process content, match patterns and calculate checksums to protect the network from viruses.

Anti-Spam

While there is no easy way to gauge the volume of e-mail messages sent in any period of time, one estimate puts it at 68 billion per day worldwide for the year 2004. It is even harder to estimate the percentage of that e-mail which is unsolicited, bulk e-mail ("spam"), although a conservative, published estimate puts it at 52%. Anecdotally, of course, any user with a known e-mail address and an unprotected inbox can attest to the high volume of spam s/he receives on any given day, but even after deployment of a filter at the gateway, up to 17% of the messages that arrive in corporate inboxes are still spam. Furthermore, about 45% of all e-mail inboxes are not protected by a spam filter.[5]

Market Requirements

The market's requirements are simple: It wants spam to simply go away. The market's paramount requirements tread a careful trade-off between thoroughness and accuracy, and point to a spam filter that:

- traps and discards the majority (>95%) of spam, without obliging the user to review the messages or train the filter him/herself
- generates few (<1 in 100,000) false-positives; that is, does not accidentally misidentify a valid message as a bad one

[5] All figures in this paragraph attributed to "Anti-Spam Market, 2004-2008," The Radicati Group, Inc.

Other requirements include:

- stopping messages at the network perimeter, rather than at the inbox
- analyzing messages with no performance penalty
- consuming little of the administrator's or user's time
- being part of an integrated security solution

Product Requirements

From the product perspective, spam filtering is not an automatic process. Several approaches in anti-spam technology take aim at the two fundamental market requirements. Their market acceptance depends on the balance they strike between the spam they correctly identify and the valid messages they misidentify, so any spam filter is only as good as its ability to recognize and quickly match patterns in spam.

> Any spam filtering solution is only as good as its ability to recognize and quickly match patterns in spam.

The ideal solution:

- resides on the network it is trying to defend, rather than in the user's inbox
- automates the recognition of repetitive, slowly evolving patterns in spam, such as hash busting, snowflaking, embedded content and other tricks frequently employed by spammers
- also allows for the critical factor of human judgment, since there is a subjective dimension to recognizing spam
- does not place the burden of updating spam recognition patterns on users and administrators

Once again, at the heart of this balance of human intervention, constant updates and presence in the network is the compute-intensive task of content processing on the unceasing stream of incoming messages.

The Missing Piece – Acceleration

The common denominator in these core security technologies is *content processing*. Each technology depends on rules and policies, but content processing applies those rules and policies against the messages and packets moving around the network.

The UTM platform is an elegant composite of diverse security features, with one problem: The deep inspection of content and matching of patterns that used to be spread across several devices, now reside in a single device. Depending on the environment, the demands of the UTM can greatly increase the amount of content processing to be performed by the host processor. The bottleneck resulting from this increased workload violates one of the primary market requirements for each of the core technologies: thorough scanning of traffic for network threats with no performance penalty. To address the bottleneck, the UTM platform also needs acceleration.

The Tarari Solutions

If performance had not been an issue, the UTM would probably have made it to market long ago. Rounding out the platform in this reference model is Tarari's Regular Expression Content Processor (RegEx-CP), designed to offload the compute-intensive work of content processing from the UTM's host processor and to restore the UTM platform to acceptable performance levels.

In hardware, RegEx-CP fits in the PCI or PCI-X slot of a normal network appliance to offload content processing from the host processor, then to accelerate the evaluation algorithms using dedicated hardware, and finally to return the results of the evaluation to the security application running on the host processor.

Similarly in software, Tarari's RegEx-CP acceleration is available as standalone software for a competitive edge on low-end network devices and applications. The software libraries are the functional equivalent of the hardware, and offer a competitive edge on entry-level devices.

The bottleneck resulting from this increased workload violates one of the primary market requirements for each of the core technologies: thorough scanning of traffic for network threats with no performance penalty.

Scalability on a Single Code Base – The Tarari Advantage

Tarari's RegEx-CP offers another important advantage to vendors and manufacturers: a single code base on which to develop the UTM platform.

Until now, the challenge for vendors has been to scale a combined security solution across different environments (from SOHO/ROBO up to network switches) in order to increase market share and revenue. Even if the vendor reached the promised land of efficient content processing with desirable performance, there has been no easy way to duplicate that success across all market segments.

Using Tarari's content processing technology, which scales from the smallest networking devices to the largest, vendors can cost-effectively create combined solutions that offer networks of all sizes significantly greater security without degrading performance.

The Accelerated UTM Platform

Once accelerated, the UTM platform truly delivers the deep inspection of packets, messages and files required to protect the network.

- For intrusion prevention, the UTM device can inspect all fields in inbound packets and hand off the content to Tarari's RegEx-CP for accelerated comparison against an entire database of attack profiles. Positive results return to the host processor, where the main intrusion prevention application decides how to treat the offending packets.
- For anti-virus protection, the data stream moves through the UTM device to RegEx-CP for evaluation at the file level, which evaluates the files at wire-speed against a database of virus signatures and performs heuristic analysis on suspicious content. After evaluation, the anti-virus application running on the host processor takes prescribed action on any infected files.
- For anti-spam, inbound traffic recognized as e-mail goes across the UTM device to RegEx-CP, which evaluates patterns in the content against the database of spam signatures to identify offending messages. The anti-spam application running on the host processor reads in the returned values and applies policies to dispose of the message.

This combination of diverse tasks running simultaneously on RegEx-CP would overwhelm most host processors, which are already juggling threads from the operating system and applications. Yet with its capacity for up to 4Gbps of throughput and as many as 100,000 regular expression evaluations per second, RegEx-CP delivers on the robust security promise of the UTM platform.

Conclusion

Manufacturers of network security devices can now fulfill both the market's need for protection from threats and its need for speed. The UTM platform, accelerated with Tarari's RegEx-CP, blends protection from a variety of network attacks in a single appliance. With network security devouring an ever-increasing share of IT budgets, there is plenty of good reason to reduce complexity, and UTM is the new avenue of choice for reducing it.

Furthermore, RegEx-CP is available in software and hardware implementations, and both use the same code base and API. Tarari's RegEx-CP is the only content processing solution that allows manufacturers to pursue different markets all along the spectrum of price (low-end SOHO device to high-end, carrier-class appliance) and performance (10Mbps to 10Gbps) with a single engineering effort.

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 © 2002-2006 Tarari, Inc. All rights reserved.

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

This page intentionally left blank

Accelerating the Unified Threat Management Platform

Broad, Deep Network Protection at Wire-Speed

A Tarari Whitepaper

Additional information: info@tarari.com
Internet: www.tarari.com
Telephone: (858) 385-5131
Fax: (858) 385-5129

Tarari, Inc.
10908 Technology Place
San Diego, CA 92127-1874
USA

Tarari®
The Acceleration Company