Security Engine Technology for a Dependable, Safe and Secure Network Environment

KAMIYA Satoshi, UENO Hiroshi, YAMADA Kenshin, NISHIHARA Motoo

Abstract

In the next-generation network, different security levels are required for each segment of transport, network servers, network services, and enterprise networks. In order to achieve high-level overall security especially in the broadband environment where its line rate is above 10Gbps, multiple breakthroughs will be necessary in the various processing areas of network protocol processing, content check, and real-time monitoring of millions of sessions.

To achieve the breakthroughs, we have developed the security engine and related API/driver, and are hereby providing this paper. Furthermore, as system solutions utilizing our invention, we introduce 10Gbps intrusion detection system (IDS/IPS) and high-performance spam mail countermeasure system.

Keywords

network security, hardware engine

1. Introduction

Higher performance and more flexible security is required in the next-generation network than end-user security because of its vast traffic volume, repercussions to disturbances, and the need for confidentiality. Especially high-speed processing technologies aimed at broadband applications and the flexibility to meet the needs of evolving security systems are very important. Security Engine Technology is precisely the technology that addresses these issues. This paper introduces the Security Engine Technology and the security system that utilizes the technology.

2. Security for a Safe and Dependable Network

The next-generation network architecture and its requisite security functions are shown in **Fig. 1**. Items covered by next-generation network security can be classified into the transport network, network server clusters, network services, and corporate networks.

① Security for the Transport Network

The security required for the transport network is the protection of the network bandwidth, which is common resource for all network user. It will protect against the occurrence of abnormal traffic caused by DDoS (Distributed Denial of Service) attacks and malicious computer viruses such as Bots. It will also prevent heavy traffic generating services such as Peer-to-Peer based bandwidth-greedy applications from hogging network bandwidth and thereby causing disruptions in the traffic of other users.

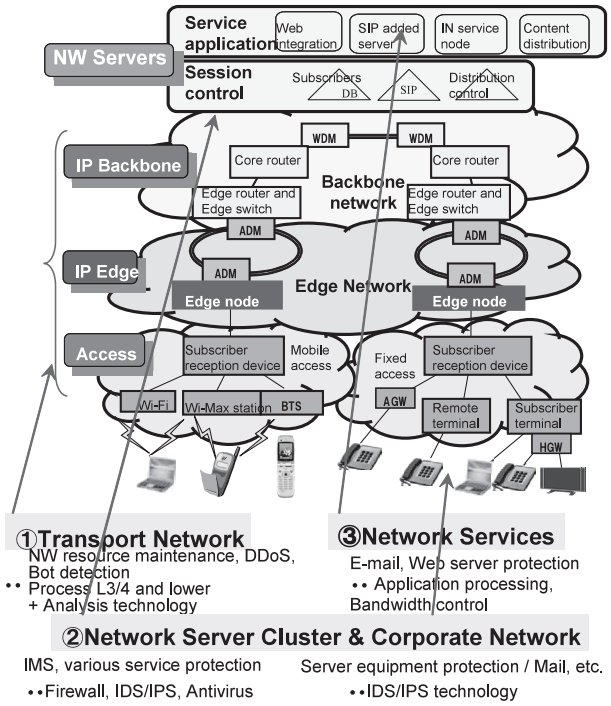

Fig. 1 Next-generation network structure and necessary security functions.

② Security for Network Server Clusters and Enterprise Network
In next-generation networks, there are high expectations for network services using IMS (IP Multimedia Subsystem) and various services by outside service providers. In this area, it will be necessary for 1) an authentication system to verify service providers and users, and 2) protection of network servers (to prevent unauthorized access, to control traffic flow, to control access, etc.)
③ Security for Network Services
In addition to conventional infrastructure services like telephone, telegraph and fax, the advent of the Internet has made it possible various new services to be constructed on the unified IP network. Currently major carrier services are voice, cellular-phone mail and Instant Messenger (IM) etc. Especially, cellular-phone mail has rapidly grown to come in the second position after telephony. Protection against spam mail, phishing, and mail viruses for cellular-phone mail has become a strong demand for public safety.

3. High-Performance Security Engine Technology

3.1 Issues Facing Its Realization

In order to satisfy the security matters listed in Section 2, there are a number of issues that must be resolved by the Security Engine.

(1) High-Speed Network Protocol Processing at the Rate of over 10Gbps
To inspect communication data at the application level, stateful management of TCP sessions and TCP reassembly technology are required. For traffic of a few hundred Mbps, software processing can achieve enough performance by virtue of accelerated processors. For traffic exceeding Gbps, however, the processing capabilities of a hardware engine become indispensable. TCP processing technology that can handle large volume processing at over 10Gbps and surveillance of a multitude of TCP sessions that surpass 1 million, is a major issue.

(2) Content Check Processing
Protocol analysis for application layer and fast pattern matching between communication content and thousand of attacking pattern data require high processing loads. Hardware engine is effective for these processing. With this technology, analyzing effective off-loading function for security application and the establishment of an hardware processing algorithm to achieve performance of over 10Gbps, will be major issues.

(3) Cooperation of Software and Hardware Engine
Considering the possibility of appearance of a new protocol or new detection methods, the integrated architecture of the software processing and the hardware engine processing is crucial. A platform where high commonality and heavy processing functions are handled by the hardware engine and others are handled by software on a processor, is necessary. To enable efficient integration between hardware and software, it is important to establish inter-processor coordination architecture and an optimized programming model to reduce the overhead of data copying and engine call.

3.2 Realization of the Security Engine

NEC has already marketed products featuring the various 1Gbps-class engines[1] that we have developed. In this time we have newly developed security engines with 10Gbps performance and a platform for them to run on, which can resolve the aforementioned issues.[2]

(1) TCP Monitoring Engine
This engine can monitor TCP processing at the rate of 10Gbps while identifying upper-layer application protocols (**Fig. 2**). The TCP monitoring engine achieved 10Gbps processing under short packet conditions of 250Bytes average per TCP payload. Furthermore, it was able to establish/tear down over 700,000 sessions per second. The number of simultaneous processing sessions it achieved was 1 million sessions.

(2) Session Management Engine
The session management engine achieved stateful TCP/IP session and UDP flow management at 10Gbps performance speed. It is equipped with an Access Control List (ACL) based packet filtering function, so it will be possible to create a firewall using this engine.

(3) Pattern Scanning Engine

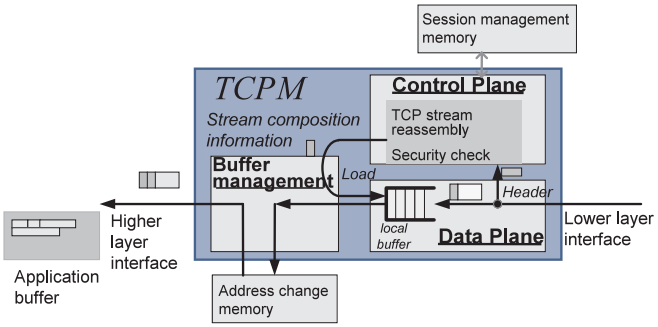

Fig. 2 TCP monitor engine block diagram.

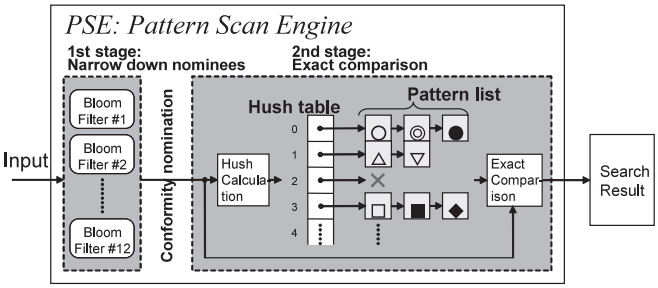

Fig. 3 Pattern scan engine block diagram.

The pattern scanning engine (PSE) functions to compare incoming data with a pre-registered keyword or character string to see if they match or not (**Fig. 3**). In a typical traffic model, PSE has about 2.5Gbps to 4Gbps processing performance per engine. Therefore, multiple PSEs make it possible to achieve 10Gbps performance through a multi-layer structure.

(4) Hardware Engine/Processor Cooperating Platform

We developed a high-speed task switching function and device drivers as the software platform necessary to integrate the hardware engines and processors and an event-controller which is the hardware mechanism that assists high-speed task switching. Due to this development, the software side can easily use hardware engines, and in terms of performance, it achieves about 100-times faster speed in task process switching than that of conventional OS performance.

3.3 Security Engine Platform

The block diagram of our 10Gbps security engine platform is shown in **Fig. 4**. The L2-L4 block is comprised of the L2/L3 section and the 10G TCP engine section, offering a traffic processing capability of 10Gbps. The L2/L3 section serves as Ethernet termination and applies IP packet processing, firewall processing, and session management, while the 10G TCP engine section applies TCP processing. The L7 block receives and manages the stream data composed at the 10G TCP engine section, and applies detection processing with the pattern scanning engine. The L7 block have APIs to external servers and embedded processors. What's more, it is also possible to use an embedded processor as a software-based off-loading engine. **Photo** shows the exterior of a common platform card.

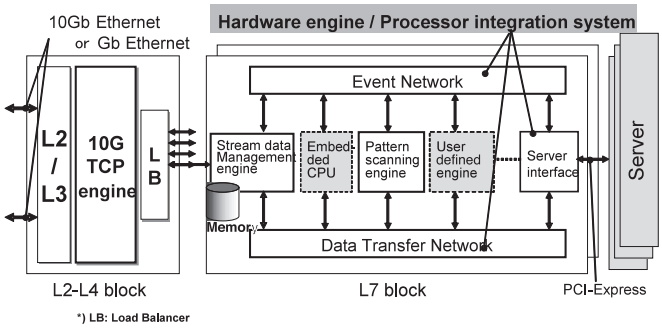

Fig. 4 Security engine platform diagram.

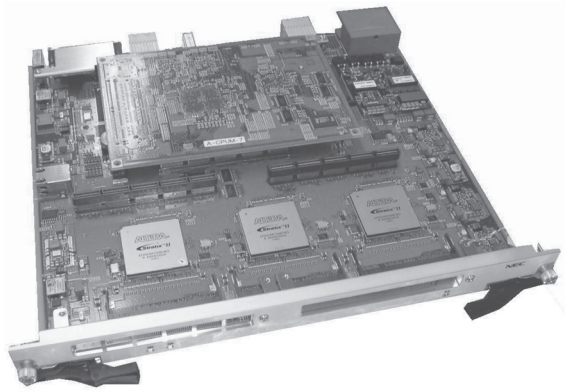

Photo Common platform card exterior.

4. Application in 10Gbps High-Speed Intrusion Detection System (IDS/IPS)

The firewall which includes monitoring of the application layer and the Intrusion Detection System (IDS) necessitate a high processing load due to the fact that it encompasses content checking of the data payload. So in high-speed networks the processing performance becomes an issue. NEC has achieved high-speed Snort[3] processing which delivers 10Gbps processing by applying a security engine platform. Snort is an IDS open source software that enables multi-layer detection, which performs intrusion detection by comparing the input data with known attack pattern character strings (signatures). In addition, by combining the intrusion detection function with the communication session management's establishment/termination function, it is possible to run it as an application firewall.

The processing block diagram is shown in **Fig. 5**. With its session management engine and TCP monitoring engine, it manages input sessions and reassembles TCP data, after which the pattern scanning engine located in the L7 filter processing section searches for matches in the signatures of incoming traffic. Furthermore, it applies a detailed search of suspicious traffic using software residing in the processor. As for hardware performance, the TCP monitor section supports 10Gbps

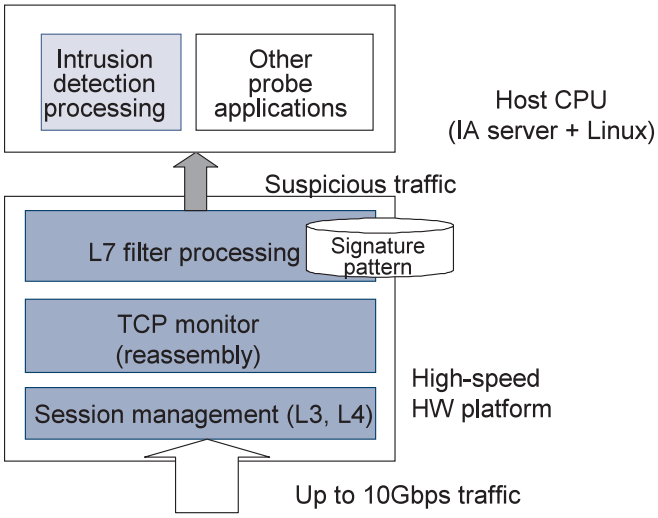

Fig. 5 High-speed IDS processing diagram.

processing, and the L7 filter section offers a processing capability of 2.5Gbps to 4Gbps per card, thereby achieving 10Gbps processing through the use of multiple cards.

5. Application in Spam Mail Countermeasure Solution: SLIMIT

The SLIMIT series[4] is a spam mail countermeasure device which features high-performance processing by a hardware engine, consisting of SLIMIT-L which offers a bandwidth control function, and SLIMIT-C which has a URL filter function. As depicted in **Fig. 6**, SLIMIT-L is a mail traffic control device that is positioned on the front end of a mail server, which regulates based on the environmental data of the mail at the application level. By drawing upon the 1Gbps processing technologies of various engines, this new development can process 1,000 mail transactions per second during TCP processing and session unit band regulation processing. SLIMIT-C is a device that processes requests from the mail server for spam mail status decisions, which offers a URL filter function that cross-checks URLs contained in email payloads against a blacklist database. By achieving payload data analysis processing and URL database cross-check processing via engine technology, decision processing for a maximum 5,000 mails per second can be rendered with little time lag.

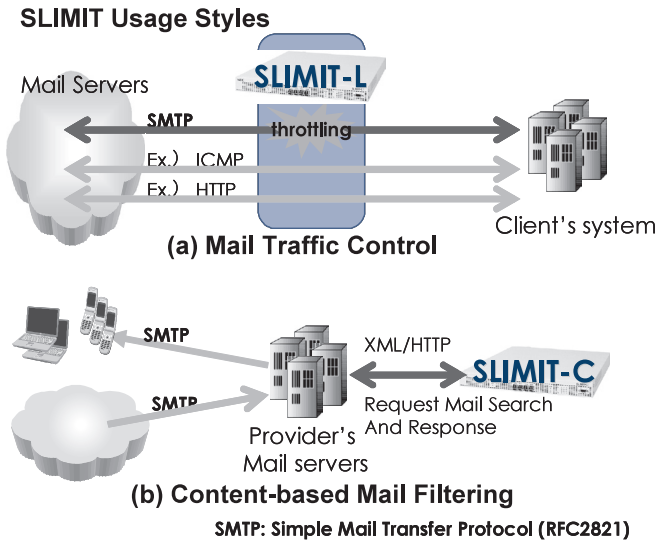

Fig. 6 SLIMIT usage styles.

6. Conclusion

We have introduced the security engine that is applicable to a wide range of network security solutions. In addition to the security engine that is meant for high-performance detection, other system technologies will also become necessary, including that for integration with individual security systems as well as search data distribution and synchronization. Along with our advances in security engine technology, from now onward we intend to continue bolstering the integration with system technologies.

This work was partly supported by Ministry of Internal Affairs and Communications (MIC).

*Snort is a registered trademark of Sourcefire, Inc.

References

1) Motoo Nishihara, et. al., "Broadband Service Gateway Platform for Readily Available and Reliable Business Applications and Services," NEC Journal of Advanced Technology, Vol.1, No.2, Spring 2004.
2) Kamiya, et al., "Development of the 10Gbps High-performance Security Engine Platform," 2006, The Institute of Electronics, Information and Communication Engineers, General Conference BS-5-13, 2006-3 (In Japanese).
3) Snort:http: //www.snort.org/
4) Mail Traffic Limiter: http://www.nec-mobilesolutions.com/application/products/mtl.html

Security Engine Technology for a Dependable, Safe and Secure Network Environment

Authors' Profiles

KAMIYA Satoshi
Principal Researcher,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation

UENO Hiroshi
Principal Researcher,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation

YAMADA Kenshin
Assistant Manager,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation

NISHIHARA Motoo
Senior Manager,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation