Security Solutions for the Next-Generation Network

OKABE Toshiya, NAKAI Shoichiro, SERA Takafumi, KAWATSU Masato, ITO Kazuhiro, KAWACHI Yasuro

Abstract

The IT environments surrounding the carrier networks are changing. The communicating individuals and organizations and the contents of their communications have changed and the capabilities of the networks and terminals have improved significantly. These are now built using open technology systems and their roles are also changing in order to become platforms that incorporate various applications. This paper introduces measures required for the carrier networks to deal with the changing environments by categorizing them as four solutions. These include: anti-attack defense, anti-disaster, traffic control and operations management solutions.

Keywords

next-generation network, security, anti-attack defense, anti-disaster, traffic control, operation management

1. Introduction

The desirable goals of the services provided by carriers remain the same even after the implementation of the next-generation networks. The most important of these are robust countermeasures against malicious users (intentional threats) (Requirement 1), an effective defense against errors and disasters (accidental threats) (Requirement 2), the fair service provisions (Requirement 3) and the efficient construction and operation of security systems (Requirement 4).

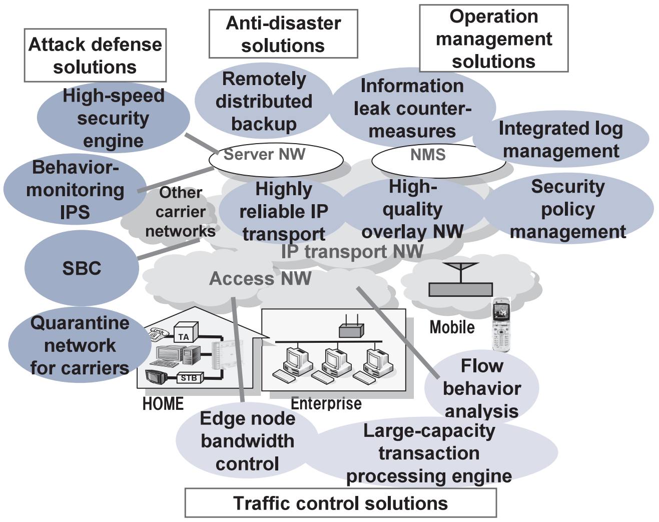
Attack defense solutions
Anti-disaster solutions
Operation management solutions
High-speed security engine
Remotely distributed backup
Information leak counter-measures
Integrated log management
Server NW
NMS
Behavior-monitoring IPS
Other carrier networks
Highly reliable IP transport
High-quality overlay NW
Security policy management
IP transport NW
SBC
Access NW
Quarantine network for carriers
TA
STB
HOME
Enterprise
Mobile
Flow behavior analysis
Edge node bandwidth control
Large-capacity transaction processing engine
Traffic control solutions

Fig. Key technologies for the security of the next-generation networks.

A dependency on outside carrier networks is expected to increase in the future as a result of interconnection with other networks, accommodation of networks of different access types and content distribution via third parties. It is also expected that diversification of business models will be advanced. Next-generation networks are expected to be accompanied by more complicated business structures. The increase in the complexity of business structures will inevitably mean an increase in vulnerability, while at the same time, it will be essential that the security level is maintained at the same high level as at present.

In the following sections we propose four solutions including; anti-attack defense, anti-disaster, traffic control and operation management solutions **(Fig.)** as the measures for meeting the four requirements of the changing environments that are outlined above.

2. Defense Solutions against Attack

Border defense such as the firewall is effective in preventing illegal access from external terminals. Border defense prevents illegal packets from intruding the network. However, most of the attacks that are aimed at the weakness of the OS or applications are hard to detect at the border so defense against them is performed at the server. Defense performed at the server or at a terminal is called host defense.

Here, the introduction of the notion of mutually complementary defense is effective. With this type of defense, the predictive information detected at an end point is sent to all of the border defense systems that are installed at key points in the network to automatically block any subsequent illegal access. This makes it possible to enlarge the defense area instantaneously and localize damage.

In the following, we will describe the element technologies for the mutually complementary defense that can improve dependability by detecting illegal actions without compromising convenience and performance.

(1) Behavior-Monitoring IPS (Intrusion Prevention System)

This system detects illegal actions and provides defense by monitoring the "behaviors" of programs running on the server[1]. For example, the legal maintenance personnel execute the authentication procedure before updating a setting file, a program that abuses an OS weakness such as buffer overflow does not execute the authentication procedure. The system takes notice of such differences in behavior to detect illegal actions and thus prevent adverse consequences.

(2) High-Speed Security Engine

The next-generation network will accommodate a huge number of terminals as a universal service platform and performance improvements are required for the intrusion detection systems as well as for the servers in the IMSs (IP Multimedia Subsystems). On the other hand, linkage with continually evolving external systems and existing open systems is also important.

To deal with this, the virus/worm detection function, protocol anomaly detection function and traffic measurement function are implemented as hardware locked into the system in order to process a large amount of packets efficiently. The component that handles the external interface is implemented as software in order to provide flexibility.

The high-speed security engine allocates the functions optimally in the hardware or software in this way in order to achieve compatibility between high speed and flexibility[3].

(3) Quarantine Network for Carrier Network

Most of the attacks using attack programs such as viruses and bots are aiming at weaknesses in the software installed at the terminals. If a terminal is connected to the network without correcting such weaknesses, the terminal is not only infected but becomes a source of infection that may permit the damage to spread. This problem can be solved effectively by taking a series of steps to diagnose the terminal safety and adopting the proper measures before connection to the network.

When a terminal is connected to an access network, it is permitted access only to a specific server called the quarantine server and receives its diagnosis. If a problem is found with it, measures are taken according to the security policy defined by each carrier and the network connection is permitted only after solution of the problem has been confirmed.

This solution makes it possible to provide countermeasures against security threats, which accompany increases in the number of connected terminals, without dependency on the skills of general users.

(4) SBC (Session Border Controller)

The SBC solves the threats that the VoIP service providers encounter, such as an increase in the processing load resulting from a large number of call setup requests, failure of emergency calls due to concentration of traffic and illegal access to the SIP server by malicious users.

The SBC monitors the call connection status of the SIP and allow only the necessary voice traffic to connect to the VoIP network. It also controls the load on the SIP server resulting from momentary increases in connection requests, executes priority processing for emergency calls and eliminates illegal access to the SIP server.

In addition, when call setup requests are concentrated in a specific area due to disaster, etc., the SBC collaborates with the SIP server to apply outgoing traffic congestion control in order to reduce the overall load of the network.

3. Anti-Disaster Solutions

The accessibility of networks and the integrity of stored data should be protected even in the case of an accidental thread such as operational errors or disaster. The accessibility of each service can be enhanced by building a high-reliability, high-quality IP network and then, in the higher layer of the IP network, forming a high-reliability overlay network that is independent from the IP network using distributed servers. The integrity of the data is ensured by the distributed data backup.

(1) High-Reliability IP Transport

Since a carrier network is a social infrastructure, interruption of its service may have serious consequences, even if this occurs only for a short period. This makes it necessary to provide high-reliability IP transport that allows the services to be continued even if a fault should occur. Transport reliability may be improved by making use of the MPLS, which has a high affinity with IP and is suitable for path control and QoS management.

The QoS server[3] performs the pass design of the optimum path with which the QoS can be guaranteed, based on the conditions set in advance. At the same time, it also sets the redundant path to prepare for unexpected faults. The redundant path can be selected from three types, which include bandwidth exclusive, bandwidth sharing, and the non guaranteed types and are designed according to the assurance and economy to meet requirements. The high reliability IP network can be built by optimum path design and the redundant paths for use in the case of faults.

(2) High-Quality Overlay Networks

Because of the difficulty in modifying an existing IP network, the overlay network that can improve the reliability and increase the speed of only a specific part of the network is attracting attention.

A virtual network (overlay network) is built on a per-service basis on a physical network (particularly an IP network). The overlay networks perform exclusive path controls specific to the higher-level services and independently from the underlining network, thus providing high-quality connectivity that is not physically affected by overloading or faults in the network.

(3) Remotely Distributed Backup

WAFS (Wide Area File Services) are attracting attention as a means of increasing the speed of file access through WAN. A relay backup system is installed in the vicinity of each of the storages that are distributed in remote locations, and performs data synchronization by utilizing high-speed access transport. The integrity of data is preserved by duplicating data between remote locations that are connected through multi-paths on low-speed wide area networks, while mitigating transmission delays and packet losses and by smoothing the multi-path traffic.

4. Traffic Control Solutions

It is necessary to apply measures for preventing occupation of network resources due to cyber attacks, such as excessive traffic inflow from other networks, DoS (Denial of Service) attacks, SPAM and SPIT (Spam over IP Telephony).

The objective of a carrier network is to provide a stable service for all, while at the same time securing the privacy of individuals. The carrier network cannot perform actions that are permitted for corporate networks, such as providing education, defining in-house regulations or monitoring the packets to eliminate traffic that is not associated with corporate activities.

In the following, we will describe the technologies of traffic control solutions that can achieve fairness in service provision by identifying traffic without peeking into packets, disposing of illegal traffic, guaranteeing the quality of emergency communications and pay broadcasting, and allocating resources optimally for the best effort traffic.

(1) Large-Capacity Transaction Processing Engine

This is a hardware engine for use in protecting the server against spam mails and mass web access by filtering or regulating the rates of transactions of applications. The SLIMIT-L is a product that applies this engine to the mail system[4], and is able to processes more than 1,000 mails per second.

As advanced web services and single sign-on will increase in the future, it is expected that the XML description language will be used in more and more situations. The transaction processing engine can reduce the XML processing load of the server, thereby enabling delivery of stressless web services for a larger number of users.

(2) Flow Behavior Analysis

This technology infers the application involved in each packet based on the information that can be obtained without peeking into packets, such as the packet size and packet arrival time interval[5]. The application is estimated based on the statistical information obtained after observation for a certain period of time and on the characteristic transition patterns of each packet.

This technology identifies the application used with encrypted traffic or traffic with disguised header information while maintaining the user traffic secrecy that is critical for carrier networks. It is also effective in the detection of Peer-to-Peer traffic, prevention of disguised priority traffic in VoIP, and for the detection of quality degradation.

(3) Edge Node Bandwidth Control

To deliver a large number of services stably, it will be more important than ever to prepare a mechanism for preventing the mutual interference of traffic of some users or some services. For this purpose, an edge node with dedicated high-performance chipsets works as a concentrator of high-speed optical access lines in order to manage the traffic flow for each service and each server and to restrict it, if the traffic exceeds the predetermined level.

Together with the dynamic control by the servers and network management system, traffic congestion control in the case of overloads due to disaster is also applied by taking the priority of both services and users into consideration.

5. Operations Management Solutions

Advanced security cannot be ensured unless a larger number and a larger variety of security systems than at present are managed properly. The Plan-Do-Check-Action cycle of security management (security design, rule setting, incident monitoring and incident analysis) encounters new issues including delays in preventive measures and countermeasures, lack of expert knowledge on the detection of attacks, diversification of services, increases in management targets and an increase in the management load due to frequent changes and modifications. In addition, countermeasures against information leakage are also important because the operation management system holds critical information such as personal information.

The efficiency of the security management systems can be improved by automation and integration of security policy management, log monitoring and information leakage prevention.

(1) Security Policy Management Technology

Improvement measures should be taken per work process in order to reduce the load of network managers.

In the process of the security design process, the access and surveillance policies should be established independently of individual equipment models. In the rule setting process, the rules (settings) in the formats that are tailored to individual equipment models should be set automatically from established policies. It is also required that, after a rule is modified manually, the consistency of the applied rule to the policies should be verified[6].

Automating the steps above makes it possible to reduce the management load, prevent incidents due to setting defects, and adopt countermeasures quickly if a critical incident occurs.

(2) Integrated Log Monitoring

In the incident monitoring and incident analysis process, the large amount of log generated by the security equipment should be subjected to integrated management for the detection of incidents such as attacks and intrusions.

The behavior monitoring analysis technology extracts specific patterns from the log and detects intrusions and attacks of the network in real time. The trend analysis technology analyzes the relatively long-term, wide-area trends of the log and detects abnormal activities or unknown threats in the overall network.

(3) Information Leak Preventions

The leakage of information can be prevented effectively by the confidential data output control and the encryption key division based on a secret sharing scheme.

The InfoCage[7] is a product that applies the data output control technology. It does not leave data in the local disks of terminals after they have viewed or edited data in the server, restricts data saved in external media, data printing, screen capturing and mail transmission, and also prevents information leakage due to abuse or mistakes by users.

In addition, the data permitted to be output is encrypted and the key is divided by means of secret sharing scheme to prevent data leaks by single or conspiring malicious users. The secret sharing divides the secret information into an arbitrary number of information items. The original information can never be guessed at from the individual items of divided information and can only be restored when a predetermined number of divided information items are available[8].

The combination of output control and secret sharing allows the carrier network management to prevent information leaks at a high level, without losing convenience.

6. Conclusion

In anticipation of the environmental changes expected to accompany the migration to the next-generation networks and of the high security levels that will be needed to cope with such changes, strategic investments in security will be required. Requirements will vary depending on the carriers and will be determined according to the network configurations, business structures, estimated risks and the balance of security investments. Besides the above solutions, it is important to find out the best combinations of the means of defense to meet requirements of each carrier. NEC will continue to provide optimum security solutions for the next-generation networks by using our wide range of technologies.

References

1) Nakae, et al., “A Server Intrusion Defense Method Based on Behaviors,” Proceedings of FIT2004 Lectures (Vol. 4), pp. 275-276, September 2004.

2) Kamiya, et al., “Development of 10Gbps, High-Performance Security Engine Platform,” IEICE General Conference, BS-5-13, March 2006.

3) QoS Server CX6800-QS: http://www.sw.nec.co.jp/netsoft/cx6800-qs/

4) SLIMIT: http://www.nec-mobilesolutions.com/application/jcontents/slimit/

5) Kitamura et al., “An Application Identification Technique Based on Flow Behavioral Analysis,” IEICE Technical Report Vol.105, No.470, NS2005-136, December 2005.

6) Okajo, et al., “Equipment Integrated Analysis System For Security Management,” IPSJ Technical Report CSEC-28, Vol. 2005, No. 33, pp. 303-308, March 2005.

7) InfoCage http://www.sw.nec.co.jp/cced/infocage/

8) Furukawa, et al., “Group Signatures with Separate and Distributed Authorities,” Proc. SCN2004, Lecture Notes in Computer Science, Vol. 3352, Springer Verlag, pp.77-90, 2004.

Authors' Profiles

OKABE Toshiya
Assistant Manager,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation

NAKAI Shoichiro
Chief Manager,
1st Network Software Division,
Network Software Operations Unit,
NEC Corporation

SERA Takafumi
Manager,
1st Carrier Solutions Operations Unit,
NEC Corporation

KAWATSU Masato
Manager,
System Platform Software Development Division,
Solution Development Laboratories,
NEC Corporation

ITO Kazuhiro
Manager,
2nd Network Software Division,
Network Software Operations Unit,
NEC Corporation

KAWACHI Yasuro
Senior Manager,
Network Platform Development Division,
Broadband Networks Operations Unit,
NEC Corporation