Solution for Virtualization to Ensure Optimal Network Security Environment

● Shoji Kohira ● Kenji Mitsuhashi ● Shuji Yahiro ● Shinichi Ikeda

The Internet became widely diffused once the Internet Protocol (IP) was defined in an Internet technical standard, Request for Comments (RFC). Meanwhile, security measures were left insufficiently discussed. Given this situation, intruders disguised as normal communication can relatively easily penetrate and disrupt Internet services. Their methods of attacks are becoming more sophisticated on a daily basis, meaning that present-day security measures cannot be guaranteed to work in the future. Against this background, security measures are becoming an indispensable technological component for an all-IP network, as opposed to a one-off program. In addition, a paradigm shift is occurring with respect to the way the cost of such measures is perceived, from burdensome expenses to investments indispensable for business continuity. In responding to this shift, Fujitsu undertakes the development of network security technology and offers network security solutions. This paper reviews issues with the current security measures, and outlines some technological factors to address them. It then describes specific features of the Fujitsu products that have introduced software-defined networking (SDN) and/or network functions virtualization (NFV)—key technologies for virtualizing network and communication services.

1. Introduction

In the 2000s, voice and data communications became progressively adapted to the Internet Protocol (IP) network. This was followed by the establishment of global standards in the 2010s for communication methods such as LTE and Wi-Fi, as well as their commodification through the growing prevalence of communication devices equipped with Android OS and the like. Meanwhile, open source software has become widely used following the standardization of communication methods, and as a result, the vulnerabilities inherent in their source codes also have become a common problem. Until the third generation (3G) mobile communication system, differences in communication methods functioned like a defense line to an extent. However, the tools and methods of cyber attacks that are globally prevalent today may target Japanese telecom carriers in the future.

The Request for Comments (RFC) provides a technical standard for the Internet, and while it facilitated the wide diffusion of IP, security measures were left insufficiently discussed. This situation allows intruders disguised as normal communication to penetrate and disrupt Internet services relatively easily.

One example is the distributed denial of service (DDoS) attack, so-called water torture, which has been a threat to Internet service providers (ISP) in Japan since 2013. This attack targets domain name system (DNS) servers (**Figure 1**).[1] User datagram protocol (UDP) can reach the application layer of DNS servers without establishing an end-to-end connection, and thus it can be abused by attackers to disrupt application services. Similarly, there has been a case in which a 400-Gbps-class DDoS attack maliciously deployed the network time protocol (NTP), which used UDP. Therefore, there is a need for further vigilance and more robust countermeasures to mitigate this risk. In view of this, Fujitsu is developing network security technology and offering network security solutions.

This paper first reviews issues regarding the current security measures, and outlines some technological factors to address them. It then describes some

Fujitsu products that leverage key technologies for network security—software-defined networking (SDN) and network functions virtualization (NFV).

2. Types of security measures

There are three network security measures that are widely deployed today:

1) Sensor-based detection and blocking attacks

This analyzes the data patterns in data traffic and communication behavior, and detects and blocks known threats. The employed systems vary depending on the communication layers and modes, but they are categorized into next-generation firewall (NGFW), intrusion prevention system (IPS), and web application firewall (WAF). Threats may remain undetected if they originate from a number of sources or the attack takes place over a long time. Thus, this type is faced with a challenge of detecting these and other unknown threats.

2) Security log analysis

This collects logs continually and analyzes them to detect the threats that cannot be identified in time-confined data. Against the threats that cannot be detected in particular communication layers, it performs a correlation analysis between log files from sensors placed on multiple layers to enhance the detection sensitivity. The drawback is the large data volume of detection logs, and it needs to have its data processing made more efficient.

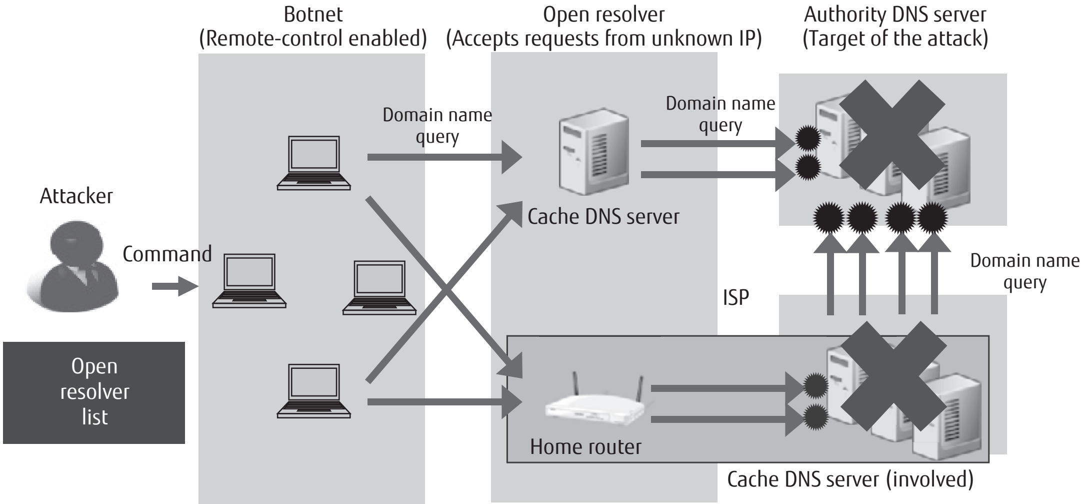
3) Preparation and execution of countermeasures based on the analysis results

This considers prevention and/or mitigation measures upon detecting attacks, and executes the aforementioned sensor-based detection/block procedures. However, the attack patterns constantly change, which makes it difficult to standardize countermeasures. It is important to shorten the lead time between the attack and implementation of the measures. The challenge here is to expedite the response through automation.

Contrary to the expectations of many telecom carriers that security products will provide a comprehensive protection against all threats, only some of such threats can be prevented in reality. We need to be aware that the ever-changing attack patterns mean there is a constant need to modify security designs. **Figure 2** illustrates how the precision in detection and analysis deteriorates if a security system is neglected for constant maintenance through its operation and monitoring. The causes and results of such deterioration are as follows:

1) Deterioration of the precision in log-based detection

The attributes of data traffic change over time due to, for example, the introduction of new application services or an increase of application data. This creates



Prepared using the data included in Reference 1) DNS *Mizuzeme* (Water Torture) attacks.

Figure 1
Mechanism of water torture attack on DNS servers.

a gap between the detection threshold and its optimal value.

2) Deterioration of the precision in log analysis

The number of network threat signatures grows through updates of the signatures as time passes. There will also be many redundant logs, among which threats may hide themselves unless they are filtered out.

In one actual case, taken from one of our customers, 80% of its detection logs were unnecessary, and the remaining 20% were comprised of investigation and attack logs. As for detection logs, it is necessary only to filter out unnecessary logs from the detection procedure. Investigation logs need to be inspected to clarify the problem, while attack logs need to have the security setting altered to be blocked. It should be noted that the basic countermeasure for the three types of logs mentioned above is to review their threshold value settings.

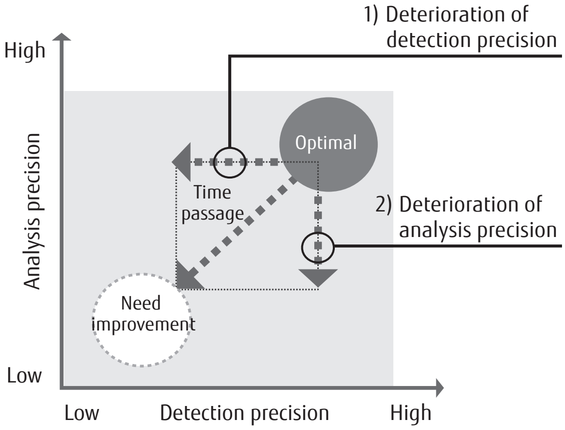


Figure 2
Key notions of security system operation.

3. Element technologies for highly sophisticated security measures

An increasing number of telecom carriers are considering launching their security operation centers (SOC) for more robust security systems. However, running such an SOC in conjunction with a network operation center (NOC) will inevitably increase capital expenditure (CAPEX) and/or operational expenditure (OPEX). In order to both reduce costs and enhance security, it is necessary to share the tasks between NOC and SOC and automate the tasks as much as possible. Key element technologies for security enhancement in this context are as follows:

1) Common platform for log analysis

Vendor firewalls (FWs), IPSs, WAFs and other monitoring systems today are capable only of monitoring the vendor's own products. Defying such a vertically divided monitoring style, all logs are collected on the common platform for analysis. As the platform is equipped with an automatic scenario execution system, human resources for SOC operation can be economized (**Figure 3**).

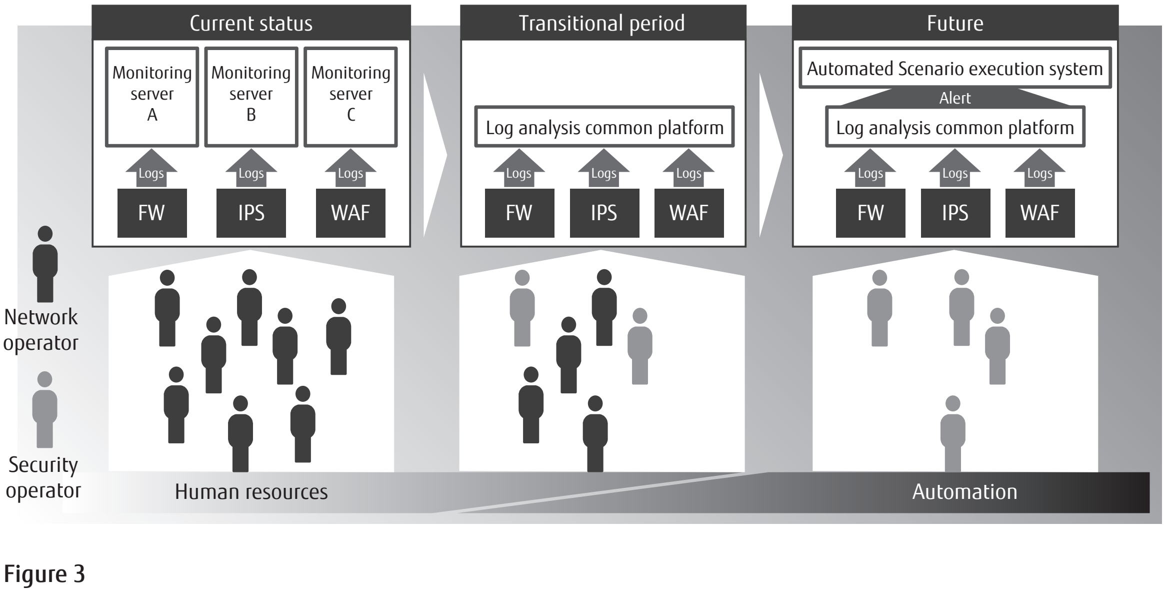


Figure 3
Automating SOC operation.

2) Analysis of unknown threats

For the analysis system, it is efficient to use a security information and event management (SIEM) system provided by vendors specializing in security systems. However, such a system focuses on referencing known threat patterns while discarding the data that does not match. This makes it possible to lose data in terms of traceability and forensic investigations, thus requiring additional measures to address this.

Fujitsu is developing a solution applying ultra-high-speed packet capturing and big-data analysis technologies[2] to a security system. It is designed to enable pre- and post-event measures against security incidents on a high-speed network with broad bandwidths typical of telecom carriers.

3) Optimization of security policy

Security systems must be kept updated at all times by tuning and optimizing security policies for sensors according to the results of threat analysis. However, it takes time from detecting attacks to implementing measures, and minimizing this lead time is a challenge. Fujitsu is developing a solution that automates the procedures of security policy optimization. Every time there is a change in the network, the solution automatically optimizes the security policy for each sensor according to the optimization rules defined by administrators (**Figure 4**). We expect that this will reduce the burden of manual tasks at SOC, and help to maintain the security at an optimal level.

4. Fujitsu's NFV Solution

Today, telecom carriers find themselves in a tighter situation as profit structures change, the quality of experience (QoE) needs to be accounted for, and they need to follow new technologies. Many of them are feeling a strain as security measures add to their cost. In this context, the virtualization technologies for telecom services SDN/NFV are a viable option for addressing those challenges and pursuing the security services business (**Table 1**). At Fujitsu, we are applying this NFV technology to the security field to create solutions that can perform on-demand application distribution, resource allocation/release, and usage/operational state monitoring. Thus

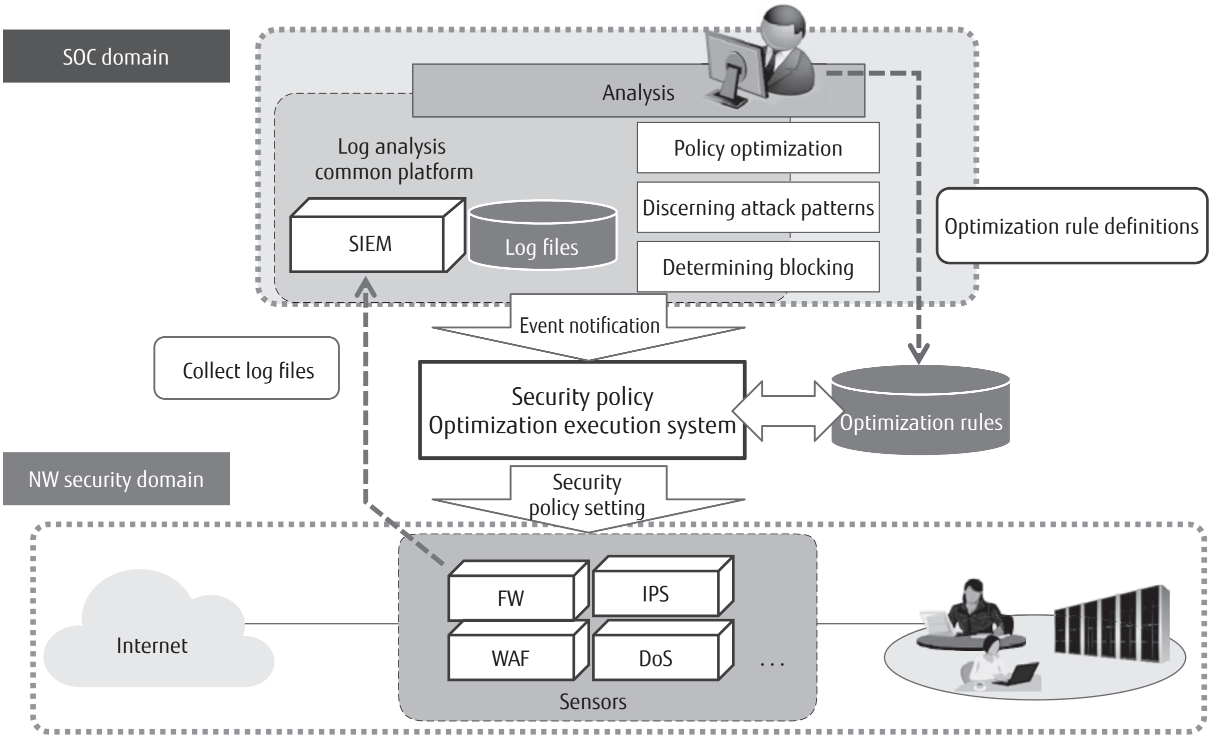


Figure 4
Automatic scenario execution system.

Fujitsu is offering FUJITSU Network Virtuora OM and Virtuora RV. Please see "Transforming Carrier Networks by Utilizing Network Functions Virtualization"[3] in this special issue for details.

An introduction of some applied cases of these solutions is as follows.

1) Network security service using service chaining

If a telecom company provides a network security service, it needs to perform network reconfigurations and setting modifications so that only those end users who signed up for the service are directed through the security system.

Table 1
Solution to network problems offered by SDN/NFV.

Problems for network administrators	Fujitsu solution
Want to develop network infrastructure quickly	Offer add-ons for cloud management software (OpenStack) to enable automated installation of package software/OS.
Want to scale facilities easily depending on customer requirements and user demand.	
Want to provide new services to customers quickly.	Offer on-demand service chaining service.
Want to make it easy to implement small start/stop for introducing new services.	Offer service lifecycle management using GUI.
Want to minimize operating expenditure (OPEX).	
Want to simplify operational procedures to mitigate operational errors.	

Virtuora OM and RV virtualize network security services such as firewalls and virtual private networks (VPN). And by applying them to service chaining (technology to control packet transmission routes for each end user in order to enable them to use necessary network functions when they need them), it minimizes the time for delivering necessary services (**Figure 5**).

2) Automated countermeasures in response to events

If attacks, for example a malicious DDoS attack on a DNS server, are detected it will require countermeasures to be newly implemented.

With Virtuora OM and RV, countermeasures can be defined. Therefore, on detecting a DDoS attack, for example, they automatically launch new protection measures, applying the firewall and quality of service (QoS) features (**Figure 6**).

5. Conclusion

This paper introduced a new solution for network security. Attackers constantly change their tactics. The

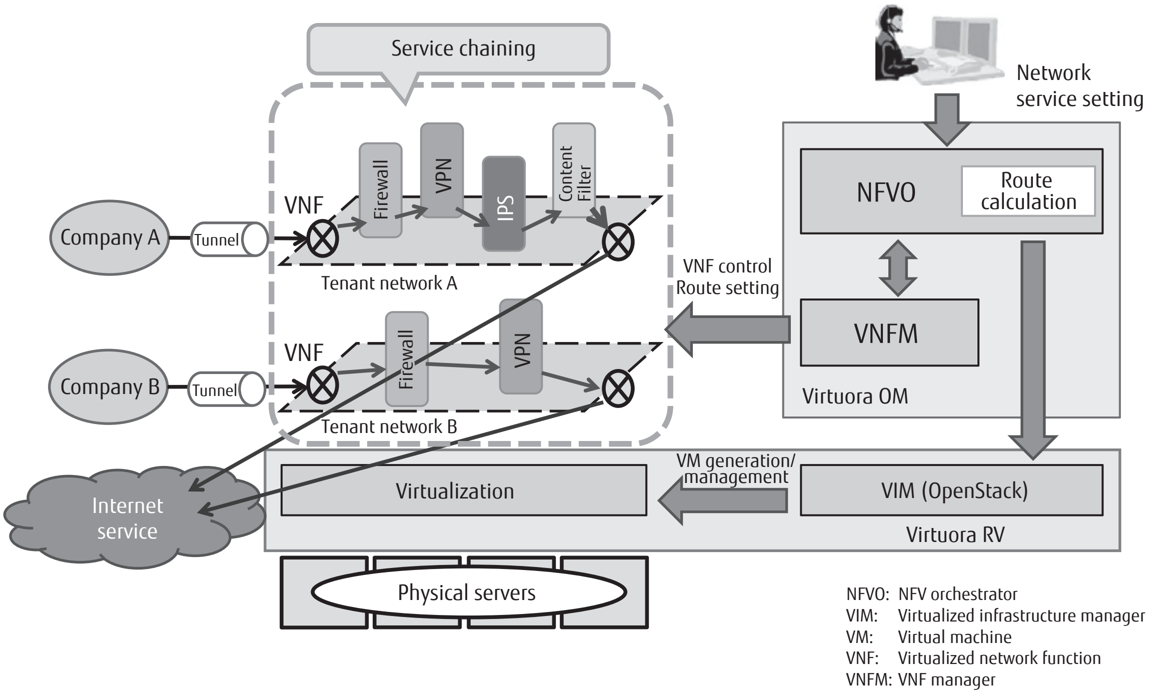


Figure 5
Service chaining for network security

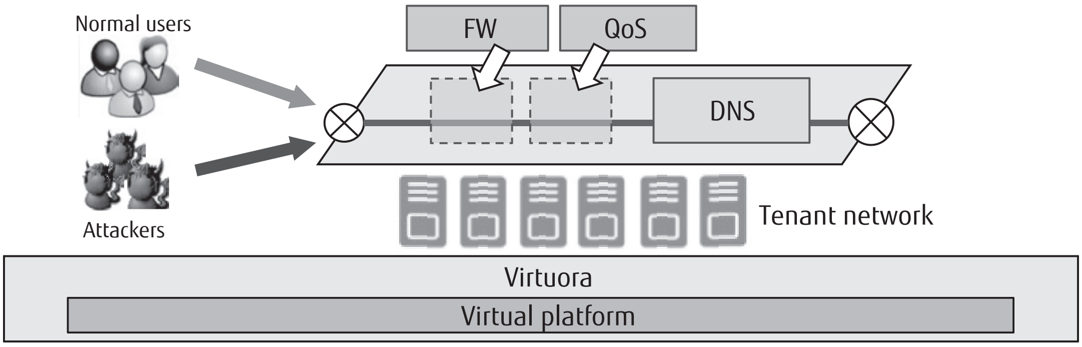


Figure 6
Countermeasures against DDoS using NFV.

present-day security measures cannot be guaranteed to work in the future. It is important to anticipate the future need for reviewing them, and make the first move by establishing a flexible and scalable baseline. It is also important to develop proactive monitoring systems. It is necessary to build up our knowledge on security measures as we operate such systems.

Similarly, security measures are not for a one-off event, but an indispensable technological component for an all-IP network. A paradigm shift is occurring with respect to the perception of security cost, from burdensome expenses to investments indispensable for business continuity. In the future, Fujitsu will need to realize sophisticated protection features that can be operated efficiently and to minimize the overhead. Also, it is important to devise a strategy in which Fujitsu's security services for businesses and end users become a new source of profit for its customers.

References

1) Y. Morishita: DNS *Mizuzeme* (Water Torture) attacks. SECCON 2014 Nagano event DNS Security Challenge (in Japanese).
http://2014.seccon.jp/dns/dns_water_torture.pdf

2) H. Chiba, et al.: Full Capture System and Big Data Analysis: Connecting Businesses and Networks in IoT Era. FUJITSU Sci. Tech. J., Vol. 52, No. 2, pp. 71–74 (2016).
http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol52-2/paper08.pdf

3) M. Okuda, et al.: Transforming Carrier Networks by Utilizing Network Functions Virtualization.
FUJITSU Sci. Tech. J., Vol. 52, No. 2, pp. 13–19 (2016).
http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol52-2/paper03.pdf

Shoji Kohira
Fujitsu Ltd.
Mr. Kohira is currently engaged in planning and development of network security solutions for telecom carriers.

Kenji Mitsuhashi
Fujitsu Ltd.
Mr. Mitsuhashi is currently engaged in planning and development of network security solutions for telecom carriers.

Shuji Yahiro
Fujitsu Ltd.
Mr. Yahiro is currently engaged in planning and development of network security solutions for telecom carriers.

Shinichi Ikeda
Fujitsu Ltd.
Mr. Ikeda is currently engaged in planning and development of network security solutions for telecom carriers.