High-Speed Scanning System for Security Diagnosis

Fumiyuki Tanemo[†] *and Kazuaki Chikira*

Abstract

To maintain effective network security, we must correctly assess the network configurations and security vulnerabilities. Our high-speed scanning system can examine the configuration of any firewall and look for security flaws in hosts such as servers and terminals.

1. Introduction

As broadband becomes widespread, more and more users now connect their networks to the Internet, but many of these networks have severe security flaws. These vulnerable networks often become the targets of malicious acts such as unauthorized computer access and denial of service (DoS) attacks. Moreover, these networks could be exploited as springboards to launch attacks on a third party. Therefore, it is very important to maintain effective network security to ensure the integrity of the Internet.

Placing a firewall in front of these networks is an effective means of achieving network security. This enables users to block most attacks from the Internet. As shown in **Fig. 1**, the firewall controls all incoming packets from the Internet based on access rules defined beforehand. The firewall prevents attacks from succeeding by intercepting unwanted packets. Moreover, it is also possible to prevent any host in the network from becoming a springboard for attacking a third party. Thus, it is very important to set up the firewall access rules correctly.

To maintain the effective security of the network, we must accurately assess the current network settings including the firewall configuration. We can perform port scanning to determine the network configuration by sending diagnosis packets to a network and examining the response packets. There are already commercial products and free diagnostic tools that implement port scanning functions. However, most of these tools are rather slow in examining firewall configurations. We need a faster port scanning tool to determine the network configurations.

2. High-speed scanning system

To assess network settings quickly, NTT Information Sharing Platform Laboratories is developing a high-speed scanning system (**Fig. 2**). This system can verify network configurations and report security vulnerabilities by port scanning. Moreover, our system

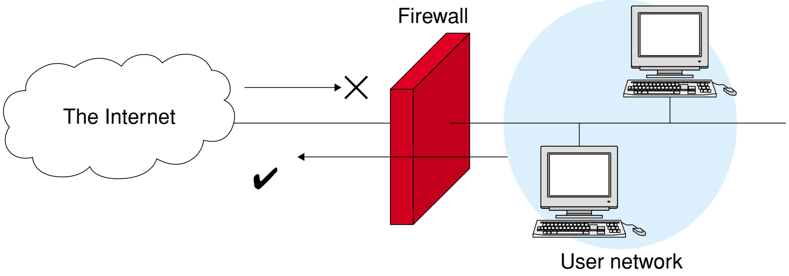

Fig. 1. Protecting a user network with a firewall.

[†] NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: tanemo.fumiyuki@lab.ntt.co.jp

can effectively shorten the time required for diagnosis.

3. Port scanning technique

An ordinary port scanning tool (**Fig. 3**) generates diagnosis packets and sends them towards the host to be examined. The diagnosis packets consist of a series of packets whose IP address, protocol number, and TCP/UDP port number are systematically changed (TCP: transmission control protocol, UDP: user diagram protocol). For instance, in order to examine all open TCP ports on a host, the tool creates a series of TCP packets targeting ports 1 to 65535.

After the diagnosis packets have been sent to the target host, the diagnosis tool examines the response packets returned from the host and determines the host configurations. If ICMP (Internet control message protocol) or ARP (address resolution protocol) is used in the diagnosis, one can determine whether a host with an arbitrary IP address exists on the network. Moreover, if TCP and UDP are used, it is possible to identify services that can be accessed from the outside.

One way to verify the firewall configuration by port scanning is to place the diagnosis tool in front of the firewall and send diagnosis packets towards a target host behind the firewall (Fig. 3). However, depending on the OS implementation, the target host does not always return reply packets. Also, the firewall may occasionally intercept the reply packets from the host. Therefore, this method cannot accurately inspect the firewall's access rule. Moreover, it is necessary to set up an extended time-limit in the diagnosis tool to allow enough time for the host to respond. Therefore, the time required for diagnosis may become unexpectedly long. Some commercial tools take about three hours to check all TCP ports and 20 hours or more to check all UDP ports.

4. Diagnosis by agents on both sides

The high-speed scanning system checks the firewall configuration by deploying agents on both sides of the firewall to perform port scanning in both directions (**Fig. 4**). The diagnosis is performed in the following steps.

1) The external agent sends diagnosis packets to the internal agent through the firewall.
2) The firewall determines whether to let each diagnosis packet go though.
3) When a diagnosis packet arrives, the internal

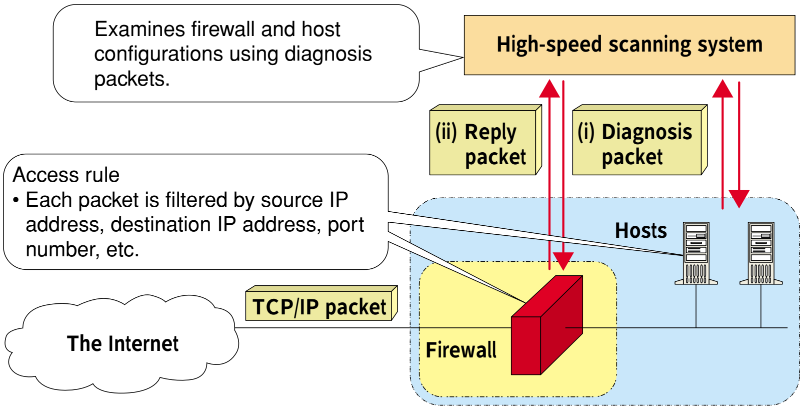
Examines firewall and host configurations using diagnosis packets.
High-speed scanning system
(ii) Reply packet
(i) Diagnosis packet
Access rule
• Each packet is filtered by source IP address, destination IP address, port number, etc.
Hosts
TCP/IP packet
The Internet
Firewall

Fig. 2. Concept of high-speed scanning system.

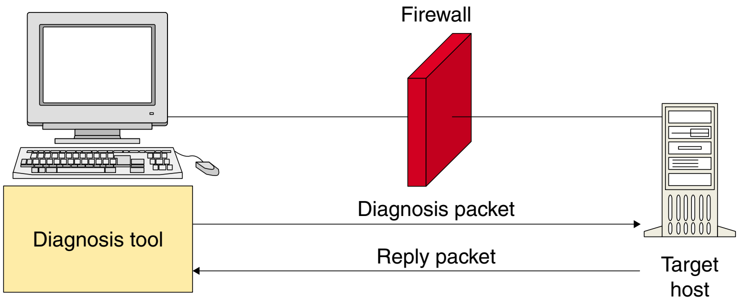

Fig. 3. Port scanning.

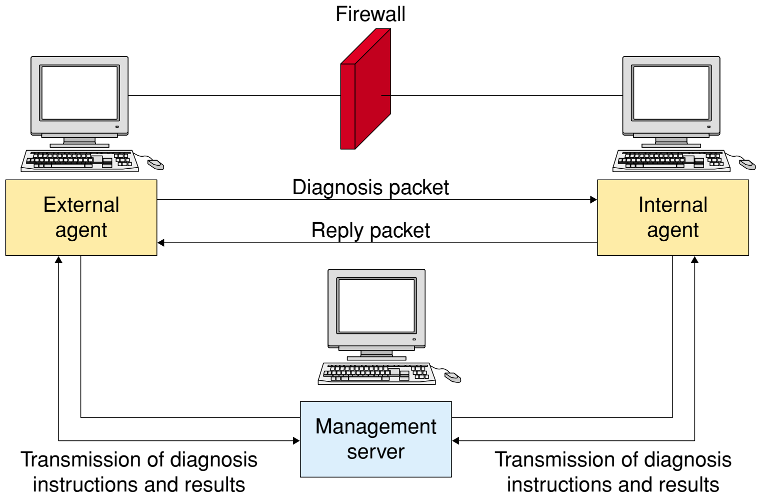
Firewall
External agent
Internal agent
Diagnosis packet
Reply packet
Management server
Transmission of diagnosis instructions and results
Transmission of diagnosis instructions and results

Fig. 4. Diagnosis using agents on both sides.

agent assumes that the corresponding port is open and sends back the response packet to an external agent. On the other hand, if the packet does not arrive within the time-limit, the internal agent concludes that the port is closed.

Using this method, our system can accurately inspect the firewall's access rule. Moreover, this method can effectively shorten the time required for diagnosis. Most existing port scanners need to wait more than one or two seconds for the response from servers they are trying to examine. Our method eliminates the waiting time for such responses because diagnosis packets are examined as soon as they reach the internal agent from the external agent. As a result, it takes less than 40 ms to examine one port. Therefore, our system can check all TCP or UDP ports in about three minutes.

5. System functions

Table 1 lists the system functions. The stateful firewall scanning function examines the firewall access rule and determines whether a packet should be forwarded according to the state of the connection session.

The integrated scanning function sequentially scans the network, host, and firewall. The system uses the results from the previous scan as the input for the next scan, and each scan is executed continuously. As a result, the entire network can be scanned with minimal overhead.

6. System deployment

Figure 5 shows an example of system deployment for an entire network. The system consists of three subsystems.

1) Agent devices: These are the external or internal agents, which generate or receive diagnosis packets. The agent devices are usually set up in all subnets of the network to be diagnosed.
2) Management server: This manages multiple agents, directs their actions, analyzes the diagnosis results, and creates reports.
3) GUI: This is the graphical user interface for the human inspector. This subsystem can be integrated with the management server as a single device.

It is necessary to deploy the agent device in such a way that the regular packets are not interrupted, such as by attaching it to a port of a hub or a mirror port of a switching hub. As shown in Fig. 5, the management server, GUI, and agent devices are connected by a local area network (LAN) constructed specially for the diagnosis. The management segment is used for sending diagnosis instructions and results and for providing the

Table 1. Functions of high-speed scanning system.

Network scanning	Looks for illegally connected devices.
Host scanning	Detects open ports. Helps determine whether there are services being used without the user's knowledge.
Firewall scanning	Examines firewall access rules.
Stateful firewall scanning	Confirms access rules of a stateful firewall by looking at packets forwarded or rejected by the firewall.
Integrated scanning	Scans the network, host, and firewall sequentially.

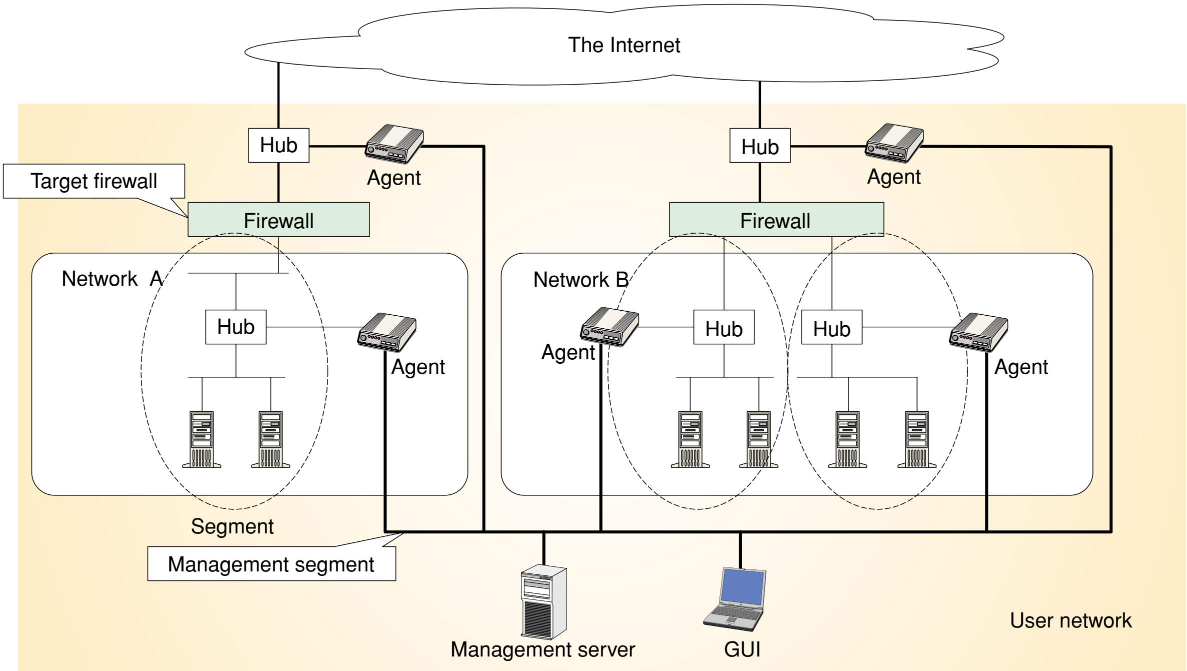

Fig. 5. Deployment of high-speed scanning system on user network.

timing control of the diagnosis packet transmission.

7. Effect of the system

We conducted an experiment to evaluate our system. The target network we selected had a typical topology with a typical firewall. We found that diagnosis was 100% correct by comparing the actual firewall configuration, the packet flow obtained, and the system diagnosis results. However, when the traffic is heavy, we may need to fine-tune the system so that the diagnosis packets are not dropped due to congestion. Compared with a free scanning tool widely used by network professionals, this system was able to scan TCP ports one hundred times faster and UDP ports several hundred times faster. Moreover, there were no side effects in the network or host during the diagnosis and the regular operations were never interrupted.

Before deploying our system, the inspector should obtain and analyze the network configuration. Moreover, it is necessary to set up agent devices, a management server, and a GUI in the network to be diagnosed. This system is very efficient because it can analyze a network in half a day, including the setup time.

8. Future development

In order to start up a new security business using our system, we are planning to: 1) combine the agents and management system into one device and 2) look for ways to deploy our system without using the management segment.

Fumiyuki Tanemo
Senior Research Engineer, NTT Information Sharing Platform Laboratories.
He received the B.S. and M.S. degrees in information engineering from Nagoya University, Nagoya, Aichi in 1991 and 1993, respectively. In 1993, he joined NTT Network and Information Systems Laboratories, Tokyo, Japan. He moved to NTT Information Sharing Platform Laboratories in 1999. He is a member of the Information Processing Society of Japan and IEEE Computer Society.

Kazuaki Chikira
NTT Information Sharing Platform Laboratories.
He received the B.S. and M.S. degrees in information engineering from Niigata University, Niigata in 1996 and 1998, respectively. In 1998, he joined NTT Human Interface Laboratories, Tokyo, Japan. He moved to NTT Information Sharing Platform Laboratories in 2003.