NEWS RELEASE

NTT

Feb. 18, 2003
Nippon Telegraph and Telephone Corporation

# Development of Moving Firewall, a System that Mitigates DDoS Attacks at Upstream and Defends the Entire Network

- Protecting Legitimate Traffic by Segregating Attack Traffic -

Nippon Telegraph and Telephone Corporation (NTT, Headquarter: Chiyoda-ku, Tokyo City, CEO: Norio Wada) has developed a prototype of DDoS countermeasure called Moving Firewall (MovingFW). The MovingFW system defends against distributed denial of service (DDoS) attacks*1 and protects the entire network effectively. A DDoS attack involves compromising multiple hosts and commanding them to send a large amount of packets towards a target server or network in order to interrupt its service.
While most conventional DDoS countermeasures attempt to defend against attacks in one fixed spot, MovingFW takes a different approach and blocks attack packets at upstream nodes close to the attacking machines.
In November last year, NTT developed the "Vision for a new optical generation -- Broadband leading to the world of resonant communication," and has directed its R&D efforts towards the vision. Moving Firewall is an R&D project that aims to realize the next-generation network architecture (Resonant Communication Network Architecture: RENA).

## <Background and objectives of the development>

The number of DDoS attacks increases at an alarming rate each year. In October 2002, thirteen domain name service (DNS) root servers that were mission-critical to the Internet were interrupted by DDoS attacks. Moreover, the Internet was crippled on a global scale by the spread of virus in late January this year. Such cyber attacks may bring even greater danger by completely suspending the entire Internet and render it useless. However, because conventional firewalls, which are usually deployed in one fixed location, cannot prevent over-consumption of network bandwidth, they cannot effectively defend against large-scale DDoS attacks.

MovingFW, newly developed by NTT Information Sharing Platform Laboratories, is able to effectively guard network bandwidth and defend against DDoS attacks, a task considered difficult using the conventional "one-spot" deployment, by means of multi-location deployment and sophisticated traffic analysis.

By deploying MovingFW in networks managed by ISPs*2 or other service providers, users are able to enjoy congestion-free networks. Moreover, e-commerce website owners are able to conduct their business on the Internet without worrying about DDoS attacks.

**<Key Features>**

(1) Total defense of the network
Based on an architecture that distributes defense intelligence close to attackers throughout the network, Moving Firewall is capable of guarding not only server hosts but also the entire ISP network. Most DDoS attacks insert spoofed source addresses in the attack packets to avoid traceability. However, using an effective backtrack algorithm, Moving Firewall is able to trace attack flows to their upstream.

(2) Protection of legitimate users
Based on sophisticated traffic analysis, MovingFW is capable of segregating attack packets with great precision according to service policies defined by webmasters or server administrators. The system minimizes the possibilities of false positive that often occurs with conventional firewalls and allows legitimate users to be served without interruption.

(3) Flexibility and Extendibility
Because Moving Firewall employs Active Network technologies*3, it is able to upgrade itself automatically to defend against new types of attacks.

**<System Overview>** (See Figure 1)

MovingFW is composed of a MovingFW management console, MovingFW software and a MovingFW device, each of which is described in the following:

(1) MovingFW management console
The MovingFW management console configures MovingFW devices and reports the status of DDoS attacks and defense graphically.

(2) MovingFW software
The MovingFW software is downloaded into the Moving FW device closest to the Web site or server to be protected and then executed to monitor incoming traffic. Detection rules can be easily configured by site administrators according to their service policies.
When an attack is detected, the system launches its defense mechanism automatically and dispatches defense program code, which includes the attack signatures, to upstream MovingFW devices hop by hop, until the code reaches nodes at the uppermost stream.

(3) Moving FW device
The MovingFW is a bridge device*4 that adopts the Active network technology and runs the MovingFW software.

**<Future Plan>**

The effectiveness of the MovingFW concept has been confirmed using a prototype. The next phase of the research will focus on deploying MovingFW on the Resonant Communication Network Architecture (RENA) by the year 2005. For the present, a series of real-world experiment will be conducted to study the effectiveness of MovingFW under various conditions.

**[ Glossary ]**

*1 : DDoS (Distributed Denial of Service) attack An attack that compromises multiple hosts using virus or other means and commands them to send a large amount of packets towards a target server in order to interrupt its service.

*2 : ISP (Internet Service Provider)
A company that provides individuals and other companies access to the Internet through telephone lines, ADSL or dedicate data lines.

*3: Active network technology
A technology that enables easy addition and customization of network services. It is composed of an execution environment for network nodes such as routers or bridges and protocols that enables program mobility.

*4 : Bridge device
A layer-2 device that relays packets without having any effect on layer-3 routing.

- Moving Firewall System Overview

For further information, please contact:

NTT Information Sharing Laboratory Group
Planning Division
Public Relations: Iizuka, Sano, Ikeda
TEL:0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp