Development of MovingFirewall, a System that Mitigates DDoS Attacks at Upstream Nodes and Defends the Entire Network

–Protecting Legitimate Traffic by Segregating Attack Traffic–

NTT has developed a prototype of DDoS countermeasures called MovingFirewall. This 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 number of packets towards a target server or network in order to interrupt its service. While most conventional DDoS countermeasures attempt to defend against attacks at one fixed spot, MovingFirewall takes a different approach and blocks attack packets at upstream nodes close to the attacking machines. In November last year, NTT developed its “Vision for a new optical generation–Broadband leading to the world of resonant communication,” and has directed its R&D efforts towards this vision. MovingFirewall 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 is increasing 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 a virus in late January this year. Such cyber attacks may bring even greater danger by completely suspending the entire Internet and rendering 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.

MovingFirewall, 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.

The deployment of MovingFirewall in networks managed by ISPs[*2] or other service providers will enable users to enjoy congestion-free networks. Moreover, e-commerce website owners will be 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, MovingFirewall 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 backtracking algorithm, MovingFirewall is able to trace attack flows upstream.

(2) Protection of legitimate users

Based on sophisticated traffic analysis, MovingFirewall is capable of segregating attack packets with great precision according to service policies defined by webmasters or server administrators. The system minimizes the occurrence of false positives, which often occur with conventional firewalls, and allows legitimate users to be served without interruption.

[*1] DDoS (Distributed Denial of Service) attack: An attack that compromises multiple hosts using a virus or other means and commands them to send a large number 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 dedicated data lines.

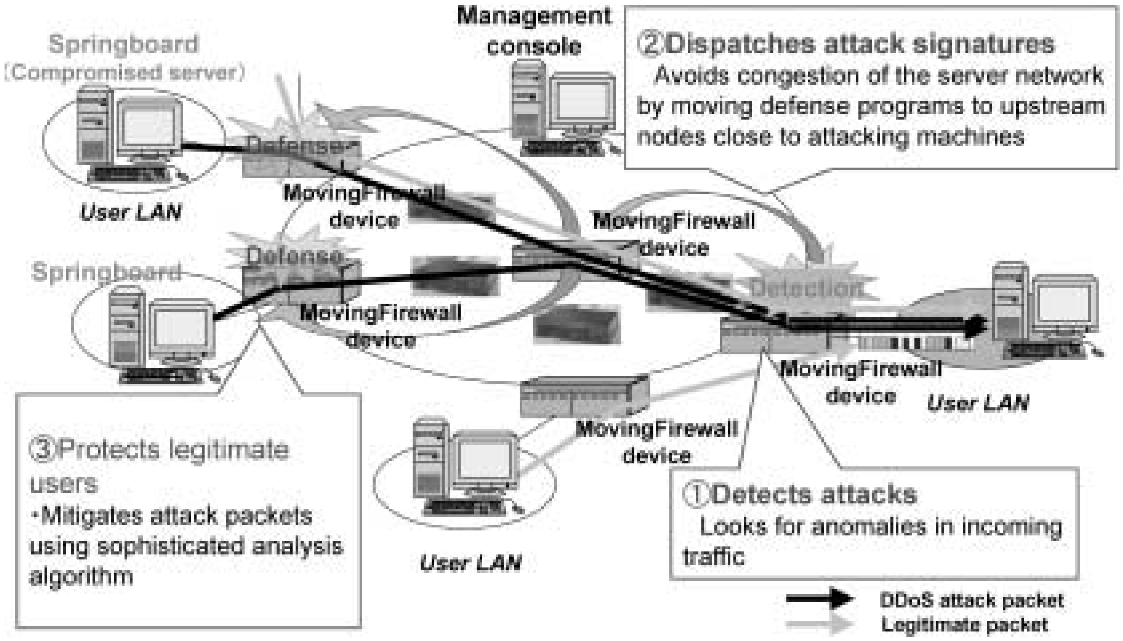
Springboard
(Compromised server)
User LAN
Defense
MovingFirewall device
Springboard
Defense
MovingFirewall device
Management console
②Dispatches attack signatures
Avoids congestion of the server network by moving defense programs to upstream nodes close to attacking machines
MovingFirewall device
Detection
MovingFirewall device
User LAN
MovingFirewall device
User LAN
③Protects legitimate users
・Mitigates attack packets using sophisticated analysis algorithm
①Detects attacks
Looks for anomalies in incoming traffic
DDoS attack packet
Legitimate packet

Fig. 1. MovingFirewall system overview.

(3) Flexibility and Extendibility

Because MovingFirewall employs Active Network technologies[*3], it is able to upgrade itself automatically to defend against new types of attacks.

System overview

MovingFirewall is composed of a MovingFirewall management console, MovingFirewall software, and a MovingFirewall device (Fig. 1). These are described below.

(1) MovingFirewall management console: configures MovingFirewall devices and reports the status of DDoS attacks and defenses graphically.

(2) MovingFirewall software: is downloaded into the MovingFW 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 MovingFirewall devices hop by hop, until the code reaches the nodes furthest upstream.

(3) MovingFirewall device: is a bridge device[*4] that uses Active Network technology and runs the MovingFirewall software.

Future plans

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

For further information, please contact
NTT Information Sharing Laboratory Group
Musashino-shi, 180-8585 Japan
E-mail: koho@mail.rdc.ntt.co.jp

[*3] Active Network technology: This 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.