MovingFirewall: A Countermeasure against Distributed Denial of Service Attacks

Hitoshi Fuji[†], *Eric Y. Chen, Koichi Okada, and Dai Kashiwa*

Abstract

Distributed denial of service (DDoS) attacks have recently attracted a lot of attention because of their potential threat to the Internet community. Conventional countermeasures deployed by end users alone are limited in their ability to secure IP networks from DDoS attacks. This article presents an innovative technology called MovingFirewall, which can be deployed by network providers to effectively cope with DDoS attacks by mitigating attack floods at multiple upstream nodes near the attacking hosts.

1. The threat of DDoS attacks

Distributed denial of service (DDoS) attacks are one of the most alarming threats on the Internet. A DDoS attacker attempts to disrupt a target web site by flooding it with illegitimate requests for information, usurping bandwidth and overtaxing web servers to prevent legitimate inquiries from getting through. The attacker uses readily available software tools to plant attack software on a large number of remote computers, called *zombies*, which, at the attacker's command, become the launch pad for a DDoS attack.

According to the Yankee Group, an attack in February 2000 resulted in a collective loss of $1.2 billion for eBay, Yahoo!, Amazon.com, and other high-profile web sites. In October 2002, thirteen domain name service (DNS) root servers that were mission-critical to the Internet were interrupted by DDoS attacks. More recently, the Internet was crippled on a global scale by the spread of a virus in January this year. Such cyber attacks may bring even greater danger by completely suspending the entire Internet and rendering it unusable.

There are two types of DDoS attacks: i) host resource starvation attacks aim to starve a server of resources by exploiting software flaws and ii) network bandwidth consumption attacks attempt to disrupt target servers by consuming their network bandwidth. One can defend against the former by deploying a conventional firewall or intrusion detection system in one fixed spot. However, such methods are ineffective in defending against the latter because they cannot prevent over-consumption of network bandwidth.

2. Overview of MovingFirewall

MovingFirewall, newly developed by NTT Information Sharing Platform Laboratories, can effectively guard network bandwidth and defend against DDoS attacks, a task considered difficult using the conventional single-spot deployment, by mitigating attack floods at multiple upstream nodes near the attacking hosts. With MovingFirewall deployed in networks managed by ISPs (Internet Service Providers) or other service providers, users can enjoy congestion-free networks. Moreover, e-commerce website owners can conduct their business on the Internet without worrying about DDoS attacks (Fig. 1).

3. Features of MovingFirewall

3.1 Total defense of the network

Based on an architecture that distributes defense intelligence close to attackers throughout the network, MovingFirewall can guard not only server

[†] NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: fuji-hitoshi@lab.nett.co.jp

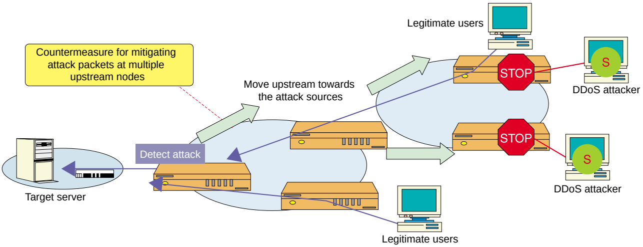

Countermeasure for mitigating attack packets at multiple upstream nodes
Legitimate users
Move upstream towards the attack sources
STOP
S
DDoS attacker
Detect attack
STOP
S
DDoS attacker
Target server
Legitimate users

Fig. 1. Block diagram of MovingFirewall.

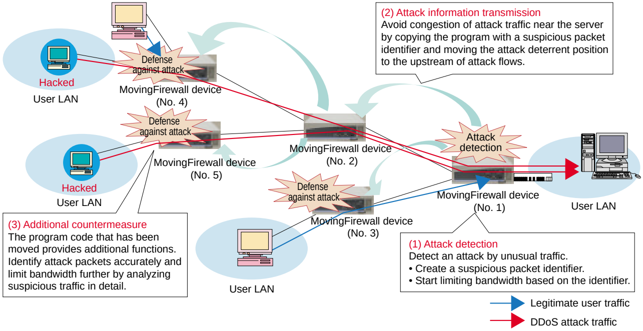

(2) Attack information transmission
Avoid congestion of attack traffic near the server by copying the program with a suspicious packet identifier and moving the attack deterrent position to the upstream of attack flows.
Defense against attack
Hacked
User LAN
MovingFirewall device (No. 4)
Defense against attack
MovingFirewall device (No. 2)
Attack detection
Hacked
User LAN
MovingFirewall device (No. 5)
Defense against attack
MovingFirewall device (No. 1)
User LAN
MovingFirewall device (No. 3)
(3) Additional countermeasure
The program code that has been moved provides additional functions. Identify attack packets accurately and limit bandwidth further by analyzing suspicious traffic in detail.
User LAN
(1) Attack detection
Detect an attack by unusual traffic.
• Create a suspicious packet identifier.
• Start limiting bandwidth based on the identifier.
Legitimate user traffic
DDoS attack traffic

Fig. 2. Overview of MovingFirewall operation.

hosts but also the entire ISP network. Most DDoS attacks insert spoofed source addresses in the attack packets to hinder traceability. However, using an effective backtracking algorithm, MovingFirewall can trace attack flows upstream.

The operation flow of MovingFirewall is shown in Fig. 2.

(1) When the nearest MovingFirewall device (No. 1) to the protected server detects a DDoS attack, it creates a signature that characterizes the attack traffic and shapes the incoming traffic based on this signature.

(2) Each MovingFirewall device relays the attack signature to its adjacent devices (from No. 1 to No. 2 and No. 3 and from No. 2 to No. 4 and No. 5, etc.) until the signature reaches the nearest device to the attacking hosts.

(3) The nearest MovingFirewall devices to the attacking hosts (No. 4 and No. 5 in Fig. 2) then mitigates the attack traffic using the attack signature. This confines the DDoS attack to a localized domain, preventing it from permeating the entire ISP network.

3.2 Legitimate user protection

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

The sequence of this mechanism is shown in Fig. 3. Before a DDoS attack occurs, all packets are classified as normal. When an attack is detected, MovingFirewall categorizes all incoming packets as suspicious and limits their bandwidth. This prevents over-consumption of the server bandwidth. MovingFirewall then analyzes the suspicious traffic in detail. Traffic identified as legitimate is reclassified as normal, while traffic identified as illegitimate is tagged as malicious and filtered out [3].

3.3 Highly flexible system

Because MovingFirewall employs Active Network technologies, it can upgrade itself automatically to defend against new types of attacks. With this technology, new counter-attack programs can be remotely installed in each MovingFirewall device from the management console.

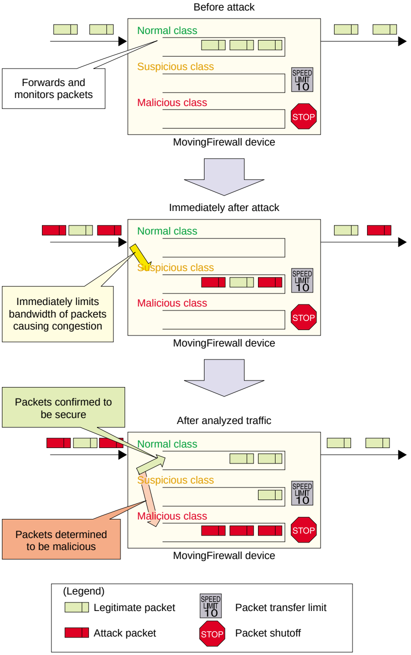


Fig. 3. Overview of legitimate user protection system.

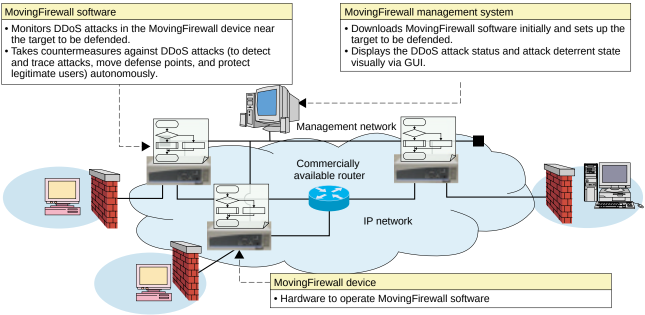
4. MovingFirewall system configuration

The system configuration of MovingFirewall is shown in Fig. 4.

The MovingFirewall software is downloaded into the MovingFirewall 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 nodes furthest upstream.

The MovingFirewall management console configures MovingFirewall devices and reports the status of DDoS attacks graphically.

A MovingFirewall device is simply a bridge, which can be deployed without replacing the existing routers. All MovingFirewall devices and the management system are connected via a dedicated manage-



MovingFirewall software

- Monitors DDoS attacks in the MovingFirewall device near the target to be defended.
- Takes countermeasures against DDoS attacks (to detect and trace attacks, move defense points, and protect legitimate users) autonomously.

MovingFirewall management system

- Downloads MovingFirewall software initially and sets up the target to be defended.
- Displays the DDoS attack status and attack deterrent state visually via GUI.

MovingFirewall device

- Hardware to operate MovingFirewall software

Fig. 4. MovingFirewall system configuration.

ment network to ensure security and sufficient bandwidth for management purposes.

References

[1] D. Kashiwa, E. Y. Chen, and H. Fuji, "Active Shaping: A Countermeasure against DDoS Attacks," In Proceedings of ECUMN'02, pp. 171-179, Apr. 2002.

[2] D. Kashiwa, E. Y. Chen, H. Fuji, S. Machida, H. Shigeno, K. Okada, and Y. Matsushita, "Active Countermeasure Platform against DDoS Attacks," IEICE TRANS. INF. & SYST. Vol. E85-D, No. 12, Dec., pp. 1918-1928, 2002.

[3] D. Kashiwa, E. Y. Chen, and H. Fuji, "A countermeasure against DDoS attacks using active networks technologies," Annals of Telecommunications, Vol. 58, No. 3-4, pp. 605-629, Apr. 2003.

Hitoshi Fuji

Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.E. degrees in industrial engineering from Science University of Tokyo, Tokyo. He also earned a Ph. D. in informatics. His current research interests are on network security, service networking architecture and project management. He is a member of The Japanese Society for Quality Control and the Society of Project Management.

Eric Y. Chen

Research Scientist, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in Computer Science and the M.B.A. degree in International Business from McGill University, Montreal, Canada, in 1997 and 2000 respectively. He joined NTT in 1997 and is currently also a Ph. D. candidate in Computer Science in the University of Tokyo, Tokyo. He received the Best Paper Award for Young Researchers of the Information Processing Society of Japan (IPSJ) National Convention in 2000 for his paper titled "Moving Firewall: An Active Networks Application for Defending Against DDoS Attacks". He is a member of the IEEE Communications Society.

Koichi Okada

Research Scientist, Cyber System Project Group, Research and Development Center, NTT EAST.

He received the B.S. and M.E. degrees in system and information engineering from Hokkaido University, Hokkaido, in 1997. From 1997 to 1999, he was with NTT Software Laboratories. And from 1999 to 2003, he was with the NTT Information Sharing Platform Laboratories. His research interests include VPN, extranet, single sign-on and privacy. He is a member of IPSJ.

Dai Kashiwa

Research Scientist, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.S., M.E., and Ph.D. degrees in engineering from Keio University, Kanagawa in 1995, 1997, and 2003 respectively. In 1997, he joined NTT. His current research interests are on network security, service networking architecture, and distributed object computing. He is a member of the Institute of Electronics, Information and Communication Engineers and IPSJ.