Performance Evaluations of IPTables Firewall Solutions under DDoS attacks

M. ŠIMON, L. HURAJ AND M. ČERŇANSKÝ

Abstract

The paper presents design, background and experimental results of the IPTables applied in IPv4 and IP6Tables applied in IPv6 network compared through several tested parameters. The experimental testbed environment is based on P2P grid utilized for DDoS attacks. IPTables tool is used for packet filtering and consequently for preventing DoS/DDoS attacks. It allows a system administrator to configure the tables, the chains and rules it stores in order to manage the incoming and outgoing packets. The packets are treated according to the rules' results provided by the packet processing. A rule in a chain can be bound with another chain in the table etc.
We employ the P2P grid environment to carry out as well as to coordinate DDoS attack on the availability of services to simulate real DDoS attack launched indirectly through many compromised computing systems. The same routing protocols as well as the same firewall rules were used for IPv4 and for IPv6 network. The main aim was to analyse pros and cons of new IP6Tables tool compared with IPTables in IPv4 networks in light of the resistance to DDoS attacks which is still one of the most significant threats in the IPv6 networks.

General Terms: networks, peer-to-peer architectures, network security
Additional Key Words and Phrases: IPv6, IPTables, DDoS attack, P2P grid

1. INTRODUCTION

Internet Protocol version 6 (IPv6) is a new phenomenon that offers technical benefits not only in addition to a larger addressing space but also takes advantage of device mobility, security, and configuration features. Recently, many companies have started utilizing IPv6, because they recognized the improvements and benefits of IPv6 that can meet the current and future Internet demands. Moreover, current operating systems allow to set IPv6 as default setting of network protocol. Companies still rely on existing IPv4 applications, which might cause numerous security problems during the coexistence of IPv4 and IPv6 in the network because a protocol might be used to utilize the other protocol if the attacker realizes the accessibility of both protocols in the network. Therefore, new security policies are required to sustain security for both IPv4 and IPv6 (ALI et al., 2011, SIMON et al., 2015).

10.1515/jamsi-2015-0010

Implementation of the IPv6 protocol brings new demands for network protecting mechanisms again cyber-attacks. One of the destructive and harder-to-prevent attacks is Distributed denial of service (DDoS) attack which still afflicts the IPv6 networks as well.

In a typical DDoS attack, attacker coordinates many compromised machines and uses them to send large numbers of useless packets to a single victim, which will consume the victim's resources in order to overwhelm its capacity and to make the victim's service unavailable.

A DDoS defense mechanism should be able to separate malicious packets sent by attacker from legitimate packages with high accuracy, minimal resource consumption and low false positive and negative rates (VARALAKSHMI and THAMARAI SELVI, 2013).

For this reason, a structure called IPTables are offen used in Linux systems. IPTables is a command and table structure that allows a system administrator to configure the tables provided by the Linux kernel firewall as well as the rule sets that control the packet filtering.

The goal of this article is to compare the IPTables applied in IPv4 and IP6Tables applied in IPv6 networks in special case of DDoS attack. The paper begins with an explanation of the IPTables, firewall rules and it introduces the DDoS testbed environment based on P2P grid. In order to be practical in the investigation, we performed an experiment that involved real DDoS testbed environment under IPv4/IPv6 network where a static routing protocol as well as the same firewall rules were used. The paper then examines the end-to-end delay and throughput of the two scenarios.

2. BACKGROUND

Brief background of used techniques is described in this section. It is focused on firewalls, DDoS attacks as well as P2P grids. The peer-to-peer architecture and an open source P2P grid middleware OurGrid (OURGRID PROJECT) was used to design of the DDoS testbed environment.

2.1. Firewall and IPTables

Firewalls represent one of the most important security mechanisms in IPv6 networks. The basic idea of firewalls is to protect network system against outside and inside attacks, so they filter all packages that enter or leave the protected network. For IPv4 networks there are many software and hardware firewalls for different platforms, but their implementation in IPv6 network demands incorporations of differences between IPv4 and IPv6 in packet filtering possibilities.

IPTables is a user-space application program that allows to configure the tables provided by the Linux kernel firewall and the chains and rules it stores. IPTables contains a set of rules that have been set by firewall administrator.

Essentially, firewalls have two default policies: discard and accept. The discard policy means that if an incoming packet does not match any rule in IPTables it is discarded. Conversely, the accept policy means that if an incoming packet does not match any rule in IPTables it is allowed to pass (ALSHAMMARI and BACH, 2013). After designing an appropriate policy, the policy is translated into rules for IPTables.

But not all security policies for IPv4 can be applied in IPv6 environment (ALI et al., 2011). IPTables is therefore used to set up, maintain, and inspect the tables of IPv4 packet filter rules in the Linux kernel. IP6Tables is applied for the similar purpose in IPv6 networks.

2.2. Distributed Denial of Service (DDoS) attack

One of the major threats in the IPv6 networks that leads to unavailability of services is distributed form of Denial of Service attack. DDoS attack misuses numerous compromised computers from different computing systems to launch and to coordinate the attack. The main goal of the attacker is to deny the availability of the victim, i.e. the set of hosts, servers, frameworks or networks. The performance degradation of a network/framework as well as consuming of computational resources and network bandwidth is the primary aim of the attack. That leads to the degradation of service quality for legitimate clients. On the other hand, this kind of attack does not compromise the system authentication nor does it allow an unauthorized access to a framework (SINGH and GYANCHANDANI, 2010).

There are several kinds of DDoS attacks. The web applications resources are targeted by HTTP Get flood attack where basic GET requests are used to barrage the targeted server. Consequently, the database resources as well as the memory of the server and its CPU capacity are significantly consumed. This kind of application attack does not utilize reflection techniques, spoofing or malformed packets.

2.3. Peer-to-peer grid

OurGrid (OURGRID PROJECT) is a middleware for the implementation of P2P grid systems where each peer offers its own idle resources; it can use idle resources from other members as well and so benefit from best-effort resource allocation. Execution of applications can be speeded up by creation of such P2P computational grids where a job can be simultaneously submitted by a node as well as a job can be executed on the node. Client broker provides the interaction of a member with particular OurGrid community. This approach hides the heterogeneity of the grid structure and gives fast application turn-around for end user (ZHAO et al., 2011).

In addition, an advantage of P2P grids compared with traditional grids is their accessibility from more social settings and geographical locations, which allows formation of brand new applications such as disaster and battlefield management,

emergency communication, entertainment industry, e-healthcare and e-learning, and so forth (HRMO et al., 2012, SILÁDI and MIŽUROVÁ, 2013).

Our testbed is based on the above mentioned open source software OurGrid. An opportunistic peer-to-peer grid environment supported by the OurGrid middleware has three main components, namely the OurGrid Worker, the OurGrid Resource Manager Peer and the OurGrid Broker (BRASILEIRO, et al., 2008). OurGrid workers compute their tasks on the grid resources and are used for attacking of the target server. It should be underlined that only ethical penetration DDoS testing was done by the proposed P2P grid testbed and network administrator was watching whole testbed environment during the attack (SIMON et al., 2013).

The opportunistic P2P grid requires the installation of an OurGrid Peer and OurGrid Workers in every node, which is similar to real DDoS attack. Maintaining as well as setting up an OurGrid framework is much simpler in contrast to other grid environments; in addition, it is particularly simple to send or to receive a command by an OurGrid worker.

3. EXPERIMENTAL SETUP AND MEASUREMENTS

Two groups of the OurGrid workers performing the DDoS attack were organized during the experiments. Connectivity of the workers in first group was via a 100Mb/s switch and consequently, the uplink port was connected to a 1Gb/s switch. As described in Figure 1, the second group of workers was connected to the second switch. OS Debian7 with OurGrid worker framework was running on all attacking workers. OS CentOS6, 1GB RAM, CPU 3.3GHz Pentium was running on both the victim server and firewall.

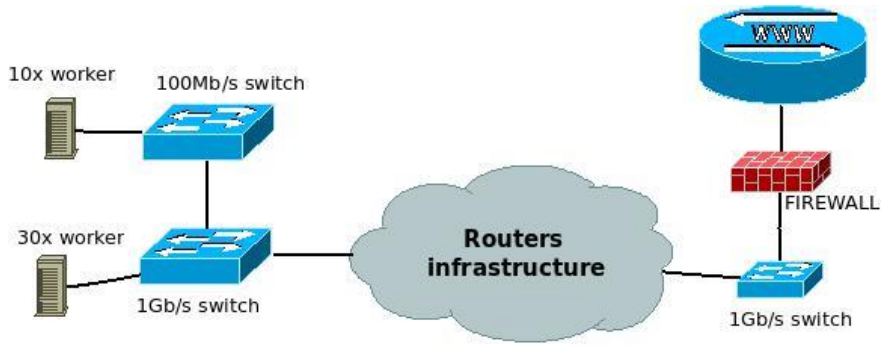

Fig. 1. Topology of the testing network

The performance of any networked system was reflected by three major metric measurements in the experimentation results. Load of the victim framework during DDoS attack is the first one, Fig 2a). Memory usage delta was the basis for the second metric, Fig 2b). And finally, the number of received and sent bytes in both versions of IP protocol was the last measurement, Fig. 3. The period of traffic generation was three minutes. All experiments were done with, as well as without http security policy in IPTables/IP6Tables, Table 1. Moreover, the end-to-end delay was measured, i.e. the time it takes for the server to respond to the host request, Fig. 4. Let us underline that a DDoS attack was carried out by OurGrid workers during all of the measurements.

Table 1. Rules of security policy in IPTables/IP6Tables against http-get flood attack.

-A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -p tcp ! --syn -m state --state NEW -j DROP
-A FORWARD -i eth0 -p tcp -m tcp --dport 443 -m state --state NEW -m recent --set --name apache-tls --rsource
-A FORWARD -i eth0 -p tcp -m tcp --dport 443 -m state --state NEW -m recent --update --seconds 30 --hitcount 20 --rttl --name apache-tls --rsource -j DROP
-A FORWARD -i eth0 -p tcp -m tcp --dport 443 -m state --state NEW -j ACCEPT

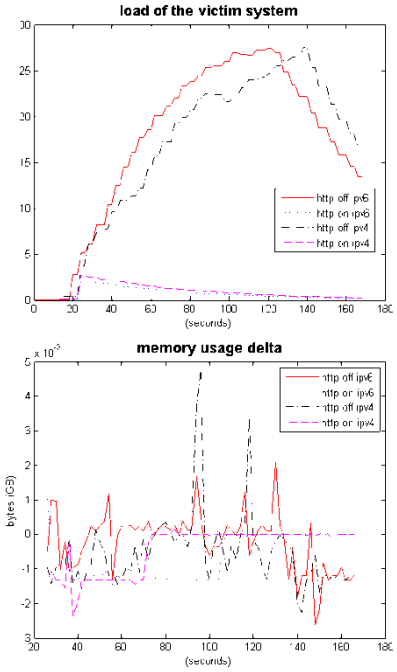

Fig. 2. a) System load average b) Memory usage delta in bytes (significant values).

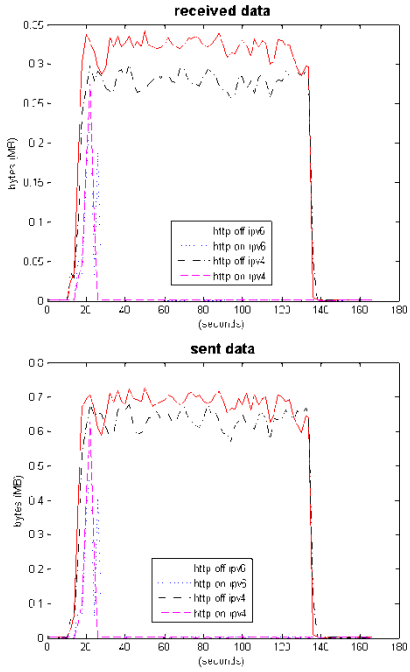

Fig. 3. Amount of bytes by the target a) received and b) transmitted to the network.

As can be seen from the Figures 2 and 3, the IPTables in both protocols effectively thwart the HTTP Get flood attack and have successfully decreased the amount of received and sent data, and consequently decreased the load of victim system as well.

If application of IPTables and IP6Tables for both protocols during the DDoS attack is compared, it can be seen that the defense technique has acted in an analogous way. But in IPv6 there are some varieties. If we consider that packet header in IPv6 is simpler than in IPv4 and therefore it does not need so many CPU resources, it should be obvious that the load of the target system in IPv6 was smaller than the load in IPv4. The difference was in average 21.8 %. Additionally, the number of received and sent bytes in IPv6 network was higher compared with IPv4, because the IPv6 header size is larger than the size of the IPv4 header. However, the average number of received and sent bytes after IP6Tables filtration was about 7.5% or 12.9% lower compared to IPTables in IPv4. It was done mainly in the starting phase where the IP6Tables filtration was applied more thoroughly. The memory usage was approximately identical in both cases.

Figure 4 plots the end-to-end delay in the experiments. The peaks are due to protocol overhead. If the values of the peaks are neglected, it can be seen that the end-to-end delay was only 0.769 seconds faster utilizing IP6Tables compared to IPTables, Fig. 4b).

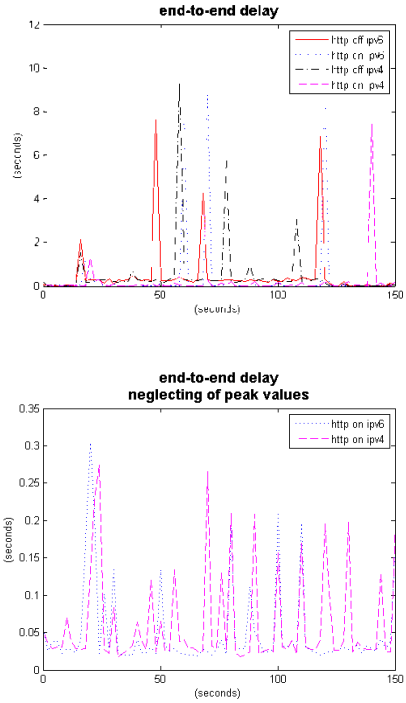

Fig. 4. End-to-end delay a) total traffic b) neglecting of peak values.

It is possible to look at experimental outputs from the perspective of the firewall. Figure 5 describes the difference of the numbers of received and sent packets in both versions of IP protocol by the firewall in inner network where the flow is corresponding to the data amount in victim case. Application of the security policy rules in IPTables/IP6Tables reduces the effect of the HTTP Get flood attack in both protocols. Simultaneously, the legitimate flows from the source network proceed unharmed.

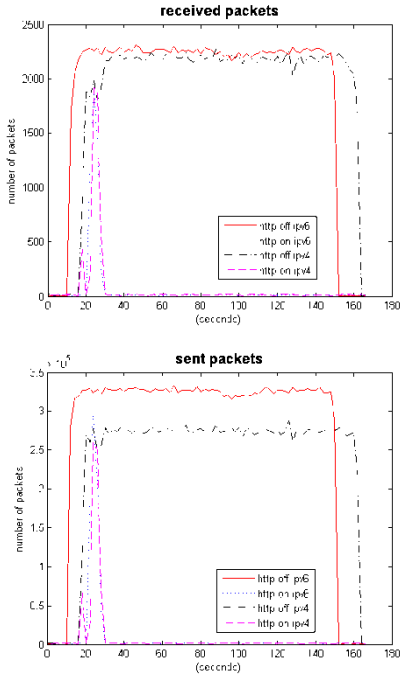

Fig. 5. Difference of number of packets by the firewall a) received and b) transmitted to the network.

4. CONCLUSION

In our paper, we show capability of IPTables to defend against DDoS attack. The IPTables applied in IPv4 as well as IP6Tables applied in IPv6 determine whether the network traffic is legitimate or not following a set of rules they contain.

Our experiments with IP6Tables demonstrate that employment of IPTables for mitigation of DDoS attacks has proved the effectiveness of this tool in IPv6 networks.

REFERENCES

ALI, W. N. A. W., TAIB, A. H. M., HUSSIN, N. M., BUDIARTO, R., and OTHMAN, J. Distributed security policy for IPv6 deployment. Sustainable Energy & Environment (ISESEE), 2011 3rd International Symposium & Exhibition in IEEE, 2011, pp. 120-124.

ALSHAMMARI, M. and BACH, C. Defense mechanisms for computer-based information systems. International Journal of Network Security & Its Applications, 2013, 5.5: 107-114.

BRASILEIRO, Francisco, et al. An approach for the co-existence of service and opportunistic grids: The EELA-2 case. In Latin-American Grid Workshop, 2008.

HRMO, R., KRISTOFIAKOVA, L., and KUČERKA, D. Developing the information competencies via e-learning and assessing the qualities of e-learning text. In: Interactive Collaborative Learning (ICL), 2012 15th International Conference on Interactive Collaborative Learning, 2012, Villach, Austria, pp. 1-4.

OURGRID PROJECT. http://www.ourgrid.org.

SILÁDI, V. and MIŽUROVÁ, V. LMS Moodle on Computing Cloud. In 4th Interantional Scientific Conference in V4 Countries, Applied Natural Sciences, Trnava, 2013

SIMON, M., HURAJ, L., and HOSŤOVECKÝ, M. IPv6 Network DDoS Attack with P2P Grid. In: Creativity in Intelligent, Technologies and Data Science. Springer International Publishing, 2015, pp. 407-415.

SIMON, M., HURAJ, L., and SILÁDI, V. Analysis of performance bottleneck of P2P grid applications. Journal of Applied Mathematics, Statistics and Informatics, 9(2), 2013, 5-11.

SINGH, S., and GYANCHANDANI, M. Analysis of Botnet behavior using Queuing theory. International Journal of Computer Science & Communication 1.2, 2010, 239-241.

VARALAKSHMI, P., and THAMARAI SELVI, S. Thwarting DDoS attacks in grid using information divergence. Future Generation Computer Systems, 29.1, Elsevier, 2013, 429-441.

ZHAO, H., LIU, X., LI, X. 2011. A Taxonomy of Peer-to-Peer Desktop Grid Paradigms. In Cluster Computing: The Journal of Networks, Software Tools, and Applications. Springer, 2011, 14(2), 2011, 129-144.

Marek Šimon
Department of Applied Informatics and Mathematics,
University of SS. Cyril and Methodius,
Slovak Republic
ladislav.huraj@ucm.sk

Ladislav Huraj
Department of Applied Informatics and Mathematics,
University of SS. Cyril and Methodius,
Slovak Republic
marek.simon@ucm.sk

Michal Čerňanský
Department of Applied Informatics and Mathematics,
University of SS. Cyril and Methodius,
Slovak Republic
michal.cernansky@ucm.sk

Received July 2015