Impact of Router Security and Address Translation Mechanisms on the Transmission Delay

Dominik Samociuk, Blazej Adamczyk, Andrzej Chydzinski

Silesian University of Technology
Institute of Informatics, Poland
email: {dominik.samociuk; blazej.adamczyk; andrzej.chydzinski}@polsl.pl

***Abstract*—We study transmission delays on an IP router caused by security and address translation mechanisms. Using a high-precision device for traffic generation and measurements and a simulated topology of two hundred end systems, we test three mechanisms of the following types: Access Control Lists, Intrusion Prevention Systems and Network Address Translation. As we show, in some cases the delay changes only a little bit, when the mechanism is turned on. In most cases however, the impact of the mentioned mechanisms is non-negligible and may increase the delay ten times in worst-case scenarios.**

Keywords–Transmission delay; IP networks, Secure architecture; Router security.

I. INTRODUCTION

One of the most important performance characteristics of computer networks is delay – the time between sending and receiving data. Transmission delays are an inherent problem of communication quality, starting with intermittent conversations via Internet telephony, through the delays in the transmission of video, ending with targeting missiles on the battlefield.

In this paper, we investigate how popular security and address translation mechanisms affect delays in IP networks. In particular, we focus on mechanisms implemented with layer 4 addressing. In the experiments, we verify the impact of Access Control Lists (ACL), Intrusion Prevention Systems (IPS) and Network Address Translation (NAT) technology on the delay generated by the device on which these mechanisms are implemented. Of course, it is to be expected that additional packet processing introduces additional delay. However, it is impossible to say in advance if this is 1%, 100% or 10000% of extra delay. Therefore, the goal of this paper is to check what is the order of magnitude of the delay induced by the studied mechanisms.

ACL [1][2][3], introduced first in Unix systems for extensive control access to files, were further extended to network devices to use higher layers in order to verify the access rights to network resources. Universal ACL consists of the information about source and destination Internet Protocol (IP) address, network mask, and port/protocol of higher layers [4].

IPS is a method for detecting and blocking attacks in real time [5][6]. Two modes of operation of the IPS are available (see, e.g., [7]):

- "Promiscuous" (Intrusion Detection System mode) – analyzes the traffic copy, which does not slow down the traffic, but cannot block attacks in real time.
- "In-line" (IPS mode) – analyzes the original traffic, slowing it down. "In-line" mode can, however, automatically block attacks in the real time.

A router with the IPS mechanism turned on operates in transparent mode [8]. This means that the system analyzes the traffic passing through the router as a transparent bridge, by analyzing the layers 2-7 and appropriately responding to the defined threats.

The paper is organized as follows. Section 3 contains an overview of the testbed prepared for the experiments. In Section 4 we present the results of the ACLs experiments. In Section 5 the influence of IPSs on delays is studied. Section 6 describes the impact of the NAT mechanisms on transmission delays. The paper is concluded in Section 7.

II. RELATED WORK

For now, research activities are polarized in the following directions. Firstly, studies on developing improved mechanisms, such as detecting and reducing redundancy in ACLs, [9], or classification, analysis and deleting conflicts in Intrusion Prevention and Detection Systems, [10], are carried out. In addition to the direction of improving actual features, there are studies on other architecture schemes, such as network virtualization and software-defined networks [11]. However, there are no research paper, validating security mechanism with high-precision hardware traffic generator.

III. TESTBED

The testing environment was built using a high-precision hardware traffic generator, which allows to generate artificial traffic with characteristics needed in the prepared test scenarios with full line rates, as well as measure and analyze the arriving packets with time precision of 20ns. Moreover, the generator enables simulation of a virtual topology composed of many interconnected devices.

Namely, the Ixia generator with XM2 casing was used [12]. XM2 dual-port casing provides a platform to build a topology-based Ixia's test solutions. Working with the family of test applications, XM2 is the basis of a complete environment for testing the performance and operation of the network. The casing allows installation of different modules for traffic generation: up to 32 Gigabit Ethernet ports, up to sixteen 10G Ethernet ports, and a single Ethernet port 40G, 100G or a single dual-port 40/100G Ethernet. These modules provide the necessary processing to test the application layers 2-7, the signaling, voice and video transmission, etc.

 ISBN: 978-1-61208-435-0

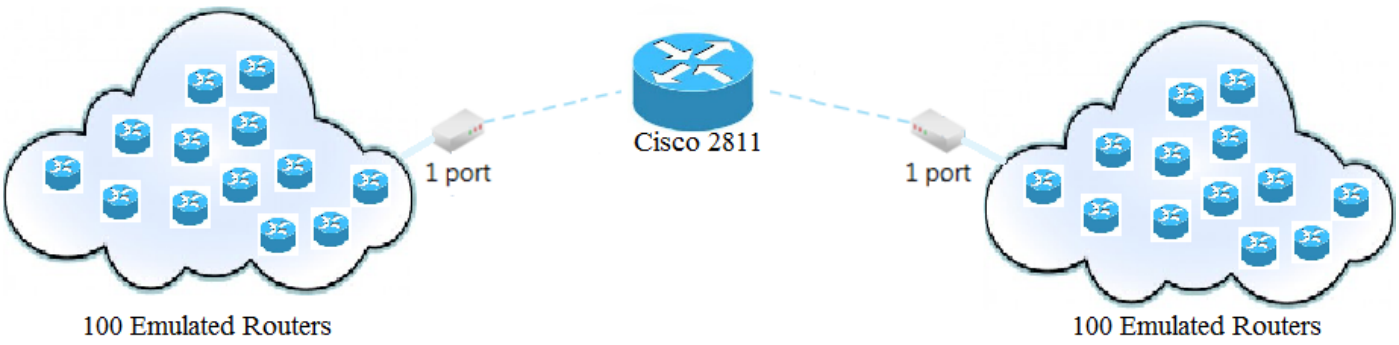

Figure 1. Virtual topology configuration.

The load module used in the tests, is an LSM1000XMVDC8-01 Gigabit Ethernet Load Module [13], offering full functionality for testing layers 2-7. Each port supports the generation and analysis of layers 2-3 with line rate, as well as high-performance emulation of routing and switching protocols. In order to monitor the traffic with high accuracy in real time, the device uses specialized programmable circuits. The load module used in this study was 8 ports (copper or fiber), operating in the range from 10Mbps to 1Gbps. Each port on the card has a separate RISC processor running Linux and a fully optimized stack for testing TCP/IP. This architecture provides the performance and flexibility in testing of routers, switches, broadband and wireless Internet access, access devices, web servers, video servers, gateways, firewalls, etc.

The Ixia's IxNetwork software is an application designed to test the performance and functionality of routers and switches [14]. IxNetwork works on separate modules and processors for each port. From the software perspective, each of them is a separate instance of Linux operating system. With this solution, each interface is tested independently, and the state of the corresponding instance is passed to the supervisor machine based on Microsoft Windows operating system.

IxNetwork software provides an easy-to-use graphical interface, which can be used to configure and run complex tests. Using IxNetwork tester, we can easily set up protocol variables and parameters specific to the needs of the device under test.

The specific testbed was chosen to emulate real traffic instead of just simulating it, which is usually the contemporary method nowadays. Ixia's hardware allow generate traffic with desired parameters, and then, with high-precision measured transmission delay generated by described security mechanisms. Devices chosen for tests have been selected to meet the specifications for possibility to configure discussed security mechanisms.

The configuration of the testing environment used in the experiments is depicted in Figure 1. The first topology is simulated on the input port, and the second topology on the output port of the Ixia's load module. Each topology consists of 100 devices. This is meant to simulate the connection between different pairs of addresses (Media Access Control- MAC, IP, etc.), transferred through the device under test. All the tests were carried on a single Cisco 2811 router (as in the middle of Figure 1), however due to similar architecture devices from the same class (access class devices for our studies) should generate comparable delays.

The traffic generated by the generator had the following parameters:

- direction of the flow, D, which was H or F (H meaning the alternating two-way traffic, i.e., half-duplex, F meaning the simultaneous two-way traffic, i.e., full-duplex),
- lack of optimization (Quality of Service (QoS) settings and IP Type of Service (ToS) Precedence),
- package size, S, in bytes,
- duration of the test, T, in seconds,
- load of the line, C, in percentage (e.g., 10% means that the percentage of transmission data including individual headers is 10% of the total capacity of the link).

The delay was measured from the time of completing the generation of the entire package to the last received bit on the receiver side (Last-In-Last-Out - LILO methodology). This is the default schema of time-stamping on Ixia devices.

Each test was repeated 1000 times. In the following sections, the resulting delays are presented in terms of the mean value and standard deviation based on the unloaded variance estimator.

IV. The Impact of Access Control Lists on Delay

The purpose of this set of tests was to verify the delay that is induced by the use and actions of ACLs in three scenarios:

- 100% of the traffic is proven through the ACL that allows traffic on the first rule,
- 100% of the traffic is proven through the ACL, in which the variable parameter is the number of traffic rules (all allowing traffic),
- 50% of the traffic is rejected by the ACL. The remaining traffic goes through a control list on the first rule and is checked whether the rejection affected the delay or not.

On the router, the standard and extended ACLs consisting of 1, 100, and 1000 dynamically generated entries were configured. The purpose of the test was to check what is the increase of delay when dealing with 1 and 1000 ACLs. An example of the extended ACL configuration with one entry (permitting traffic from 10.0.0.0/24 subnet to 10.0.1.0/24 subnet) is presented on Figure 2.

 ISBN: 978-1-61208-435-0

```
access-list 100 permit ip
    10.0.0.0 0.0.0.255 10.0.1.0 0.0.0.255
```

Figure 2. ACL configuration with one entry.

The tests of ACLs were carried out with disabled CEF (Cisco Express Forwarding) mechanism, [15].

Measurements were performed with the following parameters set:

- Direction: Full-duplex,
- Size: 64 B,
- Time: 30 seconds,
- Load: 10%,
- Number and type of checklists: a variable parameter.

TABLE I. RESULTS OF ACL TESTS.

The number and type of ACL rules	Delay [μs]
No ACL	147±1.23
1 – Standard list	150±1.89
100 – Standard list	270±2.5
100 – Extended list	310±3.3
1000 – Extended list	1500±32
2 streams – rejected + passed	150±1.93

The results of the experiments are presented in Table 1. As we can see, the implementation of ACLs may degrade significantly the observed delay. In particular, the usage of a single entry ACL had no significant effect on the delay, but a checklist of 100 entries increased the delay to 190% (standard list) and to 210% (extended list) of the original value. Exploiting ACL with 1000 entries increased the delay to 1000% of the base value.

It can be seen that the delay generated by ACLs increased approximately linearly with the number of rules.

V. DELAYS INDUCED BY THE INTRUSION PREVENTION SYSTEM

These tests were performed to verify the IPS system overhead while scanning and detecting attacks in the traffic. The configuration of the router IPS is presented on Figure 3. The presented syntax, create ips rule, add signatures for basic vulnerabilities and enable it on the device. Prepared configuration allowed to check what is the transmission delay when traffic is passed through IPS mechanism with basic security rules.

The tests of IPS mechanisms were carried with enabled CEF mechanism. In the tests, the IPS mode was set to ”Inline”, which in addition to detection of attacks enables also preventing them in real time. The default thread signature was used [16], which provides a basic level of protection against a wide range of typical dangers.

Measurements were performed with the following parameters set:

- Direction: Full-duplex,
- Size: 64 B,
- Time: 30 seconds,

```
ipips name sdm_ips_rule
ipips signature-category
category all
retired true
categoryios_ips basic
retired false
(...)
ipips signature-definition
signature 2004 0
status
retired false
enabled true
```

Figure 3. Configuration of the router IPS.

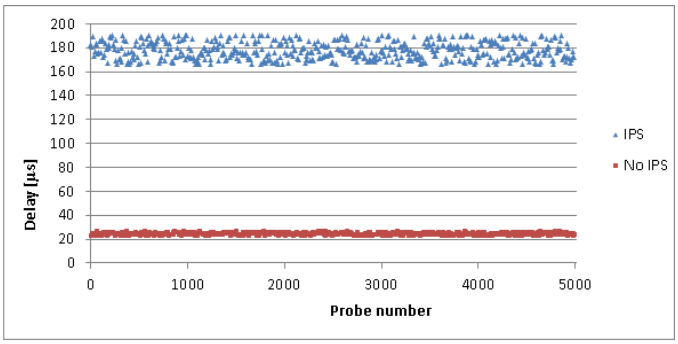

Figure 4. Distribution of probes in IPS tests.

- Load: 10%.

Packet contain random data without any specific patterns to just pass-through IPS without raising any alarms. This payload type let measure actual IPS delay without false-positives with shorter delay, due to IPSs detection time.

The measured delay without IPS averaged at 26±1.2μs. Measured delay with IPS enabled averaged at 178±5μs. The values of the delay collected during the tests without and with the IPS mechanism are shown in Figure 4.

We can conclude that even a basic set of the IPS rules significantly increases the delay (700% of the initial value). Of course, the delay would be even greater for a larger number of signatures.

In the additional tests that were performed, with IPS enabled and operating in the ”Promiscuous mode”, the delay averaged at 28±0.6 μs. This shows that in the ”Promiscuous” mode, basically no additional delay is induced. (The addition of 2μs resulting from the need to copy the traffic flow on a different port is negligible). It must be remembered, however, that this mode does not provide protection in real time.

VI. ADDRESS TRANSLATION IMPACT ON DELAY

Since the 90s, the IPv4 addressing space has been considered too small and the pool of addresses is still lowering. Creating the IPv6 standard solved the problem, but there are several issues that slow down migration to the new protocol [17][18]. Therefore, IPv6 is still not the most common method of preventing exhaustion of IPv4 addresses. Instead, local area networks use private addresses, which are translated into public

 ISBN: 978-1-61208-435-0

```
ip nat inside source static x.x.x.x
    x.x.x.x
```

Figure 5. Static NAT configuration.

```
ip nat pool xxxxxxxx PULA_NAT netmask
    255.255.255.0
ip access-list extended NAT
permit ip 10.0.0.0 0.0.0.255 any
ip nat inside source NAT pool lists
    PULA_NAT
```

Figure 6. Dynamic NAT configuration.

addresses using NAT method [19][20], when routed to the global network. RFC 1918 [21] describes the address class division and their pools due to the allocation of public and private parts. NAT concept was developed in three branches and implemented in three different ways in the network devices:

- Static Translation – one internal address is translated into one external address – no advantages associated with a reduction of usage of public IPv4 addresses.
- Dynamic Translation – some internal addresses are translated into several external addresses. The allocation is dynamically translated by the device.
- Port Address Translation (PAT) – several internal addresses are translated into one external address. Distinguishing between internal addresses is made by dynamic assignment of ports to them.

In this set of tests, the impact of NAT on network delays was verified. The following configuration was used.

- Static NAT configuration is presented on Figure 5 - where one internal IP address is translated to one external IP address.
- Dynamic NAT configuration is presented on Figure 6 - where internal IP addresses are translated to external IP addresses chosen from the specified pool.
- PAT configuration is presented on Figure 7 - where multiple internal IP addresses are translated to one external IP addresses.

The tests of NAT mechanisms were carried with disabled CEF mechanism. The measurements were performed with the following parameters set:

- Direction: Full-duplex,
- Size: 64 B,
- Time: 30 seconds,

```
ip nat pool xxxxxxxx PULA_NAT netmask
    255.255.255.255
ip access-list extended NAT
permit ip 10.0.0.0 0.0.0.255 any
ip nat inside source NAT pool
    PULA_NAT letter overload
```

Figure 7. PAT configuration.

TABLE II. RESULTS OF NAT TESTS.

Type of translation	Delay [μs]
No translation	147±2.6
Static NAT	151±2.8
Dynamic NAT	155±3
PAT	257±3.7

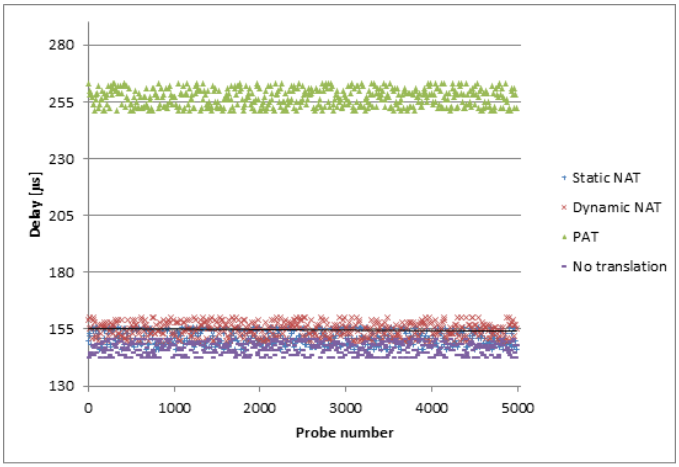

Figure 8. Distribution of probes in NAT tests.

- Load: 10%.

The results are presented in Table 2. As we can see, NAT in its static and dynamic versions does not introduce much overhead on the transmission delay. This has to be due to the simplicity of the operations that are executed and simple single cycles of the processor required for its implementation.

On the other hand, NAT with port translation (PAT) induces the delay of 175% of the original value. This is due to the need to use the layer 4 addressing of ports and analysis of data stored in the segment header.

Detailed test results are shown in Figure 8.

VII. Conclusion and Future Work

The studies conducted in the paper demonstrated the order of magnitude of additional delay induced by traffic filtering and security mechanisms. In the ACL case, the extra delay grows more or less linearly with the number of rules. For 100 rules the observed delay was twice as large as without ACL. For 1000 rules the delay increased 10 times. In the case of IPS set to in-line mode, the delay seven times larger than the original was observed. On the other hand, IPS in promiscuous mode had a negligible impact on the delay. Also the static and dynamic NAT had a minor impact of the delay. The PAT version, however, enlarged the delay by 75%.

As for the future work, the authors are working on a study of combined effects/mutual influence generated by described mechanisms. Also, an interesting continuation would be a study on the methodology of finding a secure topology design, while using as little overhead on the performance, as possible. In other words, the trade-off between the security and delay may be investigated. As long as we cannot allow for the degradation of security at the expense of increased performance, the solutions we are going to work on will focus

 ISBN: 978-1-61208-435-0

on the migration to the new ways of creating network topology, inter alia, programmable networks.

REFERENCES

[1] J. Daly, A. X. Liu, and E. Torng, "A difference resolution approach to compressing access control lists" in INFOCOM, 2013 Proceedings IEEE, 2013, pp. 2040 – 2048.

[2] R. Watson, "A decade of OS access-control extensibility" in Communications of the ACM., v.56 n.2, 2013, pp. 52 – 63.

[3] L. Zhu, H. Mao, and H.Qin, "A case study on Access Control Rules Design and Implementation of Firewall" in Proc. 8th International Conference on Wireless Communications, Networking and Mobile Computing, 2012, pp. 1 – 4.

[4] A. Sudarsan, A. Vasu, and D. Ganesh, "Performance Evaluation of Data Structures in implementing Access Control Lists" in International Journal of Computer Networks and Security, vol. 24, issue 2, 2014, pp. 1303 – 1308.

[5] H. Ling – Fang, "The Firewall Technology Study of Network Perimeter Security" in Proc. IEEE Asia-Pacific Services Computing Conference, 2012, pp. 410 – 413.

[6] M. Z. A. Aziz, M. Y. Ibrahim, A. M. Omar, R. A. Rahman, M. M. M. Zan, and M.I. Yusof, "Performance analysis of application layer firewall" in Proc. IEEE Symposium on Wireless Technology and Applications (ISWTA), 2012, pp. 182 – 186.

[7] Z. Li, A. Das, and J. Zhou, "Theoretical basis for intrusion detection" in IEEE workshop proceedings on information assurance and security, 2005, pp. 184 – 192.

[8] M. Gil-Jong, K. Yong-Min, K. Dong-Kook, and N. Bong-Nam, "Network Intrusion Detection Using Statistical Probability Distribution" in Proc. Inter Conference: ICCSA(2), 2006, pp. 340 – 342.

[9] A. X. Liu, C.R. Meiners, and Y. Zhou, "All-Match Based Complete Redundancy Removal for Packet Classifiers in TCAMs" in The 27th Conference on Computer Communications (INFOCOM), 2008, pp. 111 – 115.

[10] E. Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan, "Conflict classification and analysis of distributed firewall policies" in IEEE Journal on Selected Areas in Communications, vol.23, no.10, 2005, pp.2069 – 2084.

[11] R. Corin, M. Gerola, R. Riggio, F. De Pellegrini, and E. Salvadori, "Network Virtualization and Beyond" in EWSDN, 2012, pp. 24 – 29.

[12] Ixia, http://ixiacom.com, [retrieved: July, 2015].

[13] Ixia Load Modules, http://www.ixiacom.com/sites/default/files/resources/datasheet/gigabit_ethernet_xmvdc_lan_services_modules.pdf, [retrieved: July, 2015].

[14] Ixia IxNetwork, http://www.ixiacom.com/products/ixnetwork, [retrieved: July, 2015].

[15] CEF Mechanism, http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfcef.html, [retrieved: July, 2015].

[16] IOS IPS Routers, http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-1/user/guide/CSMUserGuide_wrapper/ipsios.html, [retrieved: July, 2015].

[17] T. Bilski, "Network performance issues in IP transition phase" in Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference, 2010, pp. 39 – 44.

[18] K. Chakraborty, N. Dutta, and S. Biradar, "Simulation of IPv4-to-IPv6 dual stack transition mechanism (DSTM) between IPv4 hosts in integrated IPv6/IPv4 network" in Computers and Devices for Communication, 2009. CODEC 2009. 4th International Conference, 2009, pp. 1 – 4.

[19] V. Krmicek, J. Vykopal, and R. Krejc, "Netflow Based System for NAT Detection" in Co – Next Student Workshop09: Proc. International student workshop on emerging networking experiments and technologies, 2009, pp. 23 – 24.

[20] R. Li et. al., "Passive NATted Hosts Detect Algorithm Based on Directed Acyclic Graph Support Vector Machine" in Proc. 2009 International Conference on Multimedia Information Networking and Security – Volume 02. MINES09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 474 – 477.

[21] RFC 1918, http://www.hjp.at/doc/rfc/rfc1918.html, [retrieved: July, 2015].

 ISBN: 978-1-61208-435-0