ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/273918445

Network Protection Against DDoS Attacks

Article *in* International Journal of Advances in Telecommunications Electrotechnics Signals and Systems · March 2015

DOI: 10.11601/ijates.v4i1.103

CITATIONS
8

READS
2,958

3 authors:

Petr Dzurenda
Brno University of Technology
63 PUBLICATIONS **759** CITATIONS
SEE PROFILE

Zdenek Martinasek
Brno University of Technology
51 PUBLICATIONS **623** CITATIONS
SEE PROFILE

Lukas Malina
Brno University of Technology
115 PUBLICATIONS **1,676** CITATIONS
SEE PROFILE

All content following this page was uploaded by Lukas Malina on 19 February 2016.

The user has requested enhancement of the downloaded file.

Network Protection Against DDoS Attacks

Petr Dzurenda, Zdenek Martinasek, Lukas Malina

***Abstract*—The paper deals with possibilities of the network protection against Distributed Denial of Service attacks (DDoS). The basic types of DDoS attacks and their impact on the protected network are presented here. Furthermore, we present basic detection and defense techniques thanks to which it is possible to increase resistance of the protected network or device against DDoS attacks. Moreover, we tested the ability of current commercial Intrusion Prevention Systems (IPS), especially Radware DefensePro 6.10.00 product against the most common types of DDoS attacks. We create five scenarios that are varied in type and strength of the DDoS attacks. The attacks intensity was much greater than the normal intensity of the current DDoS attacks.**

***Keywords*—Distributed Denial of Service Attacks, DDoS, Network protection, Security, Stress Testing, Cyberattacks.**

I. Introduction

Nowadays, cyberattacks have a significant role in the part of a computer crime. DDoS attacks are an integral part of these attacks. DDoS attack is a subset of a simpler and sometimes better known DoS (Denial of Service) attack. The main purpose of these attacks is to put targeted service to the nonfunctional state, it causes a denial of this service for regular users. A reason can be caused by bandwidth overload of the targeted server providing some services or any other resources. In some cases, an attacker can also get a targeted device to the inactive state. Attacks are usually aimed at web services or services of various organizations and corporations e.g. news servers, banks, government departments, enterprises etc. The main difference of DoS and DDoS attacks is in the line of attack. DoS attack uses only one network node (e.g. personal computer (PC) or server) and single Internet connectivity. The network node is directly under control of the attacker. On the other hand, the DDoS attack uses more than one network nodes and more than one Internet connectivity. These compromised network nodes are called zombies or botnets and they are not directly under the control of the attacker. It causes that the attack is consisted of large quantities of requests (usually hundreds or thousands), which can be realized from all over the world. The attacker usually creates a necessary infrastructure of botnets simply with using Trojan horses or other malware, which are running on infected network nodes of victims.

Manuscript received January 10, 2015, revised February 24, 2015.

P. Dzurenda is with Dept. of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 12, 616 00 Brno, Czech Republic, email: dzurenda@phd.feec.vutbr.cz.

Z. Martinasek is with Dept. of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 12, 616 00 Brno, Czech Republic, email: martinasek@feec.vutbr.cz.

L. Malina is with Dept. of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 12, 616 00 Brno, Czech Republic, email: malina@feec.vutbr.cz.

Nowadays, any devices (e.g. personal computers, servers, smartphones etc.) which are connected to the Internet can become botnets. The basic principle of DDoS attack is depicted in Fig.1. The DDoS attack communication behaviour usually seems as a normal traffic. Hence, it is so hard to detect and to defense against this type of attack compared to simpler DoS attack. The DDoS attacks focus on a target nodes in a certain time and with a certain intensity of attacks. The intensity is much bigger than in DoS attacks. The recent DDoS incidents from 2009 to 2012 are listed in the work [1].

In 2013, two biggest DDoS attacks of history were made. The first attack was targeted at Spamhaus cyber-assault in March 2013. The attack had intensity of about 300 Gbps. In that time it was marked as ”the biggest cyberattack in the history”. In February 2014, the second attack with intensity about 100 Gbps higher than previously mentioned attack was realized. The attack had intensity of 400 Gbps and it was targeted at CloudFlare CEO Matthew Prince. However, most of DDoS attacks (more than 80%) have usually lower intensity about 50 Mbps with duration about half an hour.

Currently, the infrastructure of botnets is ready to begin an attack anytime. This is the reason why it is important to ensure maximum protection and security of every network infrastructure. The DDoS attack is able to cause not only damages due to denial of online services to users, but can also reduce the credibility of companies and their services.

In this paper, we test the ability of current commercial IPS system Radware DefencePro against current DDoS attacks. We tested its ability to detect and filter the most common types of the DDoS attacks, such as SYN flood, UDP fload, Reset flood and Xmas flood. Moreover, the realized attacks had intensity about 900 Mbps, which is much greater than current attacks usually have. The objective was to determine whether the device is able to withstand the current DDoS attacks.

II. Types of DDoS attacks

In this section, we describe and analyze the basic types of DDoS attacks. The types of DDoS attacks are dependent on the protocol where the attack is realized, for example HTTP (Hypertext Transfer Protocol), ICMP (Internet Control Message Protocol), UDP (User Datagram Protocol), TCP (Transmission Control Protocol), DNS (Domain Name System), SIP (Session Initiation Protocol). We distinguish attacks by impact on the targeted victim (bandwidth, memory, CPU) and cut-down services based on software bugs. According to the work [1], attacks can be distinguished to two basic types, flooding attacks and logical attacks.

A. Flooding attacks

This type of a DDoS attack is aimed at overloading the server resources such as bandwidth, memory or CPU by using

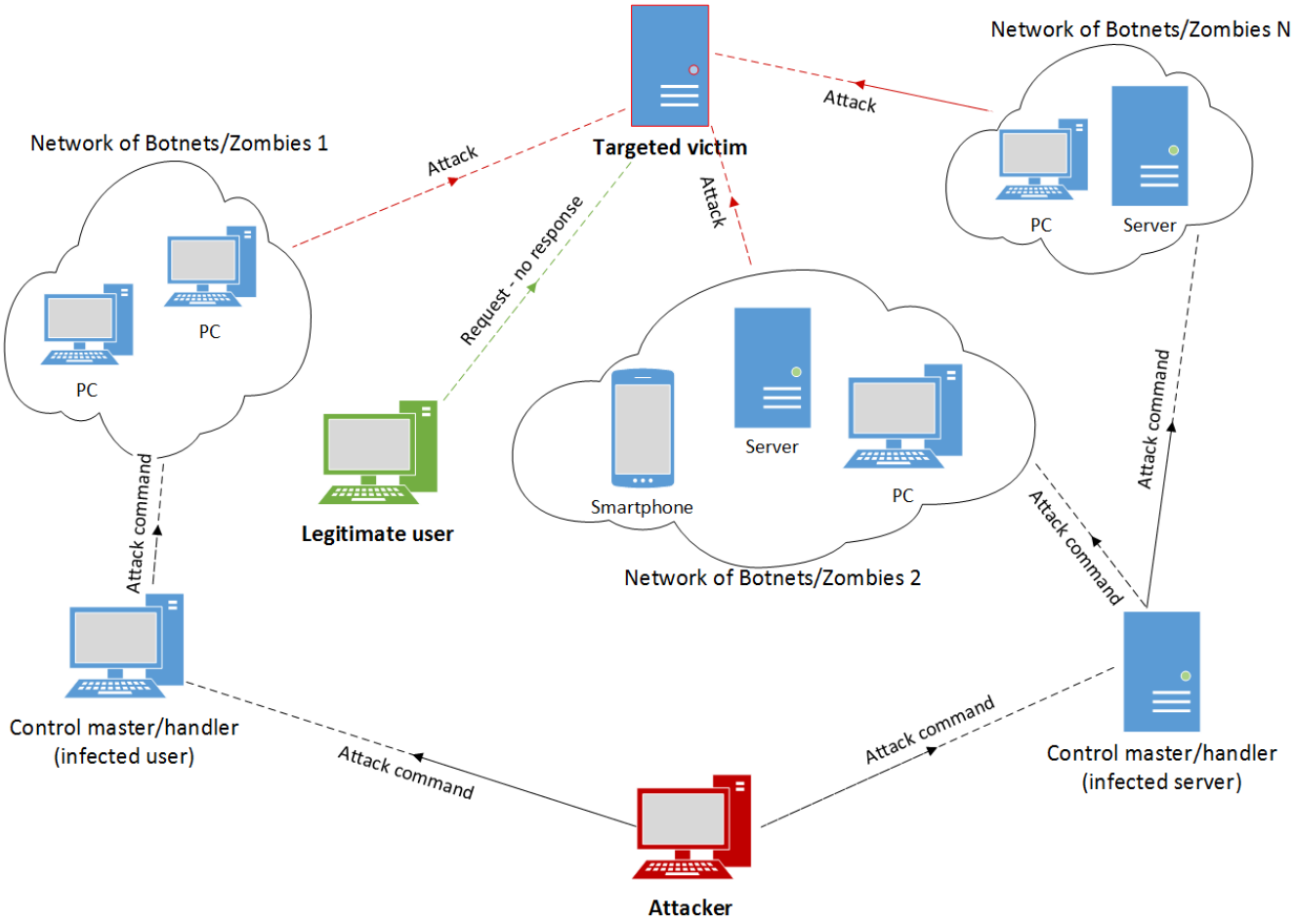

Fig. 1. The principle of a DDoS attack.

the large quantity of packets. This process causes a denial of service for the legitimate users. Flooding packets are usually implemented through the weaknesses of communication protocols (TCP, UDP, ICMP, FTP, SIP or HTTP). The most important flooding attacks are described below.

The SYN flood attack is the most common type of flooding attacks. It is based on half-open TCP connections. Classical TCP connection consists of 3-way handshake (SYN, SYN/ACK, ACK). During this attack, an attacker sends SYN packet with spoofed source IP address to the server (victim). The server reserves system resources for this potential connection and replies SYN/ACK to the spoofed IP address. The server waits for response ACK but it does not come. After some time, the server releases allocated resources. Strength of this attack depends on large quantities of SYN packets. The server exhausts its resources and it is not able to provide required services to legitimate users.

The UDP flood attack is based on sending large quantity of UDP datagrams that are targeted to random ports. A server (victim) tries to find some applications that listen on these ports. In case of no application listen, the server sends an ICMP message ”Destination unreachable”. The large quantities of UDP messages cause cut-down of the targeted system.

The ICMP flood attack is sometimes called *the Smurf attack* or *the Ping flood attack*. This attack sends a big amount of ICMP ECHO requests to the multicast IP address of any vulnerable network. A source IP address of the request is the same as the IP address of a victim. All nodes in this targeted network reply with an ICMP ECHO response message to the victim. The flood of ICMP ECHO responses cause an overload of the target system. The attack is realized on the network layer of TCP/IP. *The Fraggle attack* is similar to the ICMP flood attack, but it is realized on the transport layer of TCP/IP. The attack is based on using a UDP ECHO request (port 7) and a UDP Charge (port 19).

The ARP flood attack is based on flooding the targeted victim by spoofed ARP (Address Resolution Protocol) requests. It causes an exhaustion of computing and/or memory resources on the victim side. These types of attacks are suitable for use in a local network. Another way can be periodical sending of spoofed ARP responses (e.g. from network gateway) containing the IP address of the attacker. This attack is called *the ARP Spoofing Attack* and it realizes

known MITM (Man In The Middle) attack, when the all traffic is routed over the attacker.

The Xmas tree attack, an attacker generates so called Christmas tree packets, which have got set flags such as FIN, URG, and PSH in the TCP header. Processing these flags is difficult. This fact causes an overload of the targeted node in case of lots of incoming packets.

The Reset flood attack uses TCP packets, which contain a RST flag and spoofed source IP addresses. If lots of these packets are sent to victim's ports then there is a high probability that some existing connections will be reset.

The Unreachable host flood attack is similar to the Reset flood. An attacker sends an ICMP message "Host unreachable" to the random ports to the victim side and with a spoofed source IP address. There is a some probability that an existing session will be cancelled.

B. Logical attacks

Logical attacks aim at the weakness of applications or software on an targeted device. These attacks use small amounts of messages opposite to flooding attacks. The purpose is to get the targeted device to the non-functional state. The best known types are described below.

The Ping of death – an attacker sends a ping message with the data size higher than 65 535 b, which is maximum defined packet size in TCP/IP. The system running on targeted node tries to reassemble the packet. This may cause buffer overflow error and system may crash.

The Teardrop attack – an attacker sends two or more packet fragments with incorrect setting of offset. Fragments cannot be correctly reassembled to original packet. It often causes system crash.

The Land attack – an attacker sends a SYN packet to a victim. The packet has got spoofed source IP address and port, they are same as the victim's IP address and port. The victim tries to establish a connection to itself, which may cause its downfall.

Other types of attacks such as the DNS Query attack, the HTTP flood attack, the SIP flood attack etc. can be found in [1], [2] or in [3]. The recent versions of software systems eliminate many errors and weaknesses. However, it is necessary to periodically update these systems with actual security patches to protect them against existing logical attacks.

III. Detection of DDoS Attacks

Detection methods try to detect DDoS attacks in regular operations before a targeted device is affected. This early detection alerts the administrator of the targeted node, which can reduce the consequences of the attack to a minimum. It can be ensured by using a network security device or/and by using well-designed load balancing. Generally, the detection methods are divided as signature and anomaly detection.

A. Signature detection

The detection methods using the signatures are based on the good knowledge of DDoS attacks. Usually, the characteristics are manually constructed by a group of experts, and signatures are implemented to security and surveillance network devices. Monitoring the packet headers by firewalls, routers or Intrusion Detection Systems (IDS) helps to recognize the symptoms of incoming DDoS attacks. Signature detection methods are effective only against known types of DDoS attacks. Therefore, these detection mechanisms do not recognize new and unknown attacks. The most commonly used detection methods or symptoms are presented in [4], [5].

B. Anomaly detection

Some types of DDoS attacks are detected and classified by finding anomalies in the network traffic. For example, flood attacks using TCP-SYN, UDP or ICMP packets increase of these packets can be observed. These detection methods are trying to find some anomaly in the normal network traffic. The work [6] shows the possibility of using artificial intelligence such as neural networks and genetic algorithms to detect unusual network traffic and the classification of DDoS attacks in the normal network traffic. At first, this artificial intelligence learns how normal network traffic seems and then it tries to detect differences between them. Authors of work [7] use detection technique based on a decomposition of time series. Work [8] uses covariance analysis model for SYN flooding attacks detection and in works [9], [10], entropy-based method are used. The disadvantage of these detection methods is often a larger number of false alarms. On the other hand, these methods are able to recognize new types of attacks.

IV. Protection against DDoS attacks

Generally, a DDoS defense mechanism consists of four basic parts. At first, it is a DDoS prevention. The attack detection is the next part. This part determines the source of the attack and classifies malicious packets in the network traffic. The next part is a reaction that is designed to stop an attack, or to limit the damage caused by the effects of the attack. This involves dropping the malicious packets or providing the services on the backup device/line or ensuring the partially availability of the services by using the Quality of Service (QoS). All these actions must not influence regular traffic. The proposal of a complex security solution that is suitable for a defense against all known and unknown DDoS attacks is very difficult. DDoS defense solutions can be maintained by the sophisticated combination of a robust network infrastructure, including an active security network equipment such as firewalls, honeypots, IDS sensors (Intrusion Detection System) or IPS (Intrusion prevention System) which are capable of DDoS attack detection and providing the defense of a protected network/server. The flexible management

and supervision are often also important. It is also important to establish emergency scenarios in case of a DDoS attack. The basic methods and techniques which can partially eliminate DDoS threats are described in the following sections.

A. Network infrastructure security

A secure network infrastructure should consist of network security devices such as routers, firewalls, IDS systems or better IPS systems and so called honeypots. The main purpose of honeypots is to create a fake weakness in the infrastructure. This honeypots could be potentially attacked and it detects these attacks. Some DDoS attacks can be detected in real time using detection components as IDS systems. The malicious packets are filtered by the firewall. Border routers can also reduce the impact of DDoS attacks on the protected network or server. Redundant lines and servers can mitigate DDoS attacks and ensure access for authorized users. These basic defense types are presented in [11], [12] or in [13].

B. Black and white lists protection

Simple security solutions against DDoS attacks are presented in [14]. Transactions and request packets from legitimate users are shifted to the backup link. The IP addresses of authorized users are stored on the "whitelist" after successful authentication. If the IP addresses are detected as suspicious, they are stored on "blacklist". This type of defense may contain two firewalls, which are controlled by one management system that manages both sheets.

C. Defense by using offensive methods

In [15], the authors present a method which reduces the effect of DDoS attacks by using the offensive approach. The principle of this approach is based on increasing the number of request packets from legitimate users. Due to this fact, the legitimate user receives the response from the server with higher probability. This defensive technique is only effective for a small group of DDoS attack types.

V. Realized experiments

This section contains the description of security tests and the results from Radware DefensePro 6.10.00 against the most common DDoS attacks, such as SYN flood, UDP flood, Reset flood and Xmas flood. The test results serve as a feedback that shows the need to protect a network against these types of attacks. Furthermore, the configuration of the DDoS filter and its efficiency for network protection are presented here.

A. Security testing

In this security test, IPS (Intrusion Prevention System) Radware DefensePro is tested by using the network tester/generator (stress tester) Spirent Avalanche 3100B against the influence of the DDoS attacks. The tester enables the comprehensive testing of a network infrastructure based on IP protocol. The tester is able to generate real traffic up to 20 Gbps (2x10 GbE) and allows the emulation of network clients and servers on layers L4 – L7. The stress tester offers 15 types of DDoS attacks. A software component Attack Designer allows us to build own attacks. As a tested device, which provides a protection against DDoS attacks, Radware DefensePro 6.10.00 has been used. This device is able to detect and filter DDoS attacks up to 12 Gbps in real time. The filter supports technologies 10 Gb and 100 Gb Ethernet. The device has one management port, which is used for getting reports. To get the reports some management interfaces for example APSolute Vision, web interface and a console interface can be used. DefensePro provides the following security protection:

Network-wide protection – includes the following:

1) *Behavioral DoS* – protection against zero-day flood attacks, including SYN floods, TCP floods, UDP floods, ICMP and IGMP floods.
2) *Scanning and worm protection* – zero-day protection against self-propagating worms, horizontal and vertical TCP and UDP scanning, and ping sweeps.
3) *SYN protection* – protection against any type of a SYN flood attack using advanced SYN cookies. The SYN flood attack is usually aimed at specific servers with the intention of consuming the server's resources. However, the configuration of the SYN protection as a network protection allows easier protection of multiple network elements.

Server protection – includes the following:

1) *Connection limit* – protection against session-based attacks, such as half open SYN attacks, request attacks and connection attacks.
2) *Server-cracking protection* – zero-day protection against application-vulnerability scanning, brute-force and dictionary attacks.
3) *HTTP Mitigator* – mitigates zero-day HTTP page flood attacks.

Signature-based protection – protection against known application vulnerabilities and common malware, such as worms, trojans, spyware, and DoS.

Access Control List – provides stateful access control.

The block scheme of the security testing testbed is depicted in Fig. 2. The scheme consists of the stress tester (Avalanche 3100B), the tested device (Radware DefensePro 6.10.00), a management server APSolute Visio and a control terminal. The control terminal is used to configure both the tester and the filter, and to display results and characteristics obtained during the test. Two 10 GbE ports of the tester (Port12 and Port13) have been used during testing. The first port has been configured to generate the legitimate traffic and, in addition, some types of DDoS attacks. The second port has been configured to emulate the servers of selected protocols. Five scenarios for FTP (File Transfer Protocol) and HTTP (Hypertext Transfer Protocol) application-layer protocols have been created. The Radware filter has been connected between the ports and configured to filter the DDoS attacks while leaving the legitimate traffic without any modification. For each scenario, the test has been run with the deactivated filter. Then, the filter has been activated. The goal of testing has

been to evaluate how helpful the filter Radware is in a DDoS attack mitigation.

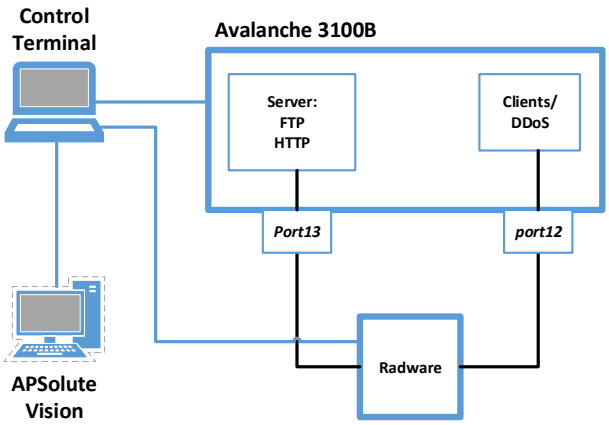

Fig. 2. Block scheme of the security testing testbed.

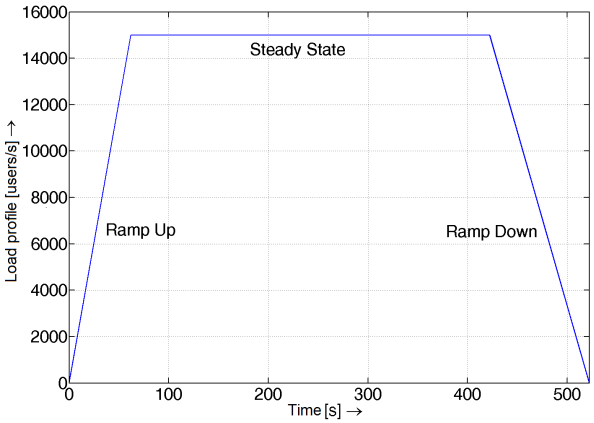

Fig. 3. FTP and HTTP load profile graphs.

B. Scenario specification

In each created scenario (a security test), the stress tester is used for simulating both communicating parties, users and servers. The Port12 is configured to generate the client traffic and the DDoS attack on the IPv4 network. The Port13 is used to emulate the servers with respective services on standard ports on the IPv4 network. In each tested scenarios, a single 1 kB file is repeatedly transferred using the FTP protocol from a server listening on ports 20, 21 and at the same time a web-page is repeatedly transferred using the HTTP protocol from a server listening on the port 80. On this regular network traffic, we apply different types of DDoS attacks such as DDoS SYN flood, UDP flood, Reset flood a Xmas flood. In first four scenarios, attacks are applied separately and in the fifth scenario they are applied together.

In all scenarios, the load profile is specified by the number of users performing defined actions per second during the entire test. In testing scenarios, each user performs FTP file transfer of size 1 kB and loads a web page. This load is specified in the tester by a load profile. The load profile graph contains the Ramp Up, Steady State and Ramp Down sections as depicted in Fig. 3 for the FTP and HTTP scenario. The detailed information regarding specification of the individual scenarios are presented in the Tab. I.

C. Achieved results

The results of the security tests of the Radware DefensePro 6.10.00 are obtained by using the Avalanche Commander, Spirent Avalanche Analyzer and APSolute Vision. The graphical representation of all scenarios results with the filter disabled is depicted in Fig. 4. In the graphs, the success rate of the application-layer transactions is depicted for all tested scenarios depending on the type and intensity of DDoS attack. The protocols success rate is 38% in the case of DDoS SYN flood attack, successful transfer for UDP flood is 80%, in case of Reset flood it is 78% and for Xmas flood it is 88%, when the DDoS attack is deployed. The fifth graph describes the successful transfer in case of an attack, when all attacks are applied together to the regular network traffic. The success rate is only 12%. The graphical representation of all scenarios results with the filter enabled is depicted in Fig. 5. All the scenarios have success rate of 100% if the filter is enabled. The results show the positive impact of the DefensePro 6.10.00 filter. The DDoS attack is completely mitigated and the network infrastructure is fully functional if the filter is enabled. All results were obtained from the Spirent Avalanche device.

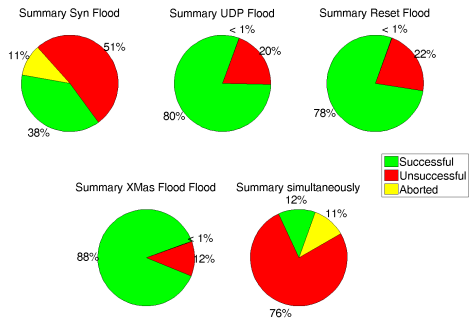

Fig. 4. Summary results for the disabled Radware DefensePro filter.

Tab. II and Tab. III show the numerical values of all tests, with the disabled and enabled filter. The tables contain the number of total successful, unsuccessful and cancelled transactions.

The results obtained from Radware DefensePro with using APSolute Vision are depicted in Fig. 6. DefensePro detects all four DDoS attacks aimed at the protected network in fifth tested scenario. The security threat of an attack is marked as ”HEAVY” and the category of an attack is detected as ”Packets Anomalies”. This means that DefensePro detects some anomalies in the network traffic (in this case increasing of network traffic) see section III-B. Network traffic (regular

TABLE I
TEST SPECIFICATION.

Client	
Physical port	Port12
Line speed	10 Gbps
Packet loss	0%
FTP, HTTP load	15 000 users/s
Protocols	FTP/HTTP
Network address/mask	192.168.0.0/16
Address space	192.168.1.17–192.168.255.254
Server	
Physical port	Port13
Line speed	10 Gbps
Packet loss	0%
FTP	
Server port	FTP(21)
Network address/mask	192.168.1.0/28
Server address	192.168.1.1
File size	1 kB
HTTP	
Server type	Apache/2.0.49
Server port	HTTP(80)
Maximum requests	64
Network address/mask	192.168.1.0/28
Server address	192.168.1.6
File	index.html
File size	566 kB
DDoS attack 1. – 4. scenarios	
Type	SYN flood, UDP flood,
	Reset flood, Xmas tree
Packets sent	18 000 000
Attack duration	180 s
DDoS attack 5. scenario	
Type	SYN flood
Packets sent	22 000 000
Attack duration	220 s
Type	UDP flood
Packets sent	18 000 000
Attack duration	180 s
Type	Reset flood
Packets sent	10 000 000
Attack duration	100 s
Type	Xmas tree
Packets sent	12 000 000
Attack duration	120 s

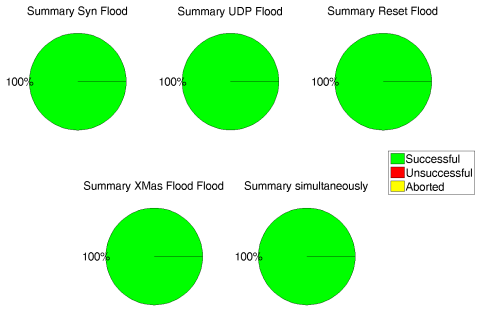

Fig. 5. Summary results for the enabled Radware DefensePro filter.

traffic and traffic represented by DDoS Attacks) traversing through Radware is shown in Fig. 7. Legitimate traffic is marked in green. This traffic is released to output without any modifications and it corresponds to the load profile of the Avalanche tester see Fig. 3. On the other hand, individual attacks, which have been started in the different time have been detected and filtered. This illegitimate traffic is marked in red. The graph marked in blue describes the increase of network traffic on the input port, which is caused by applying DDoS attacks.

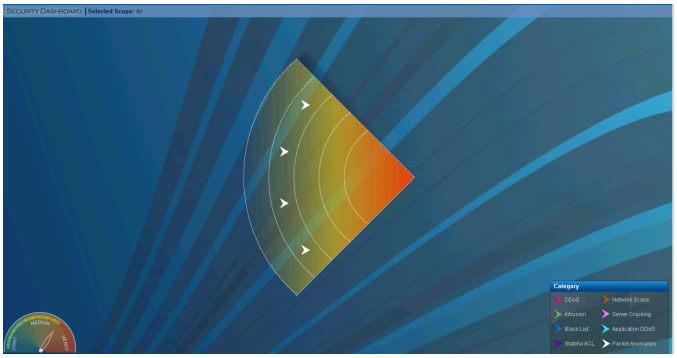

Fig. 6. DDoS attacks detection by Radware DefensePro.

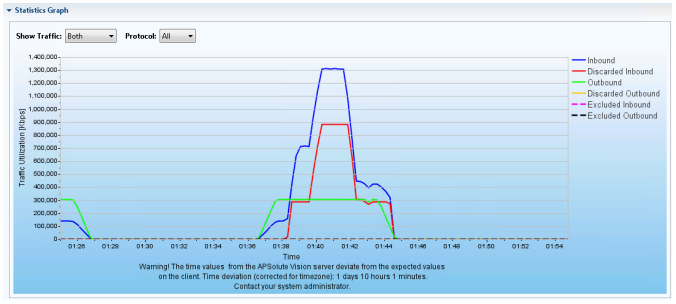

Fig. 7. Detection and filtering of DDoS attacks by Radware DefensePro in real time.

VI. CONCLUSION

In this paper, we presented basic information about DDoS attacks, their types and methods of DDoS detection and defense. In these days, there are several security solutions against DDoS attacks. A well-established security solution is usually a combination of prevention, good infrastructure with network security devices, backup resources and sophisticated crisis scenarios in the case of a DDoS attack.

In the paper, we described our testing implications of DDoS attacks on the quality of the service, such as FTP and web services. Furthermore, we tested a DefensePro 6.10.00 device from Radware company which is able to detect and filter many types of network attacks, including DDoS attacks in real time. We created five scenarios, which were aimed at the different types of DDoS attacks with a different intensity. In the first four scenarios, we implemented attacks as SYN flood, UDP flood, Reset flood and Xmas flood separately. In case of the fifth scenario, we applied all attacks from the previous scenarios together. In all scenarios, we tested the influence of

TABLE II
SUMMARY RESULTS FOR THE DISABLED DEFENSEPRO FILTER.

	Syn Flood	Udp Flood	Reset Flood	Xmas Flood	All
Total transactions	10663760	10592631	10408262	11331240	11137990
Successful transactions	4041351	8499729	8126965	10006739	1383676
Unsuccessful transactions	5489351	2087108	2274594	1320481	8508772
Canceled transactions	1133058	5794	6703	4020	1245542

TABLE III
SUMMARY RESULTS FOR THE ENABLED DEFENSEPRO FILTER.

	Syn Flood	Udp Flood	Reset Flood	Xmas Flood	All
Total transactions	10663760	10592631	10408262	11331240	11137990
Successful transactions	10663760	10592631	10408262	11331240	11137990
Unsuccessful transactions	0	0	0	0	0
Canceled transactions	0	0	0	0	0

a protected network with disabled or enabled DDoS protection services. The results of security tests show that DefensePro is able to filter all the DDoS attacks of difference types and intensity. Furthermore, the device is able to withstand the DDoS attack on the minimum intensity of about 900 Mbps, it is 18 times more than the current attacks usually have.

ACKNOWLEDGMENT

Research described in this paper was financed by the National Sustainability Program under grant LO1401. For the research, infrastructure of the SIX Center was used.

REFERENCES

[1] A. Srivastava, B. Gupta, A. Tyagi, A. Sharma, and A. Mishra, "A recent survey on ddos attacks and defense mechanisms," in *Advances in Parallel Distributed Computing*. Springer, 2011, pp. 570–580.

[2] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[3] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the dos and ddos problems," *ACM Computing Surveys (CSUR)*, vol. 39, no. 1, p. 3, 2007.

[4] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks." in *LISA*, vol. 99, 1999, pp. 229–238.

[5] V. Paxson, "Bro: a system for detecting network intruders in real-time," *Computer networks*, vol. 31, no. 23, pp. 2435–2463, 1999.

[6] R. Jalili, F. Imani-Mehr, M. Amini, and H. R. Shahriari, "Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks," in *Information Security Practice and Experience*. Springer, 2005, pp. 192–203.

[7] H. Liu and M. S. Kim, "Real-time detection of stealthy ddos attacks using time-series decomposition," in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–6.

[8] S. Jin and D. S. Yeung, "A covariance analysis model for ddos attack detection," in *Communications, 2004 IEEE International Conference on*, vol. 4. IEEE, 2004, pp. 1882–1886.

[9] G. Nychis, V. Sekar, D. G. Andersen, H. Kim, and H. Zhang, "An empirical evaluation of entropy-based traffic anomaly detection," in *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*. ACM, 2008, pp. 151–156.

[10] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to ddos attack detection and response," in *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, vol. 1. IEEE, 2003, pp. 303–314.

[11] M. C. M. Patel and A. P. V. H. Borisagar, "Survey on taxonomy of ddos attacks with impact and mitigation techniques," in *International Journal of Engineering Research and Technology*, vol. 1, no. 9 (November-2012). ESRSA Publications, 2012.

[12] A. Jain and A. K. Singh, "Distributed denial of service (ddos) attacks-classification and implications," *Journal of Information and Operations Management ISSN*, pp. 0976–7754, 2012.

[13] G. Loukas and G. Oke, "Protection against denial of service attacks: a survey," *The Computer Journal*, p. bxp078, 2010.

[14] S.-H. Kang, K.-Y. Park, S.-G. Yoo, and J. Kim, "Ddos avoidance strategy for service availability," *Cluster computing*, vol. 16, no. 2, pp. 241–248, 2013.

[15] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, "Ddos defense by offense," *ACM Transactions on Computer Systems (TOCS)*, vol. 28, no. 1, p. 3, 2010.

View publication stats