Dominance of Hardware Firewalls and Denial of Firewall Attacks (Case Study BlackNurse Attack)

Thume Vamshi Krishna[1*], Pulipati Karthik[2]

[1, 2] UG Student, Department of Information Technology, Malla Reddy Institute of Engineering and Technology, Kompally, Dhulapally, Medchal District, Hyderabad, Telangana, India 500010

Abstract: ***Network security is the most important aspect which concerns with protection of the data of an organization and firewalls play a crucial role in this. The main goal of this paper is to show that hardware firewalls perform better when compared to software-based firewalls. The performance of a firewall is the deciding factor when it comes to data breaches and data theft. Firewalls are the devices that stay upfront and act as a gatekeeper for internal networks but these firewalls are prone to DDoS attacks nowadays and giving awareness about working principles and how these DDoS attacks works is necessary. Denial of firewalling is attacks on the firewall which cause them to become unresponsive and downgrade the CPU performance.***

Keywords: Firewalls, packet inspection, Rule database, ICMP (Internet Control Message protocol), TCP (Transmission Control Protocol)

1. Introduction

A firewall is a device that is used to safeguard the internal network of an organization from outside untrusted networks. Firewalls are of many types which depend on the packet classification mechanisms they use. [6] In this sequential search method, two main operations can be performed on the packets that are pass and drop [1]. Here every packet is checked with the rule and if the packet matches with the rule, then necessary actions are taken on it [1], [2]. A single packet can be compared with more than one rule of the firewall. Many popular firewalls like CISCO PIX, Linux Netfilter, and also, the open-source CLI-based firewalls like iptables use these sequential search-based methods [1]. Every incoming packet is checked until it matches the rules and if none are found the packets are allowed into the network if the packet matches with the rule, it is quarantined or dropped [2]. SYN and RST attacks are the most occurring but also new variants like BlackNurse and DTLS are causing great damage. BlackNurse is the emerging DDoS attack primarily targeting firewalls and remarkably reducing its performance [20]. Due to the increase in the percentage of DDoS attacks, botnets are also increasing simultaneously. [7] This paper provides an analysis of rule-based firewalls and how sequential search is performed inside [3]. The efficiency of the firewall plays a vital role in forming the barrier for the private network because the firewall has to follow all the defensive procedures to form rules. Networks experience bottlenecks where the packet flow speed decreases and firewall administrators should take care while designing the firewall about the defence techniques. Firewall designers should test the performance of firewalls by following necessary tuning procedures and these rules should be implemented only after the testing phase [4].

2. Related Work

The literature describes the performance of the firewalls and analysis on rule-based packet classification called sequential search-based systems. The literature also conveys the attacks on networks like DDoS and preventive measures for it [4]. The major part of this research is to showcase the performance dominance of hardware firewalls over software firewalls and how hardware firewalls provide a viable option to inspect inbound traffic. [2] Rule database is still a widely used mechanism for packet classification because of the long and exhausting search methods of the signature-based method [2]. In the rule-based method, rules can be written easily and can be modified at any time. However, this analysis is based on our private research and may not provide accurate results. Eventually, the server cannot respond to requests and this is a denial of firewall attack [20]. The queuing model consists of a DMA ring and a DMA (Direct Memory Access) ring that is used to directly allocate packets using NIC (Network Interface Card). Rx buffer ring can also be used for allocating incoming packets directly to the NIC and the flow can be analysed using the number of incoming packets [2]. This flow can be normal packets per time and also can be undetectable low DDoS traffic [23]. Packet flows can be of two types' regular traffic to stateful firewalls and unusual traffic to it where packet headers are checked but, in our model, we assumed that the firewall we consider is stateless and it does not check for TCP headers and allows packets based on the inflow [23]. We are not considering finite packet buffer in this model because we are using a CLI (command-line interface) packet generator tool like hping3 but a GUI interface can also be used [9].

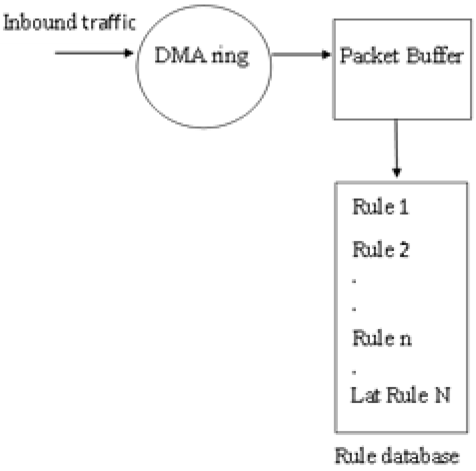


Figure 1: Rule database classification method

2.1 Limitation of previous procedures

Firewalls are classified as software-based and hardware-based whereas further types can be rule-based and signature-based firewalls [2]. In the previous methods, rule-based firewalls are considered in the test network and the formula is derived based on the Markov chain process but we consider the rule-based system using conditional probability where there is a continuous flow of packets into the test network we create. With this probability-based method, you can determine the exact stage in the rule database which causes the firewall to become unresponsive, this method is useful to determine the packet which caused the unexpected behaviour and discard it [2].

2.2 Our approach

The method we are using in this paper is relatively simple and easy to understand. Our goal is to simplify the architecture of firewalls and show the working of rule-based firewalls. The performance of a firewall can be determined only if you know the working principle behind it, so we also discuss the entire chronology of packet inflow into the firewall and the internal divisions of the firewall [5]. The test network we consider has been reduced into an effortless model to demonstrate the working of the firewalls. The switch we used consists of ternary content addressable memory chip which makes the packet classification process easier. BlackNurse is a dangerous attack and it's surprising how only a few articles have been written about it. The queuing model consists of a DMA ring and a DMA (Direct Memory Access) ring that is used to directly allocate packets using NIC (Network Interface Card) [2]. Rx buffer ring can also be used for allocating incoming packets directly to the NIC and the flow can be analysed using the number of incoming packets. This flow can be normal packets per time and also can be undetectable low DDoS traffic [22]. We are not considering finite packet buffer in this model because we are using a CLI (command-line interface) packet generator tool like hping3 but a GUI interface can also be used [9].

2.3 Challenges

Our test network consists of two software-based firewalls running on two windows host systems. Determining the performance of a firewall is not an easy task and takes a very long time so we had to check every stage in the rule database. Rule database is the area where rules are written so that every incoming packet has to go through each stage or rule in our case. We tried fuzzing the firewall with a windows-based system using a packet generator tool but the results were not convincing and up to the mark so we had to try this with a Linux distribution operating system called parrot os and it worked [16]. The test we are conducting is based on finding faults in the packet processing power of a firewall using rule-based firewalls. We also used continuous probability distribution to predict the rule number where the firewall became unresponsive due to the overloading of packets which eventually lead to a downgrade in the performance of the system running the firewall. This paper also provides insights on which is the best operable and performance-oriented firewall by considering both software and hardware-based firewalls.

3. Analytical Model

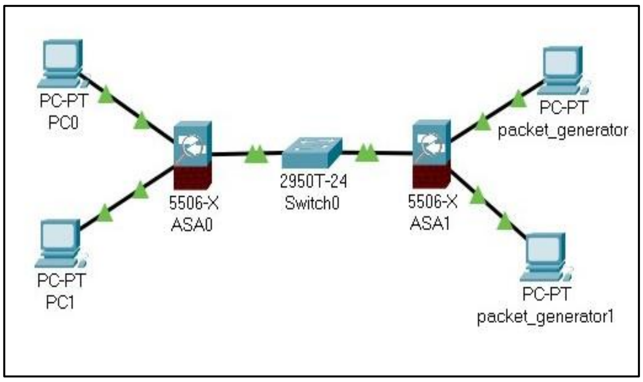


Figure 2: Test-Network Model

We had built a test network for analysis using computers and firewalls. This model is the simplified version of other test networks used in previous papers [2]. We used CISCO ASA 5506-X series hardware firewall with a DMA with an Rx chip in it. The firewall from CISCO has 4GB RAM with 100-250 Mbps throughput and also handles 246900 packets per second. The switch we used is the CISCO catalyst 2950T series model-100 Mbps. The packet generator we used is hping3 and it is running on a Linux machine which has 16Gb RAM without any swap memory. We thought of using modern day systems, switches, and firewalls to showcase the working of our formula in real-time environments. The architecture consists of two computers with software firewalls inbuilt, a switch connected to different Ethernet ports, and also connected to the internet [23]. This chip is used to directly load the packets into the memory for inspection and the systems we used have Intel, i9 processors 7980-XE version with 18 cores CPU, 16Gb RAM high speed performance. Which contains 24 ports. We needed a system with high performance because we are also running a software firewall and should also be able to handle remote ping commands. Overloading of packet buffer is done to decrease the stability of the firewalls in the systems. Later when we are done with testing the hardware firewalls, we send random ping message requests to software firewalls. Rule-based searching methods should not go unaware because understanding the methodology behind rules and dividing them based on packet headers is pivotal. Every rule is written using four or five packet header information that is source IP, source port, destination IP, destination port, and protocol being used [14]. Based on the incoming packets and header information any firewall takes required actions.

Table 1: Rule database of firewall

Rule	Source IP	Source Port	Destination Port	Protocol	Action
Rule 1	192.168.0.4	-	-	TCP	Deny
Rule 2	-		80	-	Allow
Rule 3	192.168.0.3	80	-	-	Deny
Rule 4	-	-	-	-	Deny
Rule 5		-	1234	TCP	Allow

4. Testing Methodology

The test network has both hardware and software-based firewalls and the goal is to check the packet processing time of both the firewalls. This can also be called the frequency of packet and denoted as " λ ". Firewalls are configured in the stateful mode so the header information of every packet is checked and cached [14]. The packet cache is the part of the buffer where every packet is first checked against this packet cache and if it matches then the packet is discarded and if it does not match the packet is processed and the handshake is achieved. The handshake is the authorization mechanism that helps in the allowance of the packet to access the resources. The packet generator tool we are using has an option of CLI (command line interface) which helps in providing more header options than the GUI interface. Hping3 is an efficient tool for packet creation and modification. For the hardware firewall, we used hping3 but for the software inbuilt firewall, we decided to send packets remotely using Solar Winds WAN killer packet builder [22]. It provides bandwidth speed and we considered 10-100 Mbps speed. ICMP (Internet Control Message Protocol) is a special protocol used to solve server-side network issues. It helps to check the hop machines in the network and TTL (Time to Live) value which is the overall instance of a time limit of a packet and after the expiry of TTL, the packet can never pass onto the next hop machine. ICMP echo packets are ping packets that are used to detect the hop count, TTL, and also the operating system of the target. To start with the process, use the hping3 commands as in the next page. Hping3 experiment is done exclusively on hardware firewalls by us. After the packets are received successfully by the target, we need to plot graphs based on time and the number of packets increasing. After repeating the same process 7 times we can plot the graph.

```
root[at]Sharky: ~# hping3-v 192.168.0.4-c 500-d 300-s-p 7104--flood--rand-source-w 128
using eth0, addr: 192.168.0.8, MTU: 56675
```

In the above command, we used-v as the target IP or domain,-c is the packet count,-d is the size of the packet,-s is sending only SYN packets for establishing only half connection instead of the entire handshake procedure,-p is target port, flood is sending packets continuously and the random source is our IP we can also remove this so the target machine can recognize our IP address,-w is the TCP window size of a windows operating system. Network adapter is eth0 using which we send packets. Graph can be plotted where X-axis would be number of packets sent and Y-axis would be time taken to send or start a handshake with the packets. Time is measured in milliseconds here. First graph shows that packets are sent at 10 Mbps speed to hardware firewall and later at 100 Mbps speed to check the packet processing speed.

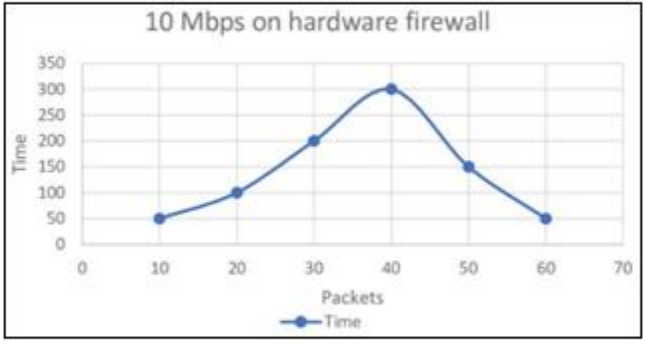


Figure 3: Graph plot for hardware firewall at 10 Mbps Speed

100 Mbps is 10X more than 10 Mbps speed so packet processing per millisecond is more. Now, we perform the same procedure with software firewalls, and graphs are plotted. But, for a change, we used Solar Winds WAN killer to remotely send packets to the system in another network that is connected to the NAT network [22]. Graphs are used to explain the per packet time allocated by the firewall. Solar Winds WAN killer is one of the most efficient packet generation tools and provides options to create probe packets. The same procedure is performed with 100 Mbps speed and a graph is plotted. As we sent a packet of size 300 bytes with 10 Mbps bandwidth the number of packets sent was 459. But due to an increase in bandwidth we are sending a packet of size 500 bytes, then we need to find out the number of packets sent with 100 Mbps speed.

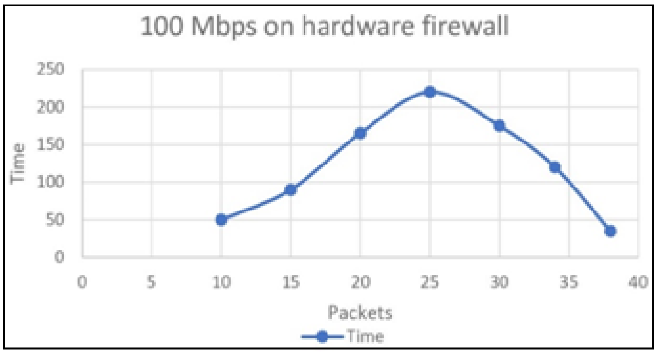
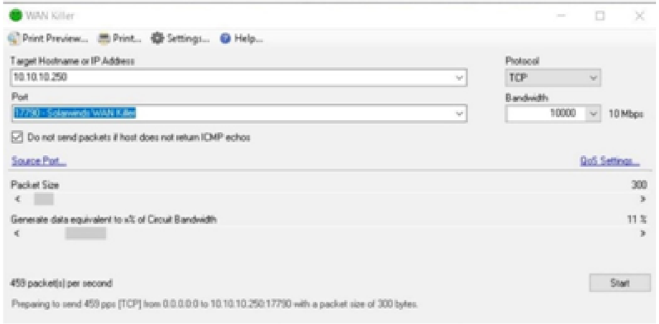


Figure 4: Graph plot for hardware firewall at 100 Mbps speed



Target Hostname or IP Address: 10.10.10.250
Protocol: TCP
Port: 17790 - Solarwinds WAN Killer
Bandwidth: 10000 10 Mbps
☑ Do not send packets if host does not return ICMP echos

Packet Size: 300
Generate data equivalent to x% of Circuit Bandwidth: 11 %
459 packet(s) per second

Preparing to send 459 pps [TCP] from 0.0.0.0:0 to 10.10.10.250:17790 with a packet size of 300 bytes.

Figure 5: WAN killer with 10 Mbps on software firewall

We also derived a formula based on continuous probability to show the packet and rule synchronization. This formula shows the stage-wise rule allocation and a responsive factor "x" is to be obtained, which describes the limit of rules where the firewall becomes passive.

4.1 Formula for Firewall Packet Inspection

“C” is the frequency of incoming packets.
“M” is the rule stage number.
“r” is the rule checking frequency.
“N” is the last packet being checked.
“ γ ” is the output packet to next stage.

$$\textbf{Stage (0, 0) } x = \int_{n}^{N} C + M_1 r_1 + \gamma_1 N\ n \leq N$$

The above equation is the initial rule stage before the packets are sent. This equation is based on our assumption and only portrays the sequential rule matching method. This equation when used in real world scenarios may also provide ways to block the inbound traffic to firewalls. For instance, let's say 100 packets are sent with a fixed packet size at a constant bandwidth. The rule stage is 2.

Stage (n, N) denotes the number of packets and stage number.

Step1: **Stage (100, 2) x =** $\int_{100}^{2} C + \mathbf{M_2 r_2} + \gamma\,{}_2\mathbf{Nn} \leq \mathbf{N}$

Step 2: **Stage (n, k) x =** $\int_{n}^{k} C + \mathbf{M_k r_k} + \gamma\,{}_n\mathbf{N}$

This formula consists of two methods where the packets are sent first and are checked until the packets reach the last rule. Here, in the last formula "k" denotes the last rule in the rule database [3]. So, after the entire testing procedure, we came to the conclusion that hardware firewalls have the best packet processing power when compared to software firewalls. Hardware firewalls also take more time and packets to become unresponsive.

4.2 Result

The result we derived is the observation that performance of hardware firewalls is more when compared to software firewalls. Packets, when sent to software firewalls, take more time when compared to hardware firewalls. Time taken is another term for packet processing time here. The performance of the hardware firewall is very effective as the packets have been processed rapidly at 10 Mbps speed. This shows that that the acceptance of packets is not so hard when in a server environment. As we sent a packet of size 300 bytes with 10 Mbps bandwidth the number of packets sent was 459. But due to an increase in bandwidth we are sending a packet of size 500 bytes.

5. Denial of Firewall

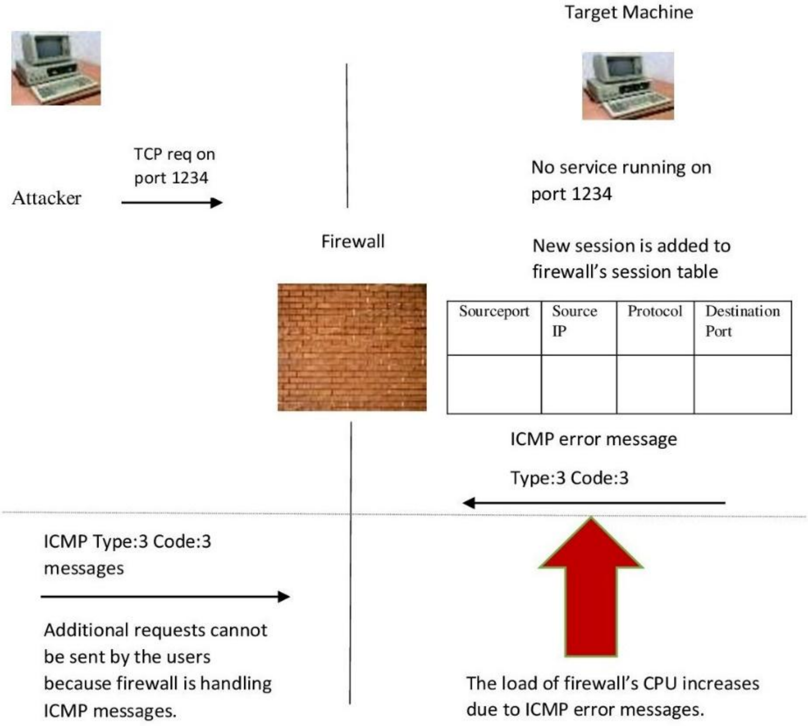
Denial of service is an attack where an illegitimate number of requests are sent to a machine where the motto of this procedure is the slow down the processing of the target machine and make it unresponsive [10]. Firewall devices are equally important in request processing because these packets are to be inspected and checked against every packet filtering rule in the rule database. New attacks have emerged where the focus lies mainly on firewalls because they use CPU resources to work and the attacker indirectly attacks the server environment by damaging the firewall so that no more requests are accepted. This way an attacker can damage the server environment by sending malformed packets to the target network. This attack is called the "Denial Of Firewall" attack [10]. These DoF attacks may also target the session table by sending malicious packets. Some of the attacks include sending packets where the packet filtering takes a very long time when being checked against every rule [14]. Using this as an advantage attacker sends half-open connections where only SYN packets are sent and the target waits for us to close or to interact with the connection but the attacker leaves the connection open.

6. Black Nurse Attack

This attack is based on ICMP packet forging techniques. ICMP is a protocol used to diagnose network issues on the server side. When a packet is not accepted it is dropped by the target firewall and an ICMP response is sent back to the sender [20]. An ICMP error response code consists of IP address information and the reason for dropping the packet that is using type and code numbers. A digit "3" is used for denoting an unreachable message [20]. This attack tries to check the service which is vulnerable to a DDoS attack by sending specially crafted packets to the target. When these packets are not accepted by the receiver they send ICMP response with destination or port unreachable message [10]. For example, the sender sends packets to access the service running on port 22 that is SSH (Secure Shell Service) but SSH is not running on the target port then a port unreachable message is sent. This attack mainly targets firewalls running on one CPU because they want to affect the request processing power of servers.

6.1 BlackNurse Attack Method

To start with the attack, we need a packet builder and two machines to work with. We need to check active service running on different ports using the trial-and-error method by sending echo requests to the destination machine, consider sending TCP requests to the destination machine on port 22. But we got an ICMP error message as (Type 0: Code 3) which indicates that the destination machine exists but the packets cannot be sent to the requested port as it does not exist [20]. This can also be broken down as the service named SSH is not running on the target machine. Now, the packet builder sends half-open (Type 3: Code 3) error-based echo requests to use the firewall's resources completely. This can be a serious attack because if this attack happens in the server environment the server cannot accept any more requests and the organization might lose its business. The firewall will be configured on the localhost and amid this attack, the firewall configuration page will become unresponsive and you cannot just disconnect it. As the incoming packet's session is already created in the session table it is difficult for the firewall to detect the malicious packet [20]. Following is the figure.


Target Machine
Attacker
TCP req on port 1234
No service running on port 1234
Firewall
New session is added to firewall's session table
ICMP error message
Type:3 Code:3
ICMP Type:3 Code:3 messages
Additional requests cannot be sent by the users because firewall is handling ICMP messages.
The load of firewall's CPU increases due to ICMP error messages.

Sourceport	Source IP	Protocol	Destination Port

6.2 Countermeasures

Well, this attack is not ubiquitous, possible countermeasures have not been proposed yet but what we can describe as a countermeasure would be an early rejection of packets. Early rejection of packets is using AI technology to be able to automatically detect the services running on the machine and allow echo requests only to that port. The incoming packets should be inspected service connection wise and the port they are trying to connect with. Packets should be configured so that sensitive messages should not be disclosed about the active machine and only necessary information should be detected. A count on echo requests should be imposed and only an allowed number of packets should be processed for services.

7. Conclusion

To conclude this paper, we wanted to discuss firewall performance and how hardware-based firewalls are capable of balancing packet floods for a longer time when compared to software firewalls. We showed the practical implementation of testing the firewalls and how vulnerable they can be. An internal network depends entirely on firewalls and they should be configured to their full potential. The firewall follows a rule-based sequential search mechanism where every incoming packet is checked against the rule, we wanted to prove at what rule stage the firewall becomes slow and unresponsive so we derived a formula for rule checking and simplified older methods of rule matching. This formula we proposed can provide an accurate result for detecting denial of firewall attacks. We also discussed the denial of a firewall attack called "BlackNurse" and how it is done and possible countermeasures.

References

[1] E. Al-Shaer and H. Hamed, “Modeling and management of firewall policies, ” IEEE Trans. Network Service Management, vol.1, no.1, pp.2–10, 2004.

[2] K. Salah, K. Sattar, M. Sqalli, and E. Al-Shaer, “A potential low-rate DoS attack against network firewalls, ” J. Secur.commun. Netw., vol.4, no.2, pp.136–146, Feb.2011.

[3] R. Beverly, “A robust classifier for passive TCP/IP fingerprinting, ” in Proc. PAM, 2004, pp.158–167.

[4] S. A. Crosby and D. S. Wallach, “Denial of service via algorithmic complexity attacks, ” in Proc.2003 USENIX Security Symposium, pp.29–44.

[5] Z. Trabelsi, S. Zeidan, K. Shuaib, and K. Salah, ‘‘Improved session table architecture for denial of stateful firewall attacks, ’’ IEEE Access, vol.6, pp.35528–35543, 2018.

[6] K. Salah, K. Elbadawi, and R. Boutaba, ‘‘Performance modelling and analysis of network firewalls, ’’ IEEE Trans. Netw. Service Manage., vol.9, no.1, pp.12–21, Mar.2012.

[7] M. Smart, G. R. Malan, and F. Jahanian, “Defeating TCP/IP stack fingerprinting, ” in Proc. USENIX Secur., 2000, pp.229–240.

[8] Q. Yan, F. R. Yu, Q. Gong, and J. Li, “Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges, ” IEEE Commun. Surv. Tuts., vol.18, no.1, pp.602–622, 1st Quart., 2016.

[9] J. Chen, H. Zeng, C. Hu, and Z. Ji, “Optimization between security and delay of quality-of-service, ” J. Netw.computer. Appl., vol.34, no.2, pp.603–608, 2011.

[10] K. Sattar, K. Salah, M. Sqalli, R. Rafiq, and M. Rizwan, ‘‘A delaybased countermeasure against the

discovery of default rules in firewalls, ’’ Arabian J. Sci. Eng., vol.42, no.2, pp.833–844, Feb.2017.

[11] E. Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan, “Conflict classification and analysis of distributed firewall policies, ” IEEE J. Sel. Areas Commun., vol.23, no.10, pp.2069–2084, Oct.2005.

[12] K. Salah, and M. Hamawi, “Comparative Packet-Forwarding Measurement of Three Popular Operating Systems, ” International Journal of Network and Computer Applications, Elsevier Science, Vol 32, No.4, September 2009, pp.1039-1048. .

[13] Q. Yan and F. Yu, “Distributed denial of service attacks in softwaredefined networking with cloud computing, ” IEEE Commun. Mag., vol.53, no.4, pp.52–59, Apr.2015.

[14] X. Feng, Q. Li, H. Wang, and L. Sun, “Characterizing industrial control system devices on the Internet, ” in Proc. IEEE ICNP, Nov.2016, pp.1–10.

[15] Chien-Ying Chen, Monowar Hasan and Sibin Mohan, "Securing realtime internet-of-things", *Sensors*, vol.18, no.12, pp.4356, 2018.

[16] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets", *SIGCOMM Comput.commun. Rev.,* vol.31, no.4, pp.15-26, Aug.2001.

[17] T. Chomsiri, X. He, P. Nanda, and Z. Tan, ‘‘A stateful mechanism for the tree-rule firewall, ’’ in Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput.commun., Sep.2014, pp.122–129.

[18] F. Al-Haidari, M. Sqalli and K. Salah, “Enhanced EDoS-shield for mitigating EDoS attacks originating from spoofed IP addresses, ” In the proceedings of the 11th IEEE Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012), pp.1167-1174.

[19] S. Yu, R. Doss, W. Zhou, and S. Guo, “A general cloud firewall framework with dynamic resource allocation, ” In the proceedings of the IEEE International Conference on Communications (ICC 2013), pp.1941-1945.

[20] Salah, K., “To Coalesce or not to Coalesce, ” International Journal of Electronics and Communications, Elsevier Science, Vol.61, No.4, 2007, pp.215-225.

[21] Z. Fu, F. Huang, X. Sun, A. Vasilakos, and C.-N. Yang, “Enabling semantic search based on conceptual graphs over encrypted outsourced data, ” IEEE Trans. Serv.comput., to be published.

[22] Z. Qian and Z. M. Mao, “Off-path TCP sequence number inference attack—How firewall middleboxes reduce security, ” in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, May 2012, pp.347–361.

[23] M. Liu, W. Dou, S. Yu and Z. Zhang, “A clusterized firewall framework for cloud computing, “ In the proceedings of the IEEE International Conference on Communications (ICC 2014), pp.3788-3793/