Secure network architecture based on distributed firewalls

Andrei-Daniel Tudosi, Doru Gabriel Balan, Alin Dan Potorac
Department of Computers, Electronics and Automation
Stefan cel Mare University of Suceava
Suceava, Romania
andrei.tudosi1@student.usv.ro

***Abstract*— Firewalls are essential for networking, because they are security devices designed to help protect an infrastructure from unwanted traffic, malicious attacks and outsiders that want to gain unauthorized access. These devices, hardware or software, can provide different levels of protection, depending on the situation where they are used and the entity's security policy. Because to the different network topologies and the evolution of exploits in different forms, classic firewalls can become inefficient. A low budget solution to these problems is a distributed firewall developed with open-source tools, which brings new features and improvements. Our approach in this paper is to propose a distributed firewall that solves problems and improves the overall results in network protection. We suggest the distribution of security policies of a firewall into distributed devices that work together and obtain better performance. The traffic is split between several firewalls that analyze and decide if the incoming packets will enter the network, be dropped, rejected, or redirected to a honeypot. Our proposed distributed firewall has the possibility to be scaled with different numbers of clients and network devices.**

Keywords*— *distributed firewall, design, network security, control plane, data plane, gateway, static route, redirect.

I. INTRODUCTION

The number of cybercrimes is increasing every year due to events that are occurring at a global level. Both companies and individuals must secure their data, in different ways. A solution to cybercrime is the implementation of a firewall, which is a software or hardware network security system that has as purpose to keep safe a network and filter the incoming and outgoing traffic inside a network after a custom set of rules [1]. These rules are usually based on several parameters that are indicated by the structure of a packet, that can be source, destination, port, content, flag and others. The protection offered by a firewall is against intrusions, which refers to the attempt of unauthorized users to access a device, against malware, which are used for information extraction, brute force attacks, being the procedure of discovering passwords and, Distributed Denial-of-Service attacks (DDoS) that try overwhelming devices with the flood tactic [2]. Firewalls can be classified into hardware, software, or a combination of both. Each solution has advantages and disadvantages and offers high performance in a certain situation. Software firewalls can provide a more detailed control over the network, giving access to a certain application and blocking others. A common software firewall is the Cloud-based firewall, being referred to as Firewall-as-a-Service (FaaS), that is functioning in the cloud. However, the drawback of software firewalls is the high usage of resources like CPU and RAM memory because they are installed on a device that also needs specific resources. Hardware firewalls are physical devices, and they act as gateways between networks. They are convenient for specific topologies of organizations; their disadvantage is that they don't provide security for inside attacks. Both firewalls provide security improvements, and for best results it is recommended a hybrid version that combines the advantages of both and covers the weaknesses [3].

Because of the number of different scenarios, firewalls have been categorized based on the manner they operate. Thereby, there are the following types:

A. *Packet filtering Firewall*

Packet filtering Firewall is a traditional firewall type, that analyzes the received packets by examining and preventing them from going forward if a predefined rule is not met. A representation of this type of firewall is presented in Fig. 1. They independently monitor each packet, and because of this, they are limited. This method is fast, cheap and effective in some situations, but because the firewall cannot examine the content from inside the packet, makes the network vulnerable. This means that they provide only basic protection at network layers, and cannot work in complex situations, this means security will have unprotected areas.

B. *Circuit-level Gateway Firewall*

This type of firewall is more advanced in technology than the packet filter one, working at the session layer and determining the security of an established connection. Circuit-level Gateway monitor and verify TCP data packets to check incoming traffic without consuming extra resources. For this reason, it is very efficient, optimizing the performance of the network. However, if a data packet includes malware and a legitimate TCP handshake can easily bypass the firewall.

Fig. 1. Packet filtering Firewall

978-1-6654-8162-5/22/$31.00 ©2022 IEEE

C. *Stateful multilayer Firewall*

Stateful multilayer firewalls are the improved Circuit-level Gateways, verifying the established connections and performing packet inspection to provide comprehensive security [4]. In this situation, this firewall is between Layer 3 and Layer 4 of the OSI model. An important advantage is that these firewalls create rules dynamically to allow incoming normal traffic instead of a set of rules created manually. They are advanced and complex firewalls that offer a secure network, but have high resource utilization and can also delay the speed of traffic.

D. *Proxy Firewall*

Proxy firewalls are implemented at the application layer with the help of a proxy device, the connections inside and outside the network being established through this firewall. They are similar to Stateful multilayer Firewalls, with the improvement that they offer deep layer packet inspection, that allows to verify the content of a data packet. This type of firewall usually operates in the Cloud and has a different mechanism of working. A client sends a request to the firewall, the firewall examines it, and if the request is approved, then the connection is realized between the client and the destination server, without knowing the location of the server. Proxy firewalls protect the identity and location of servers inside a network by preventing direct connections to them. It is a very secure method, but the setback consists in the delay and slow-down of the connections because of the extra steps.

E. *Next-Generation Firewall*

This type of firewall gained popularity across the last year due to the high technology and efficiency in network protection against cybercrime. This firewall provides extensive application control and visibility, blocks unwanted traffic, and differentiates applications from dangerous to safe ones. Next-Generation Firewall (NGFW) includes intrusion prevention, virtual private network (VPN), encrypted traffic inspection, and tracking all the traffic from Layer 2 to the application layer [5]. The limitations of traditional firewalls are covered with NGFW, because of its flexible features and architectures. All the mentioned features are combined into one single solution that is optimized and focused on high security inside a network. Because of the advanced and sophisticated features, NGFW comes with high price of implementation and maintenance.

Inside a network, there are many background processes that occur when traffic is flowing. Routing is a process that refers to the selection of a path across one or more networks. In a router, there are rules and policies about the manner that network packets are handled. These policies consist of the network control plane [6], which is the total of functions and processes that are used to determine which path is used when a packet is transferred from one point to another. Beside the control plane which is responsible for how the packets should be forwarded, there is the data plane, a high-speed path through the router, that is responsible for moving packets from source to destination. Control plane is configured and optimized to make decisions, can manage unpredictability, is policy-driven, and is easy to program. On the other side, the data plane is optimized to execute, offers limited options, is predictable, and can be hard to program. Inside a network device, beside the control plane and data plane, we have the management plane, which refers to the monitoring process of the traffic. The benefits of separating these planes inside a network offer performance, resilience, and simplicity.

F. *Distributed firewall*

As cybercrime evolves, traditional firewalls become obsolete, due to the fact that they don't block web-based attacks and can be fooled by manipulated headers. An alternative solution is distributed firewalls, with the architecture presented in Fig. 2. A distributed firewall is composed of: a security policy, policy distribution scheme and an authentication and encryption mechanism [7]. Security policy refers to rules configured by the administrator of the firewall to protect networks and determine which traffic can pass through and which is dropped or rejected. They are used to providing service management and control capabilities to offer security to the network. Before processing the incoming or the outgoing traffic, the firewall must consult the distribution scheme, which is implemented in different ways depending on the situation. The distribution scheme can be dynamic, and it offers the integrity of the security policy. The mechanism of authentication and encryption is based on digital certificates that are verified by the firewall. Encryption is realized on remote operations over an insecure network, on IP datagrams and over the data across a network. Distributed firewalls are a helpful solution for many business purposes, depending on the situation. This type can provide many opportunities due to the flexibility and scalability features. It can be configured in enterprise areas, where the network contains a mixture of different types of older and newer applications.

Depending on the scenario, there are multiple options to configure the firewall. The choice comes after the understanding of the architecture, resources and the purpose of the firewall for the desired network.

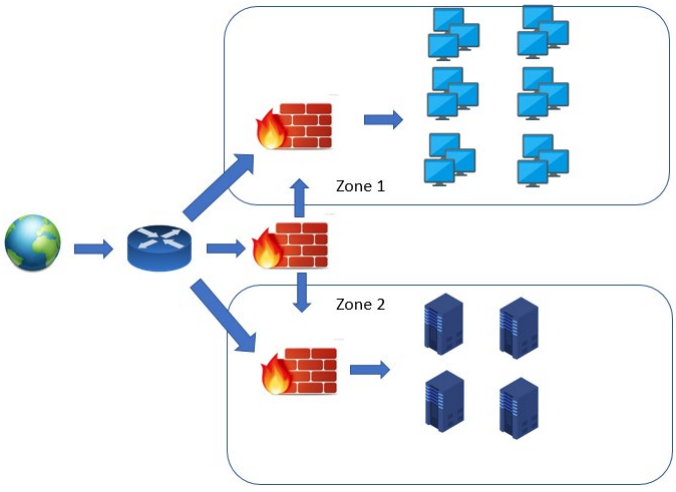

Fig. 2. Distributed firewall

II. RELATED WORK

In the past several years, distributed firewalls have been a subject studied and approached due to different types of networks, increased internet access speed and compute-intensive protocols. Some work in this direction is presented in this section.

In [8], the authors presented and proposed a Self-Adaptive Distributed Firewall (SADF), which responds to the vulnerabilities discovered and helps mitigate the risk of exploiting the vulnerability. The monitoring of SADF is made via Zabbix, a network monitoring system which handles notifications. SADF was configured to monitor the hosts of a network, which are then scanned by a Vulnerability Assessment System (VAS) with the purpose of discovering vulnerabilities. Firewall rules are adapted to react to these vulnerabilities and cover them based on network policies. Rules are also applied to individual hosts, effectively reducing exposure to vulnerabilities. The proposed solution is able to modify the firewalls from protected servers in a dynamic manner, and also obtain high performance in the environment where it was tested. SADF managed to reduce the scanning time of a group of 50 servers by 20% using the default configurations. Another interesting approach can be found in [9], where authors present an algorithm to distribute security policies of a network firewall in a Software-defined networking (SDN) environment. In their experiment, distributed placement of firewall rules has shown significant improvement compared to a centralized one, because of the ability to stop insider cyberattacks. Because of this situation, network packets can be filtered, and the bandwidth isn't congested. The results show improvements in throughput and latency in network protocols.

Authors proposed in [10] a distributed firewall in fog computing, which is positioned between the Cloud and end devices. The experiment consists in an architecture for this environment with a divided topology into different zones and a distributed firewall with a network controller. They studied the behavior of this type of firewall with the purpose to enhance security using the advantages of resource optimization and improve the topology of the distributed filtering and monitoring processes. The architecture of fog computing is composed of fog nodes, providing networking services and storing between end devices. Using migration rules between firewalls and the network controller, they managed to prevent DDoS attacks in the topology proposed. Another approach to this subject is in paper [11], where authors also presented a Distributed Firewall in Fog computing based on risk analysis, in which was introduced a distributed access control using firewalls. Their solution provides confidentiality, integrity and authentication, and their proposed intrusion prevention managed to prevent replay, password and man-in-the-middle attacks.

III. THE DEVELOPMENT OF DISTRIBUTED FIREWALL / DISTRIBUTED FIREWALL – AN EXTENSION OF A GENERAL FIREWALL

The topology in Fig 1. is a simple and very common network, where the gateway router has two interfaces; the first one connects the router to the outside Internet, and the other one, which connects the gateway router to in interior local network. The firewall is included in the router in this scenario. A lot of problems can occur in this situation, due to the fact that a high number of personal and small enterprise routers are configured by default and have minimal settings, they can be easily bypassed.

With the purpose of solving some issues of the presented firewall architectures presented above, we come and propose a new solution, presented in Fig. 3. The architecture was designed based on concepts we discussed previously. Our distributed firewall is composed of 1 main router and 4 secondary routers configured with firewalls depending on the situation. The first router is used for traffic split and redirect to the secondary ones. The secondary routers have a firewall configured, and with the help of an Intrusion Detection and Prevention System they filter the traffic to allow, reject or block it.

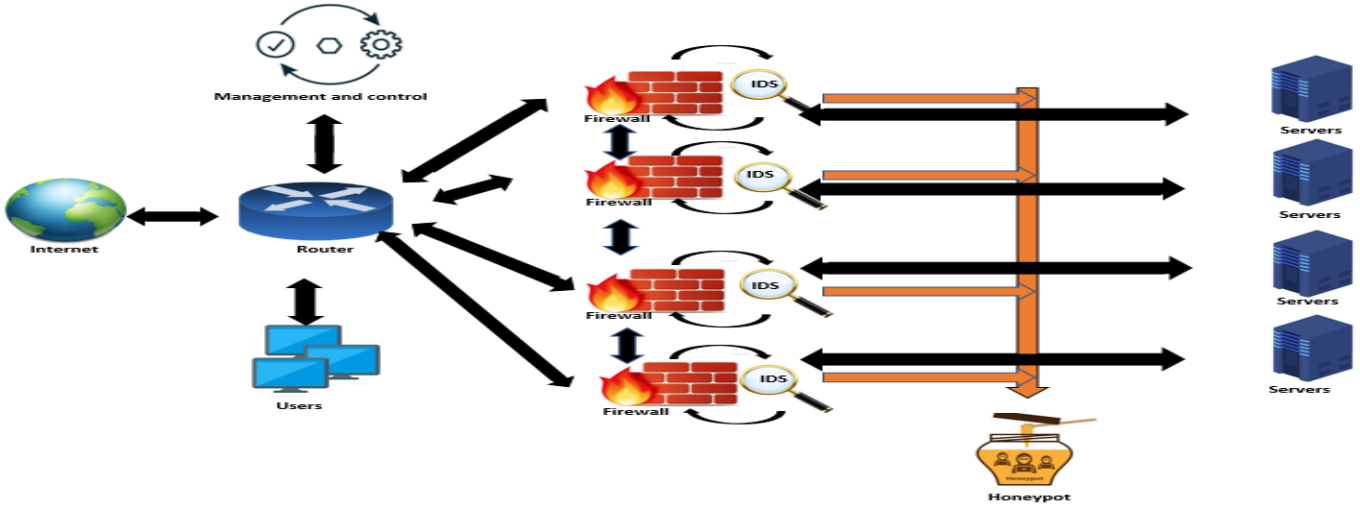

Fig. 3. Proposed distributed firewall architecture

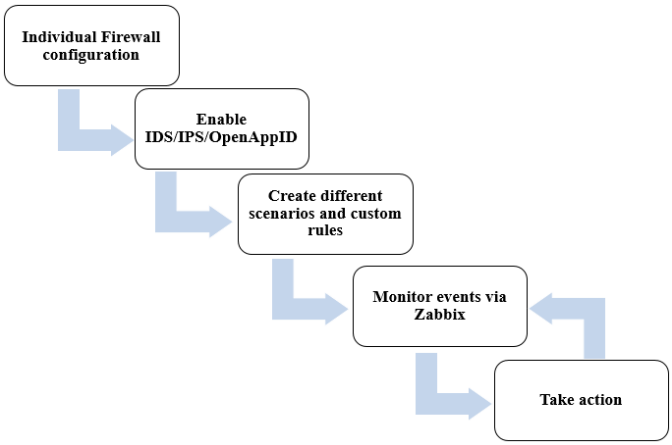

Fig. 4. . Implementation of our proposed solution

Our proposed experiment will be designed with open-source software for cost efficiency. For an accessible and clear vision over the entire network, we will use Zabbix, an open-source software used for monitoring networks, servers, cloud services and virtual machines. Zabbix Agent is set up on a target device to gather operational information such as processor, storage, bandwidth, and memory statistics. It can actively generate alerts for failures of a particular device or process. For simplicity, we will use templates of our firewalls to be integrated into Zabbix for remote monitoring with the help of SNMP, which stands for Simple Network Management Protocol. SNMP is a protocol used for reading and updating different configurations of devices across the network. Having SNMP configured in Read-Write mode means that we can set or manipulate values in the device settings. The main advantage of these monitoring tools is that it can run automatic discovery and interrogate devices to extract data, for accessible monitoring. As other advantages, we can mention: the possibility of executing remote scripts and managing hosts such as linking or unlinking hosts from a template, enabling or disabling hosts, creating or deleting groups. In our situation, we propose the usage of remote scripts for executing dynamic firewall rules. These types of rules are used to prevent security vulnerabilities caused by access that is needed only for a certain amount of time, for example, in Fig.6 we presented the procedure for users to access a web server, and in some rare situations they will access other servers connected to web server. These rules are configured as inactive and become enabled for certain events. The combination of Zabbix and dynamic firewall rules will help to develop different scenarios with the purpose of automation.

The main challenge in our experiment consists in network traffic handling, especially the distribution of traffic to firewalls. The solution consists in dynamic port forwarding rules inside the network. Traffic can be redirected to different firewalls with port forwarding. The main router receives traffic from outside the network and forwards it to the firewalls that will decide if clients can connect securely to devices inside the network. Dynamic port forwarding is a powerful tool that can be configured to process data transmissions through the network, providing extra security. The main router also contains floating firewall rules, which consist of rules that manipulate multiple interfaces at the same time. They are advanced rules that work before normal firewall rules and can perform complicated actions on different interfaces. Another important task for the main router consists in filtering, in our situation we will use ingress and egress filtering. The main router has only one ingress point, but for the secondary routers with firewalls, in certain cases we will have multiple ingress points. Egress filtering, which refers to the firewalling traffic initiated inside the network, will occur between the main and secondary routers and between secondary routers and different devices across the network.

The communication between firewalls is an important aspect of our setup. Fig. 4 shows the steps for configuring the proposed firewall. Each step is important and has its own purpose in developing our proposed solution. To improve the application awareness inside our network, we will use a security plugin optimized for application-layer network security (OpenAppID) and also, the management platform (Zabbix). The step that makes our solution an alternative to NGFW is OpenAppID, that has the purpose of giving application awareness in the network making our firewall customizable. This plugin is an application layer network security tool that will detect traffic from different chosen applications inside our network, using detectors and rules.

After realizing the connections between them using different tools like static and dynamic routing, gateways, static and dynamic port forwarding, we need to find a solution for forwarding path failures. To detect these types of problems, we will use bidirectional forward detection (BFD), a protocol that provides a failure detection method. BFD is used to monitor only one link between devices, in our situation we will configure one BFD for each link between firewalls. This protocol connects directly to routers and uses User datagram protocol (UDP) for the transportation of packets.

The firewalls communicate between them and have an active response to the incoming traffic. Traffic is filtered and if unknown signatures appear, then blocking policies are created and shared to the other firewalls. Each firewall is used to secure its sector, log traffic, and send logs to the management and control server. The security policy is divided into individual policies, on each firewall, containing custom setups depending on the situation in that sector, and a common policy that is shared with the firewalls from the network. Once the policy is created by a firewall, the policy is translated into firewall rules that deny access to traffic or redirect it. Every firewall rule has five fields: source IP address, destination IP address, source port number, destination port number, and protocol type. In some sectors, we consider application ID and service port for extensive application control and visibility. If all the parameters are matched with the security policy framed into the firewall, then traffic is allowed toward outside to inside network and inside to outside network. If the parameters are not matching, then the firewall drops, rejects, or redirects the packets. Allowed traffic will be included in a trusted domain of administration, in which the sources of that traffic are considered credible. If the traffic has been classified with an abnormal parameter, then it is considered untrustworthy and is not allowed, the source being considered malicious.

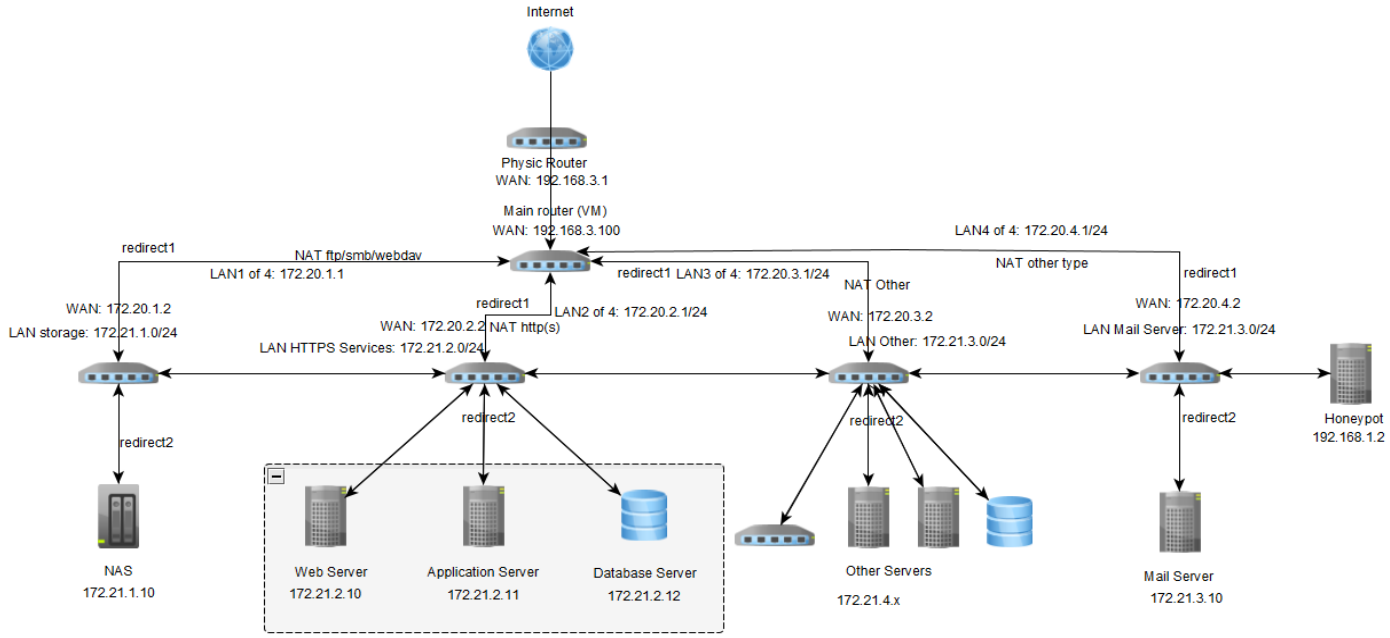

Fig. 5. Vision of the network

IV. DISTRIBUTED FIREWALL SOLUTION - SECURITY AND PERFORMANCE

A. Comunication inside the network

In Fig. 5 we present a network traffic monitoring diagram for our solution. The main router has a standard firewall, which means that incorrect traffic is dropped from the entrance of the network, then traffic goes to the other firewalls, which have configurations considered confidential due to security concerns [12]. Incoming traffic is analyzed by the firewalls; however, depending on the scenario of each firewall, there can be different approaches so traffic can be analyzed with smaller steps. Incoming traffic is split and redirected to the firewall that manages the target server. For traffic to be split and sent forward, there are some configurations to be made like: gateways for each firewall, static routes for traffic, redirects for separated traffic, a static null route for DDoS incoming traffic, and a honeypot for extra security. All the management and control are made by a specific server, thereby only the network administrator can reach all the network, only from a single point. This server is the management plane of the network, and offers a vision of the entire network. The data plane consists of the main router, and the control plane is made from all the firewalls.

B. Gateways

Due to the fact that we have multiple firewalls, each having a wide area network (WAN) and a Local Area Network (LAN) connection, we need to configure a gateway for each firewall to take advantage of the advanced feature static route. For accessing other networks, we need to create custom gateways on the main router. Without having a custom gateway, communication between the two networks doesn't work. Each firewall creates a new network, so for the connection to be functional, we need to configure one gateway for each new network.

C. Static route

Beside a gateway, in our experiment for data transfer between networks, we need static routes. Static routes are configured on the main router and are included in the routing table. Having a static route comes with a series of advantages like small usage or none of the bandwidth between routers, no routing overhead for the main router, meaning less resources consumed, and an extra security measure due to the fact that only an administrator can manage them. A static route is the path between two routers, in our case between the main router and a secondary firewall. They are fast and easy to design and implement, due to the topology of our proposed network. As for other advantages of static routing, we can mention that they do not use any protocol, don't use any complex routing algorithms, and are highly secured. We will add dynamic routes also, due to possible failovers that can occur in our distributed firewall. In Fig. 6 we display how a user can access the Web server.

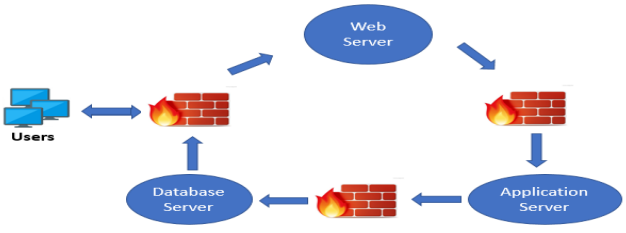

Fig. 6. Steps for accesing the web server

D. Static Null Route

An important security measure for our distributed firewall is the static null route. In a network, often it can appear incoming traffic that has the purpose of flooding and overwhelming the network via DDoS attacks. In this case, we need a destination to redirect that specific traffic, so our network can be secured, and our router does not consume extra resources. A static null route is an interface that receives traffic and discards it, being useful for removing unwanted packets and decreasing network congestion. This static null route can be configured and used to drop all the traffic generated by an attack.

E. Redirect

For our proposed solution, we also need to send divided traffic to firewalls via port forwards. These are used to allow access to a specific port on the destination, on a private internal address on the device. Port forwards are used to differentiate normal traffic from malicious one, and use firewall rules. The main router will split the incoming traffic by destination protocol and redirect it to the destination, if the traffic fulfills the security policy. Afterwards, the incoming traffic in also analyzed by the firewall, then is directed to the server. Port forwarding is a method of organizing inside our network, so we can manage the traffic and send it to the correct destination.

F. Honeypot

An extra security measure for our proposal is the existence of a honeypot inside our network. Having a honeypot means that we sacrifice a computer system as a bait for cyberattacks, consisting in a low security device to encourage intruders. Having this trap inside our network offers visibility of cyberattacks that may occur in the future and the preparations for them. We can determine where the cyber-criminal came from as geolocation, the level of threat, what are the targeted data, what is the attack method and how well-designed is our network in terms of cybersecurity. This security measure is a low cost and high value resource for our network. The honeypot will be configured for redirects for both outside and inside traffic because attacks can come from inside the network as well.

V. CONCLUSION

We propose this architecture for small enterprises or educational systems due to several advantages. We can mention: the protection from insider attacks, due to the multiple firewalls, the intrusion detection on different levels, a high standard management, and control over the entire network, a distribution of the security policies, all of this resulting in a high-performance solution for network security. Micro segmentation of the network provides visibility and accessible maintenance when needed. Also, beside improved performance of the security, we can mention scalability, due to the fact that our proposed solution can be deployed in many situations because of the flexibility. Further study needs to be done on how to improve firewall technology to better prevent illegal users from entering a network. We will focus on the implementation of the distributed firewall on a virtual platform, then implement it in a real situation with real traffic. In a real situation, we need to optimize our proposed solution due to the circumstances. Also, we will consider implementing the dynamic system including: failover alternative firewalls, dynamic security policy and firewall rules. For the automation part of the whole system, we want to consider various Python scripts with different Application Programming Interfaces (APIs) or 3rd party platforms. We believe that our work on the proposed solution can help others to learn about this topic and know more about this concept. This paper offers a reference for studying the technologies and development of distributed firewalls.

VI. REFERENCES

[1] S. Kumari, P. Singh, and R. K. Upadhyay, “Virus dynamics of a distributed attack on a targeted network: Effect of firewall and optimal control,” Communications in Nonlinear Science and Numerical Simulation, vol. 73, pp. 74–91, Jul. 2019, doi: 10.1016/j.cnsns.2019.02.006.

[2] W. Steingartner, D. Galinec, and A. Kozina, “Threat defense: Cyber deception approach and education for resilience in hybrid threats model,” Symmetry (Basel), vol. 13, no. 4, Apr. 2021, doi: 10.3390/sym13040597.

[3] N. B. S. ben Youssef and A. Bouhoula, “Automatic Conformance Verification of Distributed Firewalls to Security Requirements,” in 2010 IEEE Second International Conference on Social Computing, Aug. 2010, pp. 834–841. doi: 10.1109/SocialCom.2010.126.

[4] A. Zeineddine and W. El-Hajj, “Stateful Distributed Firewall as a Service in SDN,” in 2018 4th IEEE Conference on Network Softwarization and Workshops, NetSoft 2018, Sep. 2018, pp. 298–302. doi: 10.1109/NETSOFT.2018.8460126.

[5] E. Kaljic, A. Maric, P. Njemcevic, and M. Hadzialic, “A Survey on Data Plane Flexibility and Programmability in Software-Defined Networking,” IEEE Access, vol. 7, pp. 47804–47840, 2019, doi: 10.1109/ACCESS.2019.2910140.

[6] M. Khalil and S. A. Khan, “Control Plane and Data Plane Issues in Network Layer Multipathing,” in 2020 International Conference on Information Technology Systems and Innovation (ICITSI), Oct. 2020, pp. 263–269. doi: 10.1109/ICITSI50517.2020.9264915.

[7] C. E. da Silva, E. P. da Costa, J. ´ Unior, S. T. Medeiros, and M. Madruga, “An Architecture for Self-adaptive Distributed Firewall,” 2016. [Online]. Available: https://www.researchgate.net/publication/310325633

[8] E. P. da Costa Júnior, C. E. da Silva, M. Pinheiro, and S. Sampaio, “A new approach to deploy a self-adaptive distributed firewall,” Journal of Internet Services and Applications, vol. 9, no. 1, p. 12, Dec. 2018, doi: 10.1186/s13174-018-0083-6.

[9] Yuwei Chang and Tsungnan Lin, “Cloud-Clustered Firewall with Distributed SDN Devices,” IEEE Wireless Communications and Networking Conference (WCNC)978-1-5386-1734-2/18/$31.00 ©2018 IEEE, 2018.

[10] Y. Chang and T. Lin, “Cloud-clustered firewall with distributed SDN devices,” in 2018 IEEE Wireless Communications and Networking Conference (WCNC), Apr. 2018, pp. 1–5. doi: 10.1109/WCNC.2018.8377305.

[11] F. K. Abid, A. M. Makhlouf, F. Zarai, and M. Guizani, “DVF-fog: distributed virtual firewall in fog computing based on risk analysis,” International Journal of Sensor Networks, vol. 30, no. 4, p. 242, 2019, doi: 10.1504/IJSNET.2019.101242.

[12] F. Kamoun-Abid, M. Rekik, A. Meddeb-Makhlouf, and F. Zarai, “Secure architecture for Cloud/Fog computing based on firewalls and controllers,” Procedia Computer Science, vol. 192, pp. 822–833, 2021, doi: 10.1016/j.procs.2021.08.085.

[13] W. Song et al., “A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection,” Sensors, vol. 20, no. 6, p. 1637, Mar. 2020, doi: 10.3390/s20061637.