Next Generation Firewall – Transitioning from the “traditional” Firewall

Dillon Darroux
School of ITAS
Seneca College School of Information Technology Administration & Security
Email Address:
ddarroux@myseneca.ca

Cal Halioua
School of ITAS
Seneca College School of Information Technology Administration & Security
Email Address:
chalioua@myseneca.ca

Yasser Kassim
School of ITAS
Seneca College School of Information Technology Administration & Security
Email Address:
ykassim1@myseneca.ca

***Abstract*—This paper explores the capabilities of the Next Generation Firewall (NGFW) and determines whether or not a NGFW will one day completely replace the “traditional firewall”. We explore the capabilities and collect data by surveying selected individuals on their awareness of an NGFW and how critical it is to protect against emerging attacks in the never more reliant digital age. We also analyze data from external sources pertaining to their testing of the capabilities of NGFW and use this information to determine the scalability and overall security that NGFWs can provide. Finally, we propose a solution to address the current limitations and gaps discovered that exist within a Next Generation Firewall.**

Keywords—Next Generation Firewall (NGFW), traditional firewall, server, Intrusion Detection System (IDS), Malware, Web Application Firewall (WAF), Open-Source software

I. INTRODUCTION

In the last few years there has been a rapid evolution of internet and its applications. The number of users has exponentially increased, and the user’s utilization of the internet has also changed dramatically. As a result, more sophisticated systems are required and emerging for user's protection on the internet. One common way of protecting a network was with the “traditional firewall”. Firewalls have long been an essential part of securing a network, both for an organization and for a private network. Traditional firewalls provide stateful inspection of network traffic that is entering or exiting the network. They are only able to control the flow of traffic which is essential but not as functional as a Next Generation Firewall (NGFW). NGFWs provide the same traffic controls as traditional firewalls but also add features like deep packet inspection for application security and intrusion prevention systems as well as allowing for greater definitions of access and security. Our goal is to identify whether NGFWs can provide scalable application and network security and to see if they can prevent the download of malware. In our preliminary survey we attempt to uncover the knowledge that our colleagues have on the subject. Our research is centered around answering our questions and we will also be using the results of experiments performed by industry professionals to assist with our goal. This paper is designed to serve as a benchmark for the current level of understanding about NGFWs of current and former Seneca College students as well as showing the utility of this technology. We hope that this will translate into more education on the topic of NGFWs which will mean more industry implementation of NGFWs.

II. LITERATURE REVIEW

This section covers the most recent research that have been conducted about the Next Generation Firewall (NGFW). The goal of this section is to highlight the important contributions made by these scholarly research papers in the area of the Next Generation Firewall. Further, we identify the existing gaps that currently exist with a Next Generation Firewall. This allows us to contribute to this research area by addressing the main problem with a Next Generation Firewall.

This book by A.Wolund et al [1] covers a broad range of topics related to network security. Our focus was on chapter 5 which covered the topic of legacy and next generation firewalls (NGFW) and the many combinations and configurations that are provided by Cisco as security products. A.Wolund et al [1] further describes the individual products, their capabilities, configurations, as well as the many different features of their next generation firewalls. Beyond the specific information about their products, we were able to learn the difference between legacy and next generation firewalls. Also, this book provided us with examples of how to use NGFWs in order to enhance network security.

B. Soewito and C. E. Andhika [2] explore the roles a NGFW must play when it comes to the IoT world and how it is a feasible security solution. With the high use of IoT devices and the critical role they play in the world today, it is with no doubt that we want to protect these devices to the maximum degree possible. It is crucial that the NGFW is placed at the DMZ zone within a smart house as this is the area at risk for attack. It is determined that homes and companies still use traditional firewalls which are proven to not provide adequate protection against attacks we see today. Therefore, this paper proposes a framework for implementation of an NGFW as many that do implement it fail as it is harder than it seems and therefore it is implemented incorrectly. To do this, this paper asks questions to address what must be considered for the transition to the NGFW. This study places a traditional firewall and a NGFW connecting to a smart house and executes various attacks such as a DDoS, Phishing and an SQL injection. Overall, the NGFW either dropped or rejected all attacks while the traditional firewall allowed all but one DDoS attack. Though, the reason the traditional firewall was able to block the attack is because it was configured to do so as with an NGFW it has capabilities to detect and block attacks on its own due to the advance features it consists of. The traditional firewall for the test cases was using “IBM ISS Proventia” while the NGFW was using “Checkpoint”. This paper does a good job at addressing the questions of what needs to be prepared for the transition from the traditional firewall to the NGFW, the features an NGFW must have and ideas of test cases to ensure the upgrade really did make a noticeable and significant difference.

In this article by F. Malecki [3] we learn about the shortcomings of “earlier-generation firewalls” and the security risks that they fail to solve. The difference between Stateful Packet Inspection (SPI) and Deep Packet Inspection (DPI) is briefly covered in relation to the performance of certain firewalls. The evolution of the Internet has brought about the need and NGFWs are able to inspect the payload of packets and match them with signatures of known viruses, malware, exploits, or vulnerabilities seamlessly. The need for businesses to advance to these types of firewalls is evident based on the number of companies whose breach can be traced back to poor network traffic controls or malware downloaded from malicious websites. NGFWs are the solution and provide a multitude of protections that would require a variety of tools to achieve normally.

F. Piconese [4] states that in this increasingly digital age, companies struggle to understand the origin of cyberattacks [4]. Malicious actions can come from both the outside and the inside the business, so it is necessary to adopt tools that can reduce cyber risks by identifying the anomalies when the first symptoms appear. This thesis deals with the topic of internal attacks and explains how to use innovative Intrusion Detection Systems to protect the IT infrastructure of Medium-sized Enterprises. These types of technologies try to solve issues like poor visibility of network traffic, long response times to security breaches, and the use of inefficient access control mechanisms. In this research, multiple types of internal threats, the different categories of Intrusion Detection Systems and an in-depth analysis of the state-of-the-art IDSs developed during the last few years have been detailed. After that, there will be a brief explanation of the effectiveness of IDSs in both testing and production environments.

This article by G. Uçtu, M. Alkan et al [5], discusses the use of Next Generation Firewalls for threat prevention on a multicast network. NGFWs are used for threat prevention for web, malware, and exploit attacks since they act as both security and network devices. There were specific attacks to test the usefulness of the 5 most common NGFWs in a multicast network. A brief review of the results shows that for all the possible attacks there were no instances where 100% of any given attack was blocked by any of the NGFWs. Some of the functionality of NGFWs were not tested for this specific test, but some of the results may vary based on the design of a network and the implementation of the NGFW. The experiments performed have proved crucial to our understanding of the capabilities of these devices and we will reference these later after our own experiments and analysis. With more time and access to these devices we would have liked to create similar tests in a unicast network to see how much more effective NGFWs could be after changing the network design.

K. Neupane, R. Haddad et al [6] discuss the goal of an NGFW and how it compares to a traditional firewall. It investigates common types of NGFW solutions that are being used today and their specific goals. The authors chose NGFW is a topic to investigate as an NGFW is a promising solution to the new emerging cyber-attacks. It states how the traditional firewall is unable to provide adequate protection for emerging and advanced threats, therefore it is imperative to move to an NGFW approach. This paper makes many references to AETs (Advanced Evasion Techniques). Attackers use AETs methods to disguise their attack by manipulating the payload into smaller loads and sending them off to protocols that are barely used. The purpose of AETs is to evade the defenses of the implemented security solution. NGFW uses methods to protect against AETs by utilizing DPI which means deep packet inspection, which can detect suspicious activities occurring, inspecting encrypted traffic by decrypting the communication stream and further detecting command and control commands. This paper proposes some advancements though that NGFWs need such as deep inspection and decryption of SSL/TLS traffic, port hopping detection, data leakage protection and some others. The solution they propose is integrated into more advanced NGFW solutions though many are proposed and should become a standard for all NGFW as time goes on to provide the best defense approach. This paper can be improved by showing some practical test cases of the different NGFW solutions and how they all compare. Overall, this was a solid paper on the importance of an NGFW and its features compared to a standard firewall.

M. Manohar, S.Hiriyannaiah et al [7] explore the use of Artificial Intelligence in NGFW. By utilizing incoming traffic behaviour to identify packets with Artificial Intelligence, researchers hoped to improve the NGFW, allowing it to classify packets on its own after working with a data set and being deployed in the field. Dynamically created rules would see it create exceptions for necessary packets as well as blacklist certain actions.

This paper by M. Zaki, V. Sivakumar et al [8] discuss the increased reliance in the healthcare sector of technology over the years. Healthcare using technology to store sensitive PI must be highly protected against from unauthorized access and manipulation. Therefore, having a good IT security solution implementation is critical for the healthcare sector especially given the strict regulatory data privacy laws specific for this sector. Current implementations using a traditional firewall and how an NGFW can up in a significant way to protect healthcare assets is explored within the paper. An NGFW goes beyond the traditional firewall by protecting up till the application level instead of just lower levels. Traditional firewalls do not have the capability to detect and stop emerging cyber-attacks as the activity must be continuously monitored and manually acted upon which is not realistic. Therefore, this paper proposes an architecture for the healthcare sector which uses an NGFW approach and implements network segments for the different departments that exist. Further, the approach implements the NGFW between the external and internal network so that all traffic leaving and entering is in fact being passed through the firewall. Therefore, with deep inspection of the packets and the NGFW integrating next-generation malware protection and IPS, it will determine if a file should be allowed to enter the network or if it should be blocked and set off a security alert. The solution proposes building a solution based on open-source software which will use Snort, OpenAppId and some other integrations using programming. The proposed NGFW makes good contribution as it uses open-source tools to integrate a well thought out solution that is cost saving for the health sector. It further will create application signature malicious detection using OpenAppID to identify suspicious activity occurring within specific healthcare software and set off an alert. This paper can be improved by showing us a prototype of the solution as well as mentioning what they will use to act as a traditional open-source firewall integrated into the NGFW such as nftables.

S.Erdheim [9] states that Next Generation Firewalls (NGFWs) were created due to a variety of needs and are intended to support and implement application control, Intrusion Prevention Systems (IPS), anti-malware, email security and much more. A majority of companies that have implemented NGFWs have stated that they did so to increase security, but also that they had to do much more work to manage firewall processes. Standard firewalls need to be constantly managed due to their complexity and this complexity has exponentially grown for NGFWs since they have application control, whitelisting capabilities, new layers of policy and a multitude of new security tools.

S. Thomason [10] explores how NGFW can be improved with advanced packet inspection. Current standalone firewalls CNA no longer protect enterprises form dangers on the internet. For a firewall to be classified as NGFW it needs to have a few basic requirements that put it above the previous generation of firewall. A deep packet inspection ability allowing it to scan all files for threats. Application intelligence is required as well as it allows the NGFW to determine which applications traverse on HTTP/HTTPS ports and what these applications might be doing. Good reporting abilities remain essential as If you don't have the ability to review what is actually happening with the system then you really do not know whether the system is performing as expected. Most importantly it needs to be manageable as most system failures are due to human errors and the ability to become exceptionally fine and granular with access controls.

As evident, many of the existing papers fail to identify the gaps and the constant improvements being made to the Next Generation Firewall. Again, the purpose of our research project is to identify existing gaps that exist within the NGFW solution and further understand the capabilities provided by this solution. Therefore, we want to contribute to existing research by expanding on the capabilities and knowledge of an NGFW.

III. Experement/Survey

1) *Survey*

A survey has been conducted to further contribute into the field of NGFW. The goal was to survey both students, those within industry and academia that have some sort of knowledge of firewall technologies. The survey was split so that those with deeper knowledge of the NGFW would be able to provide specific answers this research is trying to prove such as the importance, dominance and prevalence of an NGFW model. The survey has been specially crafted and specially distributed to these groups with this kind of network security knowledge. The survey has been distributed via a Google Forms link to the chosen selection. The main objective of the survey is to prove the emergence of the NGFW and how it can soon replace the so-called traditional firewall and some other security solutions if not all. An NGFW has a huge market growth and is a must for current and new security personnel to have knowledge about. Therefore, it is crucial to see the existing knowledge of firewalls, the knowledge of security professionals to date of firewalls and believed opinions of the potential of a firewall. From here we will be able to identify the gaps, actions to be taken to correct these critical gaps and how we can speed up the emergence of a NGFW which has never been more crucial. We have performed various data analysis of the survey results for the twenty questions asked and have drawn meaningful information from this raw data to help advocate the gaps to be corrected.

2) *Experiment 1*

We would like to also cover a few of the experiments performed in "A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls" [5]. Though their focus was specific to a multicast network, the relevance of the threat prevention capabilities of NGFW applies to help better our understanding of the application security and malware prevention. One of the experiments in this article that were performed was the experiment where a few different NGFWs with different configurations had many different malware files were sent through to discover if any of the NGFWs could successfully identify and block all of the malicious files.

3) *Experiment 2*

Another experiment from the same research paper as above was to see how many exploits the firewalls could successfully block to protect the web applications. The same firewalls as in the previous example were used as well as some vulnerable applications. This test was used to determine how well the NGFWs that were used in this example are able to protect web applications.

IV. Data Analysis and Results

The following details the results of our survey and what they mean in a larger context. We distributed the survey to a small group of selected individuals both students and professors from the IFS program.

1) *Firewall Knowledge Satisfaction*

The following is the visual representation of how individuals rated themselves for their firewall knowledge:

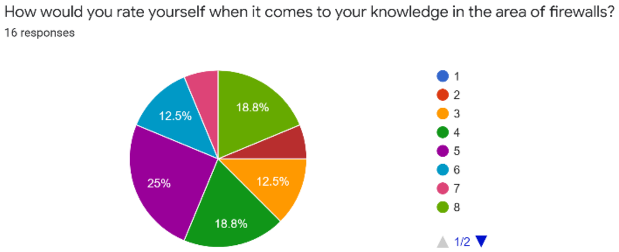


Figure 3.1.1 – Firewall context knowledge.

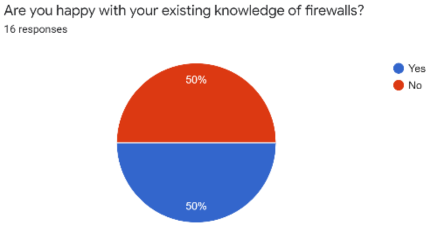


Figure 3.1.2 – Satisfied about current firewall knowledge.

We can see in Figure 3.1.1 that the range of existing knowledge rating of firewalls is between 40% to 80%. Further in Figure 3.1.2 we can see that overall, not many are very happy about their current knowledge about firewalls and its capabilities. This can be an indication that the firewall emphasis amongst IFS students needs to be improved quite significantly. This can potentially be achieved by updating the firewall course with newer technologies such as NGFW and emphasizing it throughout the curriculum as it is very crucial.

2) *Survey Group Area*

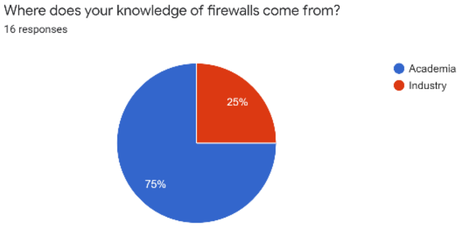


Figure 3.2.1 – Firewall knowledge source.

We can see above that most of the survey has been distributed to IFS students with 1/4 being professors.

3) *Firewall Area of Interest*

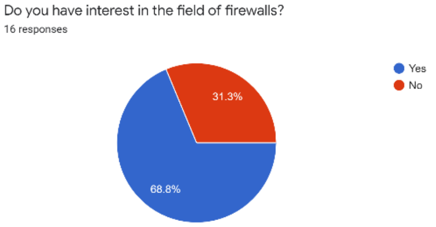


Figure 3.3.1 – Firewall interest.

Above, we can see that over 2/3 of the individuals surveyed are interested in the field of firewalls. Though, we should not eliminate the other 1/3 as it can be a result of the lack of interest and emphasis from the IFS program. We strongly believe if all have a higher degree of knowledge of firewall technologies, especially NGFW, the figure would be near 100%. This is why we are conducting this research, to bring deep awareness amongst ourselves to pass on the knowledge to the IFS program.

4) *NGFW Knowledge Area*

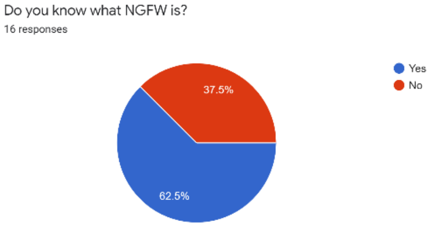


Figure 3.4.1 – Knowing what NGFW is.

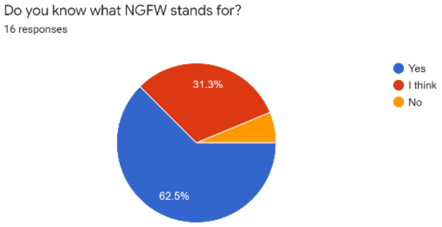


Figure 3.4.2 – Knowing what NGFW stands for.

In the above figure, we can see that almost 1/3 do not know what NGFW stands for which is problematic especially considering the increased demand for an updated firewall technology.

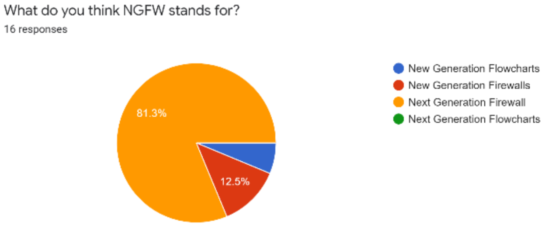


Figure 3.4.3 – Guessing what NGFW stands for.

It is good to see though, that most respondents are able to piece together the most appropriate answer even if they have never heard about an NGFW. This can even be a result of IFS students hearing it about one or two times and forgetting the acronym when just seeing "NGFW".

5) Firewall & other Security Solutions importance rating

In the next series of survey questions, we asked about the importance of a firewall solution based on opinion from what IFS students and professors currently understand about the different security solutions.

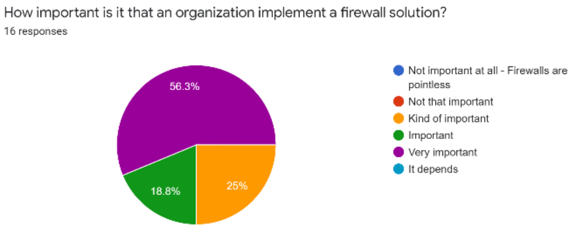


Figure 3.5.1 – Importance rating.

In the above figure, we can see that more than half agree that it is very important. The rest mostly believe that it is kind of important and just important. This can be due to the lack of emphasis on firewall technologies, their purpose, goal and ongoing capability improvements and of course NGFW.

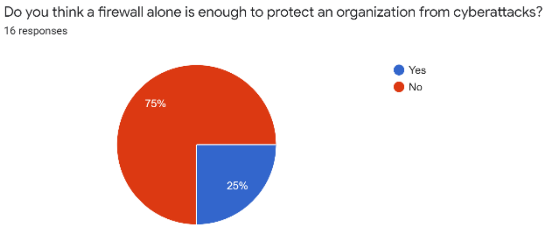


Figure 3.5.2 – Firewall acting on its own opinion.

In the above figure, we can see that about 2/3 believe a firewall alone is not enough to protect an organization against attack. The traditional firewall depending on the complexity and assets that exist within the infrastructure of the organization would not be enough. In many cases though, an NGFW is proven to replace many of the security solutions that once operated independently. NGFW can be enough to protect many types of organizations. Though again, when entering a largescale organization that is highly complex and has various servers an NGFW alone would likely not be enough. In an instance like this, the largescale organization may also consider implementing a WAF (Web Application Firewall) for their web-based servers as most NGFW solutions will not have this capability.

Related to figure 3.5.2, we asked an open response question regarding what security solutions the individual is familiar with. The very interesting and exact point we are trying to prove has indirectly answered figure 3.5.2. As said, 2/3 believe a firewall is not enough yet most of the answers contained solutions that is implemented into an NGFW such as IDS/IPS, anti-virus and ACL. Therefore, technically this turns that figure from 2/3 saying no to nearly 95% agreeing that a firewall can be enough which that of course if it is an NGFW. Again, it is the lack of awareness of emerging security solutions that doesn't make these questions accurately answered. Therefore, it was crucial for us to word them in a way that indirectly gave us the answer we were looking for.

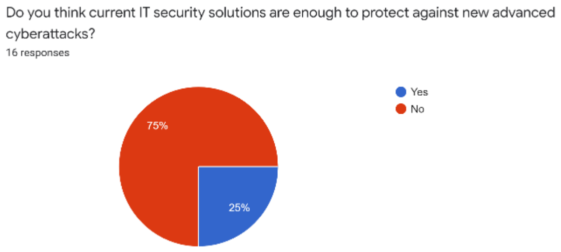


Figure 3.5.3 – Current IT Security solutions being enough.

Many agreed that current IT security solutions they believe are enough which is a good thing. This means that IFS students are confident with their skill set IFS has provided them. The others may not be that confident due to feeling that attacks are becoming far too sophisticated for existing tools. Though, the good thing is, as attacks are constantly becoming more advanced and complex, so are the security tools being developed. Therefore, it is crucial for IFS students to stay up to date with the latest IT security solutions out there such as NGFW.

Similar to the previous open response question, we asked now what firewall features the participants believe should be added. Again, most of the answers contained features that exist within a NGFW.

6) General Protection from Attacks

We then asked the participants a series of personal questions.

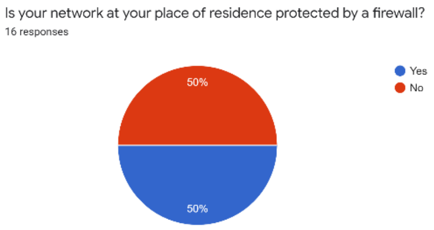


Figure 3.6.1 – Personal firewall protection.

About half of the participants personal network is protecting by a firewall. This can be due to many not feeling the need for a firewall protection on their home network as they might feel they are careful and do not have anything extremely important of value.

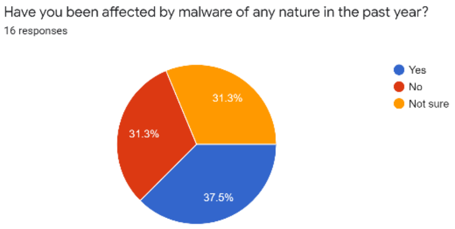


Figure 3.6.2 – Personal firewall protection.

Most have not been affected by any malware this past year which is a good thing. For those who have, a firewall implementation even host based could have prevented such attack from occurring.

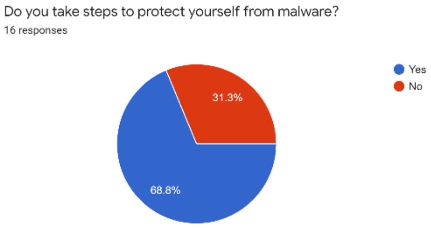


Figure 3.6.3 – Personal firewall protection.

Many agree that they do take steps to protect against malware such as being diligent on what websites they browse to and files they open.

7) NGFW Familiarity

The final series of questions were only opened to those with some sort of NGFW knowledge.

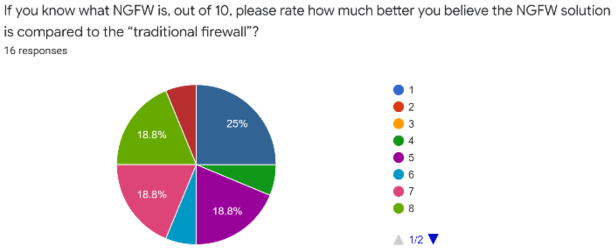


Figure 3.7.1 – How much better NGFW is believed to be.

The cumulative results show that most do in fact believe that NGFW is a much better solution compared to the traditional firewall. The others might just be too comfortable with the traditional firewall and like operating the other solutions separately compared to an all-in-one so therefore they do not believe that it is "much" better.

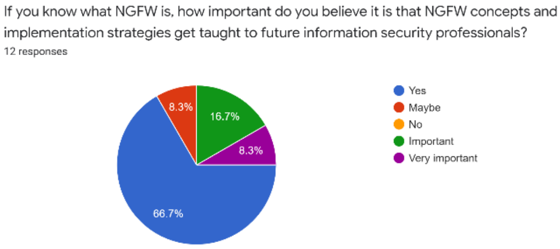


Figure 3.7.2 – NGFW education importance.

Majority do believe that it is critical that NGFW be taught to future IT professionals as this is a great skill to have going into the industry as they may be looking to upgrade their "traditional firewall". Note that both the "Very important" and the "Yes" mean the same thing.

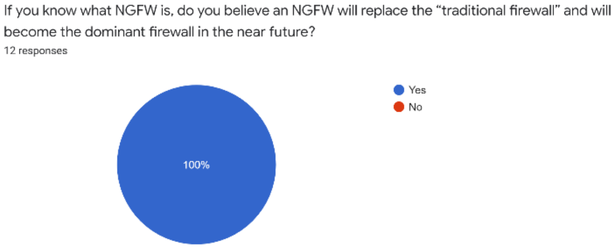


Figure 3.7.3 – NGFW becoming dominant.

The very expected result and would be kind of worrisome and require a step back into the thesis of out topic is in fact that everyone with NGFW knowledge should agree that it will become the dominant firewall. This is the exact case! NGFW can just be considered a firewall that has been upgraded to protect against modern day attacks and simply setup and administration requirements compared when multiple solutions are deployed.

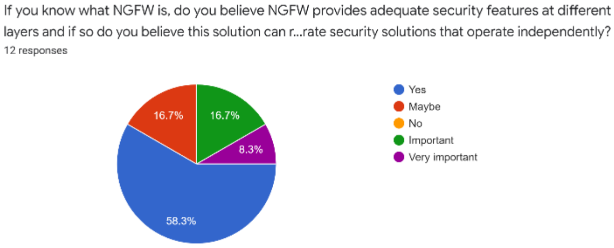
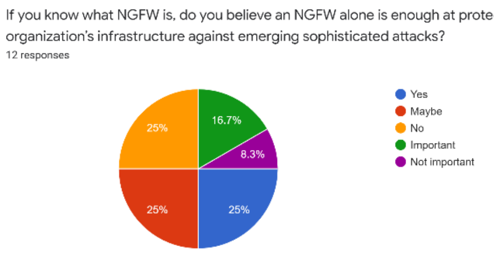


Figure 3.7.4 – NGFW Capabilities.

The full question to the above is:

"If you know what NGFW is, do you believe NGFW provides adequate security features at different layers and if so do you believe this solution can replace many separate security solutions that operate independently?"

The answer that most say is yes! Note that both the "Very important" and the "Yes" mean the same thing. This is the exact idea of an NGFW, to move on from just protecting the network from the lower layers and move to the upper layers, mainly the application layer.


If you know what NGFW is, do you believe an NGFW alone is enough at protecting an organization's infrastructure against emerging sophisticated attacks?

12 responses

Figure 3.7.5 – NGFW Level of Protection.

Most of the response area for this question is between yes to maybe. Note that both the "Very important" and the "Yes" mean the same thing. This can be due to the fact that depending on the complexity of the infrastructure, NGFW may not be enough, especially the solution that organization invested in and the capabilities. Therefore, it is also imperative to implement control measures such as physical security and host-based security OS best practices which include both policies and procedures. So yes, nothing alone is enough, security must be a holistic approach.

1) *Experiment 1*

From the results of the first experiment, we covered in "A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls" [5] we can see that none of the NGFWs were capable of blocking 100% of the malware files. Table 5 from this report shows a list of all the malware files that were tested and a 1 in the column means that the firewall was successful in blocking the malicious file. Table 6 shows the success rate of each of the firewalls in blocking the malware files, we can see that Firewall D was the most successful at 83.93% success. From this information we can safely say that NGFWs can be used to prevent malware from being sent to the internal network and being downloaded, though it may not be 100% successful and should not be the only means of security.

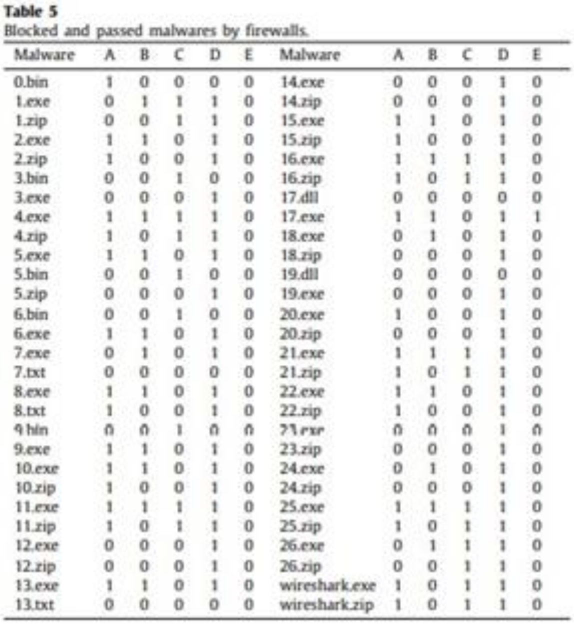


Table 5

Blocked and passed malwares by firewalls.

Malware	A	B	C	D	E	Malware	A	B	C	D	E
0.bin	1	0	0	0	0	14.exe	0	0	0	1	0
1.exe	0	1	1	1	0	14.zip	0	0	0	1	0
1.zip	0	0	1	1	0	15.exe	1	1	0	1	0
2.exe	1	1	0	1	0	15.zip	1	0	0	1	0
2.zip	1	0	0	1	0	16.exe	1	1	1	1	0
3.bin	0	0	1	0	0	16.zip	1	0	1	1	0
3.exe	0	0	0	1	0	17.dll	0	0	0	0	0
4.exe	1	1	1	1	0	17.exe	1	1	0	1	1
4.zip	1	0	1	1	0	18.exe	0	1	0	1	0
5.exe	1	1	0	1	0	18.zip	0	0	0	1	0
5.bin	0	0	1	0	0	19.dll	0	0	0	0	0
5.zip	0	0	0	1	0	19.exe	0	0	0	1	0
6.bin	0	0	1	0	0	20.exe	1	0	0	1	0
6.exe	1	1	0	1	0	20.zip	0	0	0	1	0
7.exe	0	1	0	1	0	21.exe	1	1	1	1	0
7.txt	0	0	0	0	0	21.zip	1	0	1	1	0
8.exe	1	1	0	1	0	22.exe	1	1	0	1	0
8.txt	1	0	0	1	0	22.zip	1	0	0	1	0
9.bin	0	0	1	0	0	23.exe	0	0	0	1	0
9.exe	1	1	0	1	0	23.zip	0	0	0	1	0
10.exe	1	1	0	1	0	24.exe	0	1	0	1	0
10.zip	1	0	0	1	0	24.zip	0	0	0	1	0
11.exe	1	1	1	1	0	25.exe	1	1	1	1	0
11.zip	1	0	1	1	0	25.zip	1	0	1	1	0
12.exe	0	0	0	1	0	26.exe	0	1	1	1	0
12.zip	0	0	0	1	0	26.zip	0	0	1	1	0
13.exe	1	1	0	1	0	wireshark.exe	1	0	1	1	0
13.txt	0	0	0	0	0	wireshark.zip	1	0	1	1	0

[5] Table 5

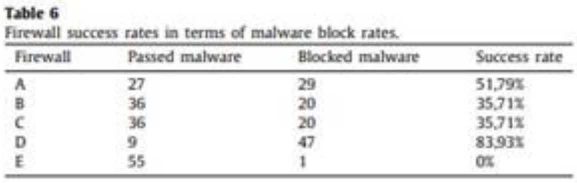


Table 6

Firewall success rates in terms of malware block rates.

Firewall	Passed malware	Blocked malware	Success rate
A	27	29	51,79%
B	36	20	35,71%
C	36	20	35,71%
D	9	47	83,93%
E	55	1	0%

[5] Table 6

2) *Experiment 2*

The results of a second experiment in the same research paper as above was that most of the firewalls were able to block at least 50% of the exploits from reaching the web applications. The best success rate was Firewall A with 75% but the other NGFWs were between 40-60% success rate. This experiment was tested in a multicast network and could possibly have different results in our own tests.

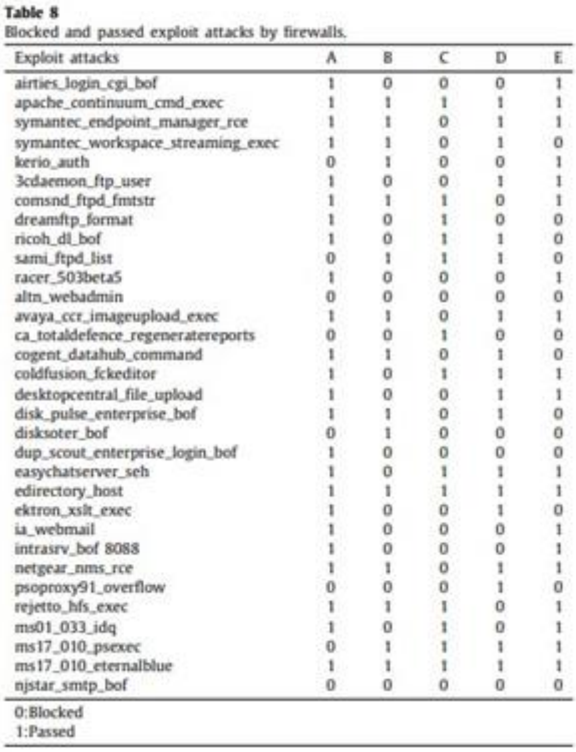


Table 8

Blocked and passed exploit attacks by firewalls.

Exploit attacks	A	B	C	D	E
airties_login_cgi_bof	1	0	0	0	1
apache_continuum_cmd_exec	1	1	1	1	1
symantec_endpoint_manager_rce	1	1	0	1	1
symantec_workspace_streaming_exec	1	1	0	1	0
kerio_auth	0	1	0	0	1
3cdaemon_ftp_user	1	0	0	1	1
comsnd_ftpd_fmtstr	1	1	1	0	1
dreamftp_format	1	0	1	0	0
ricoh_dl_bof	1	0	1	1	0
sami_ftpd_list	0	1	1	1	0
racer_503beta5	1	0	0	0	1
altn_webadmin	0	0	0	0	0
avaya_ccr_imageupload_exec	1	1	0	1	1
ca_totaldefence_regeneratereports	0	0	1	0	0
cogent_datahub_command	1	1	0	1	0
coldfusion_fckeditor	1	0	1	1	1
desktopcentral_file_upload	1	0	0	1	1
disk_pulse_enterprise_bof	1	1	0	1	0
disksoter_bof	0	1	0	0	0
dup_scout_enterprise_login_bof	1	0	0	0	0
easychatserver_seh	1	0	1	1	1
edirectory_host	1	1	1	1	1
ektron_xslt_exec	1	0	0	1	0
ia_webmail	1	0	0	0	1
intrasrv_bof 8088	1	0	0	0	1
netgear_nms_rce	1	1	0	1	1
psoproxy91_overflow	0	0	0	1	0
rejetto_hfs_exec	1	1	1	0	1
ms01_033_idq	1	0	1	0	1
ms17_010_psexec	0	1	1	1	1
ms17_010_eternalblue	1	1	1	1	1
njstar_smtp_bof	0	0	0	0	0

0:Blocked
1:Passed

[5] Table 8

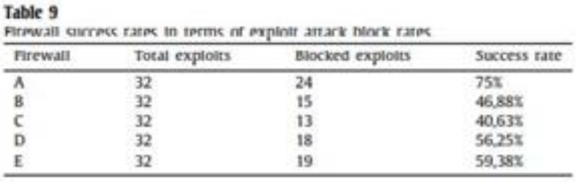


Table 9

Firewall success rates in terms of exploit attack block rates.

Firewall	Total exploits	Blocked exploits	Success rate
A	32	24	75%
B	32	15	46,88%
C	32	13	40,63%
D	32	18	56,25%
E	32	19	59,38%

[5] Table 9

V. NGFW Solution Proposal based on Existing Research and Data Analysis

There are many vendors that provide a Next Generation Firewall (NGFW), and each vendor has their specific competitive advantages over others. As mentioned, NGFW has been around for a while but is constantly improving and becoming more popular as security threats increase at an astonishing rate. Therefore, it is important for all security professionals to be aware of this solution and have somewhat familiarity with it. Though, a security professional that has knowledge of the many security solutions on the market should not find it difficult to understand what an NGFW is. For IT security students that many clearly lack deep knowledge of a NGFW should become familiar the same way they learn about the "traditional firewall". This is what we refer to as going beyond iptables and nftables. To achieve this in the academia setting, we must have easy access to a free open-source tool that can provide this adequate knowledge. This means an open-source solution that can be pieced together similar to M. Zaki, V. Sivakumar, S. Shrivastava, and K. Gaurav [8] solution. This specific solution though only offers Snort as an IPS with OpenAppID. We need to take a step back and add basic firewall capabilities such as nftables as all NGFW start out as a "traditional firewall". Further, it is critical to understand the "traditional firewall" before moving onto an NGFW. This open-source tool can be further contributed to by adding some additional functionality such as a VPN, antivirus software and sandboxing deep analysis. Further, to create something unique, we can add a Web Application Firewall (WAF) to the open-source solution which can address other uncertainties that currently surround the NGFW as noticed in the data collection and analysis phase. We then need to determine based on the network packet how the tools will all come together to create a holistic all-in-one approach working seamlessly with one another providing the maximum security. With some sort of open-software like this all pieced together that is easily accessible and reliable, we can start fixing the existing gaps that currently exist with the Next Generation Firewall. This can have a very strong domino effect as providing this kind of knowledge and practice to students in IT security can keep more people secured and safe from cyber threats and attacks.

VI. Conclusion

Based on the results of the different experiments and now knowing that NGFWs have all the capabilities of a traditional firewall and much more, we can answer our initial question. "Are Next Generation Firewalls capable of providing scalable application and network security? Will they prevent malicious files from being downloaded"? We have determined that Next Generation Firewalls can provide scalable application and network security. Though they are not successful 100% of the time, used with other mitigation tactics they could prevent some serious vulnerabilities from being exploited on a company's resources. Traditional firewalls should have been fully replaced by NGFWs since they can provide multi-layer security, but cost is likely to be the biggest setback in terms of their implementation. Next Generation Firewalls will be an essential tool for all networks. Its ability to combine separate logging, IDS (Intrusion Detection System), IPS (Intrusion Prevention System) and Management systems into a single device is invaluable and companies can use that to justify the expense of the upgrade. When used in conjunction with other tools a NGFW will improve the overall security of any network. Therefore, it is imperative to build on existing ideas and approaches on open-source solutions that will be easily accessible and provide many capabilities. This tool can then be used in both academia and industry to easily learn, gain the required experience and deploy an equipped Next Generation Firewall.

Acknowledgment

We thank Dr. Lutful Karim in his guidance and assistance throughout this research project. We also thanks all those that participated in our research survey to further identify the gaps that currently exist amongst professionals and students in the field of network security.

References

[1] A. Woland, V. Santuka, M. Harris and J. Sanbower, Integrated security technologies and solutions - Volume I, Cisco Security Solutions for advanced threat protection with next generation firewall, intrusion prevention, AMP, and content security. Cisco Press, 2019. [Accessed 27 May 2021].

[2] B. Soewito and C. E. Andhika, "Next Generation Firewall for Improving Security in Company and IoT Network," *2019 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 2019, pp. 205-209, doi: 10.1109/ISITIA.2019.8937145. [Accessed 27 May 2021].

[3] F. Malecki, "Next-generation firewalls: security with performance," *Network Security*, vol. 2012, no. 12, pp. 19–20, 2012, doi: 10.1016/s1353-4858(12)70114-9. [Accessed 27 May 2021].

[4] F. Piconese. "Deployment of Next Generation Intrusion Detection Systems against Internal Threats in a Medium-Sized Enterprise." Core.ac.uk, Oct. 2020. [Accessed: 31-May-2021].

[5] G. Uçtu, M. Alkan, İ. Doğru and M. Dörterler, "A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls", *Future Generation Computer Systems*, vol. 124, pp. 56-67, 2021. Available: doi:10.1016/j.future.2021.05.013. [Accessed 27 May 2021].

[6] K. Neupane, R. Haddad and L. Chen, "*Next Generation Firewall for Network Security: A Survey*," SoutheastCon 2018, 2018, pp. 1-6, doi: 10.1109/SECON.2018.8478973. [Accessed: 30-May-2021].

[7] M. Manohar, S. Hiriyannaiah, G. Siddesh & K. Srinivasa. (2021). Risk Measurement and Cyber security in Industrial Control Systems. IOP Conference Series: Materials Science and Engineering. 1110. 012014. 10.1088/1757-899X/1110/1/012014.[Accessed: 31-May-2021].

[8] M. Zaki, V. Sivakumar, S. Shrivastava, and K. Gaurav, "Cybersecurity Framework For Healthcare Industry Using NGFW," *ieeexplore*, 31-Mar-2021. [Online]. [Accessed: 31-May-2021].

[9] S. Erdheim, "Deployment and management with next-generation firewalls", Network Security, vol. 2013, no. 10, pp. 8-12, 2013. [Accessed 26 May 2021].

[10] S. Thomason, Dr.. Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices. Global Journal of Computer Science and Technology, [S.l.], Aug. 2012. ISSN 0975-4172. [Accessed: 31-May-2021].