Next Generation Firewall for Network Security: A Survey

Kishan Neupane*, Rami Haddad*, Lei Chen+
Department of Electrical Engineering*
Department of Information Technology+
Georgia Southern University
Statesboro, GA 30460, USA
{kn01559, rhaddad, lchen}@georgiasouthern.edu

Abstract— **In today's world, with the advent of internet, the network security has become a necessity to protect the usability and integrity of network and data. Traditional firewalls are incapable of coping with emerging threats such as targeted and data focused attacks. In this paper, a survey of the different types of current and next generation firewalls are discussed in details highlighting their potential functionalities. The different technologies implemented in Next Generation Firewall (NGFW) for network security are highlighted. Additionally, the advantages of the next generation firewalls were compared against the traditional firewalls. Also in this paper, the primary network security goals, their recent emerging security threats, and their potential solutions to protect the network are discussed.**

Keywords— **Network security, firewall, next generation firewall**

I. Introduction

In the last few years, due to the rapid evolution of internet and its applications the number of users has exponentially increased and the users' utilization to the internet has also changed dramatically [1]. More sophisticated protection systems are needed to protect internet users from emerging threats in which traditional firewall are not efficient. Firewalls are security devices that monitor and control the flow of network traffic based on a set of predefined rules. To block current and emerging threats such as botnets and targeted attacks, more proactive firewalls are needed. To protect network systems from more sophisticated attacks any organization need to update their firewall and intrusion prevention/detection capabilities [2]. Deep packet inspection intrusion prevention systems (IPSs) can protect against known attacks that target operating systems and software but cannot successfully detect or block the misuse of applications. Gartner Research uses the term "next generation firewall" to indicate the evolution of firewall that deals with the emerging network security threats compromising the network systems [3]. For example, botnets delivery methods have mostly been undetectable to first generation firewall. The contributions of this paper are to:

- provide motivation and need of next generation firewall for network security
- present a survey on recent advances in security threats in network and countermeasures with next generation firewall
- present different firewall technologies and their benefits
- provide the advantages of next generation firewall
- provide the current state of art techniques of NGFW for different vendors (Palo alto, Fortinet, Check Point and so on) in terms of security function and performance

This paper is organized as follows. Section II presents the security goals and the types of advanced attacks. It also provides an overview of firewalls and addresses the need of next generation firewalls. Section III highlights the Next Generation Firewall (NGFW) and its application in different layers. Section IV discusses recent advancements in the next generation firewall and advantages of NGFW over traditional firewall. Finally, conclusion and future scope are presented in Section V.

II. Security Requirement and Types of Attacks

A. Security Requirements

The primary network security requirements and their objectives are summarized in Table I:

TABLE I: Network Security Goals

Requirements	Specific Objective
Confidentiality	Ensure that the sensitive information are limited to authorized user only
Authenticity	Ensure that the identity of the subject or resource is the identity claimed
Integrity	Ensure that information is kept accurate and consistent unless authorized changes are made
Availability	Ensure that information is available to authorized user whenever needed

B. Types of Attacks

Traditional firewalls mainly deal with network and transport layers, block IP addresses, and protocol ports to tackle traditional types of cyber-attacks which were visible and opportunistic. Recently, the cyber-attacks are becoming stealthier, targeted, and focused on applications and their sensitive data [4]. To defend the application-based complex attacks a new generation of firewalls is required as threat move up the OSI layers. Many next generation firewalls have the capability to inspect all traffic but are not equally able to scale, integrate,

978-1-5386-6133-8/18/$31.00 ©2018 IEEE

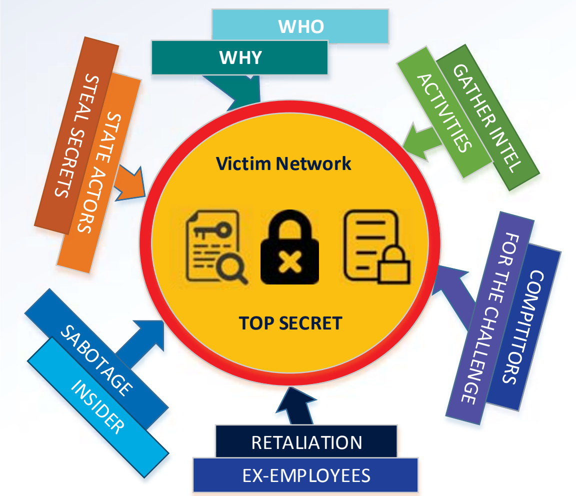

Fig. 1: Attacks Model: Who and Why?

and detect advanced attack methodologies. Figure 1 highlights the types of attackers and the motivation for such attacks.

The following are the emerging threats that are vulnerable to traditional firewalls that led to the evolution of the next generation firewalls:

1) Advanced Evasion Technique: The type of network attack that combines different evasion methods to create new attack technique over several layers simultaneously. Advanced Evasion Techniques (AETs) disguise malicious payloads by splitting them into smaller frames and sending frames across rarely used protocols. AET attacks operate silently and hide from traditional firewalls in legitimate traffic and ports leaving no traces of the attacker's action [5]. Figure 2 shows how advanced evasion techniques work by fragmenting codes and sending them through unexpected ports to execute the attack on the network.

2) Targeted Cyber-Attacks: Targeted cyber-attacks are malicious attacks in which tNfic individual or systems rather than an entire network while maintaining the anonymity. These attacks are not well known but expected to actively pursue and compromise a target infrastructure. The malicious actor first identifies, collects and gathers publicly available information of the target. Based on the gathered information, then the attackers conduct APTs to get deeper and deeper into a target's individual or network [6]. To infiltrate into target's infrastructure, the attacker can use various methods such as phishing email, zero day attack, social engineering components and platform to entice targets. Attackers can adapt themselves to counter victim's defenses by adapting, modifying, and refining their method of attacks. The ultimate goal of these attacks is stealing sensitive information rather than causing damage to the network [7]. In Figure 3, the six stages of a targeted attack are shown to explain how attackers get into the target network. Each stage of targeted attack has different features that affect the network. These features are presented as follows:

(a) *Intelligence Gathering:* the first stage of a targeted attack is to collect information about the internal or external target network.

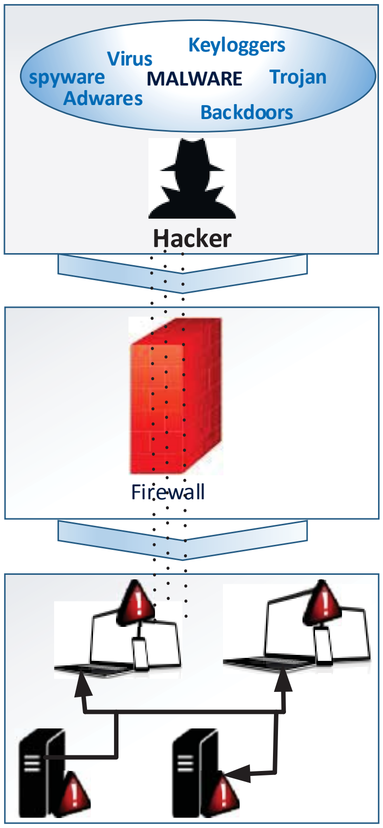

Fig. 2: a) Attackers apply AETs to disguise their attack, b) AET penetrates the target individual or network undetected successfully and continue APT attacks, and c) APTs are targeted attacks on individual or system which require high order of stealth over long period of time for successful hacking

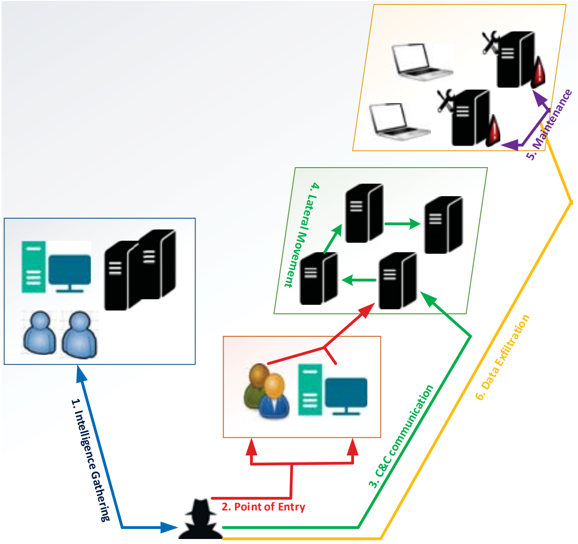

Fig. 3: Components of targeted attacks

(b) *Point of Entry:* the most effective technique attackers deploy to enter into the target network is spear phishing and watering hole attacks. Apart from the initial point of entry, different target network segments are continuously targeted to increase the chances of successful attack.

(c) *Command and Control:* attacker use internal servers to control a compromised machine before progressing to other compromised machines inside the target network.

(d) *Lateral Movement:* includes the use of a legitimate system to steal sensitive information and keep activities hidden after establishing their presence within the target network.

(e) *Maintenance:* after gaining access to the target network, the attackers ensure that their presence remains undetected and access remains available by installing a backdoor or using command and control servers to enter the target network.

(f) *Data Exfiltration:* The ultimate goal is to extract confidential information from compromised machine(s) in the target network.

3) Web Application Attacks: web applications vulnerability using injection attacks have been considered to be the number one source of threats for almost a decade. The major threat vector for a website is that web applications have no access restrictions. The advancement of Web2.0, use of social networking to share information, and organizations' adoption of web has played a major role in increasing web application attacks. According to the 2015 Web Application Attack Report (WAAR), the major source of web application attacks is cross-site scripting and SQL Injection attacks which make up more than 50% of the attacks. The web application attack area is highly dynamic, multi-faceted, and has the potential to go up further to the top of security threats in the near future [8].

4) Data Focused Attacks: The main reason for initiating attacks is to steal confidential data and exfiltrate it from the targeted networks. Even with the advancements in data collection, filtering and forensic analysis, it is extremely difficult to estimate the amount of compromised data. Most of the victims do not know which of their sensitive data was compromised, therefore, focusing on data flow is critical to protect any individual or system against data breaches [1].

According to Verizon 2015 Data Breach Investigation report, the total financial loss from 700 million compromised data was about 400 million dollar in which 70 countries were involved [9]. More than 70% of incidents of cyber-espionage pattern have featured phishing. Table II highlights the most trending cyber-threats in 2015 and the change in their popularity compared to the threats of 2014.

TABLE II: Trending cyber-threats in 2015 compared to 2014 [10]

1	Malware	⇑
2	Web Based Attack	⇑
3	Web Application Attack	⇑
4	Botnets	⇓
5	Denial of Service	⇑
6	Physical Damage	⇔
7	Insider Threat	⇑
8	Phishing	⇔
9	Spam	⇓
10	Exploits Kits	⇑
11	Data Focused Attack	⇔
12	Identity Theft	⇔
13	Information Leakage	⇑
14	Ransomeware	⇑
15	Cyber Espionage	⇑

Notation: ⇑ Increasing, ⇓ Decreasing, ⇔ Same

C. *Advanced Threats Patterns*

Attackers inspect how their targets secure their networks and find a way to bypass and impose security threats as discussed in Table III.

III. Next Generation Firewall

A. *Motivation*

To know more about the need of next generation firewalls, it is essential to know its history. The first generation firewalls, developed in early 1990's, were not designed to inspect network web traffic that uses internet to connect to applications and other sensitive information. With the exponential increase in network threats, the effectiveness of the first generation firewalls have been limited. Figure 4 represents the major market drivers which paved the way for the evolution of the next generation firewalls.

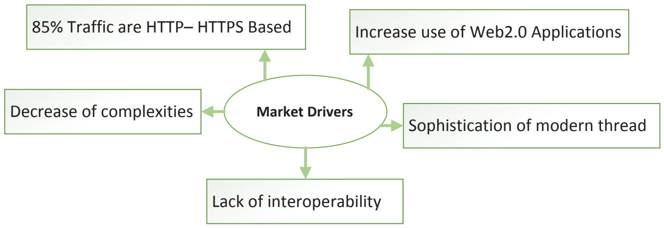
85% Traffic are HTTP– HTTPS Based
Increase use of Web2.0 Applications
Decrease of complexities
Market Drivers
Sophistication of modern thread
Lack of interoperability

Fig. 4: Market Drivers

The drawbacks of the first generation firewalls which led to the evolution of the next generation firewalls are summarized as follows:

- Unable to protect against emerging threats like botnets and targeted cyber attacks.
- Failure to examine real-time web traffic.
- Unable to facilitate the clustering of firewall which limits its scalability.
- Inefficient and expensive management.
- Limited network operability, only functional over the network and transport layers.

B. *Evolution of Firewall*

To understand the evolution of the next generation firewalls, it is warranted to address the different types of firewalls. Table IV summaries the different types of firewalls in terms of their main characteristics, range of operation within the OSI layer, design type, and capabilities. As depicted from Table IV, these firewalls differ significantly. For example, the next generation firewall uses deep packet inspection that combines intrusion prevention systems and other more advanced network

TABLE III: Advanced Threats Patterns

Technology	How AET bypass?	How NGFW works?
Antivirus	Antivirus and antimalware work on endpoint devices. Threats bypass antivirus and antimalware by hiding activities in trusted systems and processes	With application awareness, an NGFW analyze application traffic and report the potential threats by detecting malicious applications tunneling inside legitimate applications. Traditional firewall is limited to IP address and port.
Legacy Firewall	Advanced threats disguise activity as ordinary HTTP traffic or encrypt their data	With the feature of application-specific content in NGFW, it can inspect encrypted traffic for malware by decrypting the packet stream.
Network Security Device	Advanced threats planted internally open holes through firewall and network security. Because of access to user accounts, hackers bypass internal network access controls.	Most holes are created with command and control channel applications using well known ports, which can be detected by filtering application data. NGFW are capable of detecting outbound control and command protocols used by botnets

traffic flow control which is the core of all the new generation of stateful firewalls [11].

The management of the first generation firewalls became a major source of security threat. To secure the network from current and emerging threats the blend of powerful traffic inspection capabilities, simple management, and high accessible capabilities firewalls are needed. To overcome the shortcoming of the first generation firewalls, according to Gartner Research, next generation firewalls should have the following attributes [3]:

- Must leverage all capabilities of existing firewalls
- Must integrate the intrusion prevention system and firewall capabilities
- Must integrate deep packet inspection
- Application based awareness
- Support for inline configurations

C. Future advanced features needed for next generation firewall

Next generation firewalls must have the following advanced features to analyze and inspect traffic in a fine level of granularity.

1) Encrypted traffic control: SSL/TLS provides authentication but creates blind spot which challenges traditional layered defenses. This help attackers to leverage SSL tunnels to inject malware into the network, hide command and control traffic and steal confidential data [12]. Therefore, next generation firewalls must have the ability to decrypt and inspect SSL/TLS traffic to eliminate blind spots threats. Gartner estimates that more than 50% of the attacks will use SSL/TLS by 2017 [13].

2) Port hopping: Attackers often use random port hopping to get beyond traditional firewalls. Thus, the next generation firewall must be able to detect those ports when being used.

3) Application control: the next generation firewall should not look at layer 3 and layer 4 header rather it must be more application aware, so that it has the ability to restrict access to web apps.

4) Identity based control: the next generation firewall must be able to map specific security policies to defined user groups and individuals.

5) URL filtering: the next generation firewall must be able to restrict web surfing to limit the exposure to harmful and inappropriate sites.

6) Data leakage protection: the next generation firewall must be able to restrict the egress of confidential data.

7) WiFi network control: the next generation firewall must ensure that Wi-Fi networks have the same level of security stance and abilities.

8) Network access control: the next generation firewall must ensure that each connecting end point device has appropriate security.

9) WAN Routing & Optimization: the next generation firewall should be backed by QoS and priority capabilities.

D. How traditional firewall fails and why next generation firewall is the solution?

Firewalls can control the flow of network traffic based on a set of routing rules and block DoS attacks. However, they cannot identify the attacker intention by looking inside the packets information to detect malware and help protect the network from threats. Table V summaries the shortcoming of traditional firewalls that are addressed by the next generation firewalls.

TABLE IV: Generation of Firewall

Generation	1^{st}	2^{nd}	3^{rd}	Next Generation
Firewall Type	Packet Filter	Stateful Packet Inspection	Application Proxy	Deep Packet Inspection
OSI Layer	Transport Layer	Transport Layer	Application Layer	Application Layer
Main Functions	Filter packets based on source and destination IP addresses, port and protocols	Filter based on state and context of packets. Keeps track of each traffic using state table	Different proxy required for each service allowed. Acts as middleman between source and destination to reestablish a new session	Looks deeps into packet and makes granular access control decisions based on packet header and payload. Excels in managing application and data driven threats. Incorporates intrusion detection and prevention technology features.

TABLE V: Traditional Firewall Vs Next Generation Firewall

Goals	Traditional Firewall	Next Generation Firewall
Prevent Advanced Persistent Attacks	• Only part of network security supplemented with IPS, URL filtering, gateway antimalware-malware products • Separately managing security tools is expensive	• Offer complete set of security technologies in one package • Combine all features of traditional firewall • Integrated package is easy to install, configure, deploy and manage as a unit which reduces administrative cost
Inspect SSL Traffic	• Cannot decrypt and inspect SSL traffic • Attacker can create SSL tunnels inside out to exchange command and control message	• Use Deep Packet Inspection technology to decrypt and inspect SSL traffic in both inbound and outbound direction • Detect and block botnet command and control message • Prevent advanced persistent threats using SSL
Control Web Applications	• Not application aware • Application control is a serious deficiency	• Offer application intelligence and control • Recognize specific application • Provide chart to visualize and control traffic by application
Manage Users & Use Policy	• No correlation of network traffic with users	• Allow application control at user group and individual level • Impose acceptable policies at high level of granularity • Allow to identify traffic by user and user group who pose security threats or involuntarily affect productivity through traffic visualization
Trade off Security vs Performance	• Administrator turn off monitor on specific ports, disable firewall rule and limit deep packet inspection which affect performance	• Parallel processing hardware architecture • Apply efficient approaches

IV. Recent Advancements in Next Generation Firewall

A. Palo Alto Next Generation Firewall

Drastic change in application usage, user behavior, and complex network infrastructure create vulnerabilities in traditional port based network security. Data center expansion, network virtualization, and mobility are imposing an initiation to protect the networks from new and more advanced persistent threats such as botnets and targeted cyber-attacks. Palo Alto Next Generation Firewall is the core of next generation security platforms designed to address the emerging threats. The next generation firewall inspects all traffic including application, threats and content and ties them to the user. Palo Alto next generation security platform discover unknown threats, reduce response time to incident and streamline security deployment [14]. The following are the important features of the Palo Alto next generation firewall:

- Enable application, content and user by classifying traffic, allow and protect access to SaaS applications
- Eliminate unsolicited application by reducing threat footprint and block known advanced persistent threats by applying targeted security policy
- Protect data center by validating application, isolation of rouge application and high speed threat prevention
- Deploy, enforce and maintain security policies with increased visibility and control for cloud computing environment
- Extend next generation security platform to user and devices regardless of geographic location

B. Vendor to Vendor Feature Comparison

The features of different firewall vendors are compared in terms of performance, application control, intrusion prevention systems, security, and flexibility in Table VI.

Figure 5 illustrates the 2015 firewall market share percentages allocated to different vendors.

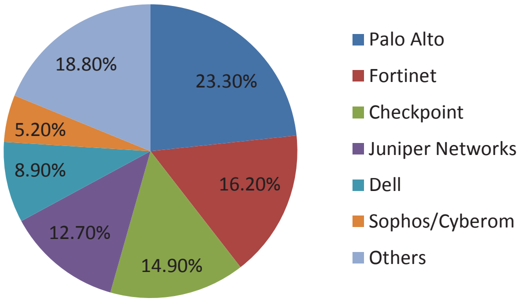

Fig. 5: 2015 NGFW Market Share [18]

TABLE VI: Vendor to Vendor Features Comparison

	Palo Alto [14]	Fortinet [15]	Check Point [16]	Juniper Networks [17]
Performance	Use of the shelf processor	Built FortiASIC processor integrated with IPS, app control, VPN, antivirus	No ASIC related security or hardware acceleration	No ASIC related security or hardware acceleration
Application Control	Capable of controlling more than 1300 applications	Full visibility and granular control of more than 1900 apps and protocols including Web2.0	Need to buy separate application control software based on requirement	Limited support of application control
Intrusion Prevention System	Inferior IPS, VPN and firewall performance. Limited signature coverage	Advance FortiASIC security processor to optimize content inspection	Inferior IPS, firewall and VPN performance	Inferior IPS, firewall and VPN performance
Security Technologies	Does not offer UTM security functionality and user third party agreement for content filtering	Offer UTM security functionality	Does not offer UTM security functionality and user third party agreement for content filtering	Does not offer UTM security functionality and user third party agreement for content filtering
Flexibility and scalability	Cannot support large service, no modular flexibility	Support small to large enterprise and service providers, flexible modularity	Complex distributed network security deployment and feature development	Complex distributed network security deployment and feature development

V. Conclusion

The next generation firewall offer more accessibility to network traffic, operability across the OSI layers, and advanced features to protect the networking infrastructure against emerging threats. In this paper, the network security goals and emerging network threats were summarized. The discussion mainly focused on the technology implemented in NGFW for network security. In addition, the advantages of next generation firewall in comparison with traditional firewall were further discussed and the advanced features of NGFW were highlighted. Finally, a comparison of current state technique and different NGFW available in market was provided highlighting their various parameters such as security function and performance.

References

[1] "Global internet report 2016." [Online]. Available: https://www.internetsociety.org/globalinternetreport/2016/

[2] "Cisco annual security report 2016." [Online]. Available: http://www.cisco.com/

[3] J. Pescatore and G. Young, "Defining the next-generation firewall," *Gartner RAS Core Research Note, from http://www. ga1tner. com*, 2009.

[4] K.-K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers & Security*, vol. 30, no. 8, pp. 719–731, 2011.

[5] M. Chammem, M. Hamdi, and T.-H. Kim, "Extending advanced evasion techniques using combinatorial search," in *Security Technology (SecTech), 2014 7th International Conference on*. IEEE, 2014, pp. 41–46.

[6] "Multi-staged attacks driven by exploits and malware." [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/

[7] "Targeted cyber attacks." [Online]. Available: http://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks

[8] "Web application attack report 2015." [Online]. Available: https://www.imperva.com/DefenseCenter/WAAR

[9] "Verizon data breach investigations report." [Online]. Available: https://msisac.cisecurity.org/whitepaper/

[10] "Enisa threat landscape 2015." [Online]. Available: https://www.enisa.europa.eu/publications/etl2015/

[11] A. Abdel-Aziz and J. Esler, "Intrusion detection & response-leveraging next generation firewall technology," *SANS-Institue, Tech. Rep*, 2009.

[12] "Eliminate blind spots in ssl encrypted traffic." [Online]. Available: https://www.venafi.com/assets/pdf/sb/SSL-Visibility-Solution-Brief/

[13] "Security leaders must address threats from rising ssl traffic." [Online]. Available: https://www.gartner.com/doc/2635018/

[14] "Palo alto networks, palo alto next generatin firewall." [Online]. Available: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall

[15] "Fortinet, the next generation firewall solution." [Online]. Available: https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-firewall/next-generation-firewall-ngfw.html

[16] "Check point software technologies, next generation firewall." [Online]. Available: https://www.checkpoint.com/products/next-generation-firewall/

[17] "Juniper networks, next generation firewall." [Online]. Available: http://www.juniper.net/us/en/solutions/next-generation-firewall/

[18] "Next generation firewall cy2015 - nss labs, inc." [Online]. Available: https://www.nsslabs.com/research-advisory/library/infrastructure-security/next-generation-firewall/next-generation-firewall-cy2015/