Survey on Next Generation Firewall

Jayesh Surana, Kriti Singh, Neha Bairagi, Nivedita Mehto, Nupur Jaiswal
Professor, Student, Student, Student, Student
Information Technology,
SVITS, Gram baroli , Sawer road, Indore, MP, India

Abstract— **This paper will address a recent trend in network security, which is leveraging next-generation firewalls (NGFW) at the network perimeter. The paper will demonstrate check point provides customers of all sizes with the latest data and network security protection in an integrated next generation firewall platform, reducing complexity and lowering the total cost of ownership. Whether you need next-generation security for your data center, enterprise, small business or home office, Check Point has a solution for you.**

***Index Terms*— NGFW (Next Generation Firewall system),Intrusion detection, Network**

I. INTRODUCTION

A Next-Generation Firewall (NGFW) is an integrated network platform that is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS). Other techniques might also be employed, such as TLS/SSL encrypted traffic inspection, website filtering, QoS/bandwidth management, antivirus inspection and third-party identity management integration (i.e. LDAP, RADIUS, Active Directory)

II. EVOLUTION

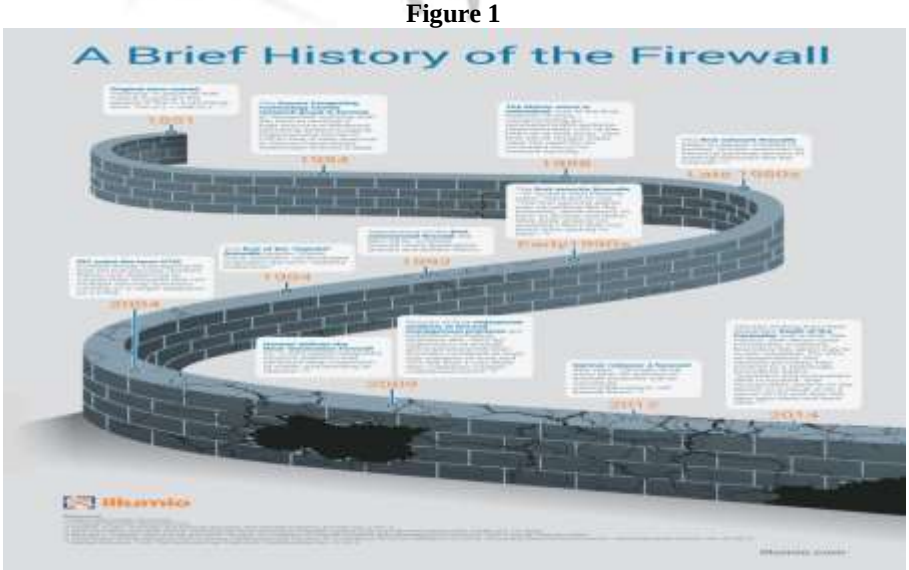
Modern threats like web-based malware attacks, targeted attacks, application-layer attacks, and more have had a significantly negative effect on the threat landscape. In fact, more than 80% of all new malware and intrusion attempts are exploiting weaknesses in applications, as opposed to weaknesses in networking components and services.

Stateful firewalls with simple packet filtering capabilities were efficient blocking unwanted applications as most applications met the port-protocol expectations. Administrators could promptly prevent an unsafe application from being accessed by users by blocking the associated ports and protocols. But today, blocking a web application like Farmville that uses port 80 by closing the port would also mean complications with the entire HTTP protocol.

Protection based on ports, protocols, IP addresses is no more reliable and viable. This has led to the development of Identity-based security approach, which takes organizations a step ahead of conventional security appliances which bind security to IP-addresses. NGFWs offer administrators a deeper awareness of and control over individual applications, along with deeper inspection capabilities by the firewall. Administrators can create very granular "allow/deny" rules for controlling use of websites and applications in the network.

III. HISTORY

Figure 1



IV. ROLE OF FIREWALL

If we wanted to summarize the role of a firewall by answering one simple question: "What does the firewall do?" The simple answer would be: "The firewall controls data flow." Whether the firewall is a personal firewall used by an end-user to control data flow to and from the computer, or a network firewall controlling data flow to and from different security zones (DMZ, Internet, LAN, etc.); the firewall is basically controlling what data is allowed, or not allowed, to flow according to predefined firewall rules that enforce the organization's security policy. As noted earlier, firewall technology has been around for some time, as early as the 1980s ; therefore researchers have had ample time to advance the technology. The next section briefly discusses firewall types.

V. TYPES OF FIREWALL

Figure 2

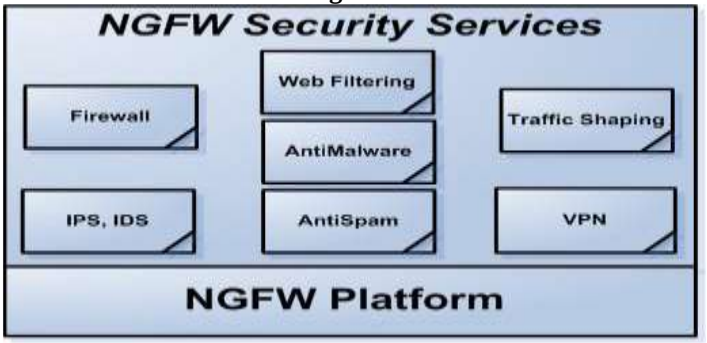
Firewall Type	Packet-Filter	Stateful Packet Inspection (SPI)	Application Proxy	Deep Packet Inspection (DPI)
OSI Layer	Transport Layer	Transport Layer	Application Layer	Application Layer
Generation	First Generation	Second Generation	Third Generation	Fourth Generation
Main Characteristics	Looks at destination and source addresses, ports, and services requested. Routers using ACLs dictate acceptable access to a network.	Looks at the state and context of packets. Keeps track of each conversation using a state table.	Acts as a middleman between communicating systems by breaking the session and reestablishing a new session to each system. Different proxy required for each service allowed. retains	Looks deep into packets 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.
Resource Requirement	Low	Low-Medium	High	Medium
Firewall Design	Initial Design	Design Considered Evolution of Packet-Filter Author	Alternative Design	Design Considered Evolution of Stateful Packet Inspection

VI. NGFW SECURITY SERVICES

A. Current NGFW Security Services

The different security services of the NGFW work together to provide a higher level of security than stateful packet inspection (SPI) firewalls, due to deep packet inspection (DPI) capability. The security services below are based on Fortinet technology but represent more or less the current state of next-generation firewalls.

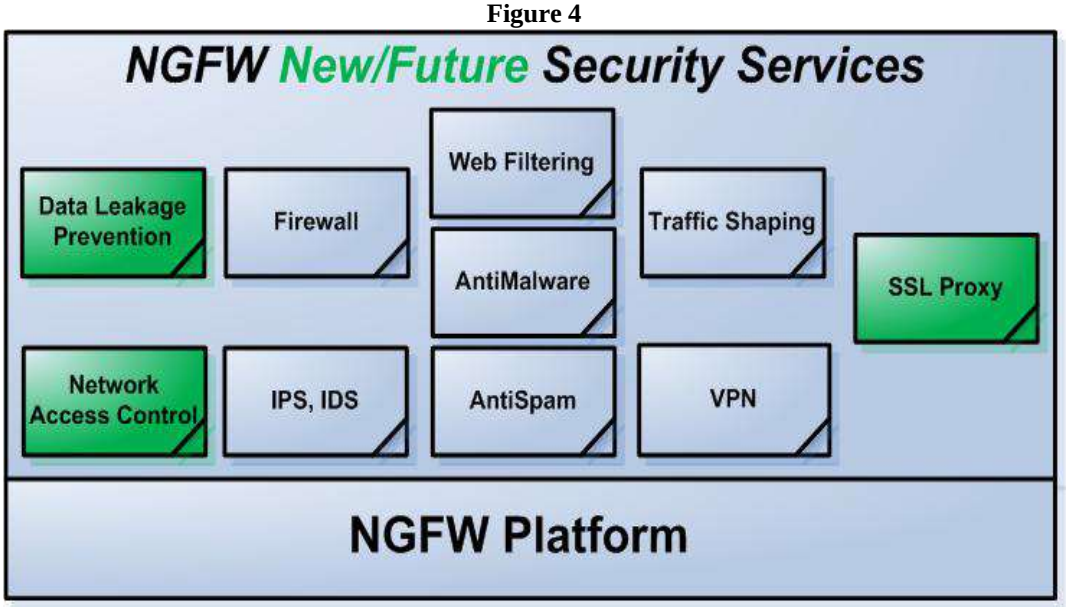
Figure 3



B. New & Future NGFW Security Services

To provide finer and more granular control on network traffic flow to cope with changing business requirements and blended threats, new security services are being integrated into NGFWs. Stateful firewalls focused on network ports and protocols, while NGFWs focus deeper on the applications and data. The new security services address current blind spots (caused by encryption), and allow decisions to be made based on content and context (Higgins, 2007); for example, decisions such as allowing credit card numbers and intellectual property to move only from one security zone to another, otherwise traffic is denied; or being able to detect and prevent SSL encrypted threats. The following represents a sample of new or future security services offered by NGFWs; Palo Alto Networks, a new vendor in that space supports a number of these services (Palo Alto Networks, 2008).

Figure 4



SSL Proxy: Manage encrypted threats by selectively terminating SSL connections, decrypting, analyzing traffic, and re-establishing encrypted connections transparently.

- Data Leakage Prevention (DLP): Control flow of intellectual property, credit card numbers and other sensitive information.
- Network Access Control (NAC): Integrate with Network Access Control (NAC) solutions in provisioning appropriate network access.

VII. Benefits And Drawbacks

Benefits-

- The tight coupling of the various security services in the NGFW, especially latency-sensitive services -IPS and Firewall- has the potential of providing basic level and tested integration between the various services. This introduces operational advantages over many point products offering the same security services. With the right integration, higher security effectiveness can be achieved. For instance, a web-filtering component detecting a compromised host connecting to a known malicious IP can quickly make the firewall component block communication, leading to better intrusion detection and response. Better intrusion detection and response is crucial when most compromises are within days, most discoveries of compromises take months, and 82% of compromised cases already had the data to prove compromise (Baker, Hylender, Valentine, 2008).

- Complexity in architecture and self-management of many point products works against security, when the needed high level security skills are not available.

- Integration of security services in one appliance can also provide economic advantages.

Drawbacks-

- On the other hand, best-of-breed point products are multi-vendor. The combination of multiple security services in one box has the tradeoff of missing out on best-of-breed products.
- Relying on one vendor for firewall, IPS, Web filtering, Antimalware, and other security services represents a single point of failure, especially if no high availability features are put in place.
- Performance can become an issue due to the high resources required to simultaneously fulfill the many security requirements of a large number of sites, users and connections.

VIII. USEFUL TIPS AND TECHNIQUES

Policy-based routing for web traffic inspection & caching

Policy-based routing provides the freedom to route packets based on the organization's needs, instead of routing packets based solely on their destination IP address and the local routing table. There are many benefits to policy-based routing; however this subsection addresses using policy-based routing to implement a transparent web proxy. The main benefit of this technique is leveraging a separate web security gateway appliance in a transparent manner; the policy based routing is configured to redirect HTTP, HTTPS and FTP traffic to the web security gateway, which listens for the traffic and acts as a transparent/implicit proxy. This would allow use of additional specialized network and security services not commonly present in NGFWs, such as web caching and HTTPS traffic inspection

Firewall Considerations & Firewall Policy Violations

It is included here to emphasize its importance in intrusion detection, especially outgoing firewall policy violations. For easier firewall audits, better performance, and proper firewall policy implementation, a few actions are suggested:

- Minimizing the number of firewall rules for easier firewall auditing.
- Ordering firewall rules to match specific cases before generic ones.
- Ordering firewall rules to match more frequent cases before less frequent ones.

Applying Basic Data Leakage Prevention (DLP) Controls

Basic data leakage prevention controls (DLP) can be configured on the NGFW. On a Fortinet NGFW, FTP uploads can be denied altogether or restricted based on the user by using the FTP_PUT service in a firewall rule. This would still allow FTP downloads but controls FTP uploads. By using a specially defined watermark in documents such as "Organization Confidential", the deep packet inspection engine can be configured to drop & log any connection with the watermark included in the network traffic.

IX. NEXT-GENERATION FIREWALL VS. TRADITIONAL FIREWALL

NGFWs include the typical functions of traditional firewalls such as packet filtering, network- and port-address translation (NAT), stateful inspection, and virtual private network (VPN) support. The goal of next-generation firewalls is to include more layers of the OSI model, improving filtering of network traffic that is dependent on the packet contents.
NGFWs perform deeper inspection compared to stateful inspection performed by the first- and second-generation firewalls. NGFWs use a more thorough inspection style, checking packet payloads and matching signatures for harmful activities such as exploitable attacks and malware

X. WHY FUTURE OF SECURITY WILL BE CONTEXT-BASED?

Context-based security systems are designed with built-in 'intelligence' to use situational information – identity, location, time, device, business function etc. – to make more effective security decisions. They are well suited to today's mobile and cloud-based environments as they can respond more intelligently and quickly to unexpected situations. By understanding the context of a user request, the security system or firewall can adjust the security response and control how information is delivered to the user, greatly simplifying an increasingly complex computing world

XI. UPCOMING FIREWALL AND ITS SERVICES

Cisco ASA Next-Generation Firewall Services are a modular security service that extends the Cisco ASA 5500-X Series Next-Generation Firewall platform. The solution blends a proven, stateful inspection firewall with next-generation capabilities and a host of additional network-based security controls for end-to-end network intelligence and streamlined security operations. Cisco ASA Next-Generation Firewall Services enable organizations to rapidly adapt to dynamic business needs while maintaining the highest levels of security. Cisco ASA Next-Generation Firewall Services deliver application and user ID awareness capabilities for enhanced visibility and control of network traffic. In addition, Cisco ASA Next-Generation Firewall Services enable administrators to control specific behaviours within allowed micro applications, restrict web and web application use based on the reputation of the site, proactively protect against Internet threats, and enforce differentiated policies based on the user, device, role, application type, and threat profile.

XII. CONCLUSION

Next-generation firewalls (NGFW), like almost any type of technology, are as useful as you make them. The more knowledge and effort put into understanding and deploying NGFWs, the more effective they are in mitigating risk and enforcing security policy. The information in this paper has demonstrated how NGFWs can be used in intrusion detection, analysis and response. Specifically, the paper demonstrated how NGFWs use deep packet inspection to manage application and data driven threats, the pros and cons of NGFWs, how they can be used to control both threats, how they can be leveraged in incident handling, and finally useful tips and techniques were demonstrated to make even better use of NGFW technology.

All this should help in making optimum use of Fortinet NGFWs, in addition to enabling the use of other vendors' NGFWs. In the end, NGFWs are only one of many security technologies forming a subset of an organization's ISMS (Information Security Management System). Technology, people and process should all work together to create a mature security posture for an organization. It will be interesting to see how next-generation firewalls will evolve, and what type of security services they will become capable of in the future.

XIII. GLOSSARY AND ABBREVIATION

HTTP (Hyper Text Transfer Protocol): Is a communications protocol used to transfer information (very often HTML) on the Internet or Intranet between a client making an HTTP request, and a server providing an HTTP response. HTTP is a protocol that resides in the application layer of both the ISO and TCP/IP network models; it commonly relies on the TCP protocol as the transport layer protocol.

IDS (Intrusion Detection System): Software employed to monitor and detect possible attacks and behaviors that vary from the normal and expected activity. The IDS can be network based, which monitors network traffic, or host based, which monitors activities of a specific system and protects system files and control mechanisms.

IPS (Intrusion Prevention System): Is a preventative and proactive technology that not only detects a malicious activity as an IDS does, but prevents the activity as well.

IP (Internet Protocol): The protocol that specifies the format of packets and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

SSL (Secure Socket Layer): A protocol developed by Netscape to transmit data in encrypted form, using a public/private key pair.

Virtual Private Network (VPN): A way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

REFERENCES

[1] https://www.sans.org/readingroom/whitepapers/firewalls/intrusion-detection-response-leveraging-generation firewall-technology-33053

[2] https://en.wikipedia.org/wiki/Next-Generation_Firewall

[3] Cisco Systems, (2002). Evolution of the Firewall Industry. Retrieved January 3,2009, from Cisco Documentation Web site: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm

[4] Intro to Next Generation Firewalls - By Eric Geier, 06 September, 2011

[5] *"Why the Future of Security will be Context-Based ?"*. *www.gajshield.com. Retrieved 2017-01-15.*