Next Generation Firewalls

Rob Cavana

East Carolina University

ICTN 4040 Enterprise Information Security

Dr Phil Lunsford and Mrs. Constance Boahn

April 13th 2015

Abstract

I will be reviewing Next Generation Firewalls. Next Generation Firewalls provide many advantages over their predecessors which I will cover in detail. We will cover the benefits of these advantages and why a company that is looking at adding a new firewall or replacing an existing firewall will want to consider making the investment in a Next Generation Firewall to take advantage of these benefits.

Next Generation Firewalls Reviewed

"One of the most important pieces in securing a network is the implementation of a firewall" Wilkins, S/Smith III, F (2011). In today's enterprise networks the majority of Network Engineers and holders of Network management positions are aware of this fact but there are still questions that remain. "Which firewall will provide me with the best protection? Where is the best place for the firewall or firewalls to be located in our topology? What features do we really need and which ones can we get by without? Which firewall that I buy today will provide me with the best investment protection for the long term?" Some of these questions are answered more easily than others but to move forward with the best decision it is best to understand what actually makes a Next Generation Firewall a Next Generation Firewall. Then the question becomes "Is a Next Generation Firewall what I need"?

Before you can solve the problem you first have to understand what is the problem or the question that we are trying to solve? Once that is established the next step is to define what the expectations for the solution are. To be more specific, what needs to be delivered for parts of the problem or the questions to be considered solved or answered?

So before our Network Engineer's and Network Managers can have all of their questions answered they first need to know what it will take answer the questions. This is something that a growing number of Information Technology professionals miss when they begin the process of replacing, upgrading or bringing in a new technology into the enterprise. This is due in part to Information Technology budgets are constantly be analyzed for ways to reduce spending which leads to a cheapest fit technology selection. "The key for IT administrators is to ensure that the NGFW solution they choose is absolutely scalable to their projected network performance

requirements, and delivers the most robust performance, most useful network analytics and insight, and ease of implementation and administration". Malecki,F. (2012)

Understanding which solution that best solves your problem by meeting your expectations is not likely to be the most inexpensive option, if you are trying to stop the latest Security threats.

Where are we today? First Generation Firewalls

A First Generation or Stateful Firewall is a device that is generally deployed as perimeter security device and with little or no integration with other enterprise security solutions is truly a standalone device. " Traditional stateful inspection firewalls have effectively become obsolete because of two significant limitations. First, they don't inspect the data payload of network packets. Second, while more and more network traffic uses Web protocols--including legitimate business applications, non-business applications, and attacks--traditional firewalls don't have the fine-grained intelligence to distinguish one kind of Web traffic from another and enforce business policies, so it's either all or nothing" Ohlhorst, F. J. (2013).

Another drawback is the administrative overhead tied to the static rule based approach. For every layer three address and layer 4 port required for an application to pass through the firewall a rule has to be built to permit this traffic. If you are using the firewall to perform NAT between your internal private IP address space and the public Internet IP space a rule must be built to perform that NAT translation. Next if the firewall is configured for AAA rules must be built to bypass authentication. Lastly is any sort of content filtering is in place the traffic must be redirected off the firewall, receive a pass/fail from the external filtering solution before finally being permitted to leave the firewall. All of these steps are required for one application and require the use of IP addresses not DNS host names. If the IP address changes either internally

or externally then all of these rules must be reconfigured to reflect the new IP address. In this type of scenario as the list of applications required to traverse the firewall grows the amount of staff/resource time to support them grows exponentially.

Where are we trying to go? Next Generation Firewalls

Gartner defines a Next Generation Firewall as "a deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall" "At minimum, Gartner states an NGFW should provide:" Ohlhorst, F. J. (2013).

Non-disruptive in-line bump-in-the-wire configuration

A bump-in-the-wire configuration is something may be easily overlooked but is necessary because the firewall should not become a bottleneck for traffic flows in the network. With all of the features or services that the Next Generation Firewall are providing it is paramount that they take place in real time thus the need for wire rate or near wire rate performance.

Standard first-generation firewall capabilities, e.g., network-address translation (NAT), stateful protocol inspection (SPI) and virtual private networking (VPN) and so on

It should go without saying that the goal of a Next Generation Firewall is to improve on the first generation firewalls and the all of the features that made first generation firewalls security device stalwarts must be present in the Next Generation Firewall. It should also be

noted that for an effective security posture it is still a best practice recommendation to have all of these features be present in addition to the new feature sets that are added.

Integrated signature-based IPS engine

The Next Generation Firewall has the signature-based IPS engine capability built in as a requirement where as some of the first generation firewalls had this capability as an add-on feature. By bringing the IPS directly onto the firewall Next Generation Firewalls are simplifying the traffic flow by having one less inline device or span port and they are reducing the need for standalone IPS sensors in the network.

Application awareness, full stack visibility and granular control

Application awareness, full stack visibility and granular control leverage the Next Generation Firewalls ability to perform deep packet inspection. “And then there is Deep Packet Inspection (DPI). DPI is a technology used to inspect the packets of information that travel across the Internet. A more extensive examination than a simple “Packet Inspection,” which looks only at the headers of each packet for information, DPI is increasingly used to examine the protocols and data within each packet” McClure, D. (2008).

As attacks become more complex the ability to inspect the entire packet to make sure that it is behaving in line with the protocol standard for the application running that protocol is a must have feature.

Capability to incorporate information from outside the firewall, e.g., directory-based policy, blacklists, white lists, etc.

The next Generation Firewall's ability to leverage directory-based policy, blacklists, white lists, etc. is an attempt to simply the administrative overhead challenges that are faced today when utilizing first generation firewalls. Applications that need to traverse the firewall can now be place into groups or lists based off of a configurable set of rules for the application by type. This allows the logic of the Next Generation Firewall to profile the traffic flow and not focus on the static rules and more to the behavior of the traffic flow.

Upgrade path to include future information feeds and security threats, and SSL decryption to enable identifying undesirable encrypted applications

Upgrade path, Information feeds and security threat and SSL decryption are all valuable with regards to investment protection in a Next Generation Firewall. **"**With the good guys and bad guys both using encryption, making malicious traffic visible through decryption—and inspecting it—becomes essential." Butler, M. (2013). If the firewall cannot decrypt the data to see the actual application that is running inside the traffic flow then it cannot protect against any attacks that originate from this type of traffic flow. "Now companies are accepting even more encrypted traffic as they shift toward greater use of cloud services." Butler, M. (2013). As this process becomes more wide spread the ability to decrypt the SSL session and still maintain a high level of throughput and performance will be a balancing act.

Performance Considerations

All of these features and requirements for Next Generation Firewalls are great additions to the security portfolio of any enterprise network looking to mitigate today's security threats but now the real question. Can it perform at an acceptable level for today's businesses? This question must be answered on a case by case basis and it will be different for each organization. Also as traffic patterns change and new applications are added the question needs to be asked what impact will it have to the firewall? What level of performance can you business operate with? These are questions that should not be taken lightly when making these decisions.

Detailed Reporting

One the most commonly over looked components of any solution not just first or Next Generation Firewalls is detailed reporting. C. Oxendine (personal communication, March 9, 2015) Supervisor of Network Security at FirstHealth of the Carolinas suggested that one of the most common requests from upper management is to provide a "human readable" report on user activity or incident investigation. This requires pulling information from firewall logs in addition to other sources. "Having a firewall that has canned reports that can be run and produce an easily readable PDF document is a must have feature for me and makes my job much easier. In performing a "bake off" between Source Fire and Palo Alto Networks we found the reporting on the Source Fire solution to be leaps and bounds above what the Palo Alto Networks box could do."

How much information should be logged? "If you can log all blocked and passed connections. A lot of times this is not feasible because of the large number of connections

passing through the firewall." Marty, R. (2009). With a large amount of traffic moving through the firewall and all of the features that are taking place this can be a lot of logging. A decision needs to be made up front as to the amount of log data that an organization wants to keep and if an external sys logging solution is the best fit.

Conclusion

In conclusion Next Generation Firewalls have proven themselves to be a key piece equipment for enterprise networks and should be considered a must have for today's enterprise businesses. However there are a lot of variables to consider before a decision should be made on which Next Generation Firewall should be implemented and which features should be deployed. Understanding the features and having a good understanding of how they will work in a given environment is key to a successful product selection and implementation.

References

Wilkins, S/Smith III, F (2011). *CCNP Security SECURE 642-637 Official Cert Guide*. Indianapolis, IN: Cisco Press.*

Ohlhorst, F. J. (2013). Next generation firewalls 101. *Network Computing - Online,* Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1313388589?accountid=10639*

Malecki, F. (2012). Next-generation firewalls, Volume 2012, Issue 12, December 2012, Pages 19-20, ISSN 1353-4858, Retrieved from http://www.sciencedirect.com/science/article/pii/S1353485812701149*

McClure, D. (2008). Deep packet inspection. *CPA Technology Advisor, 18*(7), 50. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/232917944?accountid=10639*

Butler, M. (2013). Finding Hidden Threats by Decrypting SSL, Retrieved from http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840

Marty, R. (2009). *Applied Security Visualization*. Boston, MA: Pearson Education, Inc.