Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 13 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices

By Steven Thomason
East Carolina University

Abstract - Standard firewalls alone can no longer protect the enterprise from Internet dangers; new technologies such as next generation firewalls and advanced packet inspection devices can improve security around your gateways.

GJCST-E Classification: C.2.0

Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices

Steven Thomason

Standard firewalls alone can no longer protect the enterprise from Internet dangers; new technologies such as next generation firewalls and advanced packet inspection devices can improve security around your gateways.

Why do we need to improve firewalls at the perimeter? In the beginning there was the Internet and it was only used by a limited number of people due to the cost and limited content. The general public was just not interested in what the Internet had to offer. If you wanted to connect to the Internet, you connected your computer to a modem and dialed into an Internet provider at speeds up to an average of 33600 bps, which is incredibly slow compared to today's access rates. Security was not much of an issue. Someone sitting on the other side of the world did not have much incentive to try and break into your system. Then came ISDN, frame relay, and T1 connections to the Internet and security issues started to appear. Content on the Internet grew at rapidly expanding rates. The most likely security issue was a user getting infected software that caused damage to their computer or company network. A typical method of blocking incoming or outgoing connections was to configure an access list on a router or on a basic firewall to block the IP address or IP port being used by that virus or Trojan.

As viruses and hackers became more motivated and more technical, a better method for protecting the company network was needed. Firewalls now were developed to actually inspect what was contained within each packet. The first firewalls only looked at the header information showing source, designation, and port for each packet. There was not much of a visibility into the actual packet. Now a days standard firewall shave the ability to look at specific strings within each packet. This ability now allows for signature or pattern based inspection at the network or session layer of the OSI model, but not at the application layer. Some of the more current models have advanced packet inspection abilities.

Blocking ports and IP addresses is no longer good enough. Operating systems contain security vulnerabilities and often as soon as they are discovered are exploited. The most common ports open on almost every firewall are the browsing ports 80 and 443, ftp, and frequently email smtp port 25. It is impossible to know about every possible new security hole or new virus that is written and released into the wild. According to 2008 report on the US-CERT[i] government website, over 200 new Trojans and viruses and an untold number of variants are released each month.

The Internet carries several types of traffic; the two most common are TCP and UDP. TCP traffic is connection oriented so the firewall knows when the connection has terminated. The sending and receiving of packets is acknowledged so the firewall can add timestamps and other methods to verify where the traffic is coming from. UPD traffic however is connectionless. It is up to the sending or receiving application to build up and take down the connection. If the application does not terminate the connection, then the firewall or security device has to have a timer to drop the connection when traffic has completed. This gap gives unauthorized traffic time to build a connection to your end point and have access through your gateway.

Now about one third of the people in the world have access to the Internet. Almost every company in business today needs to have access to the Internet. One third of every cell phone in the world has access to the Internet and that number is expected to grow to over 65% by 2015. Companies have confidential and proprietary data that criminals want. They want account information, names, passwords, anything that they can get that could possibility make them money. If they cannot get that information because it is well secured or there is nothing that they deem of value, then they want control of your computers to use them in attacks against other systems.

Up until now firewalls that performed stateful packet inspection were adequate to handle the traffic flowing into and out of the corporate network. That changed with the introduction of Web 2.0. Web 2.0 is more of a concept than an actual software product. Previously, applications were used or provided to access websites and their content. For example, if you wanted to "blog" on a certain website you installed their software on your computer and saved your data to the website for others to view.

Now with Web 2.0 multiple applications are run from the website itself and not on the client computer. According to Tim O'Reilly, Web 2.0[ii] now allows the web to be presented as a platform where services and not packaged applications are now the main focus. People now purchase and use a service instead of a single application. A typical site might create many different "applets" that allow different functions, such as video, data sharing, social media, and collaboration to take place within a single website. All of this can take place over http on port 80 and https on port 443. About two thirds of the traffic on the Internet is web traffic. While this allows for ease of access for the end user, it allows attackers the ability to "sneak" illicit programs and attacks through a standard stateful firewall. This ability to pass through the border defenses of the network can make it harder for intrusion detection systems to catch the intrusion. NSS Labs has stated that technical sophistication of the criminal element has grown at a rate faster than security companies' abilities to stay up-to-date. [iii]

Here is where the next generation firewalls come into play. They not only perform deep packet inspection but also can evaluate the data coming into the network at the application layer of the OSI model, Layer 7. Up until the introduction of next generation firewalls (NGFW), a fully protected network had an application or appliance firewall, an intrusion protection system, an intrusion prevention system, and probably a syslog server to gather logs from all of the different devices for analysis[iv]. At a basic level, what a NGFW does is to combine all three systems into a single device so that the data is checked on a single pass making it more efficient.

In 2010, only between 5 percent and 10 percent of the number of security devices deployed were next generation firewalls. According to Gartner by 2014 35 percent of installed firewalls will be next generation firewalls with 65 percent of new purchased being next generation firewalls.

What next generation firewalls bring to the table is the ability to look within the data streams passing through the firewall and determine whether or not the actual application or command is allowed or suspicious[v]. SQL queries are very common within websites. A NGFW should have the ability to scan your HTTP traffic, look for SQL commands and check to see that the format of the command is acceptable or possibility malicious. NGFW also should give you the ability to be more granular with your firewall rules. Many businesses today reluctantly need to grant access to social media sites such as Facebook. With a standard firewall you would either allow complete access to Facebook or completely block Facebook. A NGFW gives you the ability to allow or block based on user access credentials or group membership such as being able to allow only the marketing group to use Facebook. Restricting types of access to a website is also possible. Companies could allow all users access to Facebook pages but disallow Facebook games such as Farmville and Treasure Isle.

To be classified as a next generation firewall, the system needs to be able meet at a minimum 5 basic requirements[vi].

1. It needs to have the deep packet inspection ability that currently exists on today's firewall. Confirm that the NGFW scans all files for threats including encrypted files. Some systems may allow large files through to increase performance.
2. The system needs to have application intelligence. In other words, it has to have the ability to know what applications are traversing on http and https ports and what the applications are doing. Vendors must be able to provide updates, as new applications are available.
3. Since a NGFW has to be able to look deeper into what is happening, performance is an issue. The system has to be able to perform all of its functions at wire speed. An underpowered system will become a network bottleneck and/or miss anomalies that it is looking for. Due to the requirements of these systems, many vendors are creating specialized hardware devices to run their software. Processing much take place in real time.
4. A NGFW needs to have good reporting abilities that are easy to understand. If you don't have the ability to review what is actually happening with the system then you really don't know whether or not the system is performing as expected. You need to be able to see more that just the source and destination IP addresses and ports. If you cannot see what is happening, you cannot optimize it.
5. It needs to be manageable; most system failures are due to human errors and misconfiguration. Check the system to see if each instance is managed separately or if a number of NGFWs can be managed centrally. How intuitive is the interface?

Other criteria that define a NGFW are the ability to become very granular with rules and access. Controls need to be available for specific user access and specific application layer controls. Another attribute of an advance firewall system is the ability to learn new applications and dynamically have the ability to apply new application signatures to its rules. To use Facebook as an example again, when a new application becomes available on the website a new signature update would allow that application to be specifically allowed or disallowed based on the company policies. Another key feature of a NGFW is the ability to look within HTTPS SSL connections. Current firewall systems do not have the ability to look within encrypted sessions.

Currently Gartner's Magic Quadrant only has two players in its top right corner, Check Point Software Technologies and Palo Alto Networks[vii]. Some of the other major players are Barracuda Networks, Fortinet, Juniper Networks, Sonic WALL, Cisco Systems, and Stone soft.

Check Point Systems - http://www. checkpoint. com/products/appliances/index.html

"Today's enterprise security gateway needs to be more than just a firewall – it must use multiple technologies to secure and protect networks against evolving threats."

Palo Alto Networks - http://www.paloaltonetworks.com/

"Using a Palo Alto Networks next-generation firewall, your security team can strike an appropriate balance between blocking all personal-use applications and allowing them. Secure application enablement begins with first knowing exactly what applications are being used and by whom."

Barracuda Networks - https://www. Barracuda networks.com/

"Barracuda Networks offers the broadest range of advanced security solutions in the industry. Leveraging the benefits of hardware, cloud and virtual technology — backed by threat intelligence from Barracuda Central - our solutions consistently deliver zero-hour protection."

Cisco Systems – www.cisco.com

"The Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM) delivers industry-leading threat protection and content control at the Internet edge providing comprehensive antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering-all available in a comprehensive easy-to-manage solution delivered by industry leaders."

Fortinet - http://www.fortinet.com/

"Fortinet'sFortiGate consolidated security platforms provide you with the ability to protect your network with the fastest firewall technology on the market. You also have the freedom to deploy the widest range of security technologies available, to fit your dynamic network environment."

Juniper Networks - http://www.juniper.net/us/en/

"Juniper Networks Adaptive Threat Management Solutions adapt to changing network security threats and risks throughout the distributed enterprise. The result is a responsive and trusted security environment for high-performance networks."

Sonic WALL - http://www.sonicwall.com/

"Dell® Sonic WALL® Next-Generation Firewalls, deliver superior intrusion prevention, malware protection, application intelligence and control, real-time traffic visualization and inspection for SSLencrypted sessions at the gateway by tightly integrating a patented Reassembly-Free Deep Packet Inspection® engine with multi-core hardware."

Stonesoft - http://www.stonesoft.com/en/

"The Stonesoft Security Engine changes how network security is delivered. Unlike traditional security products, the Security Engine is one solution that delivers the adaptability, agility and scalability of a service."

Other companies have systems that they are calling NGFWs but don't meet the current definition of a next generation firewall[viii]. Some have all of the required components but are not integrated into a single pass device. For instance their current firewall may allow you to add an IDS/IPS module, avirus-scanning module, and an Internet proxy module. There is little difference in having multiple systems doing different functions from having one device with multiple modules other than maybe physical size and cost. A true NGFW is a single device that combines all of the required functions along with reporting into a single pass-through single scanning system.

Many enterprises have no idea what is traversing their firewalls and have just now started to implement IDS and IPS systems. Those that are aware of their shortcomings are reluctant to increase the complexity of the firewalls and the policies controlling them. For those not quite ready to do a rip and replace there are two options for introducing NGFWs. One method is to place the NGFW in front of the Internet and keep the existing firewall as a safeguard until comfortable with the new system. The other method is to place the NGFW behind the firewall and see what is actually getting through and into your network. However, according to Greg Young, a Gartner research VP, 95% of next generation purchases are for firewall replacements. Since many companies are replacing separate logging, IDS, IPS, and management systems with a single device, they are easily justifying the expense of an upgrade.

So what a NFGW gives you is the ability to look deeper into what is entering and leaving your network. It gives you the ability to have greater control over what access is granted to users within your network and to users coming to your websites. By being able to look at Layer 7 applications you also have a much greater chance of catching anomalies or attacks coming at your network and internal systems. Attacks are getting much more sophisticated and presenting a much more challenging job for network security. Next generation firewalls are the next step in the line of defense for corporate networks.

[i] United States Computer Emergency Readiness Team http://www.us-cert.gov/

[ii] WhatIs Web 2.0 September 2005 http://oreilly.com/web2/archive/what-is-web-20.htmlJune 9, 2012

[iii]Next-generation firewalls: In depth, Neil Roiter, October 17, 2011, http://www.csoonline.com/article/print/691651, July 1, 2012,

[iv]What is a next-generation firewall? Joel Snyder, August 22, 2011 http://www.networkworld.com/reviews/2011/082211-palo-alto-next-gen-test-249395.html July 22, 2012

[v] http://www.networkcomputing.com/security/232601723?pgno=3

[vi] How to Choose a Next-Generation Firewall, Patrick Sweeney, February 29, 2012. http://www.crn.com/blogs-op-ed/channel-voices/232301521/how-to-choose-a-next-generation-firewall. htm; jsessionid=2HIUeJMfJrxkHSSq-o9FnQ**.ecappj03July 1, 2012

[vii] RSA: Trio Of Next-Gen Firewalls Try To Keep Up With Evolving Threats, Robert Mullins, February 2012, http://www.network computing.com/security/232601723?pgno=2 May 24, 2012

[viii] Choosing a next-generation firewall: Vendor comparison. March 2011 http://searchnetworking. techtarget.com/feature/Choosing-a-next-generati- on-firewall-Vendor-comparison June 9, 2012.

Next-Generation Firewalls will include Intrusion Prevention http://www.gartner.com/research/spotlight/asset_91268_895.jsp

The Cisco ASA 5500 as a Superior Firewall Solution http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white_paper0900aecd8058ec85.html

Next Generation Firewall http://www.nsslabs.com/research/network-security/firewall-ngfw/

The Network Security Sonic OS Platform Next-Generation Firewalls http://www.sonicwall.com/us/products/Next-Generation_Firewall.html