**Security Technology Tools**

**Firewalls: A Comparison**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**SLP 02**

INTRODUCTION

In today’s rapidly growing technology market, information security is a growing concern. To fully protect a user’s machine it should be equipped with, a firewall, antivirus software, and an antimalware application. This discussion defines what software and hardware firewalls are and gives a comparison of the two.

Software firewalls are firewalls that monitor the integrity of flowing traffic processes through variables such as, incoming and destination IP addresses, transfer times, download sizes, and killing connections that don’t meet expectations. They monitor outgoing and incoming traffic; thus, blocking programs like IP spoofing from attacking individual machines once inside a network (Sebastian, 2015).

Layer seven of the Open System Interconnection (OSI) model is the application layer. Application/proxy firewalls operate at this level and the device the firewall is installed on acts on behalf of the client (proxy) for requested services (Dowler, 2007).

Windows is a graphical operating system that is, developed, marketed, and sold by Microsoft. In August of 2004, Microsoft’s service pack 2 for Windows XP, a new update at the time, included improved protections. This improved protection came with pop-up-ad blockers for Internet Explorer and Windows Security Center which is a centralized console for all the user’s security software settings.

What Microsoft considered a crucial element of this improved protection was its improved firewall. The Windows Firewall has been proven to control the incoming network traffic from the internet, but it does not check the outgoing traffic or prevent personal data or any other information from leaving the user’s machine (Biersdorfer, 2004).

Linux is an open-source product that puts the controls in the user’s hands. Linux Firewalls are built into the Linux kernel and provide, strong filtering, Network Address Translation (NAT), state tracking, and application layer inspection capabilities. But Linux is not popular because, it’s not as user friendly as commercial tools like Microsoft Windows or Apple’s Mac OS (Macintosh Operating System) (Rash, 2007).

OS X is Apple’s operating system for their Macintosh computers. All versions of OS X come equipped with *ipfw*, a packet-filtering firewall that is Unix-based. Additionally, OS X is equipped with a socket-filtering firewall, otherwise known as an application firewall. The combination of these two firewalls protect the user against inbound traffic, and simultaneously restricts outbound traffic by ports and IP addresses (Pepper et al., 2015).

Web Application Firewalls (WAF) are another form of a software firewall, but it can be network based or host-based. These type of firewalls protect a web application by “controlling its input and output and the access to and from the application” (Rouse et al., 2015). WAFs run as either an appliance or a server plug-in or a cloud-based service and inspects data packets; for example, HTML, HTTPS, SOAP, and ML-RPC data packets. Fully customizable WAFs are able to prevent damages from cyber-attacks like, XSS, SQL injection, session hijacking, and buffer overflows.

Hardware firewalls are firewalls that are automatically built into a device. A router, for example, will tag all outgoing traffic with a specific network ID that is also attached to any corresponding incoming traffic. This allows the router to determine the origin of the incoming packets and blocking any transfers that weren’t initiated from behind the firewall. It also prevents files from being downloaded without the user’s knowledge and stops first step intrusions known as port scan attacks. This gives the user confidence that updates are truly updates and not spyware (Sebastian, 2015).

Layer five of the OSI model is the session layer and circuit-level gateways operate at this level. These gateways are considered host based and reside on individual clients and servers inside the network (Stevens, 2011).

Layer two of the OSI model is the data link layer. This is the layer where data packets are encoded and decoded into bits. Media access control (MAC) firewalls operate at this level and they control how a computer gains access to data and discerns whether or not that computer can transmit the data or not (Sutton, 2013).

Routers are among the most common devices that have firewalls automatically built into them. There are different classifications of routers; for example 802.11g, 802.11n, and 802.11ac.

The 802.11g wireless router offers faster file sharing than its 802.11b predecessor. It operates with the same 2.4 GHz band with speeds increased from 11Mbps up to 54Mbps – depending on the device. Adding multiple computers without bogging down the network was also another significant improvement. (Mitchell, 2015).

The 802.11n wireless routers simultaneously broadcast Wi-Fi signals on both 5 GHz and 2.4 GHz frequency bands. The two main configurations for these routers is, dual-stream (cap speed of 600Mbps) and three-stream (cap speed of 900Mbps). These routers are ideal for sharing internet and casual home networking (Ngo, 2015).

The 802.11ac wireless routers are a recent improvement on the 802.11 architecture. These routers operate at cap speeds of up to 1.3 Gbps, use only the 5 Hz channel, and utilize beamforming. Beamforming is a way for the transmitting device to identify its intended receiver(s) and amplify the signal in that particular direction. It allows for a greater quality of coverage to that/those device(s) rather than the general radiation that the standard omnidirectional transmission delivers (Kelly, 2015).

Virtual Private Networks (VPN) encrypt the data that you send and receive over the internet. Since the data is sent in a private tunnel via the public internet, there is no need for costly devices and additional networks to be established. This is a form of information security and helps with things like keeping passwords and other personal information safe. While the VPN does block some intruders, it does not fully protect the user. Additional steps would need to be taken to be fully protected from viruses and other dangerous software the user may inadvertently download (Biersdorfer, 2014).

There are two different ways to connect to a VPN, remote-access VPN and site-to-site VPN. Remote-access VPNs use the internet to provide remote users with secure access to their organization’s network. The site-to-site VPNs use a gateway device to connect one entire network in a given location to another network at a different location. Rather than utilizing the public internet, site-to-site VPNs use Multiprotocol Label Switching (MPLS) – a mechanism that directs data from one network to the next. Examples of site-to-site VPNs are, an intranet (password-protected site for company employees) based VPN connects LAN to LAN and extranet-based VPN connects LAN to LAN between multiple companies.

There are three different types of VPNs; they are, secure, trusted, and hybrid. Secure VPNs encrypt and decrypt data that is to be transferred over the internet, known as tunneling. In addition, mobile employees are empowered with the ability to connect to their respective VPN servers by using VPN client software installed on their machines/devices that use the internet to complete the connection. Trusted VPNs are a legacy VPN technology or schema where Internet Service Providers (ISPs) assured their customers that they would have a dedicated line and private IP addresses. With time, trusted VPNs proved to be, costly, unrealistic, unsecure, and ultimately untrusted. (McCoy, 2014).

CONCLUSION

This discussion defined what software and hardware firewalls are. To take advantage of the highest levels of security, it is clear that not one particular firewall is going to be able to provide a significant level of security to protect sensitive data. For the highest levels of protection, use a hybrid firewall solution with hybrid VPNs. For simple home or personal use, use a router and a firewall on your PC.

REFERENCES

Biersdorfer, J. (2004, August 18). Firewall Protection Without the Conflicts. Retrieved November 23, 2015, from [http://www.nytimes.com/2004/08/19/technology/q-a-firewall-protection-without- the-conflicts.html?\_r=0](http://www.nytimes.com/2004/08/19/technology/q-a-firewall-protection-without-%09the-conflicts.html?_r=0)

Biersdorfer, J. (2014, November 20). How to Use a VPN. Retrieved November 24, 2015, from <http://www.nytimes.com/2014/11/21/technology/personaltech/using-a-vpn.html>

Boran, S. (2002, October 16). The IT Security Cookbook - Firewalls: Securing external Network connections. Retrieved November 20, 2015, from [http://www.windowsecurity.com/whitepapers/misc/The\_IT\_Security\_Cookbook/The\_IT\_Securit y\_Cookbook\_\_Firewalls\_Securing\_external\_Network\_connections.html](http://www.windowsecurity.com/whitepapers/misc/The_IT_Security_Cookbook/The_IT_Securit%09y_Cookbook__Firewalls_Securing_external_Network_connections.html)

Dynamic NAT. (2015). Retrieved November 20, 2015, from <http://www.webopedia.com/TERM/D/dynamic_NAT.html>

Dual-homed host. (2015). Retrieved November 20, 2015, from <http://www.webopedia.com/TERM/D/dual_homed_host.html>

Kelly, G. (2015, May 11). 802.11ac vs 802.11n - What's the difference between the Wi-Fi standards? Retrieved November 23, 2015, from [http://www.trustedreviews.com/opinions/802-11ac-vs- 802-11n-what-s-the-difference](http://www.trustedreviews.com/opinions/802-11ac-vs-%09802-11n-what-s-the-difference)

McCoy, S. (2014). Learn About Secure VPNs. Retrieved November 24, 2015, from <https://www.juniper.net/techpubs/en_US/learn-about/secure-vpns.pdf>

Mitchell, B. (2015). Best 802.11g Wireless Routers for Home Use. Retrieved November 23, 2015, from http://compnetworking.about.com/od/wirelessrouters80211g/tp/80211ghome.htm

Ngo, D. (2015, November 3). Best 802.11n routers of 2015 - CNET. Retrieved November 23, 2015, from http://www.cnet.com/topics/networking/best-networking-devices/802-11n/

Pepper, C., & Mogull, R. (2015). Mac Security: Firewalls. Retrieved November 23, 2015, from <http://www.macworld.com/article/1135888/firewalls.html>

Rash, M. (2007). Linux firewalls attack detection and response with iptables, psad, and fwsnort. San Francisco: No Starch Press.

Rouse, M., & Bacon, M. (2015). What is Web application firewall (WAF)? - Definition from WhatIs.com. Retrieved November 23, 2015, from [http://searchsecurity.techtarget.com/definition/Web- application-firewall-WAF](http://searchsecurity.techtarget.com/definition/Web-%09application-firewall-WAF)

Sebastian, L. (2015, April 3). Firewalls as Fast As Possible. Retrieved November 20, 2015, from <https://www.youtube.com/watch?v=N2sOPGhva1M>

Stevens, J. (2011, August 10). The Session Layer: Understanding layer 5 of the OSI Model. Retrieved November 16, 2015, from <http://www.computerworld.com/article/2470634/network-hardware-solutions/the-> session-layer--understanding-layer-5-of-the-osi-model.html

Sutton, C. (2013, September 11). Is the Extra Layer Better? Layer 2 Versus Layer 3 Networking. Retrieved November 16, 2015, from <http://smallbiztrends.com/2013/09/osi-model-layer-> networking.html

Wack, J. (1995, February 3). Screened Host Firewall. Retrieved November 20, 2015, from <http://www.vtcif.telstra.com.au/pub/docs/security/800-10/node57.html>

Wack, J. (1995, February 3). Screened Subnet Firewall. Retrieved November 20, 2015, from <http://www.vtcif.telstra.com.au/pub/docs/security/800-10/node58.html>