**Security Technology Tools**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**Case 02**

INTRODUCTION

As the amount of data in the world increases, threats to the security of that data become more prevalent. To ensure the integrity of information systems security it is crucial to install effective firewalls to protect clients and hosts against cybercrime. This discussion explores five different types of firewalls based on their processing modes.

PACKET FILTERING

Packet filtering firewalls are among the most basic of firewalls and typically a first step in taking measures to protect users within the firewall from information security threats, attacks. These firewalls only allow packets of data, which are traveling through the internet, to pass through a network interface provided they meet the firewall policy. The most commonly used criteria are, source and destination address, source and destination port, and protocol. There are two types of packet filtering firewalls, stateless and stateful filtering (Sharma, 2010).

Stateless filtering is a type of filtering where the firewall does not retain the information of the previously passed packets of data. Each packet is examined individually and the decision to allow it to pass or deny access is performed on a case by case basis (Sharma, 2010).

Stateful filtering is a type of filtering where the firewall retains the information of the previously passed packets of data. This type of filtering is also known as, Dynamic packet filtering or smart firewalls (Sharma, 2010).

A packet filtering router has several advantages. An entire network can be protected by a single, strategically placed packet filter router. If there are no other routers connected to the network, the network security can be significantly enhanced by doing packet filtering on this individual router. Simplicity of use and ease of access are other advantages packet filtering provides; for example, packet filtering doesn’t require user knowledge or cooperation and it’s widely available on many routers (Chapman et al., 1995).

CIRCUIT GATEWAYS

Layer five of the OSI (Open System Interconnection) 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).

When a client makes or sends a request to a host machine to retrieve a website its request goes through the circuit-level gateway. The gateway then records the IP address and the port information. When the host machine receives the request it sends back the appropriate webpage to the gateway. The gateway then compares the packet’s contents for a match with the IP address and port information. Lastly, the gateway makes the decision to allow the information to be passed back to the client or to be discarded (Riley et al., 2002).

A major advantage of circuit-level gateways is that they keep the client machine private while the gateway is what represents the client to host machines; therefore, anytime the client sends a web request it remains ambiguous to the host machines. As far as the host machines are aware, the request came from the gateway.

APPLICATION GATEWAYS (PROXY SERVERS)

Layer seven of the OSI model is the application layer. Application/proxy firewalls operate at this level and the device(s) the firewall is installed on act on behalf of the client (*proxy*) for requested services.

The proxy server receives the particular request from the client and then connects to the host machine for that site, which thinks the request came from the proxy server, and retrieves the data sending it back to the proxy server. The proxy server then examines the address and port information to ensure the validity of the transaction. Additionally, it runs proxy applications to view common types of data (like HTTP for web-pages, FTP, SMTP or POP3for email, etc.) before it is allowed through the firewall” (Dowler, 2007).

There are several advantages of having an application firewall. Because application/proxy firewalls act as an intermediary between the internet and the client, they provide an additional layer of protection against cybercrimes like port scans and application attacks. Additionally, ports can be patched quickly in the event a security breach is discovered (Blair et al., 2009).

MAC LAYER FIREWALLS

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).

MAC layer firewalls, also known as MAC Filtering, is another type of security access control methodology. In this methodology, the 48-bit address that is assigned to each network card is used to determine access to the network (Gite, 2009).

Each device comes with a unique MAC address that identifies it on a network. The default for a router is to allow any device to connect to it, provided the appropriate pass-phrase is submitted to it. Routers can be programmed to only allow MAC addresses that are recognized via logging those MAC addresses, typically, via a web-based graphical user interface for the router. In this case, the router will only allow access to a device if it has been specifically approved. This method is a weak standalone measure of security because, of the relative ease for hackers to find a device’s MAC address and use it (Hoffman, 2014).

HYBRID FIREWALL

A Hybrid firewall, as its name implies, is a firewall that is comprised of multiple security access control methodologies. A firewall may be designed with packet-filtering and proxy servers or circuit-level gateways coupled with proxy servers or any other combination of firewalls (Khodenko, 2003).

CONCLUSION

This discussion explored five different types of firewalls based on their processing modes. If you only have a laptop at home, as I do, then, you will only need a single router to connect to the internet and PC firewalls will, typically, suffice for the needs of information security. If you work in a small business then, Small Office/Home Office (SOHO) firewalls will offer you sophisticated security levels with simple configuration requirements. If you work in a large company then, they typically offer large enterprise type firewalls that offer, centralized administration, multi-firewall administration, and support for, Internet, Intranet, and Extranet, services.

REFERENCES

Blair, R., & Durai, A. (2009, May 21). Chapter 1: Types of Firewalls. Retrieved November 11, 2015, from [http://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of- firewalls.html](http://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-%09firewalls.html)

Chapman, B., & Zwicky, E. (1995). [Chapter 6] Packet Filtering. Retrieved November 11, 2015, from <http://www.diablotin.com/librairie/networking/firewall/ch06_01.htm>

Circuit level gateway. (2013). Retrieved November 12, 2015, from http://www.thenetworkencyclopedia.com/entry/circuit-level-gateway/

Dowler, M. (2007). Beginners Guides: Firewalls and Internet Security. Retrieved November 12, 2015, from <http://www.pcstats.com/articleview.cfm?articleid=1450&page=5>

Gite, V. (2009, February 18). Security Through Obscurity: MAC Address Filtering ( Layer 2 Filtering ). Retrieved November 16, 2015, from <http://www.cyberciti.biz/tips/linux-unix-> bsd-mac-filtering.html

Hoffman, C. (2014, December 9). Why You Shouldn't Use MAC Address Filtering On Your Wi- Fi Router. Retrieved November 16, 2015, from <http://www.howtogeek.com/204458/why-> you-shouldn’t-use-mac-address-filtering-on-your-wi-fi-router/

Khodenko, A. (2003, May 1). Firewalls. Retrieved November 16, 2015, from <http://khodenko.tripod.com/Firewalls/>

Mehdi, S. (2012, November 23). Firewall. Retrieved November 16, 2015, from http://www.slideshare.net/jojonaqvi/firewall-15317689

proxy firewall. (n.d.). Retrieved November 10th, 2015, from <http://www.yourdictionary.com/proxy-firewall>

Riley, R., & Hoekstra, T. (2002, January 24). Patent US20020010800 - Network access control system and method. Retrieved November 16, 2015, from https://www.google.com/patents/US20020010800

Seemab, K. (2003, July 10). Patent US20030131258 - Peer-to-peer communication across firewall using internal contact point. Retrieved November 12, 2015, from <https://www.google.com/patents/US20030131258>

Sharma, G. (2010, June 27). Packet Filtering Firewall: An Introduction. Retrieved November 9, 2015, from [http://securityworld.worldiswelcome.com/packet-filtering-firewall-an- introduction](http://securityworld.worldiswelcome.com/packet-filtering-firewall-an-%09introduction)

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