James Driscoll

ECPI University

CIS 425: Advanced Defense and Countermeasures

Professor Johnson

25 March 2022

In the realm of network security devices there are numerous options available for any size business. The most common security appliance is a firewall. Now, there are five types of firewalls. 1) Packet filtering firewalls. 2) Circuit-level gateways. 3) Application-level gateways. 4) Stateful inspection firewall. 5) Next-Generation firewall (NGFW) (DeCarlo & Ferrell, n.d.). Threat actors are always evolving and changing how they operate. So, businesses, to keep pace with them, need to also evolve their cyber security and change how they operate to keep them from infiltrating the network and stealing information. Our company is going to go with an NGFW. With an NGFW we will get the ability for deeper packet inspection, attack and malware identification and the ability to block those threats. While researching the plethora of these firewalls, the following items were considered: the price, scalability, and features available so the company gets a good Return on Investment (ROI).So, after careful consideration the recommendation is to go with the Check Point 1550 Next Generation Appliance.

**Specifications**

The Check Point 1550 Next Generation Appliance have a lot of features that are beneficial to our company. These features include: a next generation firewall, site-to-site VPN, remote access VPN, application control and web filtering, IoT device recognition, intrusion prevention, anti-virus, anti-bot, anti-spam, and sandboxing (1500 Security Gateways, n.d.). So, with a price of $789.17 that includes a one-year subscription package (Check Point 1550 Next Generation Appliance, n.d.), this NGFW will have a positive ROI.

Let’s look at some of the some of the features that are not publicized too much when it comes to NGFW’s that the 1500 has. The setup and configuration are simplified with this device. It has pre-loaded policies that can be utilized or there is a setup wizard that will take the administrator step-by-step through the process (1500 Security Gateways, n.d.).

This device is capable of handling 3/4G/LTE. Of course, the 3G is not really a big deal since the major carriers are shutting down those networks. It also supports both types of SIMs: nano and micro. It can also be used anywhere on the planet as there is global coverage (1500 Security Gateways, n.d.)

Another feature is that it facilitates a zero-trust deployment and cloud management. This is beneficial because that means that this device can be not only configured but also managed by a Managed Service Provider (MSP). Plus, it has a portal that allows for cloud hosting that is capable of handling 10,000 Check Point Small Business Appliances (1500 Security Gateways, n.d.).

Reporting is simplified with the Check Point 1500 series Security Gateway. It has a web interface that not only displays the logs, but also which devices are active; along with hourly, daily, weekly, and monthly reports. It is also capable of analyzing the network and can display the applications and users and how much bandwidth they are using. This is useful when there is a lot of lags due to network congestion. Administrators can also view which users are going to suspicious websites and using suspicious applications. Finally, if there were incidents or infected hosts found during a reporting period, they can also be viewed (1500 Security Gateways, n.d.).

The 1500 series also provides a mobile application for both iOS and Android. This application has the same functionality as the software that is installed on a computer such as being able to view the logs and what devices are connected. It also provides alerts in real-time. It facilitates threat mitigation. The application is also capable of managing multiple devices (1500 Security Gateways, n.d.).

**Pros and Cons**

**Pros**

The Check Point 1500 series Security Gateways has numerous advantages for our company. 1) As with all firewalls, it protects the internal network from the outside network. 2) Facilitates investigation of suspicious files via sandboxing. 3) Accomplishes application and URL filtering. 4) There is a user-friendly GUI. 5) Logs are easily read and contain all information about the packet. 6) Comes with detailed pre-configured reports which adds to the simplification of use (Check Point Quantum Security Gateway, n.d.).

**Cons**

Anything that has pros is also going to have cons, the 1500 series is no different. Some of those cons include: 1) Blocking of malicious domains needs to be constantly tuned. 2) While setup and management are simple, the licensing is somewhat difficult. 3) Since it has pre-configured reports, there is limited functionality in creating custom reports. 4) Training can be an issue as some of the tools are complex and there can be a steep learning curve. This means learning can take longer than some competitors devices. 5) The ability to optimize log file size is somewhat difficult (Check Point Quantum Security Gateway, n.d.).

**Conclusion**

The Check Point 1550 Security Device has the all the tools needed for out business to not only detect, but also stop security threats from occurring and to remediate any threats that mange to bypass it. It facilitates cloud management by an MSP. If the company starts growing faster than we can hire information technology personnel, we can transfer management over to an MSP and it can be handled via the cloud. Plus, if the company does grow, this device will not have to be upgraded for a long time as it is capable of handling 500,000 concurrent connections (1500 Security Gateways, n.d.). One issue is the Bring Your Own Device (BYOD). Employees want to be able to use their smart phones, tablets, laptop computers while at work. Now, while this is a policy issue that needs to be determined, the 1550 is capable of handling that traffic as it supports 3G/4G/LTE cell networks. It is also capable of creating a Wi-Fi network.

So, the question could be asked if a “free” or “low-cost” firewall could do the job versus having to pay for one. The answer to that is yes and no. The thing to remember about anything that is “free” or “low-cost” is that it is going to be a striped down version with only the very basic functionality. This would be optimal for a very simple network such as a home network. A “free” or “low-cost” firewall is going to leave too many holes open in a business network so those are not going to be a viable option for us.

All Check Point Security Devices come with a one-year SandBlast subscription. This subscription includes obviously the device, but also premium support which included 24 x7 support, and software upgrades. Also included is a device health monitoring service, the firewall, VPN, application control, Intrusion Prevention System (IPS), anti-virus, anti-bot, and threat emulation (sandboxing) (1500 Security Gateways, n.d.).

# References

*1500 Security Gateways*. (n.d.). Retrieved from Check Firewalls: https://www.checkfirewalls.com/datasheets/1500-security-gateway-datasheet.pdf

*Check Point 1550 Next Generation Appliance*. (n.d.). Retrieved from Check Firewalls: https://www.checkfirewalls.com/1550.asp

DeCarlo, A. L., & Ferrell, R. G. (n.d.). *The 5 Different Types of Firewalls Explained*. Retrieved from Tech Target: https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls