How to Effectively Use Firewalls to Protect You

Brittany Baisley, Carina E. Martinez-Lopez, Randall Seymore, Robert Martinez, Zoe Medina

Professor Steven Templeton

CYBR 508 – Secure Network Engineering

Shiley-Marcos School of Engineering (SMSE)

University of San Diego

ABSTRACT:

What if you could have a personal security guard for your computer? Firewalls monitor network traffic to prevent unauthorized access to the computer network. Firewalls can be viewed as gate guards for your computer. They stop and check all incoming traffic to ensure it is not hostile to your device or will compromise your personal information. Firewalls play a pivotal role in network security and without them, there would be no way of identifying malicious traffic attempting to enter your computer and modify, steal, or sell your data. Here at Eternal Guard, we will help you protect your network by ensuring you are using the optimal firewall solution that suits your needs. Below we will discuss a few solutions to consider and why they are beneficial.

BACKGROUND:

A firewall-only solution is precisely what it sounds like, only using a firewall and no additional protection against harmful traffic trying to solicit your data. A firewall-only solution is not the most effective manner to provide the best level of security, because it does not provide defense in depth. Just as humans commit mistakes, technology can as well. Using one single firewall can be a risk because if one error or malfunction occurs there is no longer a line of detection. Having multiple firewalls or using a solution is prime in ensuring your data is secure. Firewalls can be deployed as hardware, software, and cloud-based. Using multiple firewalls and deploying them in different manners can provide defense in depth. In addition, there are a variety of tools that can be used alongside firewalls to enhance their overall performance and reliability. We will discuss three different solutions and why they each can be beneficial to you.

FIRST SOLUTION - SNORT:

Snort is a widely used network-based intrusion detection and prevention system. This system operates by analyzing network packets in real time and comparing their contents to a database of known attack signatures (Garg and Maheshwari, 2016). Snort refers to these signatures as rules. While the application is a free open-source system, they do offer paid subscriptions. With a paid subscription the end user will get updates to the rule packages at least twice weekly, whereas the free version has rules package updates approximately every 30 days. Snort offers three primary configurations that can be deployed for either personal use or for business use. These three modes that Snort can be configured in include a packet sniffing mode, a packet logger mode, and a network intrusion prevention system (*Products,* n.d.).

Packet Sniffing Mode: As mentioned above, one of the three primary ways that Snort can be used is as a packet sniffer. In this mode network traffic can be recorded, monitored, and analyzed by inspecting data packet transfers across the network. The system will take the raw data contained in each packet and display it in an easy-to-read breakdown of the packet's contents. This type of analysis can be beneficial in troubleshooting the network data flow, as well as aid in cybersecurity efforts in detecting malicious activity.

Packet Logging Mode: Packet logging, another one of the previously mentioned configurations of Snort, is great for monitoring network traffic. The packet logging mode differs from the packet sniffing mode by simply not analyzing the packets. The logger mode records the packet transfers across the network but does not go into the details of the data that the packet sniffing mode does. Packet logging can be a quick way to ensure that firewalls are properly configured and blocking traffic as intended by the set rules.

Intrusion Prevention Mode: The intrusion prevention mode is arguably one of the most powerful features of Snort. As described earlier in this paper, IPS takes network traffic security to a much higher level. In this mode, Snort will not only monitor the traffic but will block and prevent any anomalous activity as defined by the systems rule packages.

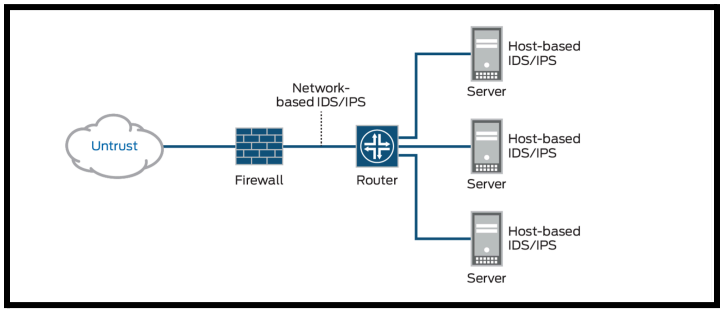
WHY SNORT IS GOOD FOR SMALL COMPANIES:

Snort is a great option for small companies because it is affordable, can be deployed with ease, and offers several features all in one user-friendly package. Affordability is a factor that typically comes into play for small companies when it comes to selecting cybersecurity tools. Many of these small operations simply cannot afford some of the top-shelf security software on the market. By choosing to go with Snort, companies can have features and qualities that are found in some of the more costly solutions, at little or no cost. Along with the low product cost, companies can also save time and resources due to the easy deployment of Snort. System administrators will not be burdened with difficult configuration or complex deployment of the software. Lastly, the features offered are quite impressive and give the company several tools built into one package that is easy to maintain and operate. There is no question that Snort should be a consideration for small companies when seeking out quality, affordable security solutions.

INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM:

Another alternate solution to pair with Snort would be to implement an intrusion detection system (IDS) and intrusion prevention system (IPS) into the business network. The intrusion detection system will identify any threats in the network by raising alerts in the system and notifying the appropriate personnel. The intrusion prevention system will monitor the network to prevent any incidents from occurring. While IDS is more passive by monitoring and

notifying, IPS is more active by actively preventing malicious activity from attacking the network. There are various benefits the IDS and IPS provide that improve security for the client's network. Both intrusion systems will be able to "lower the risk of successful attacks" (Rapid7, 2017). When malicious activity is logged by IDS, the IPS will use its tools to stop the attack from occurring. Both intrusion systems will also "reduce business risks and additional security" (Rapid7, 2017). This is due to signature-based detection, which compares signatures against observed events to identify possible incidents, and anomaly-based detection determines what is considered a normal not uncommon, activity in the network depending on the business requirements. If there is any abnormal activity, the network will block it.



Source: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

To enhance the firewall, the intrusion detection system (IDS) and intrusion prevention system (IPS) will work in parallel with the firewall by acting on the traffic after it has been filtered. This means that once the allowed traffic is inside the network, each packet will be analyzed and monitored to ensure that network security is protected. This is also essential to the security infrastructure. without IDS and IPS implementation, the business network will be vulnerable. Hence, having this is a requirement for a successful network.

SECOND SOLUTION - Software Defined - Wide Area Network (SD-WAN):

A SD-WAN is a software-defined wide area network that uses software to manage network traffic and connectivity. It is typically responsible for finding the best route in real time

for traffic and passing the packets along. In this way, it can enhance the performance of the network to improve business productivity and communication. However, an SD-WAN also includes the capabilities of a firewall, router, and other WAN optimization devices, making it versatile, secure, and easy to configure.

A secure SD-WAN provides multiple defensive methods for protecting a network. This includes deep-packet inspection, access controls, event logging, IDS/IPS capabilities, and DDoS protections. Previously, IT personnel would be responsible for multiple devices to perform each of the defensive methods for a defense depth setup. This would lead to equipment sprawl, making it difficult to keep track of all security assets and potential vulnerabilities. The vast amount of diverse equipment would cost the company a great amount of time and money to implement and maintain. By implementing a secure SD-WAN into the network, IT personnel can consolidate a variety of security network functions into a single appliance. This makes it much easier to maintain the defensive methods by creating a centralized interface for managing configurations. This also provides a company with the flexibility to open remote offices and push configurations without needing the equipment on-site, also known as zero-touch provisioning.

Zero-touch provisioning also reduces the need for specialized IT personnel on-site since all security configurations and changes can be done remotely. Centralizing all configurations for security devices ensures that all devices follow the same security policies. Typically, IT personnel would have to manually configure each branch firewall with the same rules to support company security policies, increasing the chances for a misconfiguration to occur and potentially decreasing security. This would also result in the slow and inefficient process of adding or removing policies from each of the firewalls in the case of a change in security policy. Through

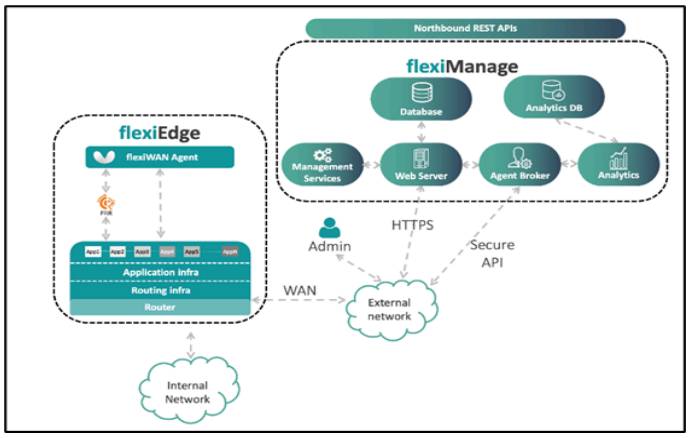
zero-touch provisioning, security configurations can be made and pushed to other firewalls within minutes, keeping them up-to-date against known issues and vulnerabilities quickly.

The implementation of a secure SD-WAN creates a lean network architecture, where only a single device is needed to manage the security of the network from a central location. This can be achieved with a physical SD-WAN device, such as on top of a WAN edge router, or through virtualization. Placing the SD-WAN in a virtual environment will further reduce the need for multiple hardware devices. Instead of having a dedicated device to host the SD-WAN, it can be placed amongst the other virtual environments on a single server. This will help save a company money on power consumption and make it easy to open more offices without worrying about installing more devices to accommodate them.

Overall, a secure SD-WAN is more efficient, flexible, and cost-effective than a traditional firewall solution. With a single firewall no longer being an effective security solution, many companies are looking for methods to supplement their firewalls. However, a secure SD-WAN is a replacement for a firewall that has great benefits. As more services and applications switch to cloud-based platforms, a direct connection via an SD-WAN makes access easier and faster. Network traffic no longer needs to route through the main office before reaching the Internet, reducing transport costs and removing the need for private leased lines. A secure SD-WAN solution also provides a company with the flexibility to open more branches with fully configured security defensives more quickly without worrying about the cost of buying more equipment. Traditional firewall solutions could not handle the same level of flexibility and therefore would hinder a company's future growth.

FlexiWAN:

FlexiWAN is an open-source Software Defined Wide Area Network (SD-WAN) architecture that centrally manages multiple networks to create agile, robust, reliable, low-cost, and customizable network infrastructure. The benefits associated with using FlexiWAN include:



Source: https://docs.flexiwan.com/overview/architecture.html

- Faster networks
- Agile network architectures
- Reliability of the network
- Network automation
- Reduced operational expenditure
- Reduced capital expenditure

Faster Networks and Agile Network Architecture Benefits (Direct Internet Access)

Any device running the FlexiWAN software is categorized as a FlexiEdge device, collectively registered as FlexiEdge within the network. FlexiWAN utilizes multiple FlexiEdge devices to enhance the speed of delivering applications to its end users. The use of Direct Internet Access (DIA), enables FlexiWAN to connect directly to the Internet, rather than routing traffic through a central hub. Reduced latency, improved application performance and faster network response times are a few key benefits that are accomplished by implementing FlexiWAN. Since the FlexiWAN architecture provides the network administrators with automation capabilities, it streamlines various network management tasks to create an agile and efficient network infrastructure that can be adapted to any expanding business.

Reliability, Resiliency, and Network Automation (FlexiEdge)

FlexiEdge is the key platform that brings reliability and resiliency to the FlexiWAN network. It provides a comprehensive range of key features and capabilities, which is achieved through defined failover and load-balancing policies. An example of this is when a site experiences a loss of connectivity due to a single dedicated link failure. FlexiEdge, in coordination with DIA connections, will dynamically reroute network connectivity to an alternative path or an available link to ensure continuity and minimize any disruption to its end users. The network is automated to change routes based on predefined policies and real-time conditions by continuously monitoring link availability and network congestion levels (*SD-wan*, 2023).

Reduced Operations and Expenditure (FlexiManage)

FlexiManage is the central management platform within the FlexiWAN architecture. FlexiManage is serviced by a scalable web server that allows network administrators to bypass manual operations such as performing individual configurations to each edge device (*How flexiwan works,* n.d.). FlexiManage system broker is the key subcomponent within the FlexiManage architecture that works to facilitate communications between the FlexiEdge devices and web server (*How flexiwan works,* n.d.). Ultimately, these components work in harmony to reduce the costs of operations by utilizing the FlexiManage system broker and FlexiEdge devices to automate network management processes.

WHY SECURE SD-WAN IS GOOD FOR SMALL COMPANIES:

A secure SD-WAN is great for a small company because it is easy to use, cost-effective, and reduces hardware requirements for a secure network. Having a secure SD-WAN implemented in the network, creates a centralized interface for managing all configurations and

logs which makes it easier for companies with limited personnel to handle. A company would only need to dedicate one or two of its staff to managing the security of its network since everything can be seen from one software application. Furthermore, zero-touch provisioning means that smaller companies can easily push updates to branch offices without needing to hire IT personnel for those offices. This ensures that configurations made to support security policies are uniform throughout the network since they all come from the same central interface. Because a secure SD-WAN consolidates a lot of security hardware into one device, it saves money on the cost of buying all the traditional security devices and the power consumption needed to run them. Additionally, zero-touch provisioning saves the company money by not needing to hire more IT personnel for branch offices. Finally, a SD-WAN can be implemented in a virtual environment, saving physical space by placing it amongst other virtual machines. Overall, a small company would benefit from using a secure SD-WAN for their network security because it cuts down on costs, allows them to put money into other aspects of the company and support future growth, and is easy for less experienced IT personnel to manage.

SNORT VS. FLEXIWAN:

Comparing Snort and FlexiWAN is not a straightforward process considering that they each serve to satisfy different aspects of network security. They both accomplish security very differently where snort specializes in real-time packet analysis to identify and prevent any malicious attacks and FlexiWAN promotes an optimized network performance with added built-in security. Considering that the business is concerned with identifying and preventing network-based attacks, Snort is considered the most suitable solution. Snort stands out between the two products, since it has the capacity to accomplish real time detection, which includes its three modes; sniffer mode, IDS mode, and packet logger mode. Ultimately, Snort is a great tool

to utilize as an initial line of defense for implementing network security measures focused on real-time intrusion detection and prevention capabilities. This additional layer of defense provides a preemptive approach to protecting the network infrastructure against high-risk security threats.

CONCLUSION:

As discussed, a firewall-only solution is not the prime solution for defense in depth and optimal network security. When firewalls are combined with other security software or hardware, the level of security is significantly higher. Intrusion detection systems and intrusion prevention systems provide immediate detection of threats, while intrusion prevention systems counteract the threat. Both IDS and IPS together provide detection and deterrence from a threat to secure and safely identify any vulnerabilities in a business network or system. Snort, SD-WAN, and FlexiWAN all provide an additional line of detection to increase the overall security of a business and their sensitive data. Snort is not only cost effective and user friendly, but can be configured in three different modes - packet sniffing mode, packet logger mode, and network intrusion prevention system mode. SD-WAN is cost effective, user friendly, and enhances the performance of the network to improve productivity and communication by finding the best route in real time for packet traffic. In addition, FlexiEdge devices reduces latency, improves application performance, and allows for faster network response times. Both Snort and SD-WAN offer more proficient security standards, however both accomplish their mission of enhanced security in a different manner. At the end of the day, it is important to point out all the benefits of each, however which software is used is going to be dictated by the business implementing the security software and the needs of the business.

References

Aruba Experts. (2022, September 28). *How secure SD-wan can replace traditional branch firewalls*. Network World. https://www.networkworld.com/article/3674957/how-secure-sd-wan-can-replace-traditional-branch-firewalls.html

Fruehe, J. (2020, January 30). *How SD-WAN changes the network security perimeter: TechTarget*. Networking. https://www.techtarget.com/searchnetworking/tip/How-SD-WAN-changes-the-network-security-perimeter

Garg, A., & Maheshwari, P. (2016, January 23). *Performance analysis of Snort-based Intrusion Detection System*. Ieeexplore-Ieee-Org.Sandiego.idm.Oclc.org. Retrieved August 8, 2023, from https://ieeexplore-ieee-org.sandiego.idm.oclc.org/document/7586351/authors#citations

Gomane, G. (2023, January 11). *4 main benefits of replacing branch firewalls with secure SD-wan: Aruba blogs*. blogs.arubanetworks.com. https://blogs.arubanetworks.com/solutions/four-main-benefits-of-replacing-branch-firewalls-with-secure-sd-wan/

How flexiwan works. How flexiWAN works - flexiWAN documentation. (n.d.). https://docs.flexiwan.com/overview/architecture.html

LogicMonitor. (2023, March 2). *How are firewalls and SD-wan related?*. LogicMonitor. https://www.logicmonitor.com/blog/how-are-firewalls-and-sd-wan-related

Rapid7. (2017, January 11). The Pros & Cons of Intrusion Detection Systems. Retrieved from Rapid7:https://www.rapid7.com/blog/post/2017/01/11/the-pros-cons-of-intrusion-detection-systems/

SD-wan. flexiWAN. (2023, January 18). https://flexiwan.com/resources/sd-wan/

Snort/Cisco. *Products*. Www.Snort.org. Retrieved August 8, 2023, from https://www.snort.org/products