EVANS&CHAMBERS
TECHNOLOGY

# SOFTWARE-DEFINED FIREWALLS FOR ZERO-TRUST SECURITY

Produced by Evans & Chambers Technology

EVANS & CHAMBERS TECHNOLOGY

# Table of Contents

# Chapter 1

# Introduction

## Chapter 1

# Introduction

Welcome to the Evans & Chambers Technology eBook on zero-trust security via software-defined firewalls. In this eBook, we will explore the cybersecurity challenges facing Intelligence agencies today and provide insights into how software-defined firewalls can help prevent exploits that could threaten your sensitive information.

As a member of the IC, you face unique challenges when it comes to securing your mission-critical systems. From constantly evolving cyber threats to the need to comply with strict regulations, protecting sensitive data and ensuring system availability is critical to your success. With the rise of sophisticated cyberattacks, including those by nation-states and cybercriminals, protecting sensitive information is more important than ever. To address these challenges, the IC has increasingly turned to the zero trust security model, which operates on the principle of "never trust, always verify."

This is where Evans & Chambers Technology comes in. We understand the importance of zero trust security and have developed solutions that help our clients achieve this level of protection. With over 20 years of experience in the intelligence community and a track record of delivering

innovative, reliable solutions, we can help you achieve your security goals and stay ahead of emerging threats.

At Evans & Chambers Technology, we understand the unique cybersecurity challenges faced by IC agencies. That's why we specialize in providing advanced security solutions that can help protect your network from cyber threats. In this guide, we'll discuss the benefits of software-defined firewalls and how they can help strengthen your network security.

We hope this eBook will serve as a valuable resource for you as you seek to protect your sensitive information and maintain the security of your organization. Let's get started.

Chapter 2

# Cybersecurity Challenges Faced by Intelligence Agencies

Chapter 2

# Cybersecurity Challenges Faced by Intelligence Agencies

IC agencies face a wide range of cyber threats on a daily basis. From sophisticated phishing attacks to advanced persistent threats, cybercriminals are constantly finding new ways to infiltrate networks and steal sensitive information. Some recent exploits include:

**The SolarWinds breach:** which affected multiple government agencies and private sector companies and was attributed to Russian state-sponsored hackers.

**The OPM data breach:** which exposed the personal information of millions of government employees and was attributed to Chinese state-sponsored hackers.

**The WannaCry ransomware attack:** which affected

computers in over 150 countries and caused significant disruption to organizations around the world.

Many of these exploits could have been prevented with better firewall security. Traditional hardware-based firewalls are effective at blocking known threats, but they can be slow to adapt to new threats and can be difficult and time-consuming to configure.

# Chapter 3

# Firewall Basics

Chapter 3

# Firewall Basics

A network firewall is a security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It serves as a barrier between the internal network and the external network (such as the Internet), helping to protect the network from unauthorized access, malware, and other security threats. The firewall examines each incoming and outgoing packet of data, comparing it against the predefined rules, and either allows or blocks the traffic based on the ruleset. Firewalls can be hardware or software-based and are an essential component of any organization's network security infrastructure.

At a high level, there are several types of firewalls that organizations can choose from to protect their networks and systems. These include:

**Packet-filtering Firewalls:**

These firewalls examine individual packets of data as they pass through the network. They use predefined rules to allow or block packets based on factors such as source and destination IP addresses, port numbers, and protocol types.

**Stateful Inspection Firewalls:**

Stateful firewalls keep track of the state of network connections and monitor the entire communication session. They analyze not only individual packets but also the context and state of the connection to make more informed decisions about allowing or blocking traffic.

**Application-layer Firewalls:**

Also known as proxy firewalls, these firewalls operate at the application layer of the network stack. They inspect and filter traffic at a more granular level, understanding the protocols and data within the packets. By acting as intermediaries between clients and servers, they provide an additional layer of security by enforcing application-specific rules.

**Next-Generation Firewalls (NGFW):**

NGFWs combine traditional firewall functionality with additional features such as intrusion prevention systems (IPS), deep packet inspection (DPI), SSL inspection, and application awareness. They offer more advanced threat detection and prevention capabilities by analyzing the content and context of network traffic.

**Virtual Firewalls:**

Virtual firewalls are designed for virtualized environments and cloud computing platforms. They provide security and network segmentation within virtual networks, allowing organizations to isolate workloads and enforce security policies across virtual machines or containers.

## Web Application Firewalls (WAF):

WAFs are specifically designed to protect web applications from various types of attacks, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). They monitor and filter HTTP/HTTPS traffic to detect and block malicious requests targeting web applications.

It's important to note that these firewall types can be implemented in different forms, such as hardware appliances, virtual appliances, or cloud-based services. Organizations need to consider their specific requirements, network architecture, and security needs to choose the most suitable type of firewall for their environment.

Chapter 4

# The Problem with Traditional Hardware-Based Firewalls

Chapter 4

# The Problem with Traditional Hardware-Based Firewalls

Deploying and managing hardware-based firewalls can be time-consuming and costly for organizations, especially in cloud environments. In contrast, software-defined firewalls offer a number of benefits that make them a more attractive option.

One key benefit is agility. Software-defined firewalls can be deployed quickly and easily in cloud environments such as AWS or Azure, often taking only a fraction of the time it takes to deploy hardware appliances. This means that organizations can respond quickly to changing business needs, scaling their security solutions up or down as required.

Another advantage of software-defined firewalls is flexibility. They can be customized to meet specific business

requirements and security needs, with the ability to add or remove features as needed. This is in contrast to hardware appliances, which often come with a fixed set of features that cannot be easily modified.

Cost savings is another key benefit. Hardware appliances require significant upfront capital investment, ongoing maintenance costs, and often require additional hardware for redundancy and high availability. In contrast, software-defined firewalls can be deployed on commodity hardware, or reserved cloud instances, reducing costs and increasing scalability.

The reduction of cost makes it possible to deploy the firewalls from multiple vendors such as Palo Alto, Cisco, and Juniper Networks to employ a layered approach to security, where multiple layers of security controls are used to provide better protection against various types of threats. For example, you might use one firewall solution for your perimeter security, and another for your internal network security. You might also use a different firewall solution for your DMZ (demilitarized zone), which is a separate network that provides controlled access to the internet. Another reason to use multiple firewall solutions is to provide redundancy and failover capabilities. If one firewall fails, the other can take over and provide continuous protection.

Finally, software-defined firewalls offer a more centralized approach to security management. With hardware appliances, security policies must be configured and managed on a device-by-device basis. In contrast, software-defined firewalls allow for centralized policy management, making it easier to ensure consistent security policies across the entire network.

Overall, software-defined firewalls offer a number of benefits over traditional hardware appliances, including agility, flexibility, cost savings, and centralized management. As cloud adoption continues to accelerate, software-defined firewalls are becoming an increasingly important part of an organization's security strategy.

EVANS&CHAMBERS
TECHNOLOGY

# Chapter 5

# Benefits of Software-Defined Firewalls

Chapter 5

# Benefits of Software-Defined Firewalls

Software-defined firewalls (SDFs) offer several benefits over traditional hardware appliances. Evans & Chambers has observed a major benefit of software-defined firewalls (SDFWs) over traditional appliance-based firewalls is the agility and speed they offer in deployment and management. Government agencies often face challenges with the lengthy procurement and acquisition processes required for physical hardware appliances.

Additionally, making changes to physical infrastructure can involve numerous requests and approvals, leading to delays.

In contrast, SDFWs can be set up and configured quickly, without the need for physical installations or infrastructure changes. Since they are implemented in software, they can be provisioned and deployed within virtualized or cloud environments with relative ease. This eliminates the procurement delays associated with purchasing and

installing physical appliances.

Furthermore, the management and maintenance of SDFWs are generally simpler and more efficient. Updates and patches can be applied centrally, without the need for physical access to individual devices. This reduces the burden on limited engineering resources and allows for faster implementation of security measures and policy changes.

By opting for SDFWs, government agencies can enjoy the advantage of accelerated deployment times, reduced bureaucratic delays, and improved operational efficiency. They can respond swiftly to security requirements and adapt to changing threat landscapes without the constraints of physical infrastructure. This flexibility and agility are vital in ensuring the timely and effective protection of critical government systems and data.

Here are just other benefits of SDFWs over traditional variants:

- Greater Flexibility: SDFWs can be easily deployed and configured in a wide range of environments, including cloud-based environments such as AWS and Azure. This allows IC agencies to quickly and easily adapt their network security to changing threats and environments.
- Improved Performance: SDFWs are designed to be highly scalable and can provide superior performance compared to hardware-based firewalls, especially in high-traffic environments.

- Enhanced Security: SDFWs can be configured to provide granular control over network traffic, allowing IC agencies to better protect their network from advanced threats such as zero-day exploits and advanced persistent threats.
- Simplified Management: SDFWs can be centrally managed from a single console, making it easier for IC agencies to manage their network security and quickly respond to emerging threats.
- Compliance: For customers with strict compliance requirements, SDFW can be customized to meet specific compliance standards, such as FIPS 140-2, HIPAA, and PCI-DSS.

Overall, a SDFW provides a higher level of control, customization, and visibility, which may be critical for customers with a need to secure sensitive national security information. However, it may require more resources and expertise to deploy and manage compared to firewall as a service (FWaaS). The trade-offs between FWaaS and SDFW are discussed in the next chapter.

# Chapter 6

# FWaaS vs SDFW

Chapter 6

# FWaaS vs SDFW

Firewall-as-a-Service (FWaaS) is a cloud-based security solution that provides firewall functionality as a service. FWaaS is usually deployed as a subscription service and provides centralized control of network traffic across multiple locations.

Software-Defined Firewalls (SDFW), on the other hand, are software-based firewall solutions that run on top of a virtualized environment or a cloud environment. SDFW allows administrators to define network traffic policies and control traffic flow in a software layer, which is independent of the physical network layer.

The main difference between the two is that FWaaS is a cloud service provided by a third party, while SDFW is typically installed and configured on-premise by the organization's IT team. FWaaS is a fully managed solution, while SDFW provides more flexibility in terms of customization and control.

Another key difference is that FWaaS is typically easier and quicker to deploy than SDFW, as it requires minimal setup

and configuration. SDFW, on the other hand, can take longer to deploy and requires a higher level of technical expertise.

Overall, both FWaaS and SDFW are effective solutions for securing network traffic and preventing unauthorized access. The choice between the two depends on the organization's specific needs and preferences.

# Chapter 7

# Conclusion

Chapter 7

# Conclusion

As cyber threats continue to evolve, it's more important than ever for IC agencies to take a proactive approach to network security. At Evans & Chambers Technology, we specialize in providing advanced security solutions that can help protect your network from cyber threats. By deploying software-defined firewalls, you can enhance your network security and better protect your sensitive information. Contact us today to learn more about how we can help strengthen your cybersecurity defenses.

## Ready To Get Started?

Are you looking for advanced cyber security defense for your critical assets? We'll help you gain unparalleled security, agility and operational efficiency.

Contact Us today