Hi Michael

Thank you for your well-articulated post around the different firewalls. Proxy firewalls certainly has its advantages and drawbacks. Andress (2014) mentions that companies place a heavy emphasis on proxy firewalls protecting end users from receiving spam via e-mail as well as visiting malicious websites. One of the issues arising from proxy firewalls is the introduction of network delay as a result of their filtering and inspection capabilities (Andress, 2014). Hayajneh et al. (2013) further states that due to the deeper traffic examination that proxy firewalls perform, jitter (variation in delay of received packets) and reduced throughput (actual payload received per unit time) is introduced into the network. While proxy firewalls are effective in many ways, they can certainly have an impact on employee productivity in the workplace.

Various types of firewalls are necessary and play an integral part in protecting networks. However, only making use of firewalls in today's era simply aren't enough to protect a network. Attackers have gained immense experience and have become highly skilled at bypassing firewalls using techniques such as port forwarding and spoofing as well as encryption (Klein, 2021). Encryption prevents deep packet inspection allowing attackers who have learnt how to use SSL (Secure Socket Layer) and TLS (Transport Layer Security) to pass through firewalls without being detected (Klein, 2021).

List of References

Andress, J. (2014). *The Basics of Information Security, Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd ed. Massachusetts: Syngress Publishing. Available from: https://doi.org/10.1016/C2013-0-18642-4 [Accessed 16 September 2021]

Hayajneh, T., Mohd, B.J., Itradat, A. & Quttoum, A.N. (2013). Performance and information security evaluation with firewalls. *International Journal of Security and Its Applications 7*(6): 355-372. Available from: http://dx.doi.org/10.14257/ijsia.2013.7.6.36 [Accessed 16 September 2021]

Klein, D. (2021). Relying on firewalls? Here's why you'll be hacked. *Network Security 2021*(1): 9-12. Available from: https://doi.org/10.1016/S1353-4858(21)00007-6 [Accessed 16 September 2021]

Hi Kingsley

Thank you for a very thought-provoking post around SIEM and stateful firewalls.

In addition to your points mentioned, stateful firewalls also known as stateful packet inspection firewalls uses a state table to keep track of connection states passing through the firewall; It does this by keeping track of the source and destination IP addresses, ports used and connection information (Andress, 2014). While these firewall state tables are designed to increase security, they can also be vulnerable to attacks. Trabelsi and Zeidan (2019) mentions that attackers use a technique called Denial of Firewalling (DoF) where a flood of requests are sent to add entries into the state table faster than the firewall can remove them and subsequently denying legitimate connections. Furthermore, when this happens a CPU spike is observed, and the firewall becomes unresponsive causing a network outage (Trabelsi & Zeidan, 2019).

However, echoing your sentiment, stateful firewalls are still required as a first layer of protection for networks and can provide many benefits to organisations. One of these benefits is the ability to log the behaviour of attacks allowing one to further analyse log files and thus preventing future attacks (Fortinet Inc, 2021). Logs are vital information for security engineers when troubleshooting and detecting data breaches.

List of References

Andress, J. (2014) *The Basics of Information Security, Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd ed. Massachusetts: Syngress Publishing. Available from: https://doi.org/10.1016/C2013-0-18642-4 [Accessed 23 September 2021]

Z. Trabelsi & S. Zeidan. (2019) 'Resilence of Network Stateful Firewalls against Emerging DoS Attacks: A Case Study of the BlackNurse Attack', *16th International Conference on Computer Systems and Applications (AICCSA).* Abu Dhabi, 3-7 November 2019. USA: IEEE. Available from: https://sci-hub.se/10.1109/AICCSA47632.2019.9035323 [Accessed 23 September 2021]

Fortinet Inc. (2021) Stateful vs. Stateless Firewalls. Available from: https://www.fortinet.com/resources/cyberglossary/stateful-vs-stateless-firewall. [Accessed 23 September 2021]

Hi Aldo

Great post on Anomaly Based Detection and cryptography. These are two very important techniques used in security technologies that can be discussed at length.

Chakraborty (2013) describes Anomaly Based Detection as one of the methodologies that is part of an Intrusion Detection System (IDS). In its simplest meaning, Anomaly Based Detection attempts to find patterns in data sets that do not align with normal expected behaviour. For example, in networking, this is commonly known as Network Behaviour Anomaly Detection (NBAD) which scans traffic to determine any anomalies (Chakraborty, 2013). NBAD is particularly useful to reveal malicious traffic in a network. From personal experience I can confirm that the NBAD methodology is commonly used in ISP (Internet Service Provider) networks. Traffic is monitored using network monitoring software for any anomalies; this is further logged and reported on which aids in troubleshooting.

Anomaly Based Detection has also been adopted in other industries. This includes the banking industry where it is commonly used to detect credit card fraud as well as in the military industry to perform surveillance on enemy activity (Bhuyan, 2014).

However, as Michael Geiger has correctly pointed out, the Anomaly Based Detection methodology can have some significant disadvantages.

List of References

Chakraborty, N. (2013) Intrusion detection system and intrusion prevention system: A comparative study. *International Journal of Computing and Business Research 4*(2): 1-8. Available from: http://researchmanuscripts.com/May2013/1.pdf [Accessed 24 September 2021]

M. H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita. (2014) Network Anomaly Detection: Methods, Systems and Tools'. *IEEE Communications Surveys & Tutorials* 16(1): 303-336. Available from: https://sci-hub.se/10.1109/SURV.2013.052213.00046 [Accessed 24 September 2021]

C2 General

Hi Austin

Thank you for your post. You have pointed out some interesting facts around Antivirus and Next Generations Firewalls (NGFW's).

Next Generation Firewalls are playing a vital role in protecting companies against evolving and sophisticated threats. Vendors such as Palo Alto Networks, Fortinet and Checkpoint Software Technologies remain leaders in producing NGFW's with very advance features (Gartner, 2020). In addition, Soewito & Andhika (2019) prove that NGFW's are very effective against DDOS (Distributed Denial of Service), phishing and SQL (Structured Query Language) attacks through various experiments performed on IoT and corporate networks. However, Klein (2021) mentions that relying on firewalls alone to protect networks in its entirety simply aren't enough; methods such as software-based segmentation are proving to be very effective as well. Software-based segmentation uses real-time and historical information to create policies (Klein, 2021). Further advantages include it being system agnostic as well agent based allowing it to be used across the organisation in all areas (Klein, 2021).

I further conquer with your conclusion, despite the NGFW's weaknesses mentioned it is becoming a 'must have' to protect modern day networks. Organisations will need to adopt various security technologies to ensure that networks remain protected end-to-end.

List of References

B. Soewito & C. E. Andhika. (2019) 'Next Generation Firewall for Improving Security in Company and IoT Network', *2019 International Seminar on Intelligent Technology and Its Applications 2021(1):* 205-209. Available from: https://sci-hub.se/10.1109/ISITIA.2019.8937145 [Accessed 26 September 2021]

Gartner (2020) Gartner Magic Quadrant for Network Firewalls. https://www.gartner.com/en/documents/3992870. [Accessed 23 September 2021]

Klein, D. (2021). Relying on firewalls? Here's why you'll be hacked. *Network Security 2021*(1): 9-12. Available from: https://doi.org/10.1016/S1353-4858(21)00007-6 [Accessed 26 September 2021]

Hi Jitesh

A very informative post on the importance of Identity and Access Management (IAM) and Security Orchestration Automation and Response (SOAR).

In addition, IAM has widely been adopted in the cloud computing industry for several years now as Jonathan has pointed out as well. Amazon Web Services (AWS) has announced in May 2021 its 10th anniversary of using IAM and how successful it has been (Udell, 2021). With the implementation of IAM, organisations will no longer face the challenge of maintaining credentials and multiple identities across resources and devices in a network (Mohammed, 2011).

However, there are a few disadvantages of IAM which must be considered. Mohammed (2019) mentions that one of the most common scenarios in companies is relying on IAM to prevent unauthorized usage on systems. It is therefore important that access controls and policies that form part of the IAM program are implemented correctly.

From my personal experience I can promote the fact that ISP's (Internet Service Providers) have adopted IAM together with Centralized User Management to ensure a single identity (domain username) is used to access any resource throughout the organisation. One should also consider the security best practices when working with IAM i.e., only least privilege access and permissions should be granted necessary to perform a specific task.

List of References

Mohammed, I.A. (2011) Identity and Access Management System: a Web-Based Approach for an Enterprise. International Journal of Advance and Innovative Research 1(4): 1-7. Available from: https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887611_Identity_and_Access_Management_System_a_Web-_Based_Approach_for_an_Enterprise/links/6116a022169a1a0103fc6432/Identity-and-Access-Management-System-a-Web-Based-Approach-for-an-Enterprise.pdf [Accessed 27 September 2021]

Udell, R. (2021) IAM 10th Anniversary: Top Recommendations for Working with IAM from Our AWS Heroes – Part 1. https://aws.amazon.com/blogs/apn/iam-10th-anniversary-top-recommendations-for-working-with-iam-from-our-aws-heroes-part-1/ [Accessed 27 September 2021]

Hi Thomas

Thank you for your post, highlighting the importance of End Detection Response (EDR) Software and Multi-factor Authentication (MFA).

MFA was designed to provide a higher level of safety and protection to devices and systems, while also providing a resilient way of authenticating users (Dasgupta et al., 2017). As a supplementation to your post, Ometov et al. (2018) mentions three types of factors used to authenticate that are part of MFA i.e. Knowledge factor (password, pins, security questions), Ownership factor (smartphone, key-cards, etc.) and a Biometric factor (fingerprint, face recognition, behaviour recognition, etc.).

With the increase in data breaches worldwide (Department for Digital, Culture, Media & Sport, 2020) organisations should strive to implement MFA as one of the mandatory security controls. A major contributor to data breaches are the use of IoT devices (Dahlqvist et at., 2019). MFA is also widely adopted and used in the Advance Internet of Things (A-IoT) industry providing secure authentication to Hi-End wearables, consumer drones and smart vehicles (Ometov et al., 2019). Despite the challenges experienced by developers on enablers such as finger/palm/eye scanners, facial recognition, voice recognition amongst others, the security advantages certainly outweigh the drawbacks (Ometov et al., 2019).

List of References

Dahlqvist, F., Patel, F., Rajko, A., Shulman, J., McKinsey & Company. (2019) *Growing opportunities in the Internet of Things.* Available from: https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things [Accessed 02 October 2021]

Dasgupta D., Roy A., Nag A. (2017) *Multi-Factor Authentication. In: Advances in User Authentication*. 1st ed. New York: Springer Publishing. Available from: https://doi.org/10.1007/978-3-319-58808-7_5 [Accessed 02 October 2021]

Department for Digital, Culture, Media & Sport (2020) *Cyber Security Breaches Survey 2020.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf [Accessed 02 October 2021].

Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y., Gerla, M. (2019) 'Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications'. *in IEEE Network*. USA:IEEE. Available from: https://ieeexplore.ieee.org/abstract/document/8675176 [Accessed 02 October 2021]