A GUIDE TO FIREWALL MANAGEMENT

Picture it. In the late 1980s, we were given the Motorola cell phone, The Simpsons, Seinfeld, the Gameboy and Firewalls. While we would love to talk about The Simpsons predicting major events, let's talk about how firewalls continue to be a tried-and-true piece in every cybersecurity toolset and the keys to firewall management in 2021.

Over the decades' everything cybersecurity related has increased – threats, devices, applications, tools and even a skills shortage. As NextGen firewalls (NGFW) continue to be a foundational staple for protecting against threats, it is a great place to reevaluate your approach and ensure it is maximizing security.

However, there are challenges to managing firewalls, so we asked one of Brite's SOC Analysts for thier expert insights into the state of firewall management and the keys on how to manage a firewall.

FIRST, WHY ARE FIREWALLS IMPORTANT IN SECURITY?

SOC Analyst Insights: Firewalls are such a staple in cybersecurity because they are typically the first line of defense against an attacker (this is starting to change through perimeter honeypots with security application rather than research application *shoutout to PacketViper*).

This means that a perimeter firewall is the first obstacle an attacker must overcome to complete the cyber kill chain with the end goal of exfiltrating some kind of data deemed important to the attacker.

Firewalls also eliminate much of the "low hanging fruit", meaning analysts can eliminate or mitigate the majority of threats through good use of GeoIP blocking, an often very underestimated approach to remove much of the noise caused by script kiddies and low to mid-level hackers.

To ensure firewalls successfully eliminate risk let's share some keys to ensure your firewall security is effective.

3 KEYS TO FIREWALL MANAGEMENT

1. Rule management.

Take the time to review and edit rules based on your environment today. Do they align or need updating? Firewall rule management is critical to keeping systems up to date. We recommend utilizing a strict change management policy.

SOC Analyst Insights: Firewall rules need constant care and feeding. Meaning we should be adding IP's, users, services, applications and destinations to rules as often as change management allows to fill any pinholes within the firewall and keeping with the goal of always strengthening cybersecurity posture.

2. Regular, documented assessments.

Constant firewall assessments allow the team to dedicate time to review and update rules, software versioning, licensing and feature utilization. Like with other security tools, you cannot "Set and forget it." Firewalls require consistent optimization and management.

SOC Analyst Insights: There is a lot of responsibility and accountability when working on a firewall. If something goes wrong and change management has not been followed, you are responsible for the downtime. This is can be a very stressful notion even when change processes have been followed, therefore documentation is critical.

3. Dedicate the time.

The reality is that firewall management is tiresome and requires in-depth knowledge to safely and efficiently pass rules. Explore passing it off to a managed security provider. By offloading firewall management, your team will have more bandwidth to achieve new, strategic initiatives.

SOC Analyst Insights: Firewall rules can take a considerable amount of time to create. A cybersecurity professional must spend time digging through logs, looking at IP addresses, services and users (just to name a few) when working on firewall rules to ensure production is not disrupted.

However, with Brite, you're never on your own. Being proactive in today's environment requires a divide and conquer approach. Brite's managed security service BriteProtect and its team of SOC analysts are here to have your back. See how BriteProtect can help.

ABOUT BRITEPROTECT

BriteProtect is an advanced managed security service that solves the problem of tedious alert management leading to missed critical alerts and employee fatigue. We leverage decades of cybersecurity experience to provide our customers with unprecedented visibility, swift response and expert insights delivered via people, process and technology. Now, organizations can leverage existing security tools by partnering with Brite's team utilizing new, next-generation technology to elevate its security posture and better utilize internal resources.

ABOUT BRITE

At Brite, people and technology are at the core of everything we do. We're committed to proactively protecting communities and organizations through innovative technology solutions delivered by our talented team.

Brite delivers industry-leading cybersecurity solutions to businesses in various industries across the country. We deliver the most comprehensive IT and security services by providing the right people and proven processes when technology alone is not enough.

Our proven methodology of partnering with thoroughly vetted industry-leading technology vendors, delivered by the Brite team, which is evident by our numerous awards, including a seven-time Inc. 5000 honoree.

Most importantly, we envision partnerships with clients where our team enables others with the technology and processes to better achieve their goals and objectives. And we're here to help with **Brite People. Brite Solutions.**