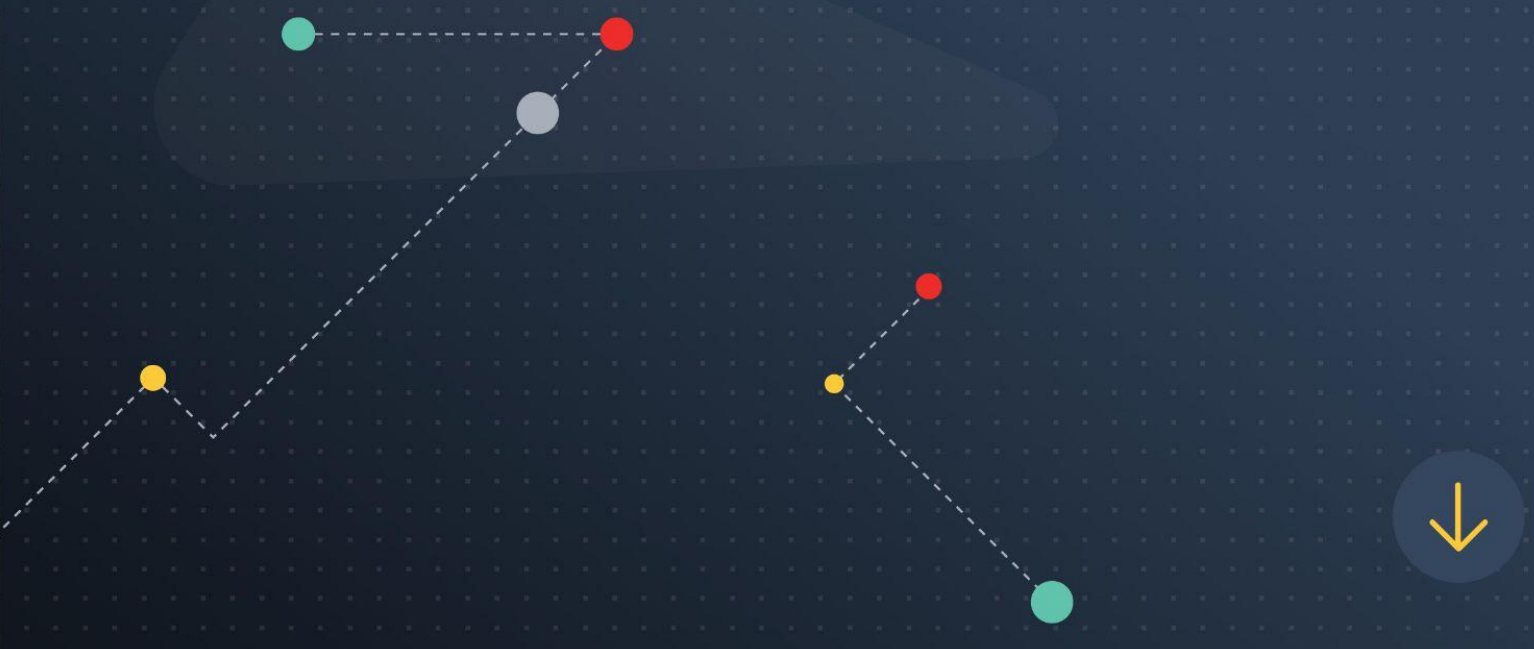
threaterR

eBook

7 Common Firewall Vulnerabilities

Just because your network has a firewall doesn't mean it isn't vulnerable to cyber threats.



7 Common Firewall Vulnerabilities

To defend your company from the danger of a breach, it's essential to familiarize yourself with the most common standard and web application firewall vulnerabilities, so you can ensure your current solution offers adequate protection.

Here are seven of the most common vulnerabilities in firewalls you're likely to find today.

Introduction

When implemented correctly, a firewall should effectively stop the vast majority of incoming threats, including phishing attempts, malware, and other actions taken by bad actors to penetrate your system. Once they're in, it's easy to gain access to proprietary data, devices, and other assets.

However, a firewall isn't just a set-it-and-forget-it security feature. A great firewall should be continually monitored, updated, and tested to ensure it works for your evolving needs. Otherwise, you could find yourself surprised by a vulnerability when it's too late to take any action.

The ideal way to protect your technology stack is to educate yourself and your team on potential firewall vulnerabilities and ensure that your system has all the latest updates and additional security features to protect your company from these evolving threats.

Leaving even the smallest firewall gap could put your security at risk and leave your company open to financial and reputational damages that can quickly skyrocket into the millions. As of 2021, one study estimated that the average data breach cost companies between $3.46 million and $5.12 million.

1. Insider Attacks

Unfortunately, one of the most common firewall vulnerabilities is that it cannot offer protection from individuals who are permitted to access the firewall itself. If a trusted individual with the proper credentials wants to bypass your firewall and steal data or assets, it's difficult to stop them.

Fortunately, while these individuals cannot be stopped, their potential for damage can be limited through network segmentation. By configuring your network into independent subnets, you can limit how much an individual can access at any time.

This offers your team the opportunity to slow down the attacker and isolate their access faster, neutralizing the damage before it becomes unfixable.

2. Lax or Inadequate Access

If your company does not have a strong password policy or has not set up two-factor authentication company-wide, there's a chance that a bad actor could enter your system through this lax access policy.

To protect your system, re-examine your current password and access security policies, then update them to the current best practices.

You can also inspect your anti-spoofing tools to ensure they offer the most protection possible. If they're set up poorly or not at all, it's a huge vulnerability that needs to be addressed.

3. Basic Inspection Protocols

Even if you've invested in a reliable and robust firewall, your IT team must ensure that it has been set up fully and has not been left on the most basic setting. This is easy to do if you aren't familiar with the setup process or are using a firewall system that's new to you. Unfortunately, this leaves you open to advanced threats.

One critical area that needs to be examined is whether your firewall can check data packets' destination, content, and origin. This is common with most next-generation firewalls. If this has not yet been configured on your firewall, it's a good idea to talk to your team and get it set up as soon as possible.

4. Outdated Software

Software is continually changing and updating in response to evolving threats, new technologies, and our growing body of knowledge. New information and vulnerabilities are constantly being discovered, and when they are, protections are developed to close them.

When a company finishes an update and wants to send it to their clients, they set it up as a patch or software update. If your IT team has been lax in checking for and installing these software patches, your firewall could be at risk.

To protect against this vulnerability, set up a regular schedule for updates and make sure your team is diligent in installing software patches as soon as they become available.

5. DDoS Attacks

One of the most common cyber threats used by bad actors is the distributed denial-of-service (DDoS) attack. This is a common technique where a firewall or server is flooded with traffic to such a degree that the system cannot process it all and shuts down.

A specific variety of DDoS attack called a protocol attack targets firewalls directly and is, unfortunately, both cheap and easy to execute.

Protecting against them is challenging and involves layers of security protocols, including a 'scrubbing' service in which traffic is routed through an intermediary who sorts out the false users from the legitimate ones.

6. Lack of Documentation

Documentation is essential in the creation and maintenance of a secure firewall. You need records of the different events that happen on your network to learn from them and prepare for future attacks.

It's also necessary due to the shifting nature of the workplace – if someone gets in an accident or leaves their job unexpectedly, you don't want to be reliant on a single person who knows your system.

Setting up and maintaining proper documentation on every aspect of your firewall can help ensure that there are no knowledge gaps that could leave your system vulnerable.

7. Limited Input Sources

Today's most secure and reliable firewalls take advantage of AI and machine learning to continually feed your firewall data on new and evolving threats. To use this feature, your team needs to engage updating and evolving sources to ensure that your firewall has access to the most information possible.

One of the best ways to do this is through an advanced security product like Threater.

Threater Protects Firewall Vulnerabilities

Defending against the most potential threats requires up-to-date cyber intelligence pulled from multiple reputable sources. To help protect your firewall, Threater synthesizes data from more than 30 threat intelligence providers and uses this knowledge to prepare your firewall for any threat it could potentially face.

Threater also helps to improve your security posture by enabling an ideal protected network while improving firewall efficiency, integrating into and enhancing your existing security stack, and mitigating false positives quickly and intuitively using automation to save you time and resources on otherwise consuming manual tasks.

Working with your IT team, we can help you implement Threater to improve the intelligence of your firewall and close gaps that put your security at risk. It's easy to use and can connect to anything in your technology stack.

About Threater

Threater is the only active defense cybersecurity platform that fully automates the enforcement, deployment and analysis of cyber intelligence at a massive scale. As the foundational layer of an active defense strategy, Threater's patented solution blocks known threats from ever reaching customers' networks. Threater utilizes immense volumes of cyber intelligence from over 50 renowned security vendors to provide unparalleled visibility over the threat landscape resulting in a more efficient and effective security posture. Block. Every. Threat. at Threater.com.