Firewalls are at the heart of any organization’s cybersecurity architecture. But we should not consider them as the ultimate security solution for your business’s cybersecurity needs. Firewall security is useful but you cannot solely rely on this one security tool due to a number of concerns.

Let’s look at five such firewall threats and vulnerabilities that you must look out for.

1. **Missed Security Patches**

This issue arises if you are unable to properly manage network firewall software. Just like any other software program, firewalls can also have vulnerabilities that attackers try to exploit. When a firewall vendor discovers a vulnerability, they try to fix them and roll out patches to fix the problem as fast as possible. However, a firewall does not automatically get patched with the release of new patches. You actually have to apply it to your firewall software. Until then, the vulnerability still exists and a hacker can exploit it any time.

The best way to deal with this is to create and follow a patch management schedule and apply the patches regularly according to it.

1. **Insider Threats**

Firewall security generally protects you from attacks originating from the outside. So what will happen if you have insider threats? At this point, a perimeter firewall is useless, since the attacker already exists in your system.

However, internal firewalls that are on top of perimeter firewalls can be useful even if an attack originates from inside your network. They help you divide individual assets in a network which makes it harder for a hacker to move from one system to another.

1. **Inability to Conduct Deep Packet Inspection**

Next generation firewall security uses deep packet inspection mode which examines the contents of an information packet before allowing or rejecting it to pass to or from a system. However, less advanced firewalls only check an information packet’s origin and destination points before allowing or denying their request. A hacker can easily spoof this information and trick a firewall that lacks deep packet inspection mode.

To avoid this, it’s recommended to use a firewall that can perform deep packet inspection.

1. **Distributed Denial of Service Attacks**

DDoS attacks overwhelm a target’s resources and either cause a shutdown or prolong their inability to function. One such category is protocol attacks that aim to drain your load balancer and firewall security resources so that they are unable to process legitimate traffic.

There is no easy fix for this. But some cybersecurity providers offer scrubbing services by diverting incoming traffic and sorting legitimate traffic out from it.

1. **Mistakes in Configuration**

Even with a firewall correctly patched, it can still create a problem if it is not properly configured. This can lead to the firewall failing to protect and result in loss of performance on the company network. For instance, dynamic routing is not generally recommended as it reduces control and, in turn, security. However, some organizations still enable it.

If you want to know more about how you can ensure strong network protection for your business, contact Aardwolf Security now and get expert advice from our cybersecurity professionals.