CYBERSECURITY NOTES

FIREWALL TYPES 101

For the non-technical people

leonel pedroza

FIREWALL TYPES 101

For the non-technical people

Contents

Decoding Firewalls: More Than Just Digital Walls

Ever actually wondered, "What does a firewall do, anyway?" If we were to personify it, it might be thought of as a cybernetics bouncer who decides who gets in and who stays out of the network. But are bouncers truly all the same? There is quite a variety of firewalls, each keeping undesirables out in their own way. Let's break matters down in a non-computer-science language.

So, we've circumnavigated all things about firewalls. But what should we take away from it? And where could anyone go should the appetite for more be there? All right, so let's put it together.

Packet-Filtering Firewalls: The Quick Checkpoint

Imagine a security guard who only glances at your ID badge – your source and destination IP address, the port you're trying to use, and the protocol. That's a packet-filtering firewall. These are the old guard, the originals. They're quick and don't ask too many questions, just checking basic info against a list of rules.

What's great about them?

- **Speedy Gonzales:** They're fast and don't hog your system's resources.
- **Simple Setup:** Generally easy to get up and running.

Where do they fall short?

- **Surface-Level Scrutiny:** They don't peek inside the "package" (the data payload) or remember if you've been there before (session state). It's like the guard not recognizing you even if you pass by every day.
- **Outsmarted by Modern Tricks:** Because they're not looking too deeply, cleverer attacks can sometimes slip right through.

Think of: Early versions of Cisco IOS ACLs, iptables (in its basic mode), MikroTik RouterOS filters.

Stateful Inspection Firewalls: The Memory Keepers

Now, picture a bouncer who not only checks your ID but also remembers you from your last visit and knows you're part of an ongoing conversation. That's a stateful inspection firewall. These are a step up, keeping track of active connections. If a random data packet tries to butt into an established chat, this firewall says, "Hold on, you're not part of this!"

What's great about them?

- **Smarter Security:** By remembering the "state" of connections, they offer much better protection.
- **Spotting Intruders:** They're good at catching those unauthorized or fishy-looking connections.

Where do they fall short?

- **A Bit More Brainpower Needed:** They need more processing oomph than their packet-filtering cousins.
- **Still Not X-Ray Vision:** While they know *who* is talking, they don't always understand *everything* they're saying at the application level.

Think of: Windows Defender Firewall with Advanced Security, pfSense (when in stateful mode), Fortinet FortiGate in its stateful setup.

Application Layer Firewalls (Proxy Firewalls): The Content Interpreters

These are the specialists, the bouncers who understand the specific language of different applications – like HTTP for web browsing, FTP for file transfers, or DNS for website lookups. They act like a middleman (a proxy), actually looking at the *content* of your traffic. It's like having a translator who also checks for contraband.

What's great about them?

- **Deep Divers:** They can sniff out threats hiding within the actual data of your applications.
- **Identity Protection:** They can cleverly hide your internal network's IP addresses from the outside world, like an unlisted phone number.

Where do they fall short?

- **Can Be a Bottleneck:** All that deep inspection can slow things down a bit.
- **Resource Hungry:** They need a good amount of resources and careful configuration to work their magic.

Think of: Squid Proxy with ACLs, Cloudflare WAF, Blue Coat ProxySG.

Next-Generation Firewalls (NGFWs): The All-in-One Powerhouses

Imagine a security checkpoint that combines the ID check, the memory of past visits, *and* has advanced scanners, intelligence feeds on known troublemakers, and can even identify users. That's an NGFW. These are the modern marvels, bundling stateful inspection with a suite of cool features like Deep Packet Inspection (DPI), Intrusion Prevention Systems (IPS), and more. They're trying to be the Swiss Army knife of network security.

What's great about them?

- **Fort Knox Vibes:** They offer some serious threat detection and give you a much clearer picture of what's happening on your network.
- **One-Stop Shop:** Many security functions are rolled into a single device, which can simplify things (in theory!).

Where do they fall short?

- **Pricey and Complex:** All that power comes with a high numbers price tag and can be a beast to manage and maintain. You'll likely need skilled folks and beefy hardware.
- **Not a Silver Bullet:** While powerful, I've seen setups where a misconfigured next-generation firewall (NGFW) can still leave gaps. It's about the whole security picture, not just one gadget.

Think of: Palo Alto Networks NGFW, Fortinet FortiGate NGFW, Cisco Firepower NGFW, Check Point NGFW.

Hardware Firewalls (Appliance Firewalls): The Dedicated Guardians

These are the physical boxes, the dedicated security appliances you often see in server rooms, standing guard at the edge of the network. Think of them as the main gate for a large corporate campus built to handle a flood of traffic.

What's great about them?

- **Built for Business:** They're designed for high performance and can grow up as your organization scale.
- **Takes the Load Off:** They handle the security heavy lifting, so your individual computers and servers don't have to.

Where do they fall short?

- **Investment Upfront:** Those boxes don't come cheap.
- **Less Agile for the Remote World:** If your workforce is spread out or heavily reliant on cloud services, a single box at headquarters might not be the most flexible solution.

Think of: Cisco ASA Series, Juniper SRX Series, Sophos XG Firewall Appliance.

Circuit-Level Firewalls: The Connection Validators

These firewalls operate a bit like a switchboard operator. They don't listen in on the calls (inspect content), but they make sure the connection itself (the TCP handshake) is legitimate before letting it go through. Are you really who you say you are, and is this a valid call request? They're often part of a bigger security team rather than the star player.

What's great about them?

- **Lightweight:** They don't consume many resources.
- **Quick on the Draw:** Good for fast session-level checks.

Where do they fall short?

- **Blind to Content:** They have minimal idea what's *in* the data packets.
- **Easily Fooled by Crafty Attacks:** Not your best defense against today's more sophisticated threats.

Think of: SOCKS5 proxies (like Dante Server), older versions of TIS Firewall Toolkit.

Cloud Firewalls (Firewall-as-a-Service - FWaaS): Security from the Sky

As more and more of our digital lives move to the cloud, so does security. Cloud firewalls are hosted services that protect your cloud infrastructure and applications. Think of it as hiring a top-notch security firm that operates entirely in the cloud, managing protection for all your cloud-based assets.

What's great about them?

- **Adapts to Your Needs:** Super flexible and can scale up or down as your cloud usage changes. Perfect for those dynamic workloads.
- **Control from Anywhere:** You can manage your security policies from a central dashboard, no matter where you are.

Where do they fall short?

- **Internet Dependant:** If your internet connection goes down, so does your firewall.
- **Ongoing Costs:** Usually a subscription model, so it's an operational expense rather than a one-time purchase. I always tell people to factor that into their budgeting!

Think of: AWS Network Firewall, Azure Firewall, Google Cloud Armor, Zscaler Internet Access (ZIA).

Software Firewalls (Host-Based Firewalls): Personal Bodyguards

These are the firewalls living directly on your individual computers and servers – your PC, your Mac, your Linux machine. Each device gets its own personal bodyguard, controlling traffic coming in and out of that specific machine. It's like having a security detail for every employee, not just the main building.

What's great about them?

- **Tailored Protection:** Each device gets security rules specific to its needs.
- **Layered Defense:** They're a fantastic addition to your main network firewall, adding another crucial layer of security. You can never have too many layers, right?

Where do they fall short?

- **One by One Management:** You've got to install and manage them on every single device. That can be a headache in larger setups.
- **Resource Sippers (Sometimes Gulpers):** They can use up some of your local computer's processing power and memory.

Think of: Windows Defender Firewall, macOS Application Firewall, UFW (Uncomplicated Firewall) on Linux.

And there you have it! A quick tour of the firewall clan. The right one (or, far more likely, the right set) entirely depends on what you're protecting. Some giant corporate network, some fancy cloud-based startup, or just your personal laptop? Each case has the perfect defender.

Finals thoughts: Building Your Digital Fortress

Here's the thing: firewalls aren't just fancy virtual doors; they're the cornerstone of any decent cybersecurity approach. Consider them a vital layer in the multi-layered cake of protection. We've had it all, from the basic packet-filtering types to the clever Next-Generation Firewalls (NGFWs). Each with their positives, and, yes, their own negatives and idiosyncrasies.

Choosing the "right" one? Well, that's a bit like picking the right tool for a job. It really boils down to what you're working with:

- How big is your network? A small home office is different from a global enterprise.
- What kind of digital nasties are you most worried about?
- How complex is your current tech setup?

Often, the smartest move is to **double up (or even triple up!)** – maybe a sturdy hardware firewall at the main gate and software firewalls on individual computers. That's what everybody calls the "defense-in-depth" principle and It's all sessions and layers.

And don't forget, setting up a firewall isn't a "**set it and forget it**" operation. Technology and threats change at light speed. So, stay on top of your systems, take a glance at your firewall's configurations from time to time, and ensure playing nice with your overall security game plan. Because, let's be honest, in the world of cybersecurity, stopping a problem before it starts is *always* way less painful (and cheaper!) than cleaning up a mess. A little prevention truly goes a long, long way.

Quick Cheat Sheet: Talking the Talk (Glossary)

Here are a few key terms to help you sound like you know your stuff:

- **Packet:** Think of it as a digital envelope carrying a small chunk of data across the network.
- **DPI (Deep Packet Inspection):** This is like opening that envelope and actually reading the letter inside (the data or payload) instead of just looking at the address.
- **IPS (Intrusion Prevention System):** A proactive security guard that doesn't just spot trouble but actively steps in to block threats it detects.
- **Proxy:** An intermediary – a go-between server that sits between your computer and another server, often to filter requests or hide your identity.
- **Session Layer:** Imagine it as the part of the network conversation (OSI layer 5, if you're feeling technical) that opens, manages, and closes the communication line between two devices.
- **Perimeter:** The digital fence line, the boundary between your safe internal network and the wild west of the internet or other external networks.
- **Endpoint:** Any device hooked up to your network – your laptop, desktop, server, you name it.
- **Cloud:** Think of it as someone else's computer – but on a massive scale. It's where your apps and data live when they're not on your personal devices. Instead of owning hardware, you're renting space and power from cloud providers like AWS, Azure, or Google Cloud.
- **Policy:** These are the rules of the road for your network. A policy tells the firewall (or any security system) what's allowed and what's not – who can talk to whom, when, and how.
- **NGFW (Next-Generation Firewall):** A high-tech, multi-talented firewall that doesn't just block bad traffic, it inspects, learns, and reacts. It combines traditional firewall features with extras like intrusion prevention, deep inspection, and even app awareness. Think Swiss Army knife for network defense.
- **SOCKS5**: A type of proxy that doesn't care what kind of traffic you send through it – web, email, torrents, you name it. It just tunnels it. SOCKS5 adds better security

and can even work with authentication, making it a flexible (but blind) traffic transporter.

- **Threat:** Anything that can potentially harm your digital world. This includes viruses, hackers, ransomware, and even innocent-looking emails that hide malicious intent. Basically, the "bad guys" in cybersecurity.
- **Sniff (or Packet Sniffing):** When someone secretly listens to your network traffic. Like wiretapping for the internet. It can be used for legit troubleshooting—or for sneaky surveillance if you're up to no good.
- **HTTP (HyperText Transfer Protocol):** The protocol your browser uses to load websites. It's like the waiter bringing you web content. Just know that without the "S" (as in HTTPS), it's not secure—anyone could peek at what you're ordering.
- **FTP (File Transfer Protocol):** An older way to move files between computers over a network. Still around, but not always safe unless wrapped in encryption. Think of it like sending a postcard—fast, but everyone can read it.
- **DNS (Domain Name System):** The internet's phonebook. When you type a website name (like google.com), DNS turns it into a number (IP address) so computers can find each other. No DNS, no web browsing.
- **ACL (Access Control List):** A digital guest list. It says who's allowed to do what – for example, which users or devices can access certain parts of the network. If you're not on the list, you're not getting in.
- **Stateful:** Means the firewall remembers things. It keeps track of who you talked to and how, so it can make smarter decisions about what to allow or block. Like a bouncer who recognizes you from last night.
- **State:** The status of a network conversation – who started it, whether it's still going, and where it's headed. Firewalls that track "state" can spot weird behavior, like a reply to a question that was never asked.
- **Stateless:** The opposite of stateful. These firewalls treat every packet like a stranger, with no memory of past interactions. Fast, yes, but a bit forgetful – like a guard who checks your ID every time, even if you just stepped out for coffee.
- **Host:** Any device with an IP address that can send or receive data – like a computer, printer, smartphone, or even a smart fridge. If it's on the network and doing something, it's a host.
- **Server:** A host with a specific job: to provide services to others. It might host a website, store files, manage emails, or stream videos. Always on, always waiting to serve.

Extra Goodies: Appendices

Appendix A: Which Firewall When? A Quick Guide

Here's a handy little table to give you a starting point:

Your Scenario	A Good Firewall Combo to Consider
Small Office / Home Office (SOHO) Network	Stateful Inspection Firewall + Software Firewalls
Everything's in the Cloud (Cloud-Only)	Cloud Firewall (FWaaS - Firewall-as-a-Service)
Big Company with Folks Working Remotely	NGFW + Software Firewalls on everyone's devices
Super-Fast Network Backbone (lots of traffic!)	A beefy Hardware Firewall
Need to Filter Content for Web Apps	Proxy Firewall + a WAF (Web Application Firewall)

Remember, these are just general ideas. Your mileage may vary!

Appendix B: Who Makes These Things? Vendors to Check Out

Curious about the companies behind these firewalls? Here are some of the well-known names in the game:

- Palo Alto Networks (https://www.paloaltonetworks.com/)
- Fortinet (https://www.fortinet.com/)
- Cisco (https://www.cisco.com/)
- Check Point (https://www.checkpoint.com/)
- Sophos (https://www.sophos.com/)
- The big cloud players: AWS, Azure, Google Cloud (they all have their own firewall offerings)
- Open-source champs: pfSense / OPNsense (great if you like to tinker!)

Want to Nerd Out More? (References)

For those who love to dive deep and get all the technical details, these resources are fantastic starting points:

- **Stallings, W. (2020).** *Network Security Essentials*. Pearson Education. (A classic textbook)
- **Cisco Systems. (2023).** *Firewall Best Practices Guide*. (Good insights from a major vendor)
- **Palo Alto Networks. (2024).** *Understanding Next-Generation Firewalls*. (Learn about the latest tech)
- **NIST SP 800-41 Rev. 1. (U.S. Government).** *Guidelines on Firewalls and Firewall Policy*. (Official government guidance – very thorough!)
- **OWASP Foundation.** *Web Application Firewalls Overview* - owasp.org (Essential for web app security)
- **Cloudflare.** ***What is a Firewall?*** - cloudflare.com/learning (A great, easy-to-understand overview from a big name in web infrastructure)

A Little About Me & Why I Do This

BSc. Electronic engineer

Senior Network Analyst | *Cybersecurity Engineer* | *Telecommunications Specialist*

So, what's my deal? I've got this personal mission, you could call it a challenge: to explain how cybersecurity works in plain English, or as I like to say, in "muggle" language. For over 12 years, I was a technical instructor for big corporate clients, and I can't even count the number of internal training sessions I ran for colleagues across Latin America. I've also had the privilege of being a university professor, teaching systems engineering to both undergrads and graduate students.

If there's one thing all those years have taught me, it's this: not everyone speaks "geek." And that's perfectly okay! My goal here, and with other stuff I create, is to cut through the dense technical jargon without losing the important stuff. I genuinely hope that if you're reading this, you feel a bit more confident and can speak up about why understanding firewalls and cybersecurity is so darn important these days. It's not just for the IT crowd anymore; it's for everyone.

→ Want to learn more or find some tools? Check out my stuff on GitHub:

github.com/leonelpedroza