Network Security Basics — Firewalls and Safe Networks

A firewall is a gatekeeper for your network — learn how networks are protected and how to stay safe on public Wi-Fi.

Introduction

Your phone and laptop are not alone — they talk to the internet all day, and the internet talks back. A network is that conversation: devices sending packets (small pieces of data) to each other. Network security is the work of making sure only the right conversations happen, and that nobody listens in or barges in.

The most famous guard is the **firewall**: a gatekeeper that checks every packet against a rule list and blocks what is not allowed. Your phone, your laptop, and your home router all have one. Behind it sit other guards: encryption on the Wi-Fi itself, a VPN that hides your traffic, and simple rules like "don't join unknown networks".

In this lesson you will learn how a firewall decides, what public Wi-Fi really risks, and the checks that keep your home network safe.

(Roman Urdu: Network security ka matlab hai apne internet connection ki hifazat. Firewall aik chowkidar hai jo har packet check karta hai — jo allowed hai andar aata hai, baqi block. Public Wi-Fi par yehi chowkidar sab se zyada zaroori hota hai.)

A beginner mistake is thinking the firewall is the whole job. A firewall blocks unwanted visitors, but it cannot stop you from handing your password to a fake website, or stop a virus you downloaded yourself. Network security is one layer among many.

Key points

- **A network is devices talking in packets.** Every message is split into small packets, each labelled with a sender and a destination address (IP address).
- **A firewall is a gatekeeper with a rule list.** "Allow web browsing out, block everything unsolicited in" is the default rule of almost every home firewall.
- **Firewalls come in layers.** Your home router has one, your laptop has one, and your phone has one. An attacker must pass all of them.
- **A port is a door number on a device.** Port 80/443 is the web, port 22 is remote login. Open ports are open doors — close the ones you do not use.
- **Public Wi-Fi is a shared room.** Anyone on the same network can try to listen. Use only HTTPS sites (the padlock), never log in to a bank on open Wi-Fi without a VPN, and turn off auto-join.
- **A VPN (Virtual Private Network) encrypts your traffic to a trusted server.** On public Wi-Fi it stops local listeners from reading what you send. Choose a reputable VPN — a free unknown VPN can be the

listener itself.

- **Your home Wi-Fi password is a network key.** Use WPA2 or WPA3 encryption, a strong Wi-Fi password, and change the router's default admin password — the one printed on the router is public knowledge.
- **Keep the router's software updated.** Routers get security fixes too, and an unpatched router guards nothing.

Examples

Example 1 — A firewall rule list, in plain words

```
Rule 1: You asked for a website  ->  let the answer in.
Rule 2: A stranger tries to connect to your laptop uninvited
        ->  block it.
Rule 3: You are sharing a file with your own printer
        ->  allow it, only on your home network.
Rule 4: Everything else  ->  block it.
```

That is the whole idea: allow what you asked for, block what you did not. Most home firewalls run exactly these rules by default — leave them on.

Example 2 — Ports are doors

```
Port 443: web browsing (HTTPS) — open, you use it all day.
Port 80:  old web browsing (HTTP) — open, but prefer 443.
Port 22:  remote login (SSH) — closed for most people.
Port 3389: remote desktop — closed unless you really use it.
```

Every open port is a door an attacker can knock on. A home user who never uses remote desktop should have port 3389 closed — an open door you never use only helps the attacker.

Example 3 — Public Wi-Fi: what an attacker sees

```
Without HTTPS or VPN:
  You open a plain HTTP site -> attacker on the same Wi-Fi
  can read the page and anything you type into it.

With HTTPS (padlock):
  You open an HTTPS site -> attacker sees you visited the
  site, but not the page, not your password, not your messages.

With HTTPS + VPN:
  Attacker sees only encrypted traffic to one VPN server —
  not even which sites you visit.
```

The padlock is the minimum. On free Wi-Fi in a cafe or university, add a VPN for anything sensitive.

Example 4 — Secure your home Wi-Fi in five minutes

```
1. Open the router settings (usually 192.168.1.1 in a browser).
2. Change the admin password from the default printed on the router.
3. Set Wi-Fi security to WPA2 or WPA3 (never "Open" and never old WEP).
4. Set a long Wi-Fi password (16+ characters, like CS.10 taught).
5. Check for a firmware update and install it.
```

Do this once, and your home network stops being the easiest target on the street.

Quick recap

- A network moves packets between devices; a firewall checks them against rules.
- Allow what you asked for; block everything unsolicited.
- Ports are doors — close the ones you do not use.
- Public Wi-Fi is shared: use HTTPS always, a VPN for sensitive work, no auto-join.
- Home Wi-Fi needs WPA2/WPA3, a strong password, a changed admin password, and updates.

Common mistakes

1. **Turning the firewall off "because it blocks something"** — a blocked program is usually a program that should not be talking to the internet. Fix: allow that one program, keep the firewall on.
2. **Leaving the router admin password as default** — the default is printed on the router and published online. Fix: change it the day you install the router.
3. **Using WEP or open Wi-Fi at home** — WEP is broken in minutes; open Wi-Fi has no lock at all. Fix: WPA2 or WPA3 only.
4. **Trusting any free VPN** — a free VPN has to earn money somehow, and selling your browsing data is the usual way. Fix: use a reputable paid VPN, or your university's official one.
5. **Auto-joining every remembered network** — your phone will happily join a fake network with a familiar name ("Free WiFi") and hand it your traffic. Fix: turn off auto-join, forget networks you do not trust.

Practice

1. Check your laptop or phone: is its firewall on right now? Write down where you found the switch.
2. List three networks your phone remembers. Do you still trust all three? Forget any you do not recognise.
3. Next time you are on public Wi-Fi, check: are the sites you open showing the padlock (HTTPS)? Write down one site that did not.
4. Log in to your home router and check two things: the Wi-Fi security type (WPA2/WPA3?) and whether a firmware update is waiting.

5. Explain to a friend why a VPN helps on cafe Wi-Fi but is not needed the same way at home — in two sentences.

Practice quiz

1. What does a firewall do?

- It speeds up the internet
- It checks network traffic against a rule list and blocks what is not allowed
- It stores your passwords
- It encrypts every website

Answer: It checks network traffic against a rule list and blocks what is not allowed

2. Why is public Wi-Fi risky?

- It is slow
- Anyone on the same network can try to listen to your traffic
- It uses too much battery
- It only allows HTTPS sites

Answer: Anyone on the same network can try to listen to your traffic

3. What should you change first on a new home router?

- Its colour
- The default admin password printed on the router, and use WPA2 or WPA3 Wi-Fi security
- Its brand name
- Nothing — defaults are safe

Answer: The default admin password printed on the router, and use WPA2 or WPA3 Wi-Fi security

---

Watch the Code Scope channel: https://www.youtube.com/@CodeScopePK — this lesson's own video joins the channel when it is recorded.

Read online: https://scopetreasure.com/notes/cs-network-security · More free tools and notes at https://scopetreasure.com