

Networking and Firewalls

Adrianna Holden-Gouveia

Website: aholdengouveia.name

: [aholdengouveia](https://github.com/aholdengouveia)

: [aholdengouveia](https://twitter.com/aholdengouveia)

Accessibility Notice

This document is also available in HTML format at:

Link: <https://aholdengouveia.name/InfoSec/labs/firewalls.html>

The HTML version provides enhanced accessibility features including keyboard navigation, screen reader support, responsive design, dark mode support, and high contrast options.

Learning Outcomes

By the end of this lab, you will be able to:

- Explain what a firewall does, and how allow and deny rules work
- Compare how two different networks look from the internet
- Create and test firewall rules for a scenario
- Explain how rule order and the default policy change what a firewall allows

Lab Instructions

Everything in this lab runs in your web browser, so you don't need to install anything. Both tools are linked under Resources.

Screenshots

This lab asks for 6 screenshots. Each screenshot should have your name, term, and year. One of the easiest ways to do that is make a text document with your name and term/year on your computer and save it to use all term. Any screenshots that don't include this information won't be counted.

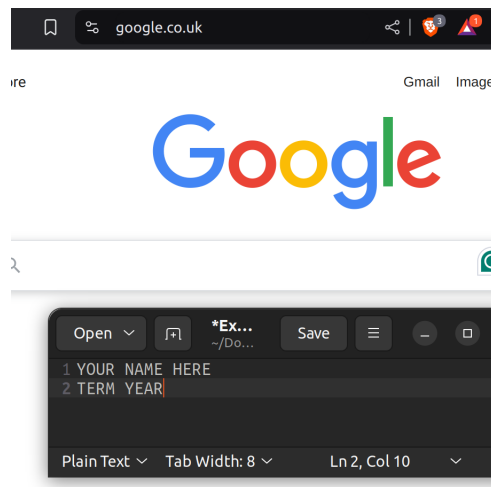


Figure 1: This is an image of what each of your screenshots should look like

Part 1: Your Network from the Outside

ShieldsUP! is a free tool from Gibson Research Corporation. It checks your internet connection from the outside, the way an attacker would see it, and shows which common ports are open. This is a port scan, the same kind of scan attackers use during network reconnaissance to find a way in. It only checks the connection you're using, so you're only testing your own network.

Run it from **two different places**, such as home and school, or home and your phone's hotspot. Only use networks you're allowed to use. If your school doesn't allow this kind of test on its network, use home and your phone's hotspot instead.

At each place:

1. Go to ShieldsUP!, select Proceed, then select Common Ports.

2. Take a screenshot of the results. Each port is shown as Open, Closed, or Stealth.
3. Write down where you were, such as home Wi-Fi or a phone hotspot, the date, and how many ports were Open, Closed, and Stealth.

Then compare the two places:

4. What was different between the two results? What was the same?
5. Why do you think they were different? Think about who runs each network, and what firewall or router is protecting it.
6. Which network looks safer from the outside, and why?
7. If any port was Open, what service uses that port? Does it need to be open?

Part 2: Build Firewall Rules

Open my Firewall Simulator. You're setting up the firewall for a small office's web server. The office network is 192.168.1.0/24. The server needs to:

- Let anyone visit the website, using HTTP (port 80) and HTTPS (port 443)
 - Let only the office use SSH (port 22) to manage the server
 - Block everything else
8. Choose a default policy, and add rules to meet these needs.
 9. Select Test all traffic, and take a screenshot of your rules and the results.
 10. Explain each of your rules in a sentence, and why you chose your default policy.
 11. Add one piece of test traffic of your own, and explain what happened to it and why.

Part 3: Rule Order and the Default Policy

12. Select Load the rule order example, then Test all traffic. Take a screenshot. The office admin can't log in with SSH. Explain why, using what the simulator says.
13. Fix it by changing the order of the rules, test again, and take a screenshot. Explain what you changed and why it worked.
14. Change the default policy to allow all, and test again. What traffic gets through now that shouldn't? A deny all default works like an allowlist, and allow all works like a denylist. Why is deny all usually the safer default?

Part 4: What Firewalls Can't Do

15. A firewall allowed the web traffic in Part 2. Give one way an attacker could still cause harm through allowed traffic.
16. Give one threat a firewall can't protect against, such as phishing, and explain why.

Deliverables

One file that includes:

- Part 1: your 2 ShieldsUP! screenshots, where and when you ran each one, and your answers to the comparison questions
- Part 2: your screenshot of your rules and results, and your explanations
- Part 3: your 2 screenshots, and your explanations
- Part 4: your answers

Resources

References, a video, a PowerPoint and some notes are available at my website
Link: <https://www.aholdengouveia.name/InfoSec/NetworkSecurity.html>

ShieldsUP! from Gibson Research Corporation, for Part 1 Link: <https://www.grc.com/shieldsup>

My Firewall Simulator, for Parts 2 and 3 Link: <https://www.aholdengouveia.name/InfoSec/labs/firewall-simulator.html>

Common port numbers and the services that use them Link: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers