Module 1: The foundation

Cloud setup & access

Cloud setup & access

Prerequisites

- **Goal:** A secure environment before deploying code.
- **Providers:** DigitalOcean, AWS EC2, Linode, or Raspberry Pi.

Cloud setup & access

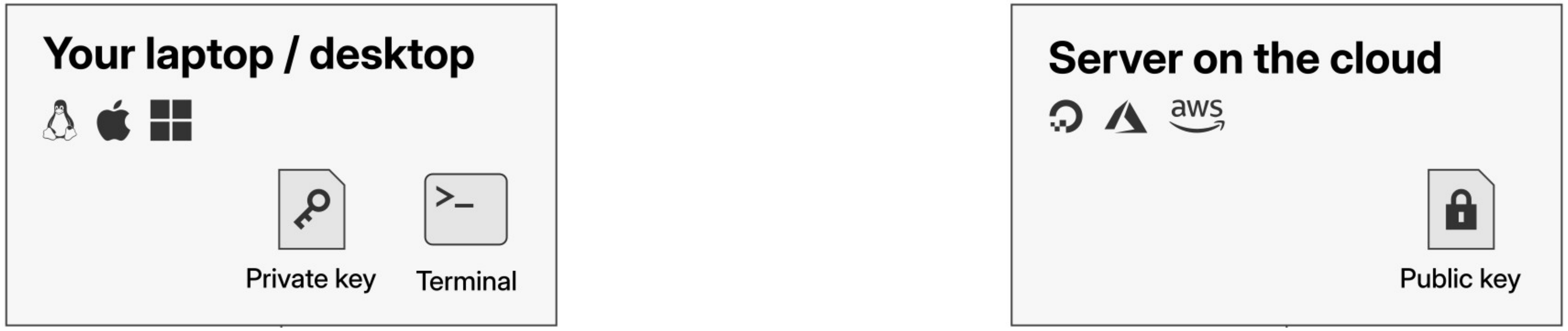
Prerequisites

- **Goal:** A secure environment before deploying code.
- **Providers:** DigitalOcean, AWS EC2, Linode, or Raspberry Pi.

Learning objectives

- Deploy a server running **Ubuntu 24.04 LTS**.
- Generate and configure **SSH Keys** (Ed25519).
- Understand the **"Lock & Key"** security model.
- **Security:** Disable password authentication completely.

How SSH keys work



Your laptop / desktop

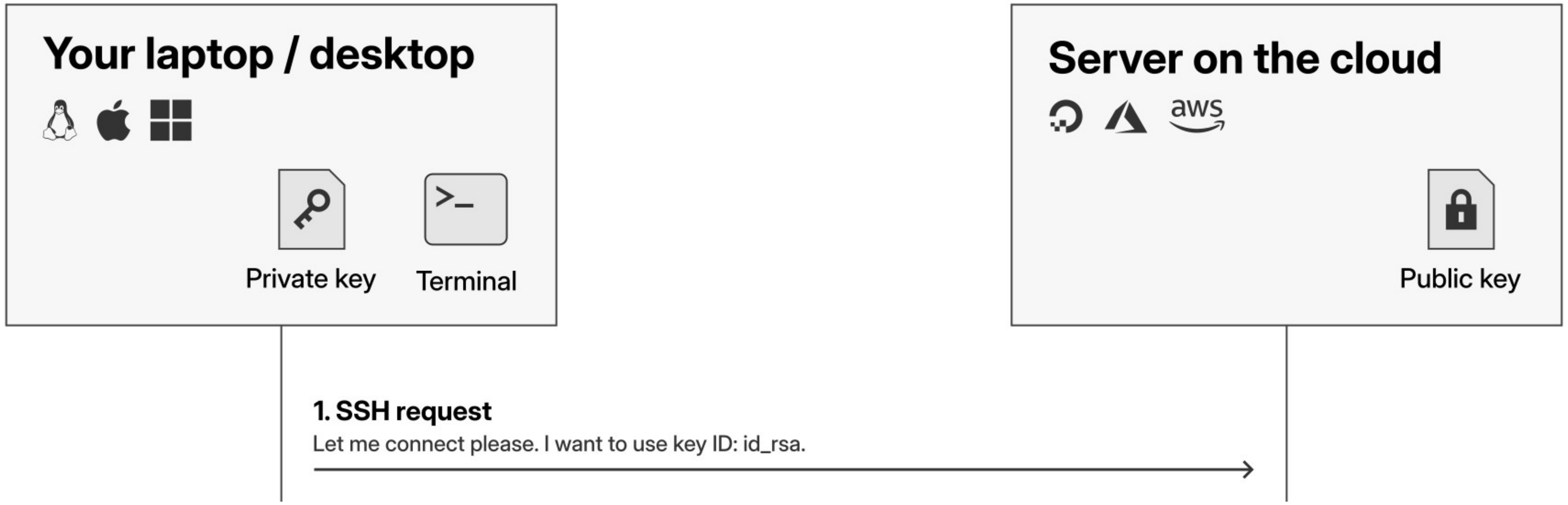
Private key

Terminal

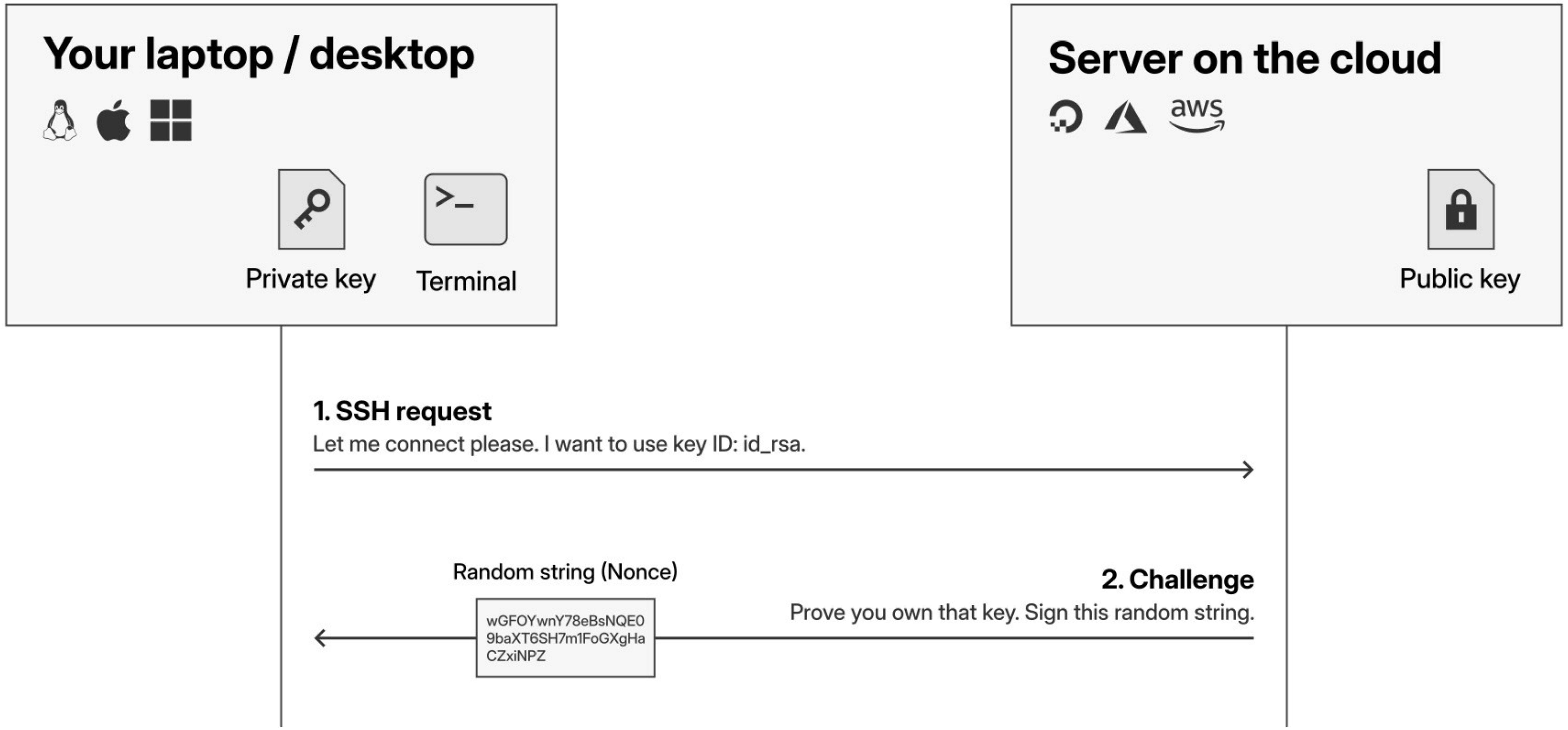
Server on the cloud

Public key

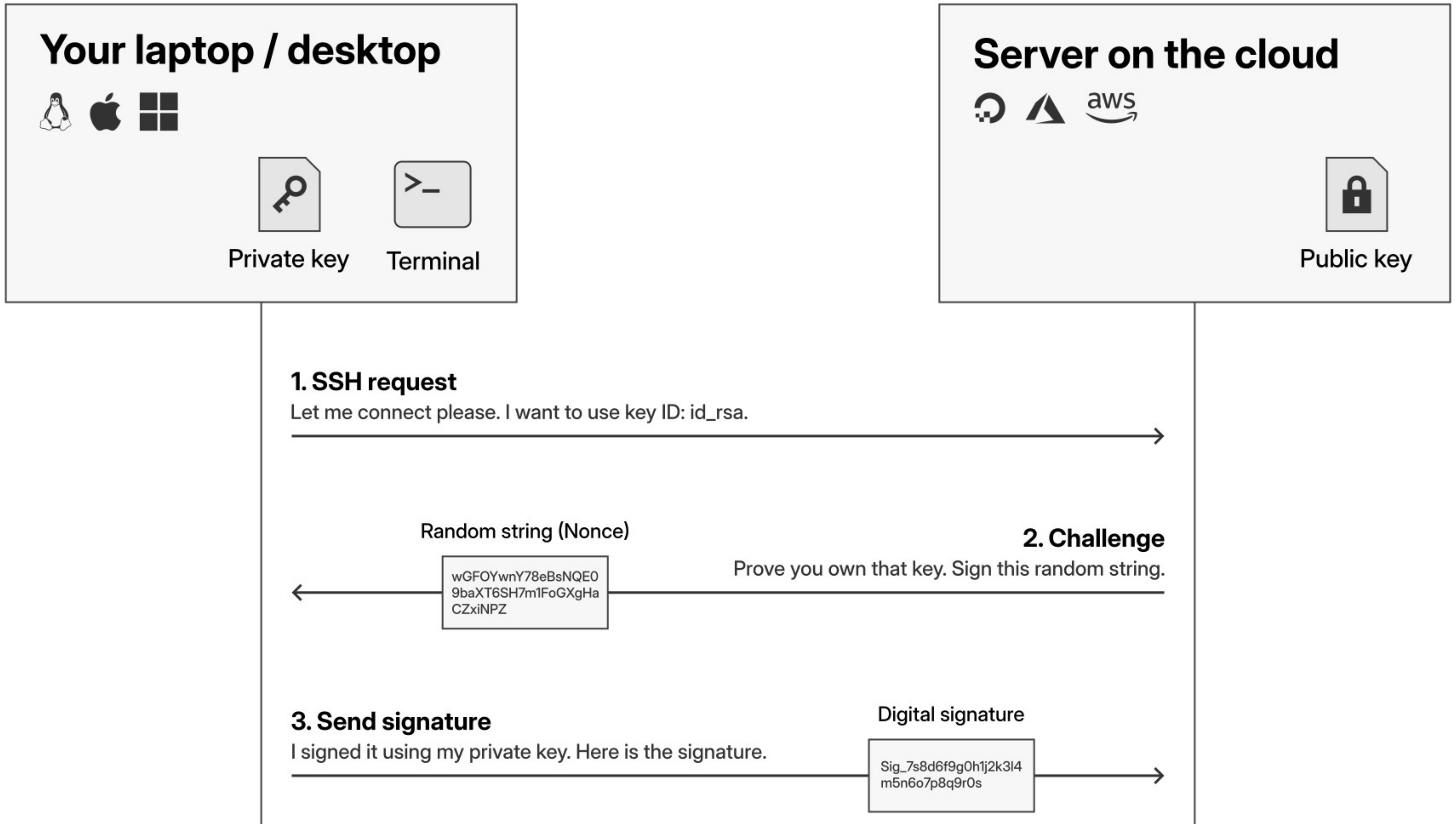
How SSH keys work



How SSH keys work



How SSH keys work

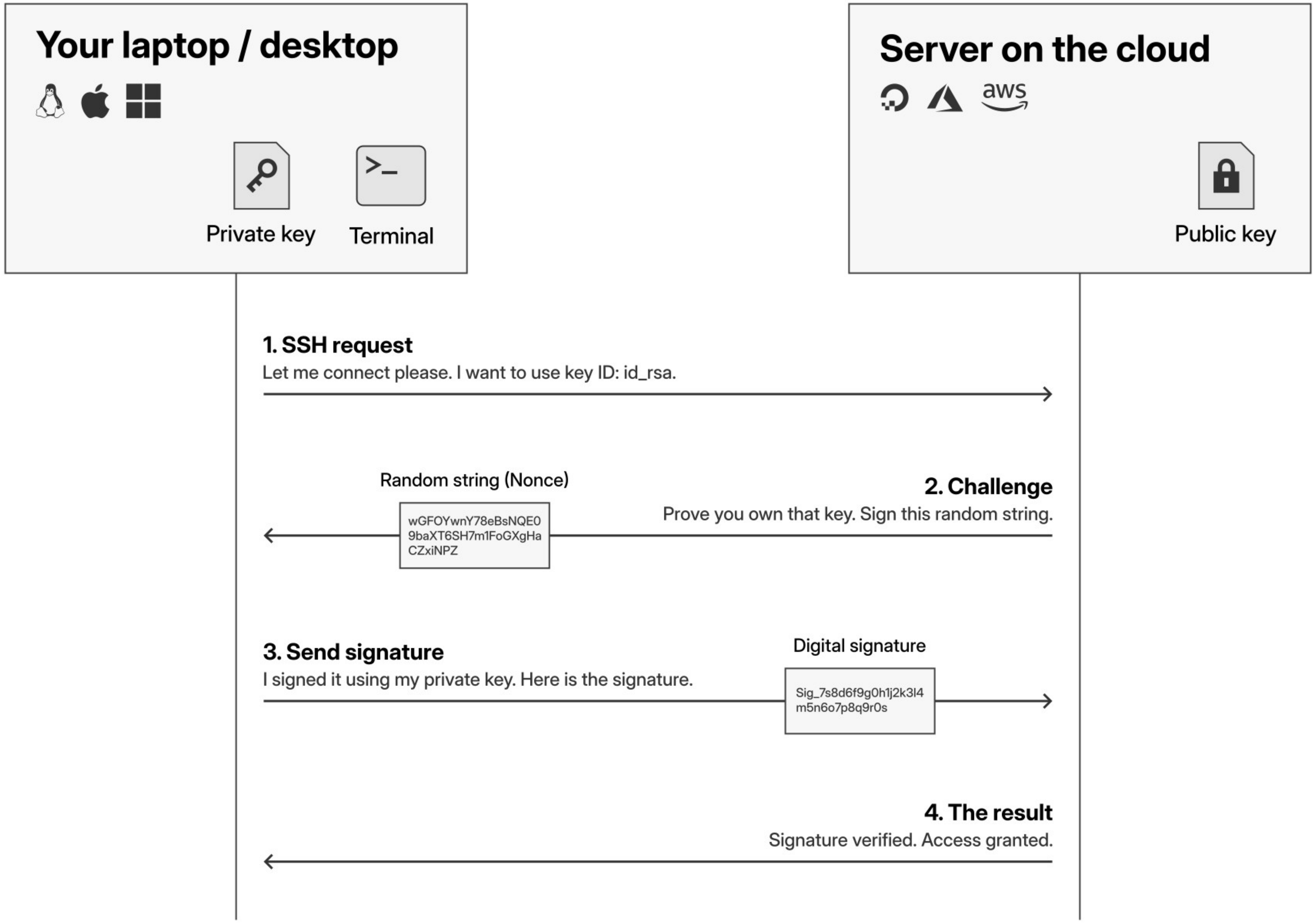


1. SSH request
Let me connect please. I want to use key ID: id_rsa.

2. Challenge
Prove you own that key. Sign this random string.

3. Send signature
I signed it using my private key. Here is the signature.

How SSH keys work



1. SSH request
Let me connect please. I want to use key ID: id_rsa.

2. Challenge
Prove you own that key. Sign this random string.

3. Send signature
I signed it using my private key. Here is the signature.

4. The result
Signature verified. Access granted.

What is next?

- **Current status:** You now have a clean, secure Ubuntu server.
- **The risk:** The server is still exposed to the open internet.
- **Next steps:**
  - **Firewall configuration:** Setting up UFW (Uncomplicated Firewall).
  - **Brute force protection:** Installing Fail2Ban to block attackers.
  - **Emergency access:** How to use the recovery console.

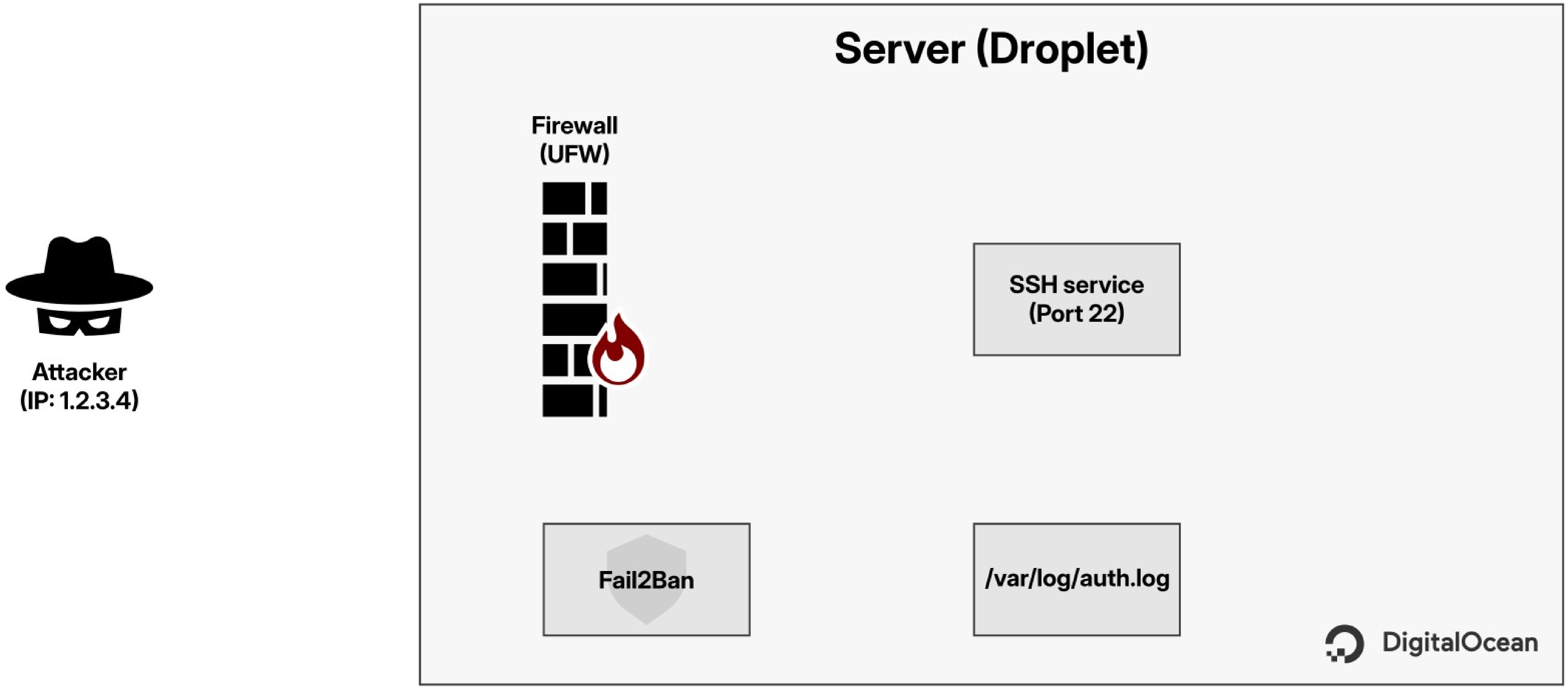
Module 1: The foundation

The firewall strategy

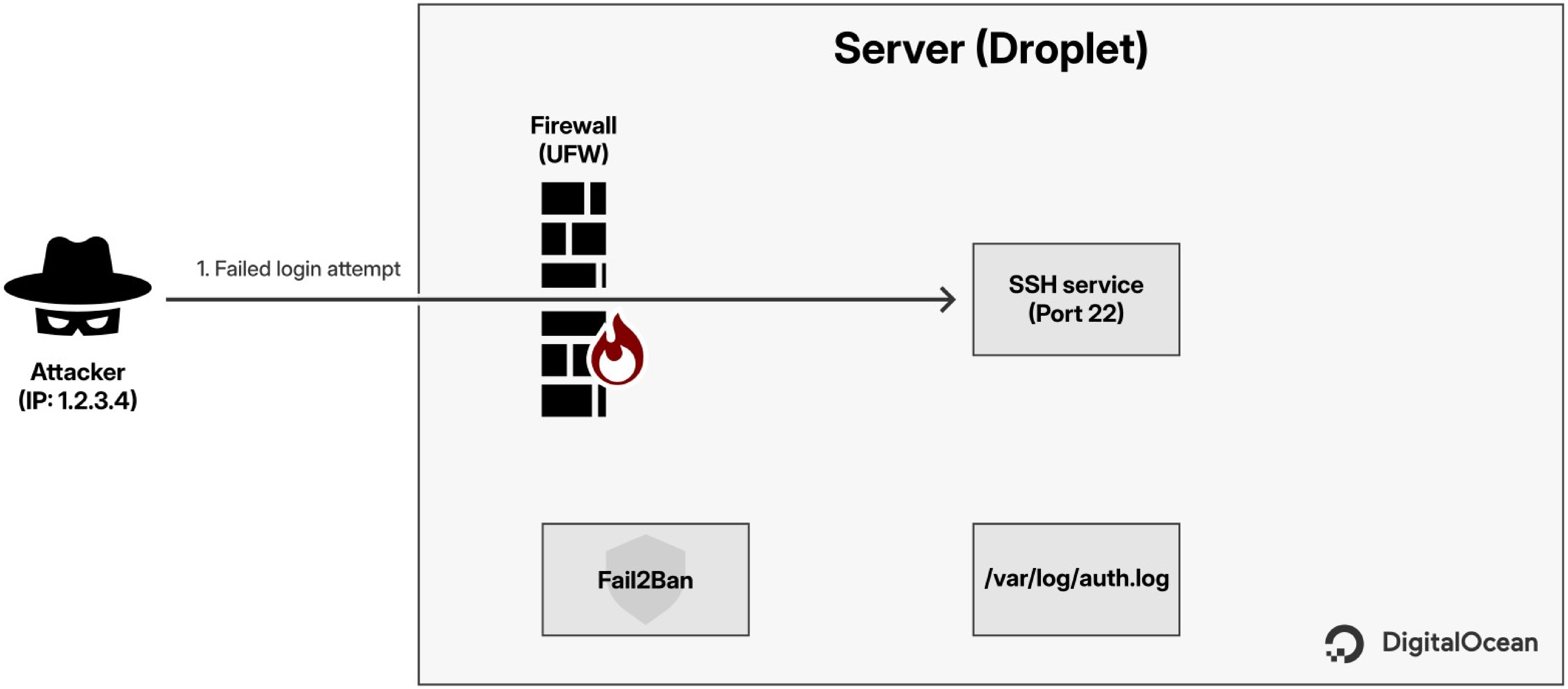
The firewall strategy

- **Problem:** Default Linux servers accept traffic on all ports.
- **Solution:** Use UFW to block everything by default.
- **Automation:** Use Fail2Ban to block bots instantly.
- **Safety net:** Using the DigitalOcean Recovery Console.

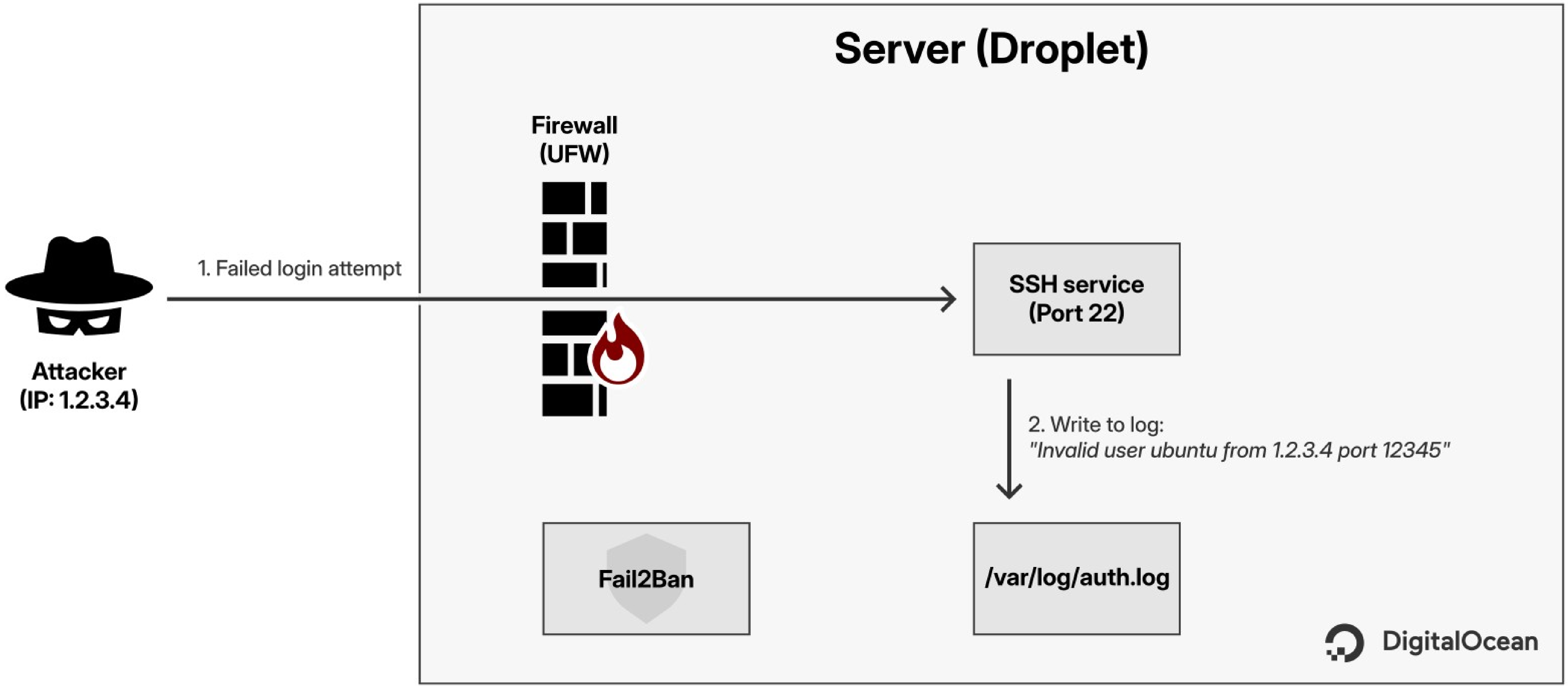
How Fail2Ban works



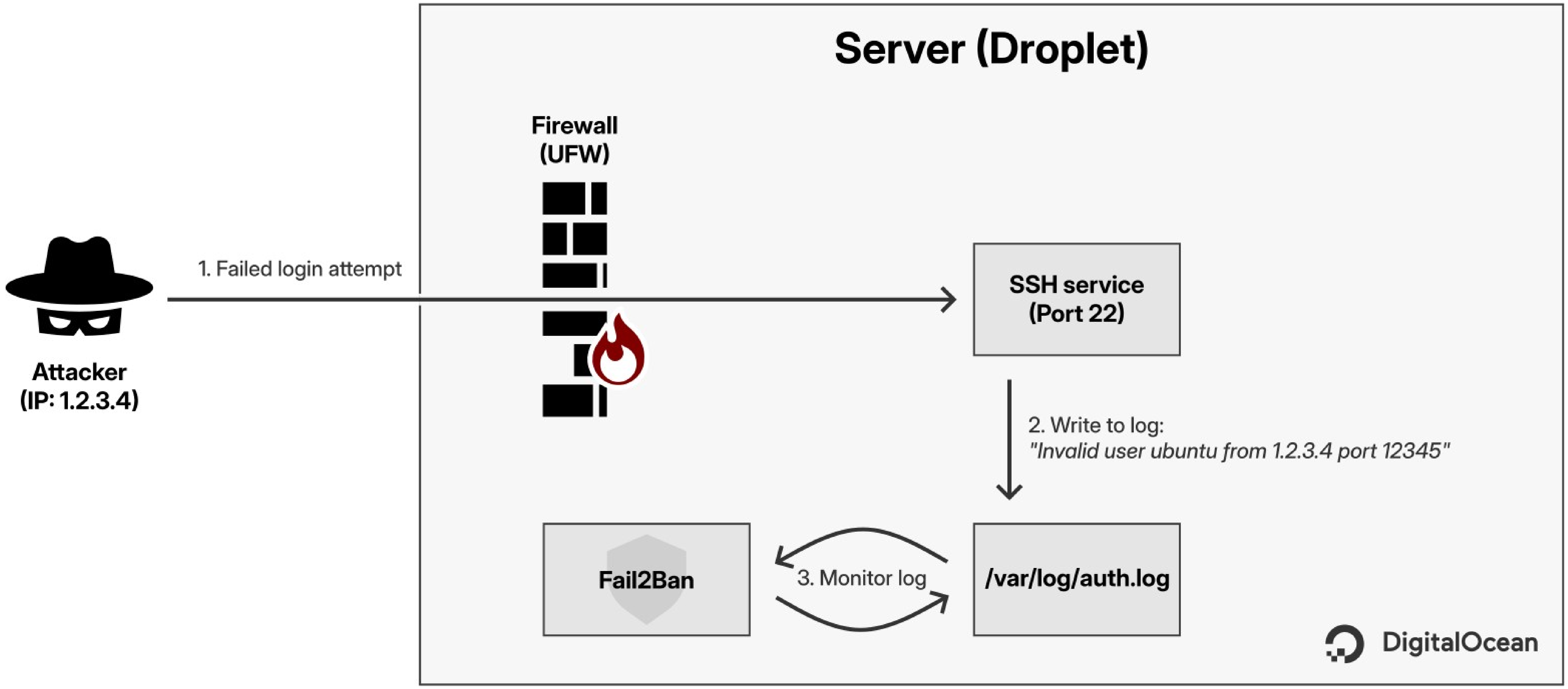
How Fail2Ban works



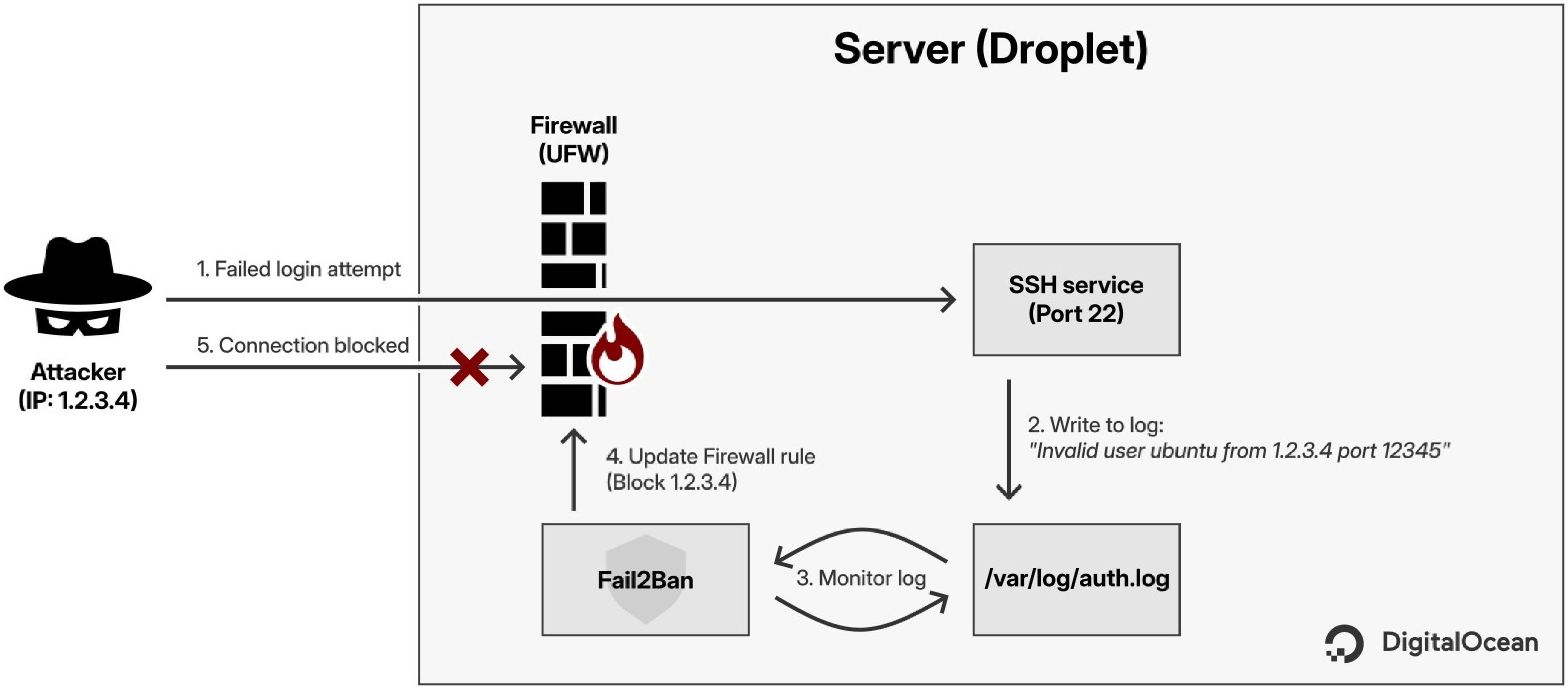
How Fail2Ban works



How Fail2Ban works



How Fail2Ban works



Server (Droplet)
Firewall
(UFW)
Attacker
(IP: 1.2.3.4)
1. Failed login attempt
5. Connection blocked
SSH service
(Port 22)
2. Write to log:
"Invalid user ubuntu from 1.2.3.4 port 12345"
4. Update Firewall rule
(Block 1.2.3.4)
Fail2Ban
3. Monitor log
/var/log/auth.log
DigitalOcean