Security: Background

In this section, we will discuss the components and fundamental concepts related to infrastructure and software security. The topics to be discussed in this chapter are as follows:

- Importance of security
- Encryption and Decryption
- Credentials and automatic rotation
- DDoS attacks
- Firewalls, and their necessity

If the reader believes themselves to already be familiar with the listed concepts, then they can feel free to skip this section and move on to the rest of the chapter.

Importance of Security

There might be readers who find the concept of securing infrastructure that they do not own to be rather uneasy. After all its their infrastructure, and we are their customer, should not the responsibility of fighting against intrusion and protecting our data be part of the contract?

Well, yes and no. While cloud infrastructure and environments do provide with some basic level of security to the prospective user, this is quite limited and easy to circumvent for any malicious agent worth their salt. Therefore, more often than not, the responsibility of protecting our data and the infrastructure being rented falls upon our own shoulders.

Failure to do so can result in the loss of crucial business data and/or cause the whole system to crash and cease functioning.

Encryption and Decryption

Converting data into an unreadable format, such that even if a malicious agent should get hold of the data, they will not be able to make use of it is called **encryption**, while the process of obtaining the original data from the converted data is called **decryption**. Both processes are performed using a cryptographic token called a **key**, and an **encryption algorithm**, the sequence of operations performed on the data using the key as a variable in order to encrypt and/or decrypt it.

Credentials and Automatic Rotation

Effective credential management is vital to maintaining secure access to infrastructure. Credentials (such as usernames, passwords, API keys, and tokens) are often required to authenticate users or systems, but when mismanaged, they can become points of vulnerability.

Automatic rotation of credentials is a practice that enhances security by periodically updating credentials without manual intervention. Regular rotations help limit the potential exposure window if a credential is compromised. Automations and services that make credential rotation more convenient will be mentioned in later sections.

DDoS Attacks

A Distributed Denial of Service (DDoS) attack aims to overwhelm an infrastructure or service with excessive traffic from multiple sources, causing it to slow down or crash entirely. These attacks are often orchestrated by malicious entities looking to disrupt operations or exploit vulnerabilities for personal gain.

Cloud providers offer DDoS protection services, which can detect unusual traffic patterns, identify DDoS threats, and automatically scale resources to absorb the increased traffic. However, the best DDoS defense strategy combines providerbased solutions with proper architectural planning, such as deploying services across multiple regions to distribute the load effectively.

Firewalls and Their Necessity

Firewalls act as a critical line of defense by monitoring and controlling incoming and outgoing network traffic based on predefined security rules. They are essential for enforcing boundaries within and outside your cloud infrastructure.

By setting up firewalls, organizations can block unauthorized access while permitting trusted communication, reducing exposure to external threats. Firewalls can operate at various levels, from network firewalls that control access to entire subnets to web application firewalls (WAFs) that specifically filter HTTP/HTTPS traffic for web applications.