Security & Fail2Ban

Security in a public cloud environment requires a multi-layered approach. This page documents the hardening process of the Ubuntu instance and the implementation of automated defense mechanisms.

1. Cloud Infrastructure Firewall (OCI)

Before traffic reaches the server, it must pass through the **OCI Security Lists**. To minimize the attack surface, only essential ports are exposed to the public internet.

Configured Ingress Rules:

Port	Protocol	Source	Description
22	TCP	0.0.0.0/0	SSH (Admin Access)
80	TCP	0.0.0.0/0	HTTP (Redirects & Challenges)
443	TCP	0.0.0.0/0	HTTPS (Encrypted Web)

2. Brute-Force Protection (Fail2Ban)

To prevent automated SSH attacks, **Fail2Ban** was installed. It monitors system logs for failed login attempts and temporarily bans the offending IP addresses.

Installation:

```
sudo apt install fail2ban -y
```

Configuration: A local configuration file was created at `/etc/fail2ban/jail.local` to protect the SSH service.

```
[sshd]
enabled = true
port = 22
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600
```

Management Commands:

```
# Check banning status
sudo fail2ban-client status sshd

# Unban a specific IP
sudo fail2ban-client set sshd unbanip <IP_ADDRESS>
```

3. Automated SSL/TLS (Certbot)

While Cloudflare provides edge encryption, the connection between Cloudflare and the OCI server is secured using **Let's Encrypt** certificates.

Installation & Certificate Generation:

```
sudo apt install certbot python3-certbot-apache -y
sudo certbot --apache -d your-domain.com
```

The certificates are automatically renewed via a systemd timer, ensuring zero downtime due to expiration.

4. Security Hardening Checklist

Additional steps taken to secure the OS:

- **System Updates:** Configured `unattended-upgrades` for automatic security patches.
- **Non-Root Access:** Direct root login via SSH is disabled; all administrative tasks are performed via `sudo`.
- **Log Monitoring:** Regular auditing of `/var/log/apache2/access.log` to identify suspicious patterns.

— **Next Step:** Proceed to the **Automated Backups** section to see how cloud data is preserved.