OCI & Cloudflare Setup

This page documents the initial deployment of the cloud instance and the configuration of the external network layer using Cloudflare.

1. Oracle Cloud Infrastructure (OCI) Setup

The primary compute instance is hosted on OCI using an **Ampere A1 (ARM)** or **AMD** instance with Ubuntu Server.

Key Steps in OCI Console:

- **Instance Creation:** Deployment of an Ubuntu 22.04 LTS instance.
- **VCN & Security Lists:** Configuration of Ingress Rules to allow specific traffic:
  - Port 22 (SSH) - Restricted access.
  - Port 80 (HTTP) - Open for initial verification and ACME challenges.
  - Port 443 (HTTPS) - Primary port for encrypted web traffic.

Internal Firewall Adjustment: Since Ubuntu on OCI comes with pre-configured iptables rules, they were updated to allow web traffic:

```
# Allow HTTP and HTTPS through the local iptables
sudo iptables -I INPUT 6 -m state --state NEW -p tcp --dport 80 -j ACCEPT
sudo iptables -I INPUT 6 -m state --state NEW -p tcp --dport 443 -j ACCEPT

# Save the rules persistent
sudo netfilter-persistent save
```

2. Cloudflare Integration

Cloudflare is used as the DNS provider and as a security proxy to hide the origin server's IP address.

DNS Configuration:

- An **A-Record** was created pointing to the OCI instance's public IP.
- **Proxy Status:** Set to “Proxied” (Orange Cloud) to ensure all traffic passes through Cloudflare's edge servers first.

SSL/TLS Settings:

- **SSL Mode:** Set to **“Full (Strict)”**. This ensures end-to-end encryption between the user, Cloudflare, and the OCI server.
- **Always Use HTTPS:** Enabled to force all unencrypted requests to upgrade to a secure connection.

3. Domain Resolution Check

Once the DNS propagation was complete, the connection was verified using the terminal to ensure the Cloudflare IP is being returned instead of the real server IP.

```
# Check DNS resolution
nslookup your-domain.com

# Verify that the web server is responding via Cloudflare
curl -I https://your-domain.com
```

4. Security Benefit

By using this hybrid setup:

```
1. **IP Masking:** Attackers cannot see the real IP of the Oracle instance.
2. **DDoS Protection:** Cloudflare automatically mitigates volumetric
attacks before they reach the server.
3. **WAF:** Basic firewall rules at the edge block common malicious
patterns.
```

From:
http://wiki.berkayhasip.com/ - **BerkayWiki**

Permanent link:
http://wiki.berkayhasip.com/doku.php?id=project:cloud:setup

Last update: **2026/03/11 09:18**