

# KOMPUTASI AWAN



Oleh :

Mochammad Iqbal  
Islamay Arsy

1941720231

TI 3F

## # 04 - Virtual Cloud Network (VCN)

### ## Tujuan Pembelajaran

1. Mengetahui layanan Oracle Cloud Infrastructure Networking
2. Mampu mengaktifkan port 80 melalui Virtual Cloud Network (VCN) di layanan Oracle Cloud
3. Mampu memasang Apache server dan mengonfigurasi IP tables Firewalls

### ## Hasil Praktikum

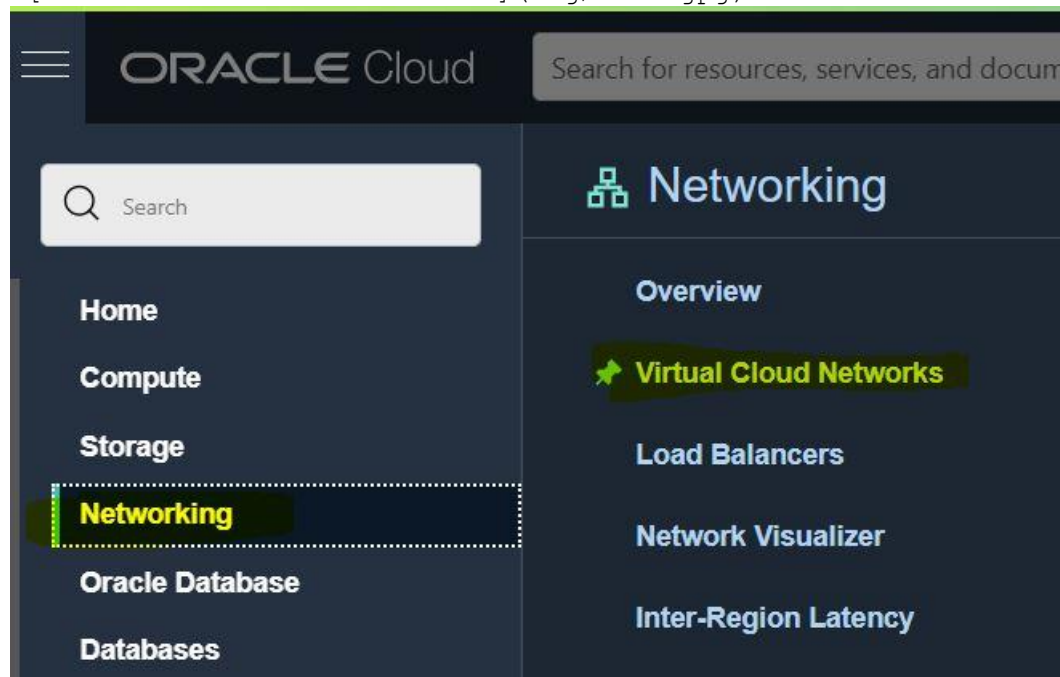
#### ### Praktikum 1: Mengaktifkan Port 80 melalui VCN di Oracle Cloud

Langkah 1: Silakan login ke akun Oracle Cloud Anda masing-masing melalui tautan ini

<https://www.oracle.com/cloud/sign-in.html>

Langkah 2: Setelah berhasil login dan ada di beranda Oracle Cloud akun Anda, silakan pilih menu di pojok kiri atas, lalu pilih menu Networking > Virtual Cloud Networks

![Screenshot Dashboard Oracle] (img/satu.jpg)



Langkah 3: Pastikan VCN sudah ada, biasanya jika berhasil telah membuat VM dari modul pertemuan sebelumnya maka VCN akan tampil di sini. Silakan klik nama VCN tersebut.

![Screenshot Dashboard Oracle] (img/dua.jpg)



Langkah 4: Pilih Security Lists di panel kiri (Resources), lalu pilih Default Security List di tabel yang tersedia.

! [Screenshot Dashboard Oracle] (img/tiga.jpg)

## Resource Search Results

1 results found

Filter by resource types:

Choose one or more resource types to filter the results

Display Name	Resource Type	OCID	Compartment	Status	Time Created
<a href="#">Default Security List for vcn-20210914-1409</a>	Security Lists	...oars5q <a href="#">Show</a> <a href="#">Copy</a>	...a3tdnq <a href="#">Show</a> <a href="#">Copy</a>	<span>●</span> Available	Tue, Sep 14, 2021, 07:13:19 UTC
<div><div><div>SL</div><div>AVAILABLE</div></div><div><a href="#">Default Security List for vcn-20210914-1409</a> <b>Resource Type:</b> Security Lists <b>OCID:</b> ocid1.securitylist.oc1.ap-sydney-1.aaaaaaaawepp6qxslvfqsm2js4jgmt7cutuaa3o56ptqwsdnlxhoars5q <a href="#">Copy</a> <b>Compartment:</b> ocid1.tenancy.oc1..aaaaaaaawlnwj72v2beb27zozuzoaxbf52uysy3a4u77a4uq467nka3tdnq <a href="#">Copy</a> <b>Time Created:</b> Tue, Sep 14, 2021, 07:13:19 UTC <b>Matches:</b><ul style="list-style-type: none"><li>• displayName: Default <b>Security List</b> for vcn-20210914-1409</li></ul></div></div>					
Showing 1 Item < 1 of					

Langkah 5: Klik tombol biru Add Ingress Rules untuk menambahkan port.

! [Screenshot Dashboard Oracle] (img/empat.jpg)

Networking » Virtual Cloud Networks » vcn-20210914-1409 » Security List Details

SL

AVAILABLE

### Default Security List for vcn-20210914-1409

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

[Move Resource](#) [Add Tags](#) [Terminate](#)

Security List Information

Tags

**OCID:** ...oars5q [Show](#) [Copy](#)

**Compartment:** e941720140 (root)

**Created:** Tue, Sep 14, 2021, 07:13:19 UTC

Resources

[Ingress Rules \(3\)](#)  
[Egress Rules \(1\)](#)

[Add Ingress Rules](#) [Edit](#) [Remove](#)

	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Prot ocol	

[Terms of Use and Privacy](#) [Cookie Preferences](#)

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

! [Screenshot Dashboard Oracle] (img/lima.jpg)

## Add Ingress Rules

### Ingress Rule 1

Allows TCP traffic 80

☒ Stateless ⓘ

To enable bidirectional traffic flow, make sure a complementary rule in the opposite direction exists.

Source Type

CIDR

Source CIDR

0.0.0.0/0

IP Protocol ⓘ

TCP

Specified IP addresses: 0.0.0.0-255.255.255.255 (4.294.967.296 IP addresses)

Source Port Range *Optional* ⓘ

All

Examples: 80, 20-22

Destination Port Range *Optional* ⓘ

80

Examples: 80, 20-22

Description *Optional*

Allow HTTP connections

Maximum 255 characters

+ Another Ingress Rule

Add Ingress Rules

[Cancel](#)

Isilah ingress rule dengan nilai-nilai seperti gambar di atas atau teks berikut:

Stateless: Checked

Source Type: CIDR

Source CIDR: 0.0.0.0/0

IP Protocol: TCP

Source port range: (biarkan kosong)

Destination Port Range: 80

Description: Allow HTTP connections

Terakhir, klik tombol Add Ingress Rules. Sekarang koneksi HTTP telah diizinkan. VCN Anda telah dikonfigurasi untuk Apache server.

Anda telah sukses membuat ingress rule yang berfungsi untuk membuka port 80 HTTP server VM Anda agar bisa diakses oleh publik.

-----  
### Praktikum 2: Setup Apache di VM

Langkah 1: Buka instance Anda melalui menu Compute > Instances, kemudian copy IP public VM yang ingin kita akses untuk diatur web server Apache.

Langkah 2: Lakukan akses ke VM atau server kita dengan perintah berikut ini.

```
ssh -i "private.key" ubuntu@140.83.56.4
```

Pada font warna merah, silakan sesuaikan dengan private key dan IP public milik Anda. Anda bisa menggunakan CMD, powershell, putty, atau terminal (untuk pengguna Linux atau Mac OS).

![[Screenshot Dashboard Oracle](img/enam.jpg)]

```
ubuntu@vm-ubuntu2:~$ ssh -i "private.key" ubuntu@168.138.101.36
Warning: Identity file private.key not accessible: No such file or directory.
The authenticity of host '168.138.101.36 (168.138.101.36)' can't be established.
ECDSA key fingerprint is SHA256:Vm2tmG77IWqj8zAGfz5iG06H8vQOk33SdMV/pWjGrOw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '168.138.101.36' (ECDSA) to the list of known hosts.
ubuntu@168.138.101.36: Permission denied (publickey).
ubuntu@vm-ubuntu2:~$
```

Langkah 3: Setelah terkoneksi dengan VM Anda, silakan lakukan perintah berikut baris demi baris untuk menginstall Apache server.

```
sudo apt update
```

```
sudo apt -y install apache2
```

![[Screenshot Dashboard Oracle](img/tujuh.jpg)]

```
ubuntu@vm-ubuntu2:~$ sudo apt update
Hit:1 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Fetched 328 kB in 2s (147 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
29 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@vm-ubuntu2:~$
```

![[Screenshot Dashboard Oracle](img/delapan.jpg)]



```

ubuntu@vm-ubuntu2:~$ sudo apt -y install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
  openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0 ssl-cert
0 upgraded, 11 newly installed, 0 to remove and 29 not upgraded.
Need to get 1866 kB of archives.
After this operation, 8088 kB of additional disk space will be used.
Get:1 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal/main amd64
libapr1 amd64 1.6.5-1ubuntu1 [91.4 kB]
Get:2 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal/main amd64
libaprutil1 amd64 1.6.1-4ubuntu2 [84.7 kB]
Get:3 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal/main amd64
libaprutil1-dbd-sqlite3 amd64 1.6.1-4ubuntu2 [10.5 kB]
Get:4 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal/main amd64
libaprutil1-ldap amd64 1.6.1-4ubuntu2 [8736 B]
Get:5 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal/main amd64
libjansson4 amd64 2.12-1build1 [28.9 kB]
Get:6 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal/main amd64
liblua5.2-0 amd64 5.2.4-1.1build3 [106 kB]
Get:7 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal-updates/mai
n amd64 apache2-bin amd64 2.4.41-4ubuntu3.6 [1180 kB]
Get:8 http://ap-sydney-1-ad-1.clouds.archive.ubuntu.com/ubuntu focal-updates/mai
n amd64 apache2-data all 2.4.41-4ubuntu3.6 [159 kB]

```

Langkah 4: Jalankan service Apache dengan perintah berikut.

```
sudo systemctl restart apache2
```

Langkah 5: Secara default pada VM Ubuntu kita untuk firewall itu statusnya disabled (tidak aktif), maka kita perlu mengaktifkannya dengan melakukan update pada iptabels terlebih dahulu. Lakukan perintah berikut baris demi baris.

```
sudo iptables -I INPUT 6 -m state --state NEW -p tcp --dport 80 -j
ACCEPT
```

```
sudo netfilter-persistent save
```

![[Screenshot Dashboard Oracle](img/sembilan.jpg)]

```

ubuntu@vm-ubuntu2:~$ sudo iptables -I INPUT 6 -m state --state NEW -p tcp --dpor
t 80 -j ACCEPT
ubuntu@vm-ubuntu2:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
ubuntu@vm-ubuntu2:~$

```

Langkah 6: Sekarang Anda dapat melakukan uji server VM Anda dengan perintah curl localhost atau buka browser di komputer/laptop pribadi Anda dan arahkan ke IP public VM yang Anda miliki. Seharusnya jika sukses, maka akan tampil seperti gambar berikut ini.

![[Screenshot Dashboard Oracle](img/sepuluh.jpg)]

