**On-Premises Infrastructure**

**Introduction**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DEVICE** | **INTERFACE** | **IP ADDRESS** | **SUBNET** | **DEFAUTL GATEWAY** |
| ROUTER 1 | Gig0/0 | 209.165.200.225 | 255.255.255.248 | N/A |
| S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A |
| ROUTER 2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A |
| ROUTER 3 | S0/0/0 | 172.16.3.1 | 255.255.255.0 | N/A |
| Gig0/0 | 10.2.2.1 | 255.255.255.252 | N/A |
| FIREWALL | VLAN 1 (E0/1) | 192.168.1.1 | 255.255.255.0 | N/A |
| VLAN 2 (E0/0) | 209.165.200.226 | 255.255.255.248 | N/A |
| VLAN 3 (E0/2) | 192.168.2.1 | 255.255.255.0 | N/A |
| DMZ Server |  | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 |
| PC-B |  | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-C |  | 172.16.3.3 | 255.255.255.0 | 192.168.2.1 |

Ozmart consist of 2 Site one is the head office (HQ) which is in Melbourne and a branch office in Sydney. Since Melbourne is the main Site, it has all the server hosted on VMware environment. Company is utilising Cisco networking products such as firewall, routers, switches and wireless access points. As the organisation is expanding the on-premises network is unable to hold the required bandwidth. The ports on switches and firewalls are megabyte and can’t hold the traffic. This document outlines the current on-premises infrastructure of Ozmart.

The whole on-premises network can be divided into 3 components: DMZ, internal and External network.

A diagram of a computer network

Description automatically generated

**VLAN’s: Virtual Local Area Network**

VLan’s are used to create a logical partition between network so that devices in same VLAN can communicate with each other and policies can be implemented between to separate the traffic and increase the security.

In our network we have use 3 VLAN namely **Internal VLAN, External VLAN and DMZ VLAN.**

**Internal VLAN:** This VLAN is used by the employees for internal communication among employees and to reach to the server. It includes laptops, desktops, computer and other networking devices. It also includes the server that doesn’t require external access.

**External VLAN:** This is where the internet comes from. The resources that need direct internet access are connected to this VLAN. The devices connected to this are firewall and router.

**DMZ**: De-militarized zone is mainly for external facing servers. This includes public facing server such as companies’ websites. In our on-premises network its connected to a switch and then connected to a firewall.

**Switches**: The on-premise consist of 3 managed switches. Switches can operate in layer 2 and layer 3. Layer 3 switches have the capability to route the traffic. However, in the current setup we have got layer 2 switches. There are 3 different type of switches Core layer switch, Distribution layer switch and access later switch. Core layer switch act as a backbone and connects to distribution layer. In our network we are using Access layer switch acts as a connection between firewall and end devices such as server, laptops, desktop and Wireless access points.

**Routers**: Routers are the intermediate devices used in the layer 3 of the network and particularly used to connect LAN or WAN. They interconnect the packets between the networks. They assist in the direction of the packets to the correct place by referring to routing table. They also assist in traffic control; NAT support and its primary task includes dynamic routing. They also help with traffic management, network address translation and provide dynamic routing protocols. Routers used in our network are configured with OSFP protocol which is used for routing IP packet within Autonomous system. It routes packets using network tropology map.

**Firewall:** Firewalls are security devices that are used to protect the network from threat and unknow access. Using firewall, we can apply traffic control to the network and decide what port can be open and what ports need to be closed. Firewall are used for Intrusion prevention, VPN access and application layer filtering.

In our on-premises network we have implemented firewall to provide control over the traffic by using access control list which define the rules and policies to permit or deny the traffic based on the requirements. Firewall provides logging and monitoring service where a network engineer can see what kind of traffic is flowing and block it if needed.

**End user Devices**: There are multiple end user’s devices that used are being used by Ozmart. Laptop, desktop, WAP, Printers. Wireless devices such as laptops and mobiles are connected.