***Pizza Pan WAN design***

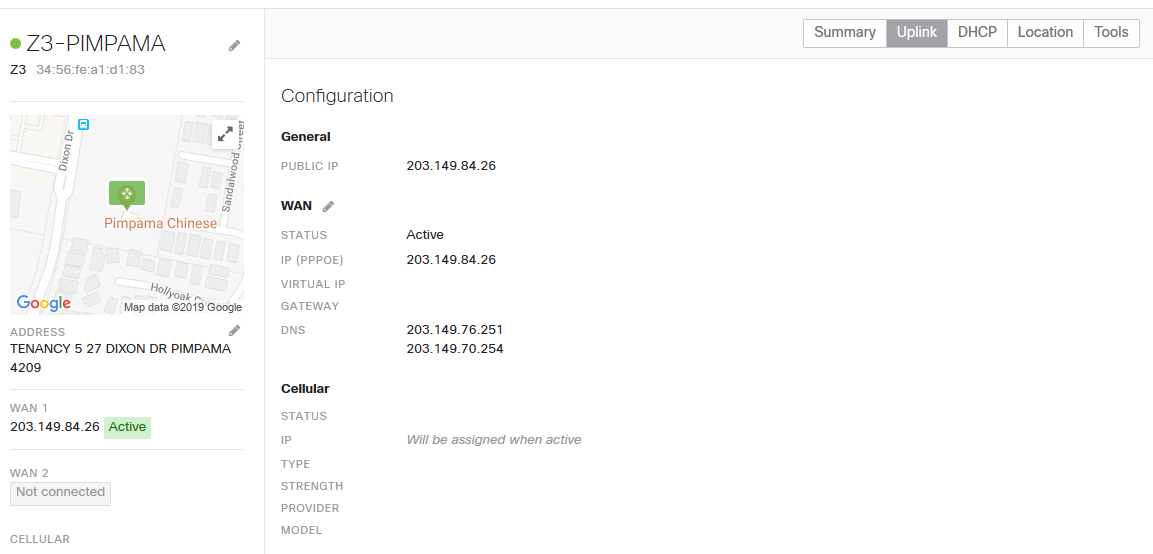
Pizza Pan SPN is no more preserved and they have deiced to go all Internet for all their Sites/Franchise stores, from a GCOMM perspective the sites will be either handed off as a NBN Internet/ ADSL Internet for majority of their stores, furthermore 4G Dongles will be used by Pizza Pan for their back up.

Meraki will be the terminating CPE at all these site. Sites are terminated on a Z3 directly apart from NBN FTTN and ADSL services, where an additional TP-Link is used as a bridging device and the Z3’s are involved with the PPPoE authentication.

GCOMM Provisioning Tasks

1. Configure Radius for NBN/DSL authentication.
2. Configure Meraki, Device and Dashboard.

***Underlined – MERAKI COMPLETE SET UP***



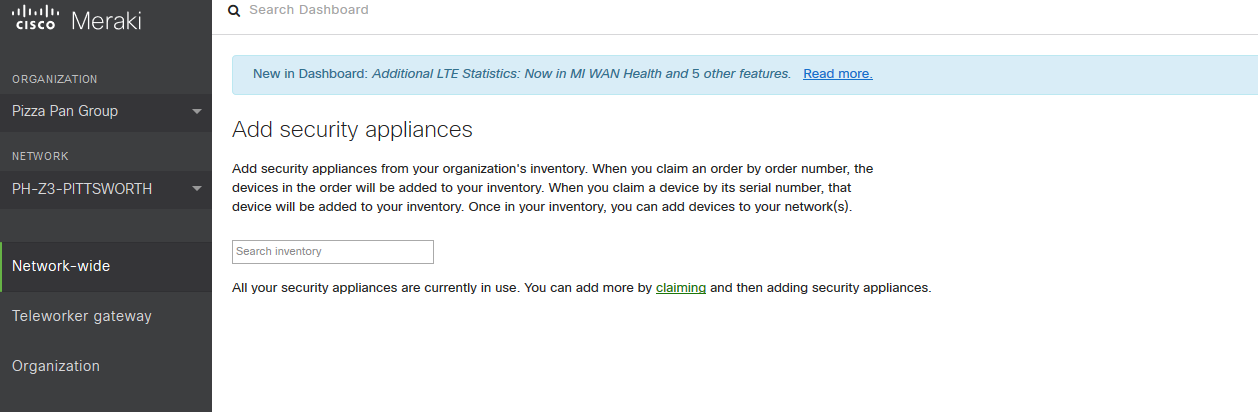
***This is how the Meraki Appliance will look once it’s connected and UP.***

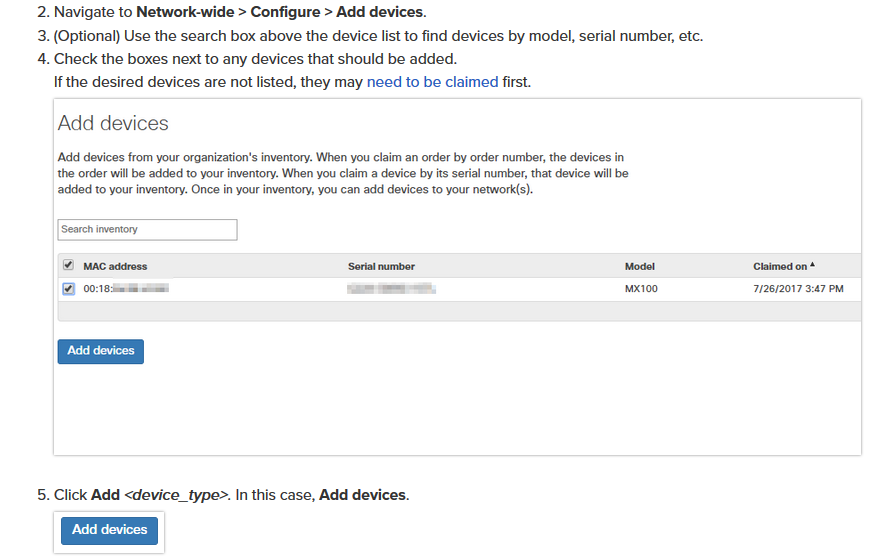
Preferred Firmware for the Z3 devices



***Adding a Z3 Device to the Dashboard***

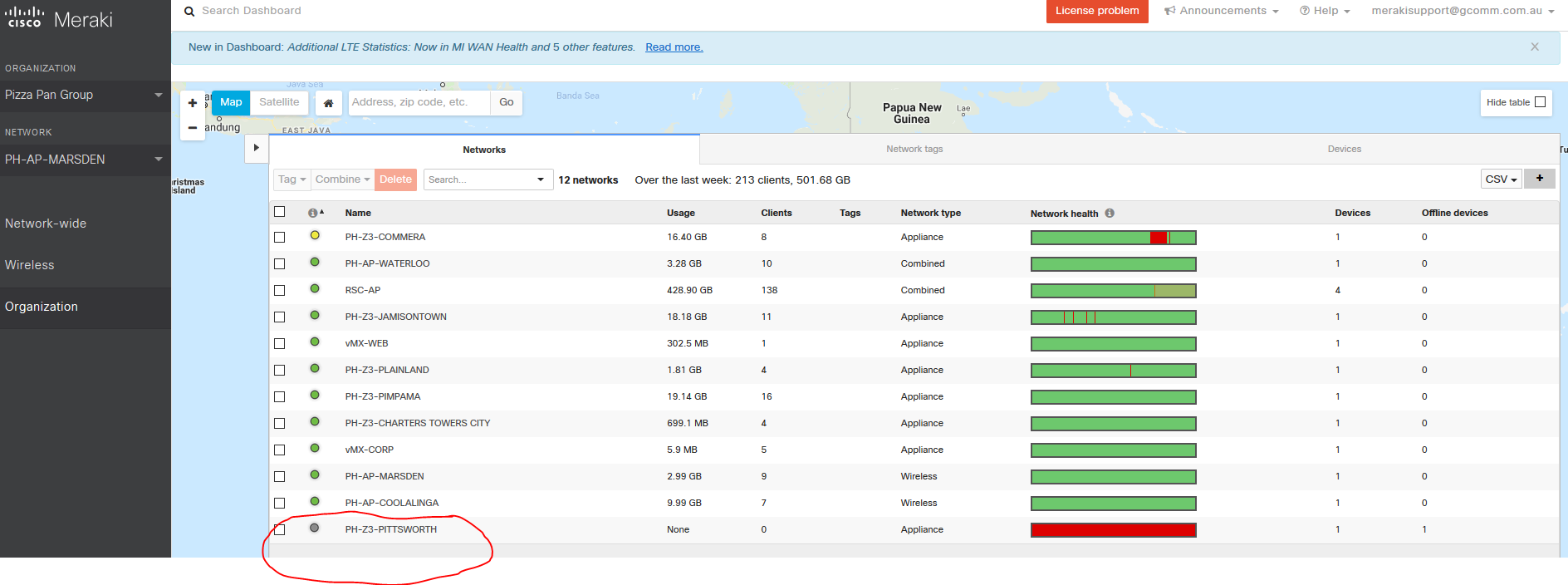
1. Select the network devices should be added to.  
**Note:** Make sure you are inside Pizza pan Group/ under organization





Once you add in the Serial-number synch happens pretty quickly.

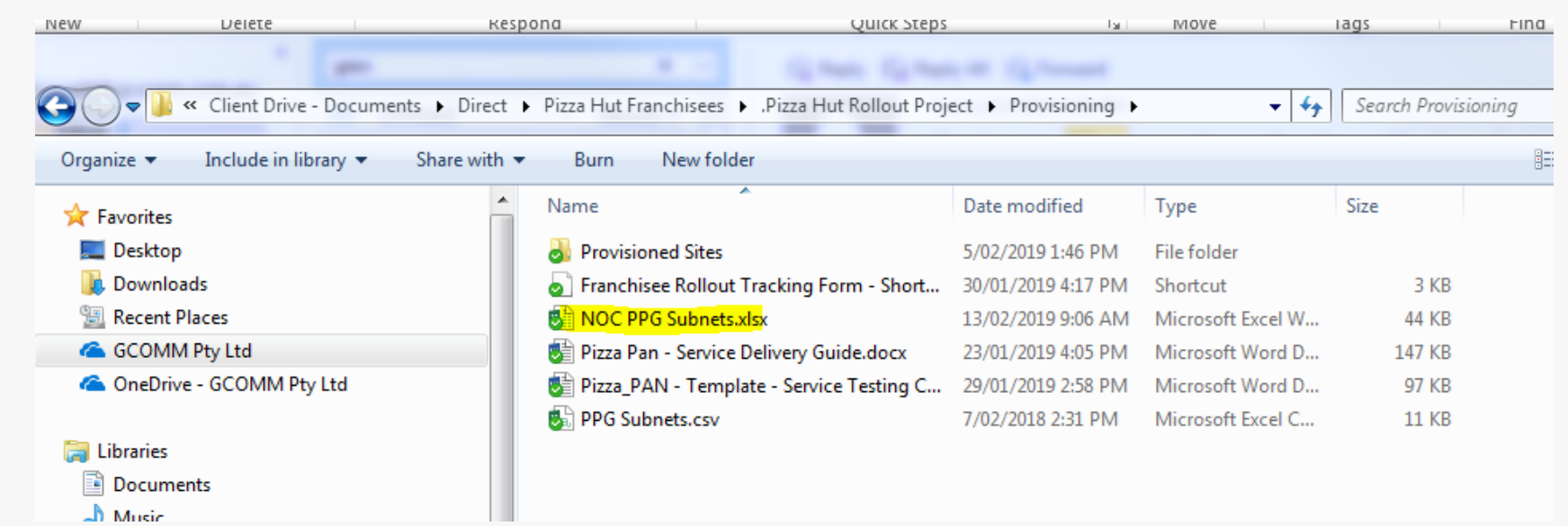
6. Now, click on Organization and make sure the Z3 added is under the Networks. It will be greyed out until the uplink is connected, but it should be visible as a network under the Organization.

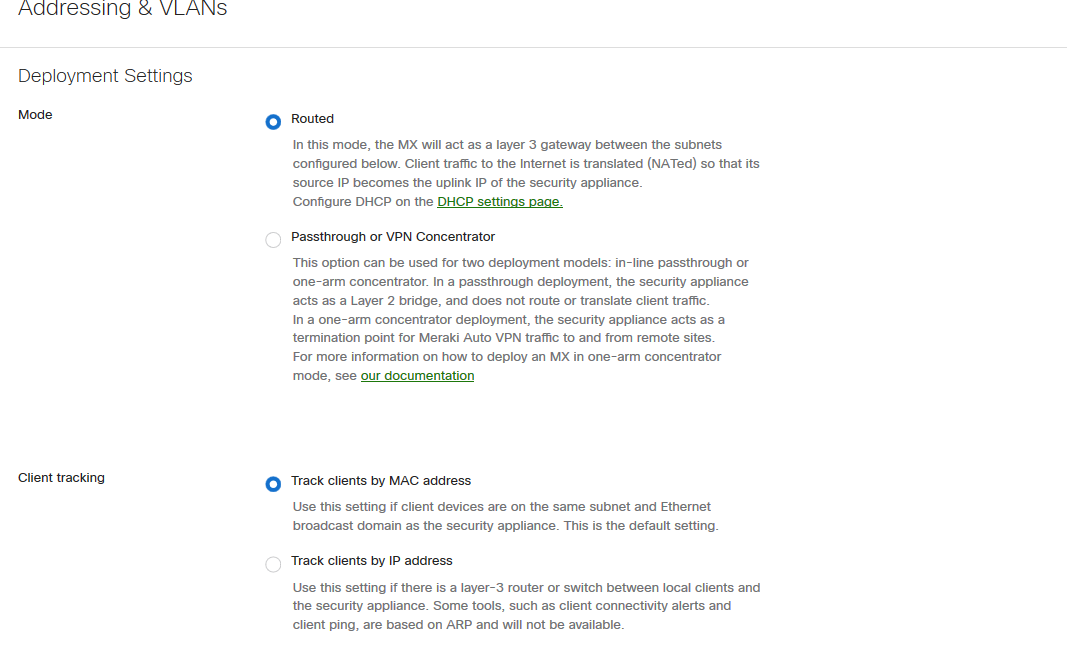


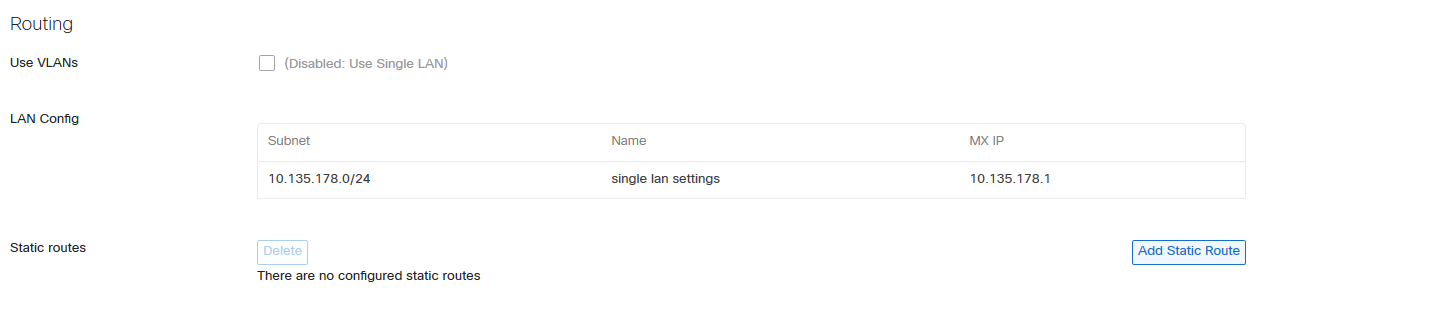
***Configuring LAN Addressing and VLAN’s***

Follow the path to the shared Pizza Pan folder to configure LAN subnets.

Do not assume, folder needs to be checked.

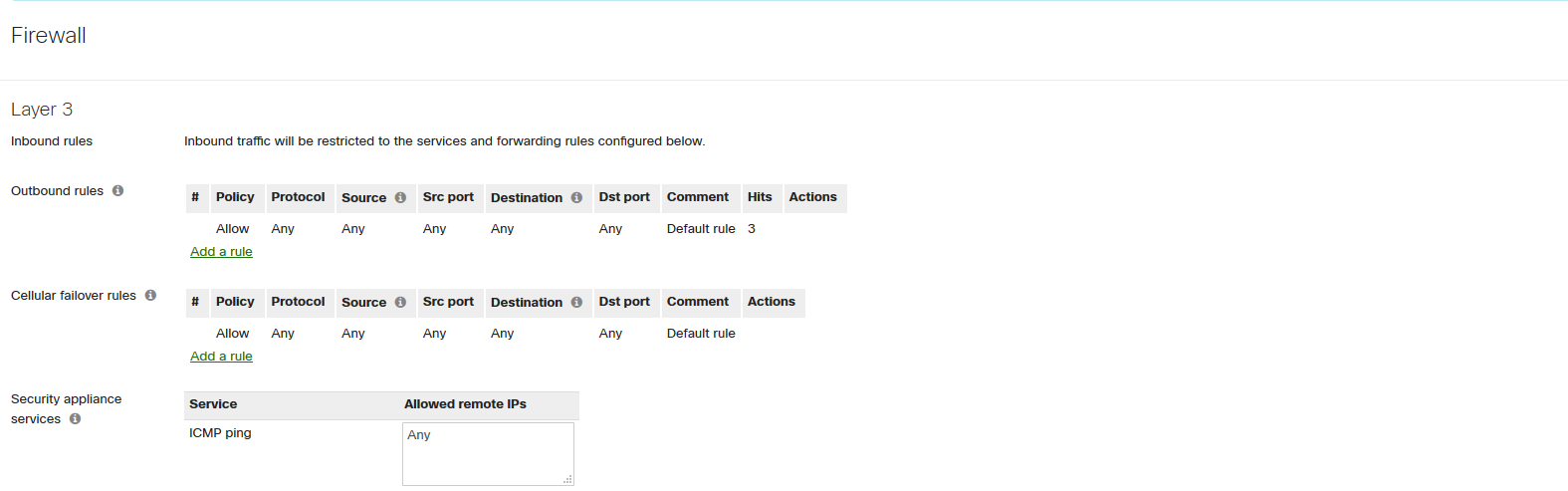






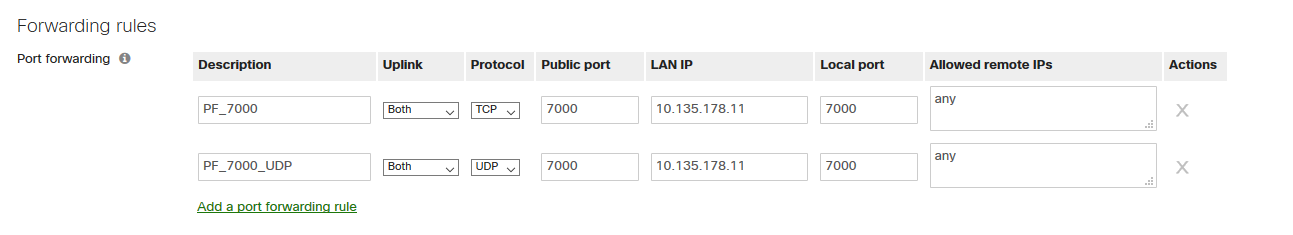
***Configuring policies/ L3 rules***

We configure a standard L3 Policy, all outbound traffic is unfiltered/ Inbound restricted by Rules.



***Port Forwarding***

This is an important configuration, to be done when the dashboard is to be configured and liaise with Pizza Pan support to make sure the store orders are pushed through via Port forward additions on the Meraki from the Internet towards their internal server.



If this is not configured, the Pizza orders wouldn’t come through, it is critical to get this right.

***Configure Auto-VPN***

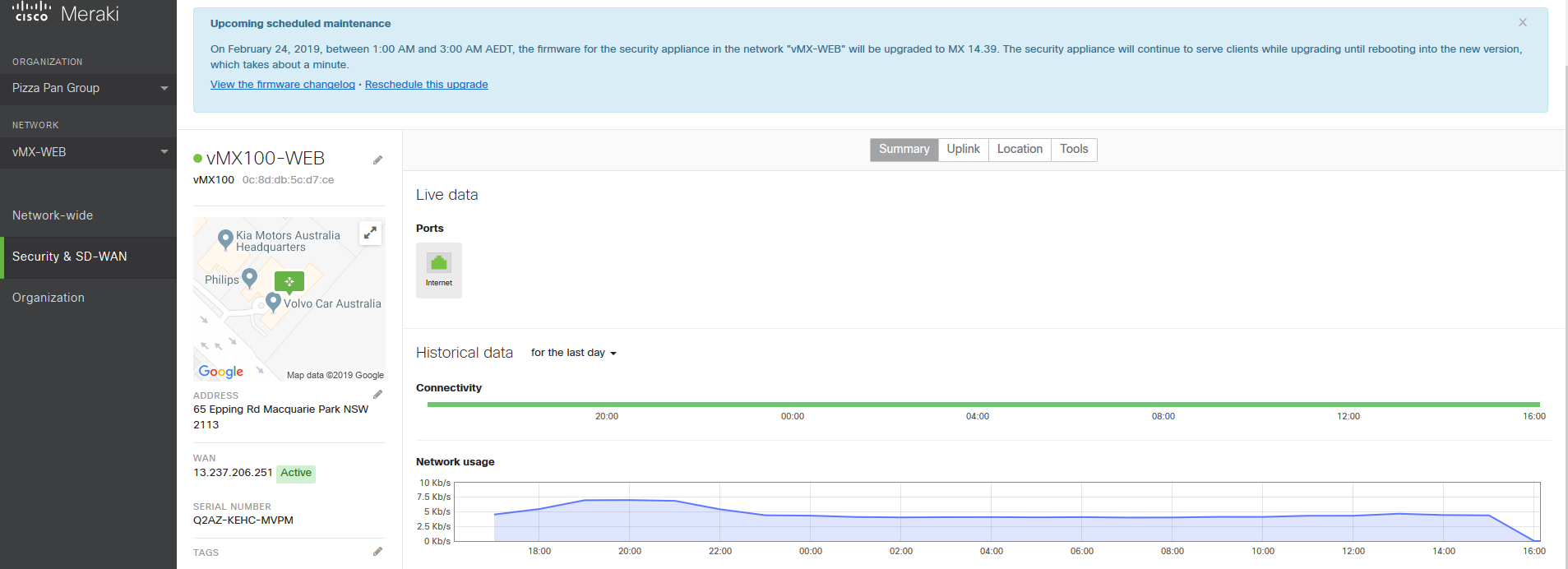
Finally, site-site VPN needs to be turned on between the sites and the vMX100 that is hosted in AWS. It is our responsibility to look after this device.

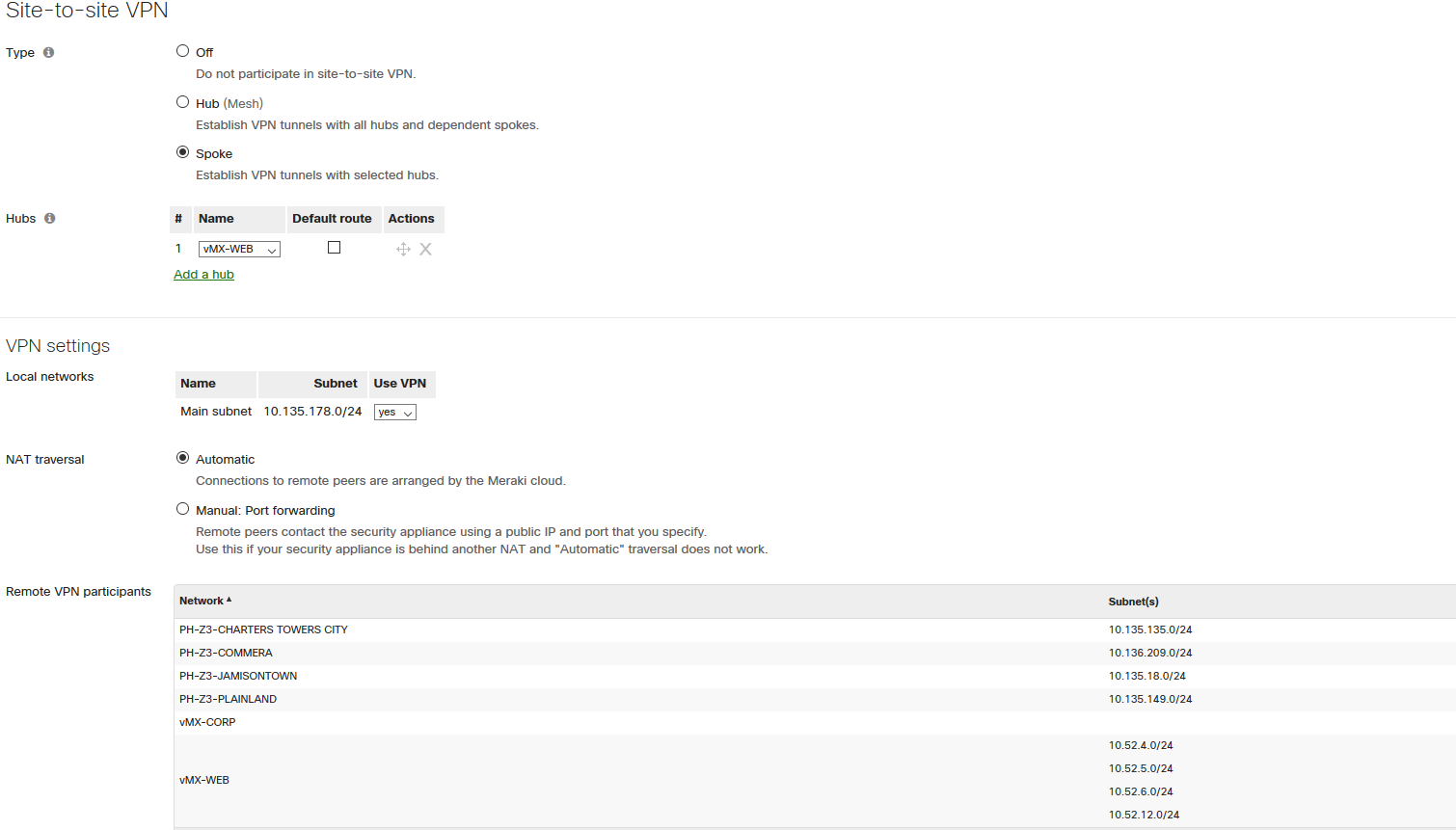
I have named the device as vMX-WEB and vMX-Corporate

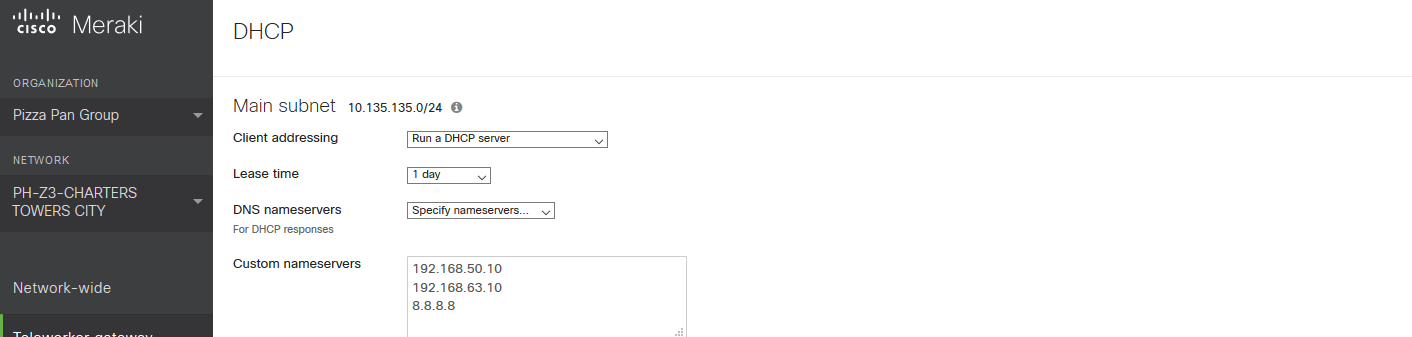
Site-Site VPN needs to be established from every store to the vMX-WEB alone, using the site as a spoke.

Refer Below

Implications: without the auto-vpn between the sites and the vMX, AWS resources cannot be accessed by sites and vice-versa.







Configure each and every Z3 with their internal DNS servers as above. The DNS Servers have forwarders to Umbrella DNS.

This is not mandatory as you could get away without the nameservers as there is an Umbrella roaming agents that are installed at site, which allows the agent to redirect DNS through Umbrella Servers.