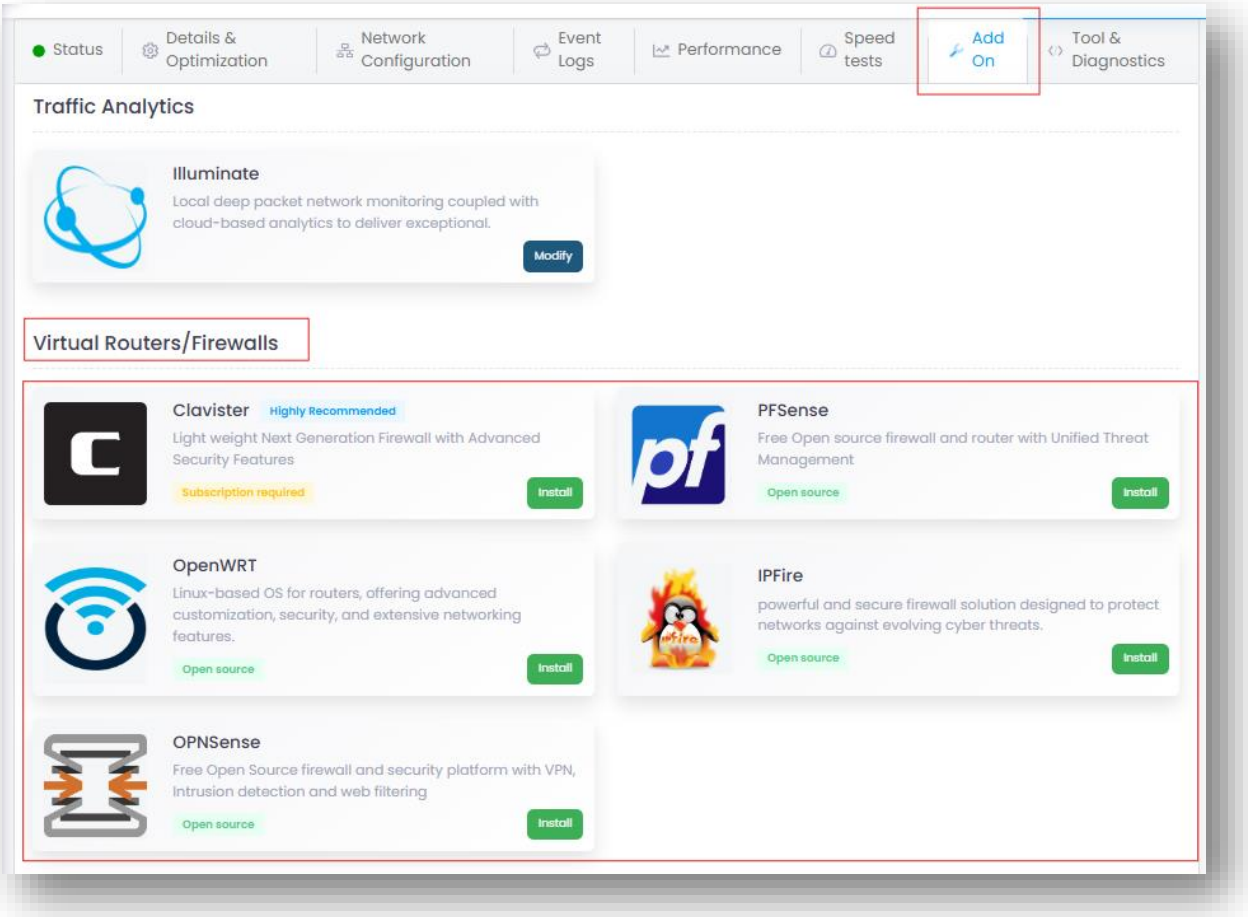
Installing a Firewall on a Node ("FON")

Once logged into **Antares**, open the page of the Node that you wish to install a local Firewall on.

In the Home Page of the Node under the [Add On] tab, you will see a number of Firewall choices.

Once you have selected the desired Firewall image, you can install the Firewall by clicking the [Install] button next to the Firewall of your choice.



** The installation can take up to 30 minutes depending on the speed of the connection(s) on the node.

Each Firewall image is pre-configured with a LAN side subnet of 192.168.100.1/24 active as a DHCP server, with DNS resolvers set to 8.8.8.8/8.8.4.4

*** Only the ***Clavister*** image has some pre-defined security policies defined. You will need to define and manage all policies on any Firewall you select.

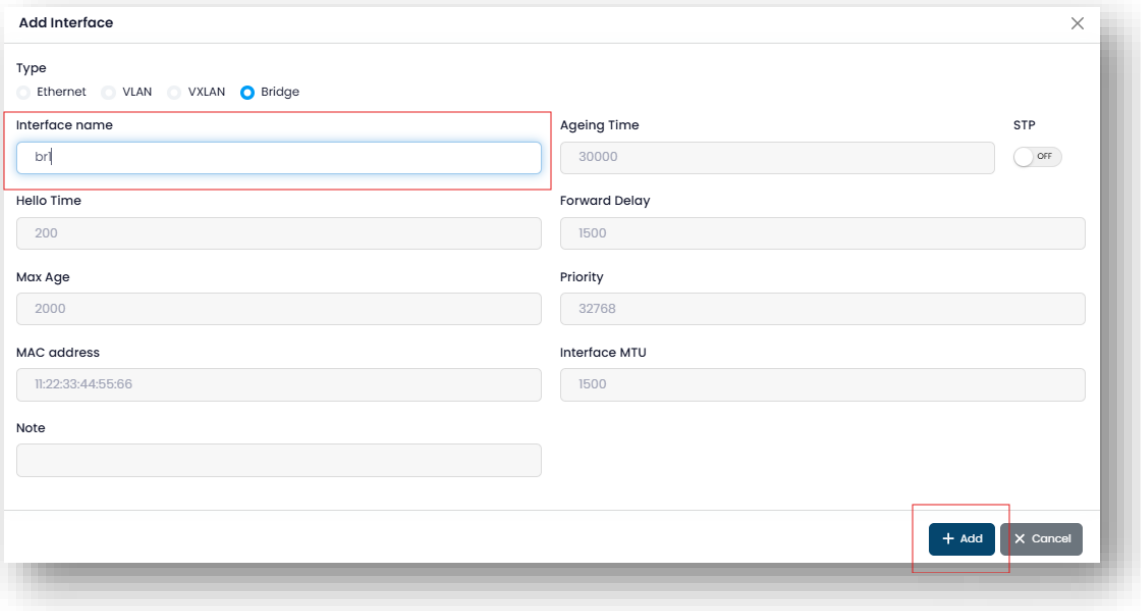
***** You are entirely responsible for the policies/restrictions on the Firewall configuration *****

Node Configuration Process

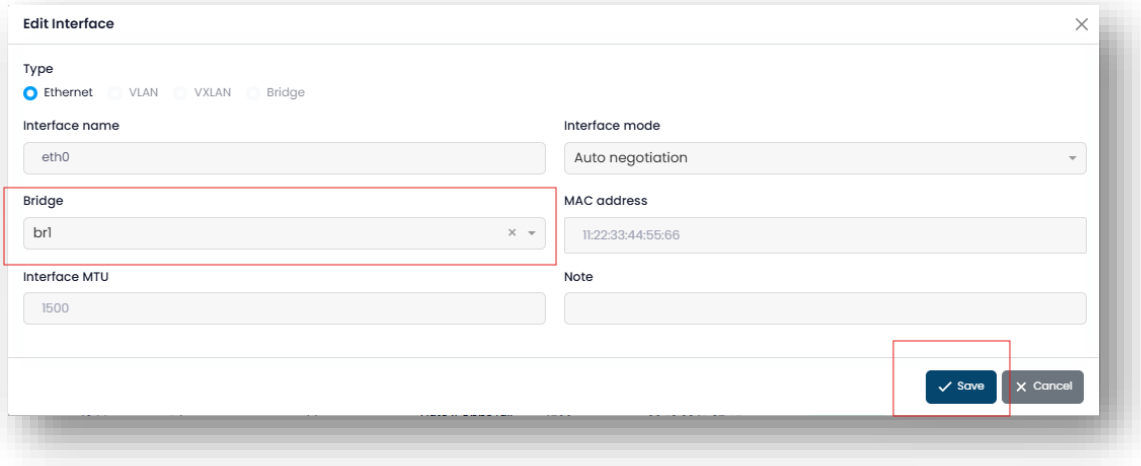
This Configuration Process is essential.

In order for your local Firewall to access the Internal and External ports of the node, the following configuration must be applied:

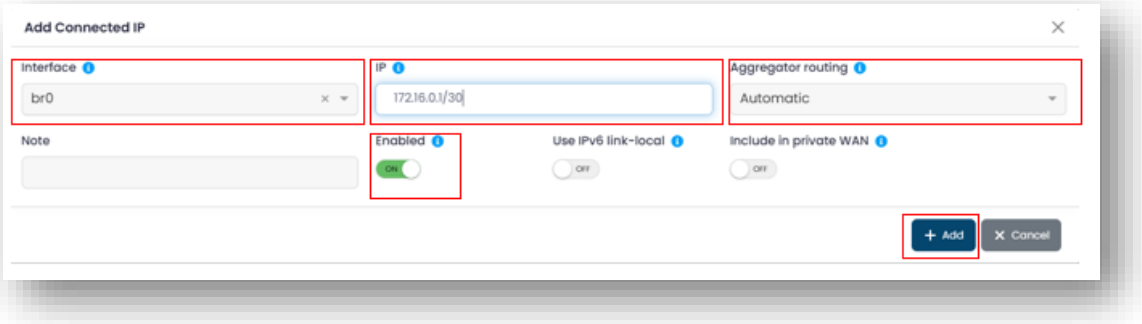
1. Remove any Connected IPs applied to *eth0*.
   If you have a CPE NAT IP, navigate to the [Network Configuration]/[LAN] tab and:
   a. create a temporary *Connected IP* of 192.168.168.1/30 on any other interface except *eth0* (for example use *eth1*)
   b. Change your *CPE NAT IP Destination* from the old IP to the new IP you just created (192.168.168.1)
2. You can now delete the *eth0 Connected IP*. The interface *eth0* should now be free of Connected IPs
3. On the [Interface] tab in **Antares**, create two Bridge Interfaces, one called *br0* and the other called *br1*.



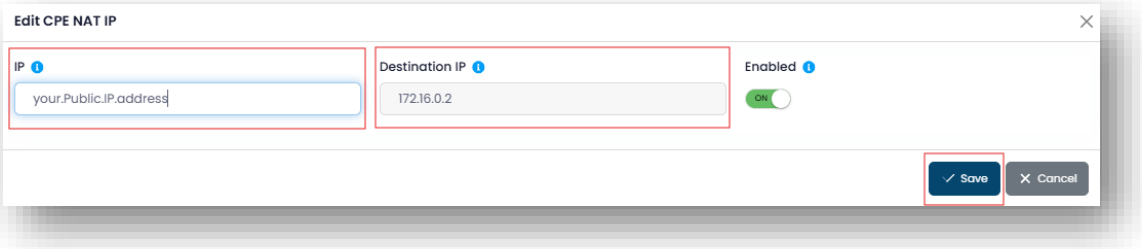
4. On the [Interface] tab, edit the *eth0* Interface to Bridge *br1* to *eth0*.



5. In **Antares** on the [LAN] tab, create a new Connected IP of 172.16.0.1/30 and associate it to *Interface br0* and leave the Aggregator Routing to be 'Automatic'

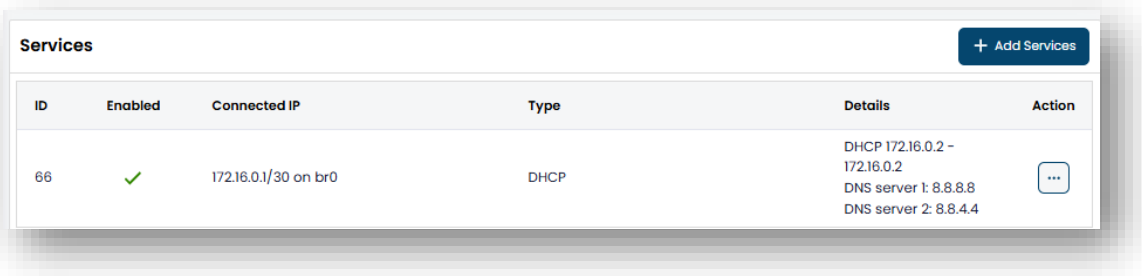


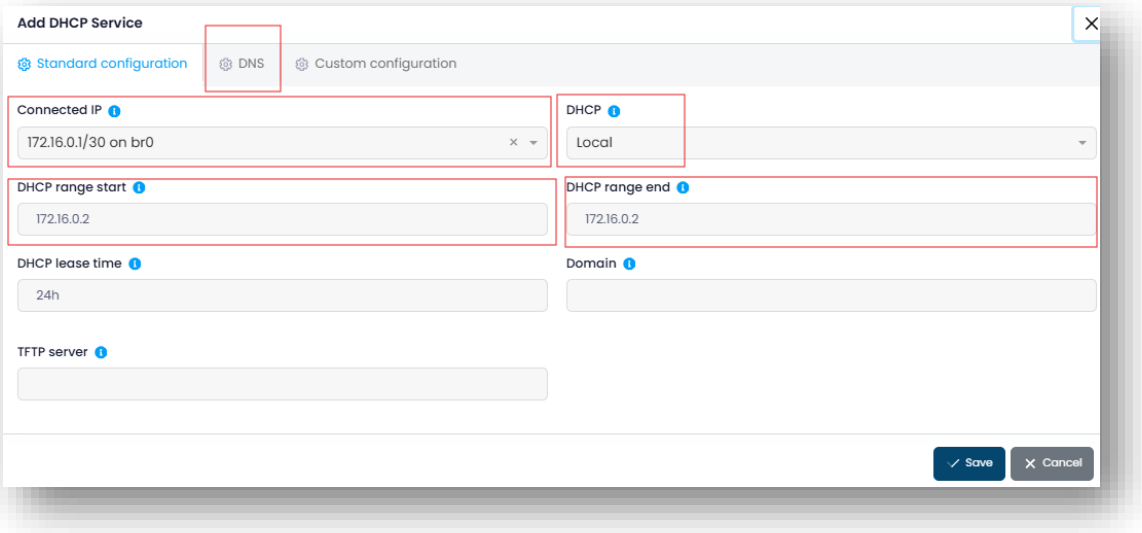
6. Then *redirect* your Public IP address to point to 172.16.0.2 by editing the *CPE NAT IP* and saving.



7. This last step is only required if you changed the pre-configured WAN details in the Firewall image to be DHCP from STATIC.

   If you changed to a DHCP WAN connection on your Firewall, add in the details below:





Accessing the Firewall

Access to the ***webgui*** to all Firewalls will be via the **Antares** *Secure Connect* protocol.

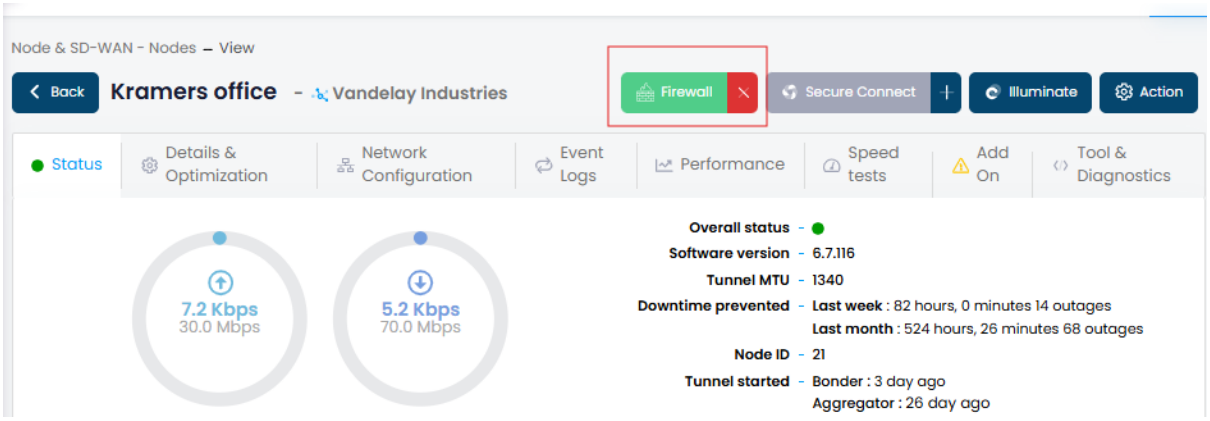
This restricts access only to users authenticated into **Antares** and who have access to *Secure Connect* permissions.

All Firewalls will be accessed by the IP on *Secure Connect* of 172.16.0.2.
There is a preloaded set of access credentials into the administration portal of the Firewalls.

If required, you can change the credentials and use these to login (this may be required to allow Firewall access only to those that have the skill to manage the Firewall).

First steps

1. After selecting the desired Firewall and Installing it, access the Firewall through the [Firewall] button on the Node Home Page in **Antares**.



2. **Take a Backup of the configuration** and save it in a safe place. Do this each time you make a configuration change. **IMPORTANT!**

3. Alter the Admin credentials if required.

4. If required, adjust the LAN side subnets to match your internal network.

5. If you happen to find the Firewall is not responding, try rebooting the node by way a power cycle.
   If that fails, simply remove and reinstall the Firewall and restore your saved backup configuration.