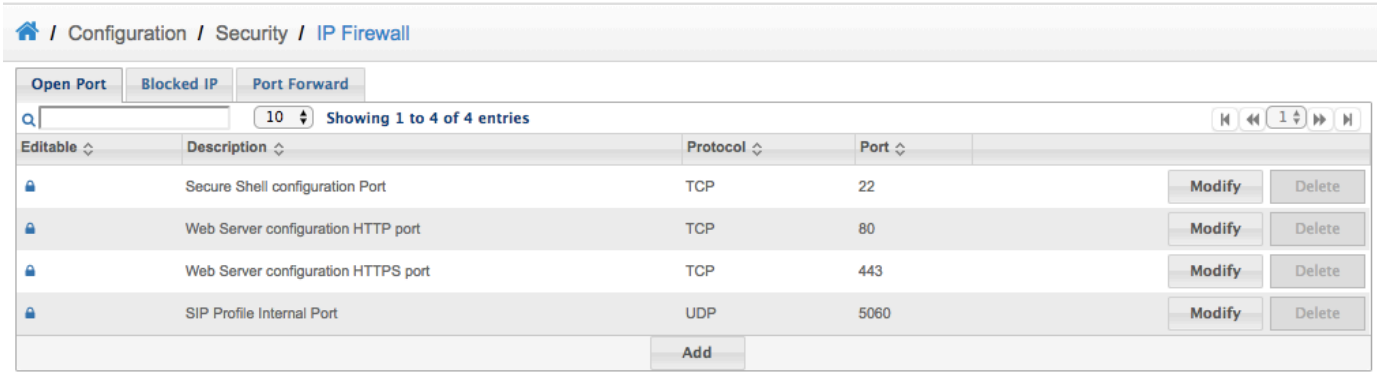
IP Firewall Security

IP Firewall should be enabled for security reason. After a successful installation, ports for SSH, HTTP, HTTPS are open. SIP Profile ports used in SIP Profile setting will be open automatically.

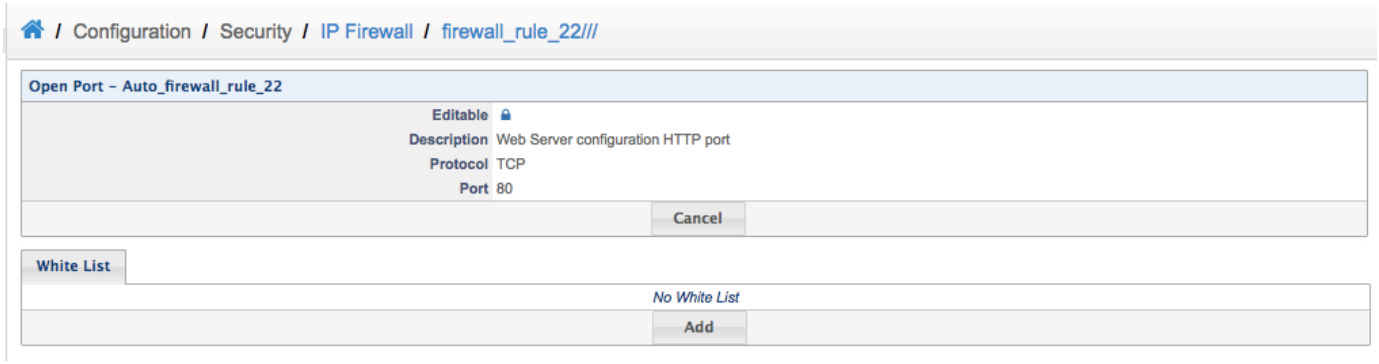


Creating whitelist

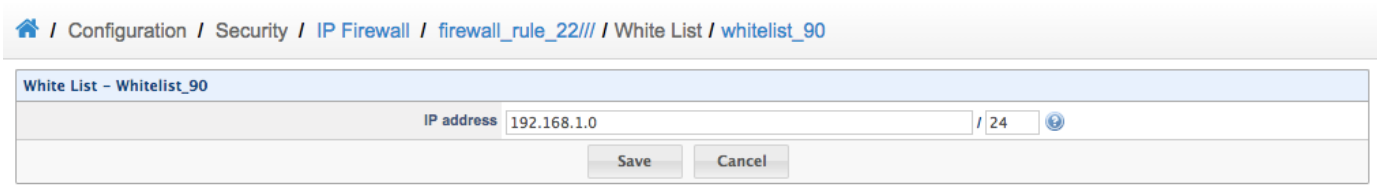
A whitelist is a list of source IP subnets that will be accepted for the service. **If no whitelist is created, all source IPs from all network interfaces are accepted.**

Note that each open port has its own whitelist, the following is the steps to create a whitelist for HTTP, you need to repeat the same for HTTPS and SSH.

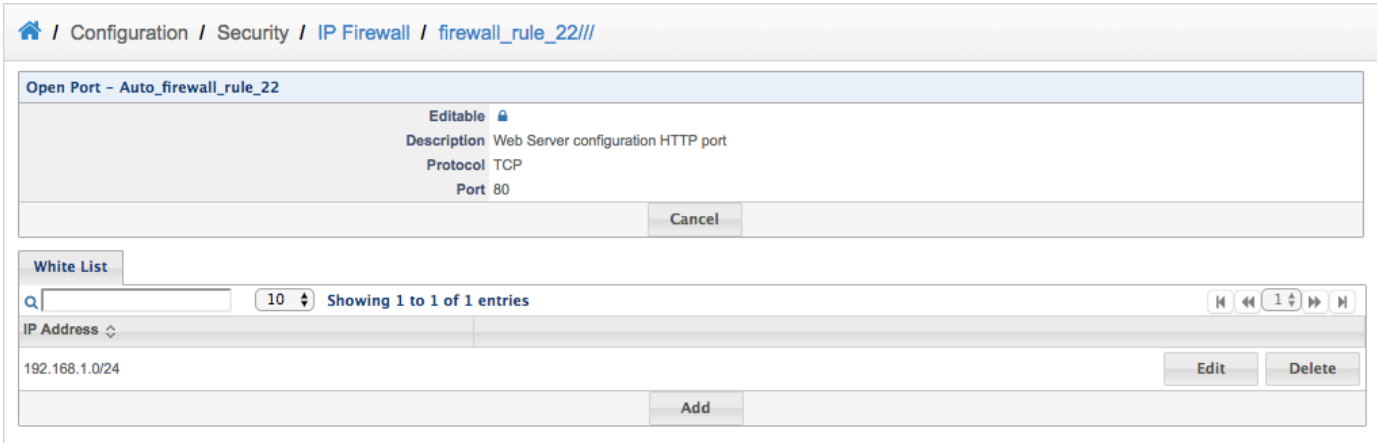
For example, click the "Modify" button for HTTP setting and you will see the following:



For better security, you can limit web UI HTTP access from your internal network only. Let's assume your internal subnet is 192.168.1.0, add the subnet to the whitelist as follow:

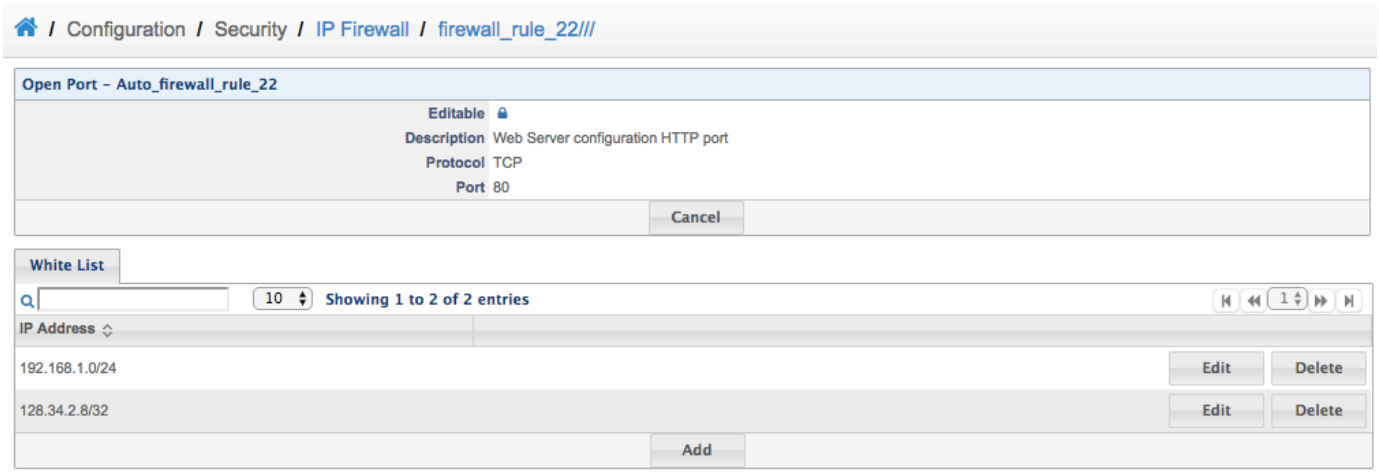


click Save:



By creating a whitelist with your internal subnet, you are blocking all HTTP access from the public external network and only allow access from the internal network.

This is the recommended setup. However, if you need access from a specify public IP in the public network, you can do so by adding it to the whitelist.



In the above example, HTTP access is accepted from the internal network and 128.34.2.8 from the public internet.