

# 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.

Home / Configuration / Security / IP Firewall

Open Port | Blocked IP | Port Forward

Showing 1 to 4 of 4 entries

Editable	Description	Protocol	Port	
	Secure Shell configuration Port	TCP	22	Modify Delete
	Web Server configuration HTTP port	TCP	80	Modify Delete
	Web Server configuration HTTPS port	TCP	443	Modify Delete
	SIP Profile Internal Port	UDP	5060	Modify Delete

Add

## 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:

Home / Configuration / Security / IP Firewall / firewall\_rule\_22///

Open Port - Auto\_firewall\_rule\_22

Editable

Description Web Server configuration HTTP port

Protocol TCP

Port 80

Cancel

White List

No White List

Add

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:

Home / Configuration / Security / IP Firewall / firewall\_rule\_22/// / White List / whitelist\_90

White List - Whitelist\_90

IP address 192.168.1.0 / 24

Save Cancel

click Save:

Home / Configuration / Security / IP Firewall / firewall\_rule\_22///

**Open Port - Auto\_firewall\_rule\_22**

Editable   
 Description Web Server configuration HTTP port  
 Protocol TCP  
 Port 80

**White List**

10 Showing 1 to 1 of 1 entries

IP Address	Edit	Delete
192.168.1.0/24		

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.

Home / Configuration / Security / IP Firewall / firewall\_rule\_22///

**Open Port - Auto\_firewall\_rule\_22**

Editable   
 Description Web Server configuration HTTP port  
 Protocol TCP  
 Port 80

**White List**

10 Showing 1 to 2 of 2 entries

IP Address	Edit	Delete
192.168.1.0/24		
128.34.2.8/32		

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