# Setting up Router to prevent attacks with Public Static IP

## 1. Background

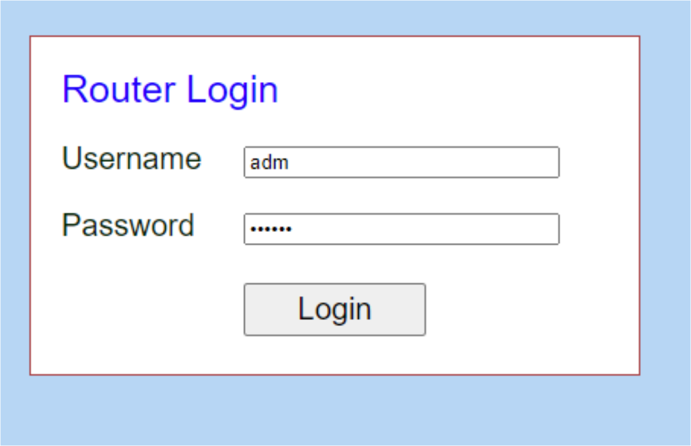
Having a public static IP allows the user to access their device from anywhere on the Internet. This allows the user to have various control over the device, if the device is online. However, the issue is that everyone on the Internet will then be able to see this device. Attackers use a bot which will scan the Internet for every single IP between 0.0.0.0 to 255.255.255.255. They will check common ports like 80, 443, 23, 22, 21 which will be HTTP, HTTPS, Telnet, SSH, FTP. Once they get a response back from the device, they will continuously attack the device, either by sending millions of ping requests, or by sending default username and password to try to login, or by sending malware to take control of the device.

For InHand cellular devices, we build a layer of console to protect the Linux system. This means the attackers can’t access Linux at all. However, the continuous pings or requests will cost bandwidth, which is money, so users will see their device using megabytes to gigabytes of data per day. Therefore, we need to change some settings such as common ports and block pings when using public static IP.

## 2. Disable Ping

This will prevent your device from responding to or accepting ping requests from the Internet, making it appear like the IP is not being or is offline. Other services like the web interface will still work.

2.1 Log into device via local connection (Default IP is 192.168.2.1) or with static IP address.



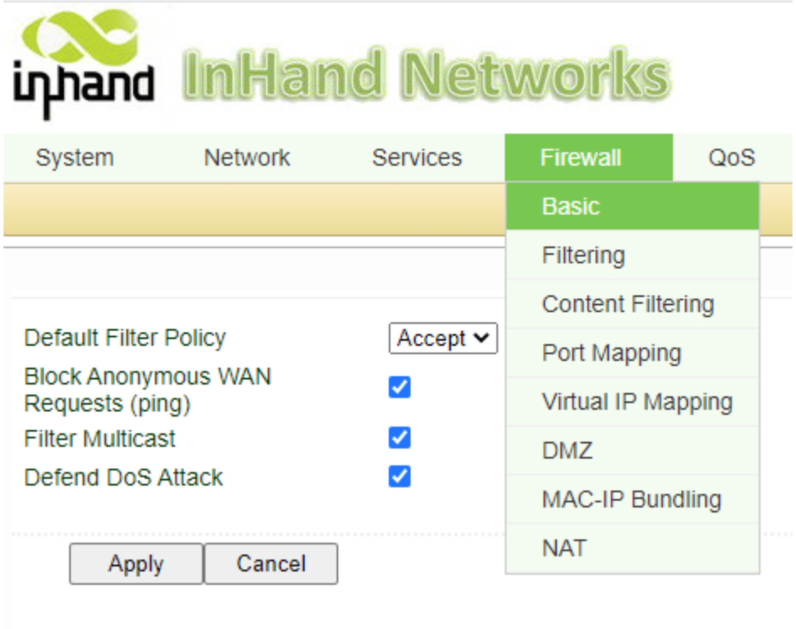
Router Login

Username: adm

Password: ••••••

2.2 Navigate to Firewall->Basic. Check Block Anonymous WAN Requests (ping) as well as filter multicast and defend DoS Attack, these will help protect user against attacks as well as keep data usage low.

Note: Once ping is disabled, users can't ping it from internet anymore, so please make a note of this for the future when engineers need to troubleshoot.



Default Filter Policy: Accept

Block Anonymous WAN Requests (ping) ☑

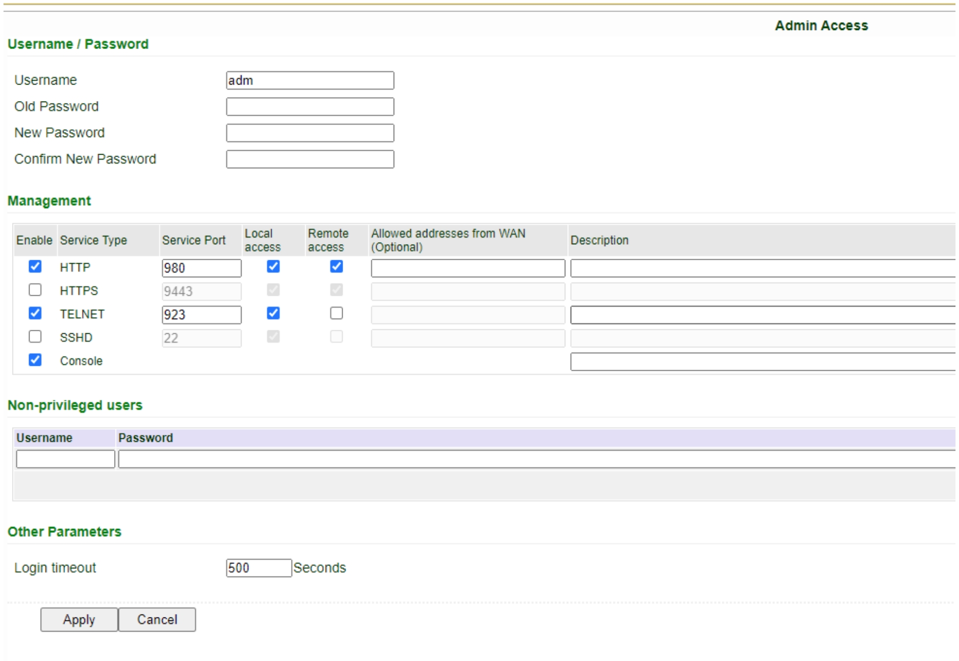
Filter Multicast ☑

Defend DoS Attack ☑

## 3. Disable Ports

If common ports aren't changed, any traffic on the public static IP that goes to the ports will reach to the router, which will consume data and might slow down the bandwidth. By changing the ports to a less common number, it makes it harder for attackers to guess which port is open.

3.1 Navigate to System->Admin access.



Admin Access

**Username / Password**

| | |
|---|---|
| Username | adm |
| Old Password | |
| New Password | |
| Confirm New Password | |

**Management**

| Enable | Service Type | Service Port | Local access | Remote access | Allowed addresses from WAN (Optional) | Description |
|---|---|---|---|---|---|---|
| ☑ | HTTP | 980 | ☑ | ☑ | | |
| ☐ | HTTPS | 9443 | ☑ | ☑ | | |
| ☑ | TELNET | 923 | ☑ | ☐ | | |
| ☐ | SSHD | 22 | ☑ | ☐ | | |
| ☑ | Console | | | | | |

**Non-privileged users**

| Username | Password |
|---|---|
| | |

**Other Parameters**

Login timeout 500 Seconds

Default HTTP is 80, HTTPS 443, Telnet 23. Change the values of these Service ports or disable the port for Remote Access. Hit apply when done.

Note: Once the Remote Access is unchecked, users may not be able to access it remotely anymore. Please also make a not of any port changes, so if engineers need to access telnet or HTTP, they will know which port to access the router from.