TEKTELIC
communications
IoT for life

Enabling KONA Link Webserver

Introduction

- This is a reference/guide on how to enable the Kona Link webserver for **older gateway devices that have been BSP Upgraded to a BSP version that supports the use of Kona Link.** If the earliest BSP on your gateway supports Kona Link as listed in the next slide, no action is needed to use the Kona Link webserver.

- List of Requirements:

1. KonaFT , a Command Line Program/Environment (e.g PuTTy/TeraTerm) or Tektelic NS / OAM server
   - If you are enabling Kona Link through the gateway command line, knowledge of the VI text editor is necessary.
2. A gateway on a BSP version that supports webserver (See Requirements Slide)
   - Instructions for BSP upgrades can be found here

- The high-level procedure involves these steps:

1. Open ports 80 and 443 through the gateway firewall
2. Change default passwords for webserver user
3. Login to webserver

Gateway BSP Versions for Kona Link Webserver

Below lists the minimum BSP version for Kona Link usage on all TEKTELIC gateway models. Please note that these initial BSP versions supporting Kona Link only support plain HTTP and is missing many features:

- **Mega** – BSP 5.0.X or higher
- **Macro** – BSP 5.1.X or higher
- **Enterprise** – BSP 2.0.X or higher
- **Micro** – BSP 4.0.X or higher
- **Micro PoE** – BSP 2.0.X or higher

Newest release for Kona Link that has HTTPS support and additional configuration features can be found on the BSP’s below:

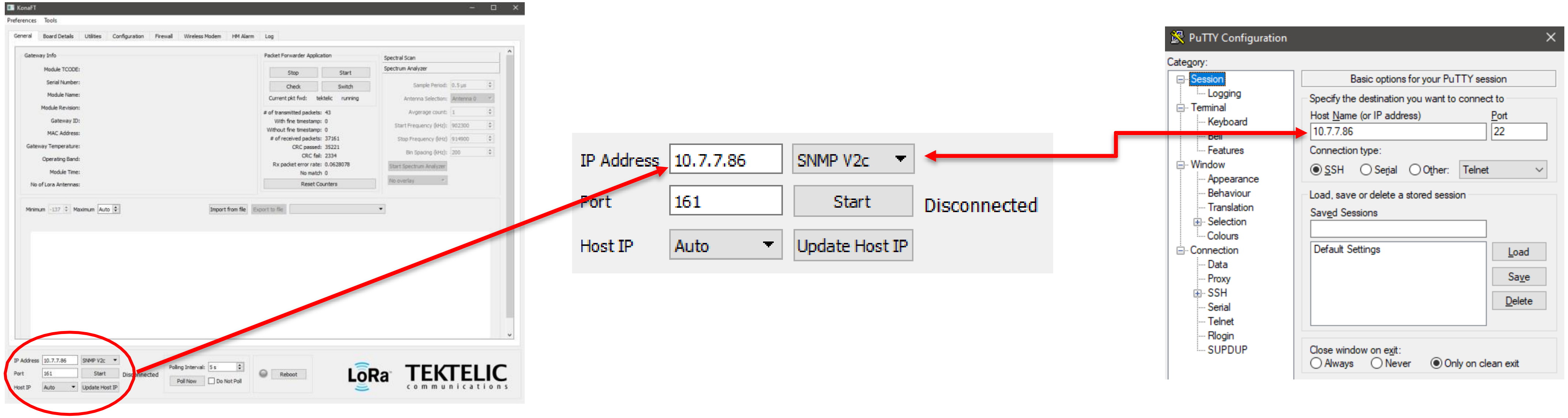
- **Mega** – BSP 6.0.X or higher
- **Macro** – BSP 6.0.X or higher
- **Enterprise** – BSP 3.0.X or higher
- **Micro** – BSP 5.0.X or higher
- **Micro PoE** – BSP 3.0.X or higher

You can confirm the gateway’s BSP version once connected in the KonaFT application through 2 methods:

1. At the bottom right of the program.
2. “Board Details” tab -> “SW Management” subtab -> “Read Versions” -> “Release” version

Requirements

- KonaFT or a program that is capable of connecting to your gateway via SSH (such as PuTTy, Tera Term, etc.)
- The Gateway and computer using KonaFT must be in the same subnet (in KonaFT, use *Tools -> Find My Gateway -> Scan* to determine your subnet/IP address).



IP Address: 10.7.7.86 — SNMP V2c

Port: 161 — Start — Disconnected

Host IP: Auto — Update Host IP

PuTTY Configuration — Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.7.7.86 — Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

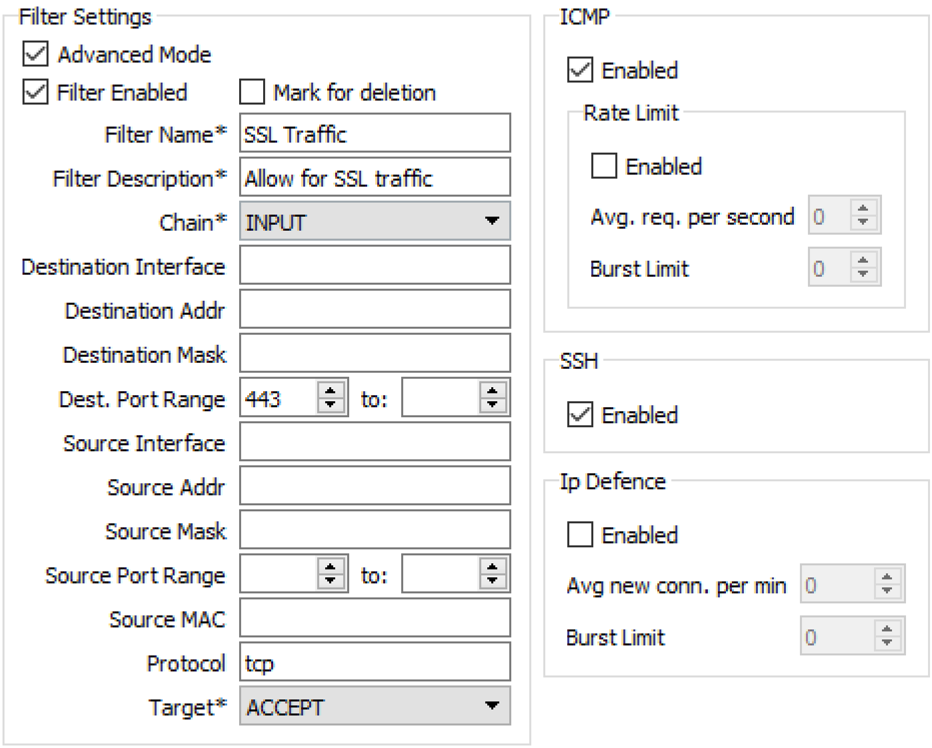
Figure-1 IP Address Configuration

Enabling Kona Link via KonaFT

- When a gateway is upgraded from an older release that did not have KONA Link, the web app gets installed but may be **disabled by default**. If a user wants to use KONA Link after updating to a supported system release, then the web ports need to be opened by editing the firewall configuration file as described below:

1. Connect to your gateway via KonaFT
2. Navigate to the “Firewall” Tab
3. Select “Read Firewall Configuration”
4. Under “Filter Settings” enter the information found in Figure 2a and 2b on the next slide
5. Select the “Filter Enabled” Box and select “Insert Filter”
6. Select “Set Firewall Configuration” once both filters for Port 80 and Port 443 have been inserted.

Enabling Kona Link via KonaFT (2)



Filter Settings

☑ Advanced Mode

☑ Filter Enabled ☐ Mark for deletion

Filter Name*	SSL Traffic
Filter Description*	Allow for SSL traffic
Chain*	INPUT
Destination Interface	
Destination Addr	
Destination Mask	
Dest. Port Range	443 to:
Source Interface	
Source Addr	
Source Mask	
Source Port Range	to:
Source MAC	
Protocol	tcp
Target*	ACCEPT

ICMP

☑ Enabled

Rate Limit

☐ Enabled

Avg. req. per second 0

Burst Limit 0

SSH

☑ Enabled

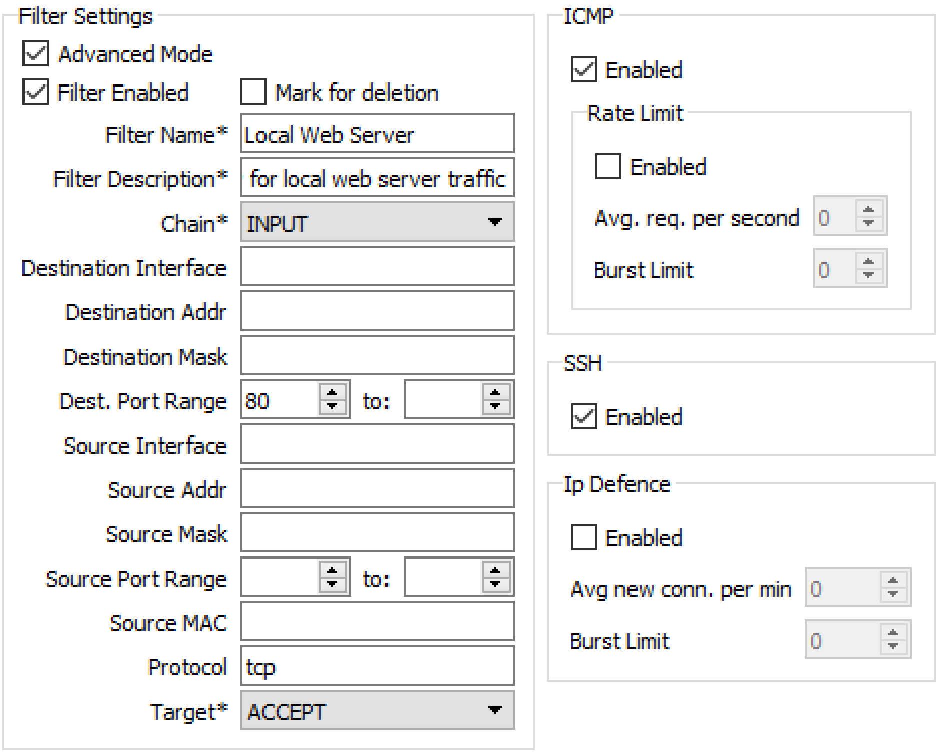
Ip Defence

☐ Enabled

Avg new conn. per min 0

Burst Limit 0

Figure-2a (Opening Port 443)



Filter Settings

☑ Advanced Mode

☑ Filter Enabled ☐ Mark for deletion

Filter Name*	Local Web Server
Filter Description*	for local web server traffic
Chain*	INPUT
Destination Interface	
Destination Addr	
Destination Mask	
Dest. Port Range	80 to:
Source Interface	
Source Addr	
Source Mask	
Source Port Range	to:
Source MAC	
Protocol	tcp
Target*	ACCEPT

ICMP

☑ Enabled

Rate Limit

☐ Enabled

Avg. req. per second 0

Burst Limit 0

SSH

☑ Enabled

Ip Defence

☐ Enabled

Avg new conn. per min 0

Burst Limit 0

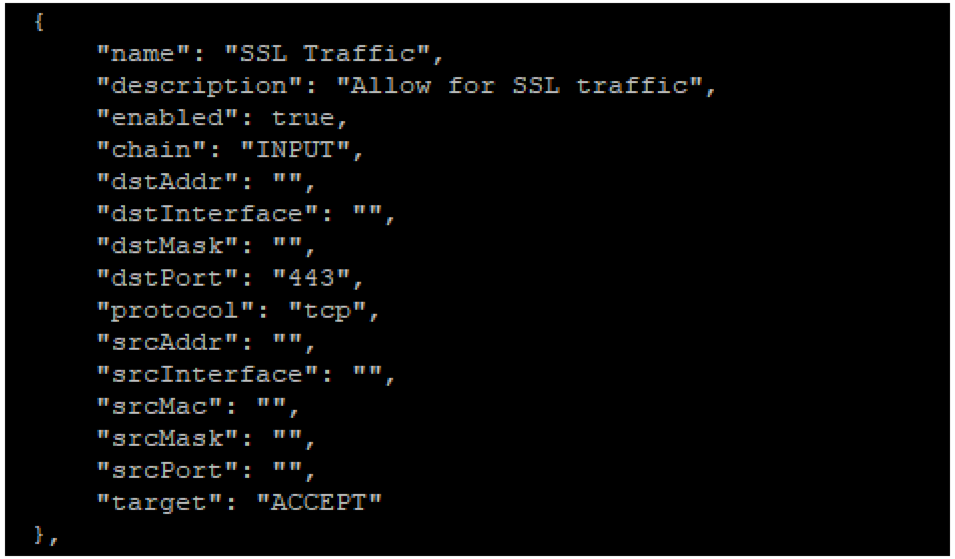
Figure-2b (Opening Port 80)

Enabling Kona Link via SSH

- When a gateway is upgraded from an older release that did not have KONA Link, the web app gets installed but may be **disabled by default**. If a user wants to use KONA Link after updating to a supported system release, then the web ports need to be opened by editing the firewall configuration file as described below:

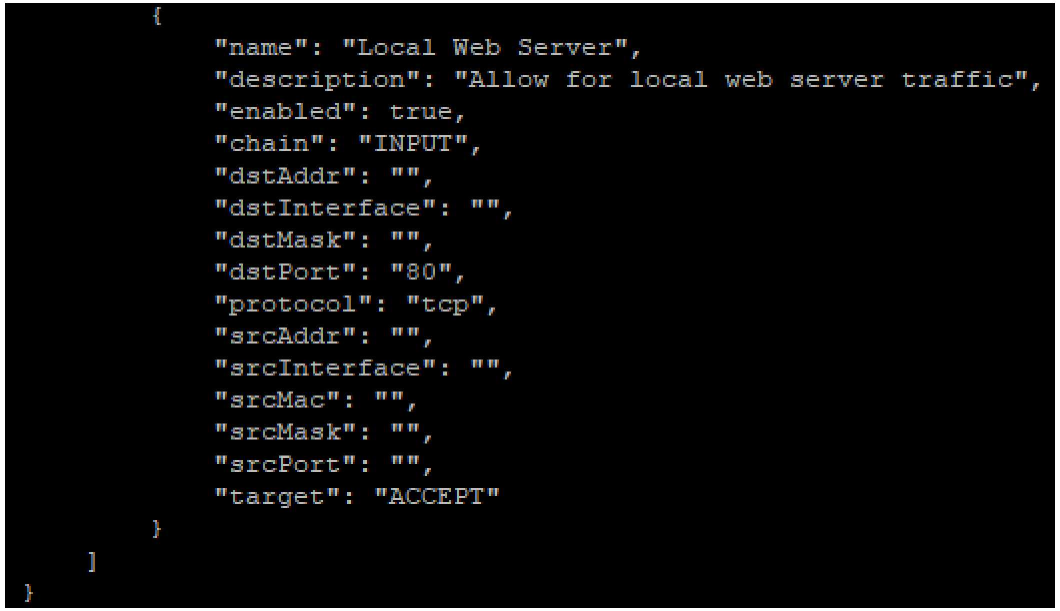
1. Connect to your gateway using SSH
2. Using the VI editor, add the entries shown in Figure 3a and 3b on the next slide to the /etc/firewall.json file using the command below:
   - sudo vi /etc/firewall.json
3. Save the /etc/firewall.json file

Enabling Kona Link via SSH (2)



```
{
    "name": "SSL Traffic",
    "description": "Allow for SSL traffic",
    "enabled": true,
    "chain": "INPUT",
    "dstAddr": "",
    "dstInterface": "",
    "dstMask": "",
    "dstPort": "443",
    "protocol": "tcp",
    "srcAddr": "",
    "srcInterface": "",
    "srcMac": "",
    "srcMask": "",
    "srcPort": "",
    "target": "ACCEPT"
},
```

Figure-3a (Opening Port 443)



```
        {
            "name": "Local Web Server",
            "description": "Allow for local web server traffic",
            "enabled": true,
            "chain": "INPUT",
            "dstAddr": "",
            "dstInterface": "",
            "dstMask": "",
            "dstPort": "80",
            "protocol": "tcp",
            "srcAddr": "",
            "srcInterface": "",
            "srcMac": "",
            "srcMask": "",
            "srcPort": "",
            "target": "ACCEPT"
        }
    ]
}
```

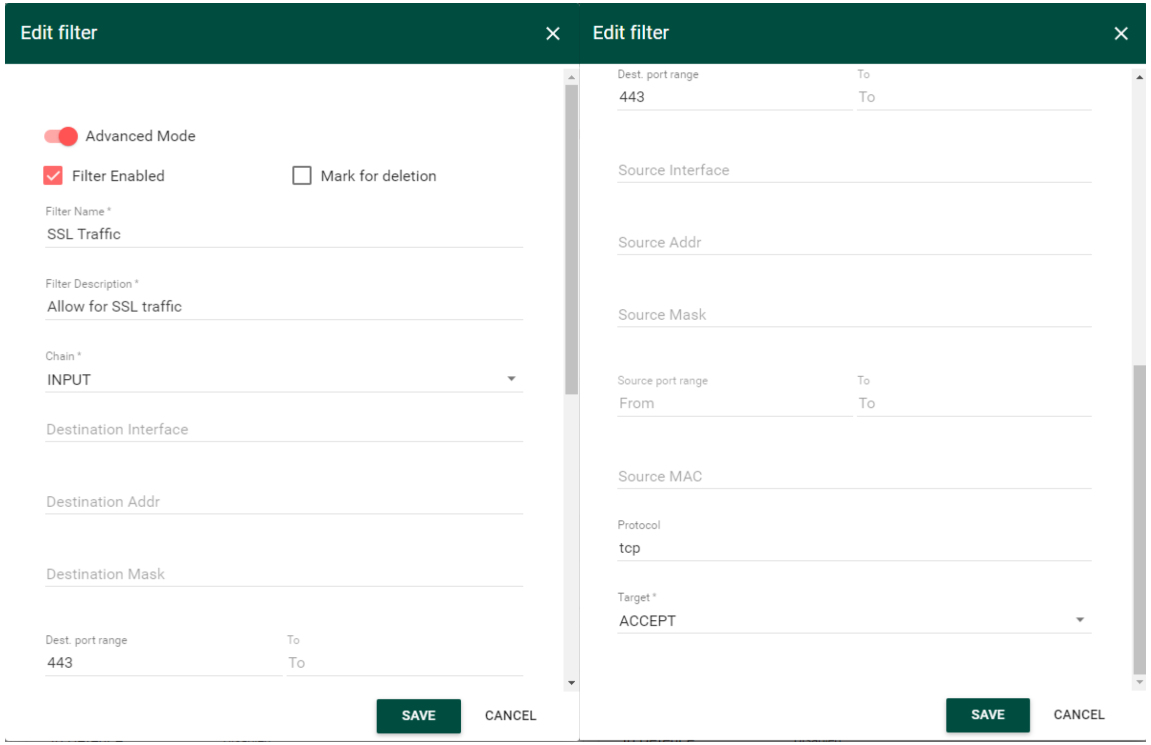
Figure-3b (Opening Port 80)

Enabling Kona Link via TekNS/OAM

- When a gateway is upgraded from an older release that did not have KONA Link, the web app gets installed but may be **disabled by default**. If a user wants to use KONA Link after updating to a supported system release, then the web ports need to be opened by editing the firewall configuration file as described below:

1. Ensure your gateway is online on the Tektelic NS / OAM Server
2. Select this gateway and navigate to the “Firewall” tab
3. Click “Read Firewall Configuration”
4. Select the “Insert Filter” Icon
5. Enable “Advanced Mode”, enter the information listed in figure 4a and 4b on the next slide and click “Save”
6. Once both filters have been added, click the “Set Firewall Configuration” button

Enabling Kona Link via TekNS/OAM



Edit filter

Advanced Mode: ●

☑ Filter Enabled   □ Mark for deletion

Filter Name *: SSL Traffic

Filter Description *: Allow for SSL traffic

Chain *: INPUT

Destination Interface

Destination Addr

Destination Mask

Dest. port range: 443   To: To

Source Interface

Source Addr

Source Mask

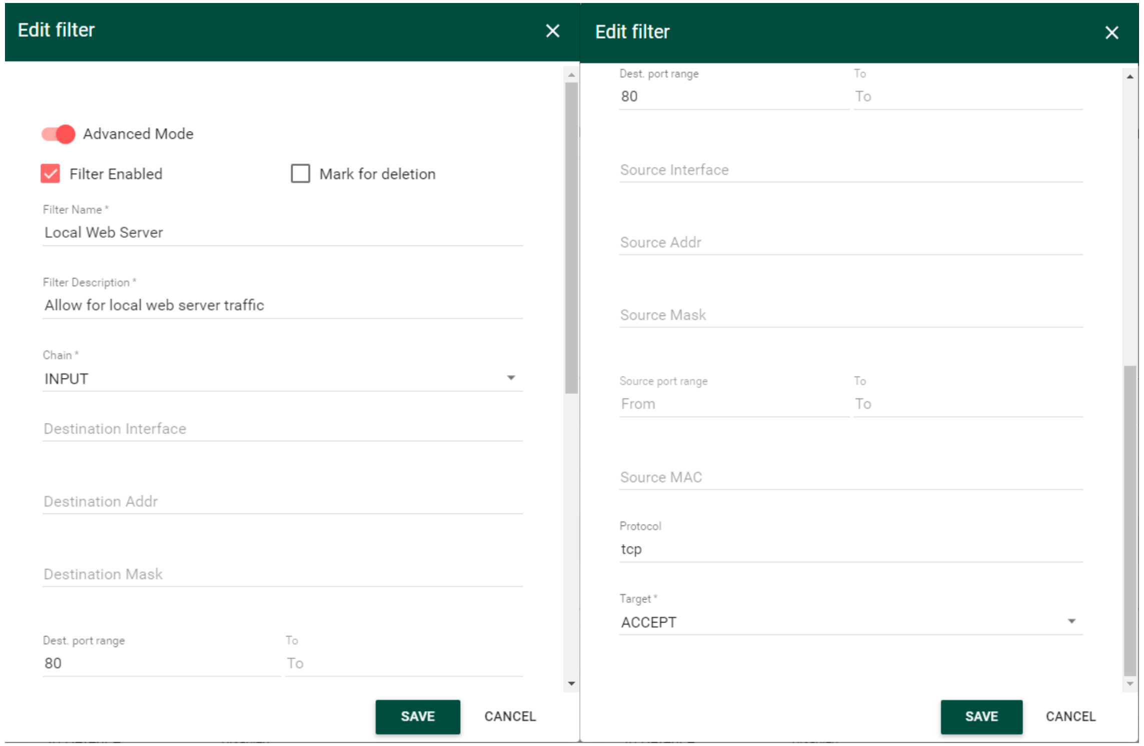
Source port range: From   To: To

Source MAC

Protocol: tcp

Target *: ACCEPT

Figure-4a (Opening Port 443)



Edit filter

Advanced Mode: ●

☑ Filter Enabled   □ Mark for deletion

Filter Name *: Local Web Server

Filter Description *: Allow for local web server traffic

Chain *: INPUT

Destination Interface

Destination Addr

Destination Mask

Dest. port range: 80   To: To

Source Interface

Source Addr

Source Mask

Source port range: From   To: To

Source MAC

Protocol: tcp

Target *: ACCEPT

Figure-4b (Opening Port 80)

Changing Webserver Default Password

- The Kona Link login credentials for your gateway can be found on the Test Report paper that is provided alongside your gateway, if the gateway came from factory with a BSP version that already has the webserver installed.

- If Kona Link is installed as part of an BSP upgrade, the default password for the user is set to the **gateway ID in capital letters**.

- If you decide to enable Kona Link it is highly recommended to change the passwords.

Kona Link passwords can be changed from the gateway command line as follows:

- webserver-configuration-manager -u basic -p "mybasicpassword"

Login to Kona Link

- Open a web browser and enter your gateway’s IP address into the URL bar to connect to Kona Link webserver.
- When prompted, log in to the webserver using the credentials you set from the previous slide, or use the credentials provided on the Test Report sheet.

Best-In-Class, Carrier Grade &
Most Cost Effective
Portfolio of Gateways, Network Server,
Sensors & Applications