Gateway User Guide

Table of Contents

Device Setup

Thunder NSI Gateway integrates cyber-security, high reliability SD-WAN, and network intelligence technologies to create simplified Next-Generation networks. Gateway devices are designed to be deployed on-premise at an organization's branch locations and managed through Thunder's cloud controller. All Gateway hardware devices integrate next generation multi-layered cyber security and support multiple Internet (WAN) connections to provide secure, reliable, networks.

Thunder offers three Gateway models:
Gateway 20 (G20) - Designed for small branch offices
Gateway 100 (G100) - Designed for medium sized branch offices
Gateway X (GX) - Virtual machine able to scale for large corporate HQ's

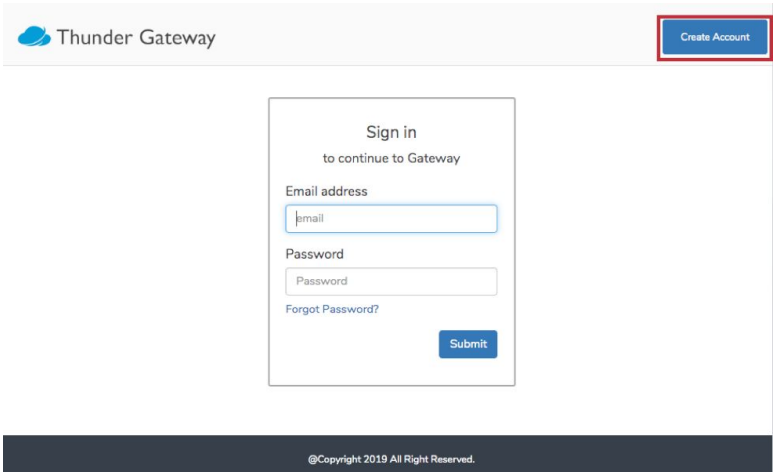
This guide treats all the devices as a Gateway device since the user interaction for each of these devices are the same even though the hardware varies.

Thunder provides two separate interfaces that admin's can use to configure their Gateway devices. Thunder recommends only using the local user interface (UI) for local troubleshooting and manually configuring the device when disconnected. The cloud UI should be used for all generation management and configuration in normal operation.

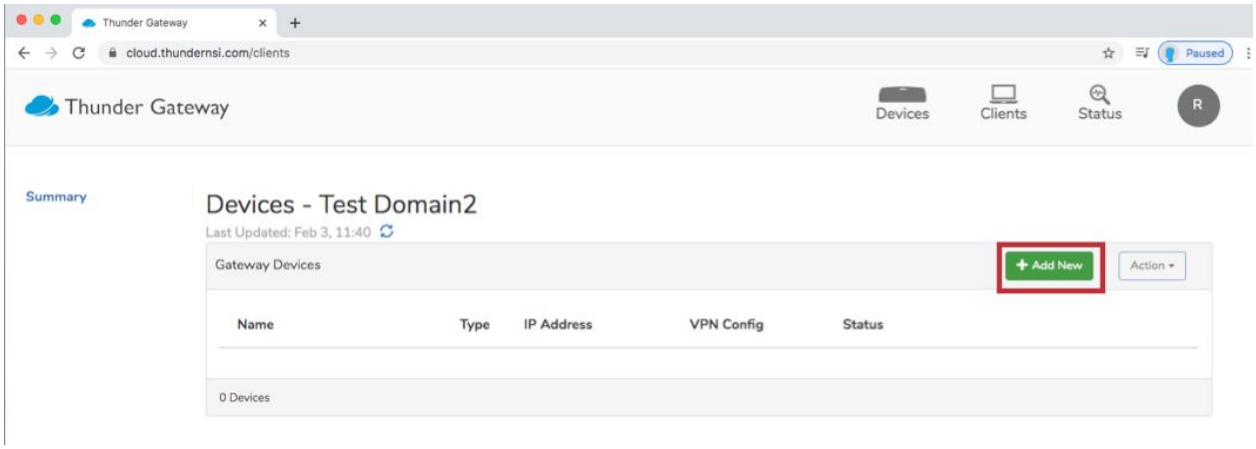
Step 1: Cloud Configure.

In most cases, it makes sense to configure the device in the cloud before it is connected to the Internet. Network admins can quickly create a cloud account by going to start.thundernsi.com and clicking create account in the top right hand corner.

Note - Gateway devices are configured to get a DHCP IP address from the upstream Internet Provider. If the Internet connection requires PPPoE or other manual settings, then the Admin will need to login into the local UI to ensure the device can connect to the Internet.

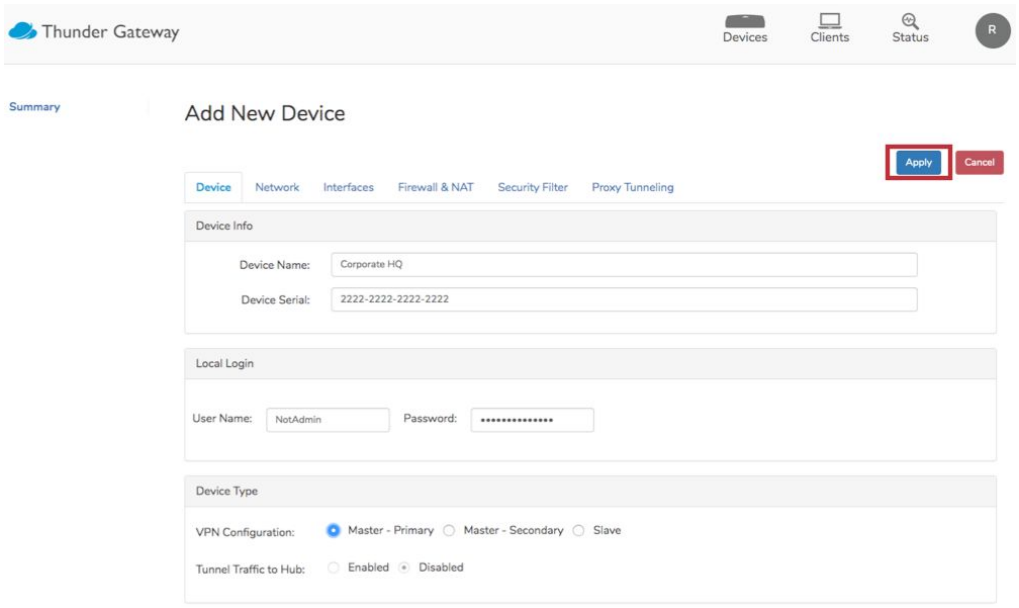


Once an account has been created and verified then the user can login to the account and start adding devices to their default network.



A new device can be added with minimal effort. Thunder automatically sets default settings that are designed to work for most networks. The only information that is required to be completed is on the first tab of the device setup. Once complete, the device is added by clicking apply.

Device Name: Unique name used to identify the device on the network (i.e. street address of building)
Device Serial: Unique serial number Thunder assigned to the device. The serial number can be found on the box label or on the label located at the underside of the physical device.
Local Login Username: Username that can be used to access the local UI of the device
Local Login Password: Password that can be used to access the local UI of the device
Device VPN Configuration: One master device is required to coordinate the creation of automatic VPN's between devices in the network. This master master device must have a public IP address. All other devices should be slaves.



Step 2: Connect Internet Cable

By default, Interface 1 is setup for the WAN (Internet) connection. Connect to the Internet by inserting the WAN Ethernet cable into the Ethernet 1 port. If connected properly the cloud LED will go solid blue. If the device does not connect properly on its own then the local UI can be accessed to modify default settings.

Step 3: Plug in Power

It is important to power up the Gateway in the correct order as described below.

Modem/Upstream Router: If accessible, the modem and/or upstream router should be power cycled before plugging in the Gateway device. Give 2-3 minutes for the modem/router to fully power cycle prior to powering the Gateway device.

Gateway device: Ensure that all Ethernet cables are securely connected and then power on the Gateway device. Once the device boots up, it will connect to the cloud and automatically update its configuration. The update process will take ~5 minutes and the device will automatically restart during the configuration process. The device will be cloud managed and functional after it completes its configuration bootstrap process.

Device Bootstrap

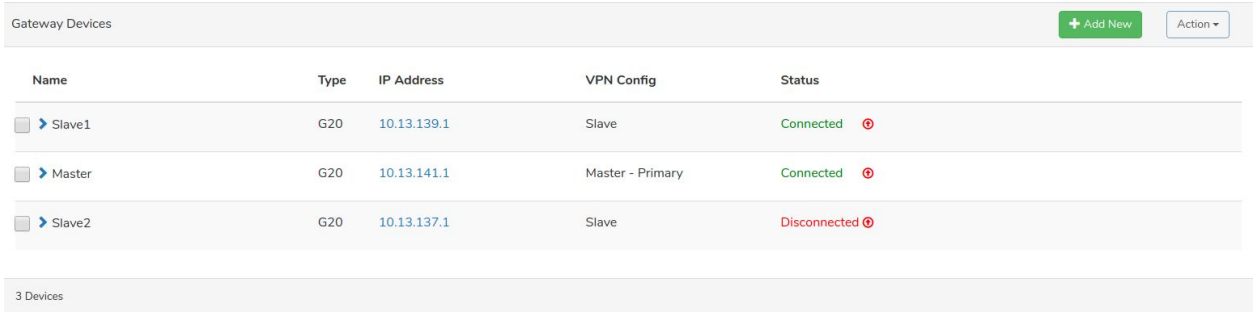
When the Thunder gateway is in the factory reset condition, it will try to connect to the Cloud to receive its configuration. If the device is configured without issues on the Cloud UI and the Thunder gateway has access to the Cloud, it will receive its configuration as well as its certificates. After receiving the configuration, the device will reboot with the new configuration.

Device Upgrade

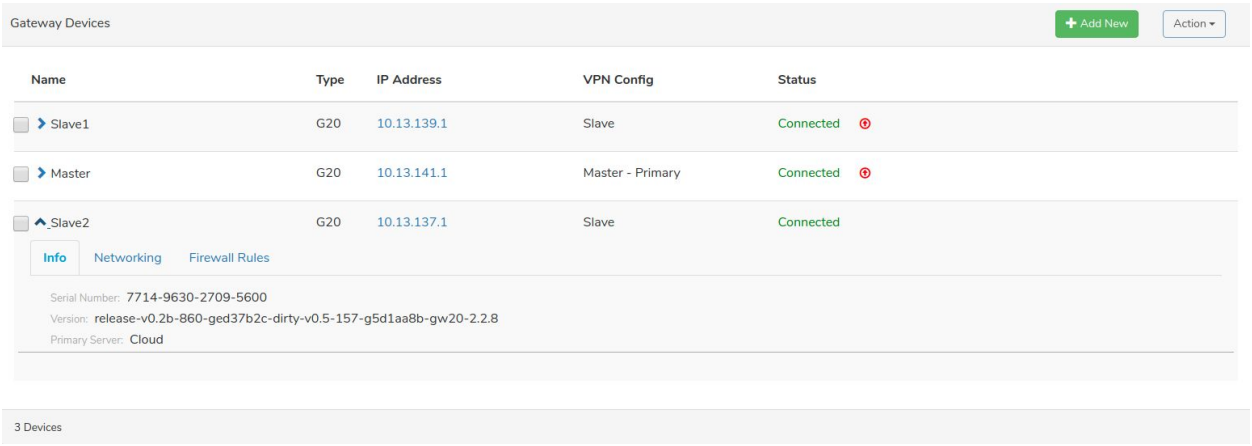
The upgrade procedure for gateway devices can be done over the cloud or manually via the local UI.

Cloud

When there is an upgrade available for a Thunder gateway, a red arrow will appear next to the device on the network summary page as such:



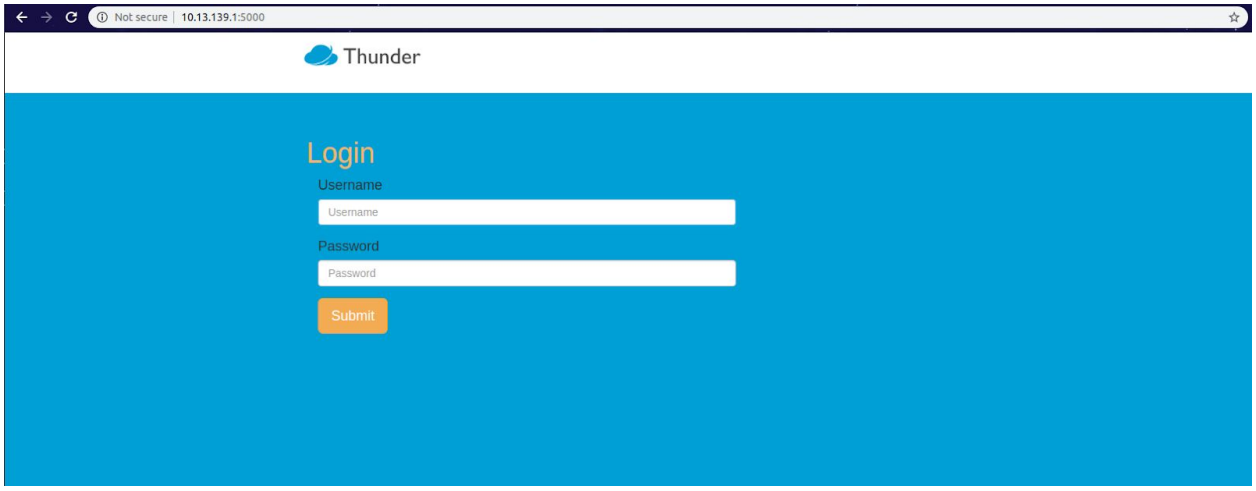
When this red arrow is clicked, the device will start the upgrade procedure if it is connected to the cloud. During the upgrade, the device will reboot several times to apply the upgrade and receive the current configuration on the cloud. After the upgrade, the red arrow will disappear and the upgraded version info can be seen in the info section of the device. To toggle this section, click the blue arrow on the left of the device.



Local UI

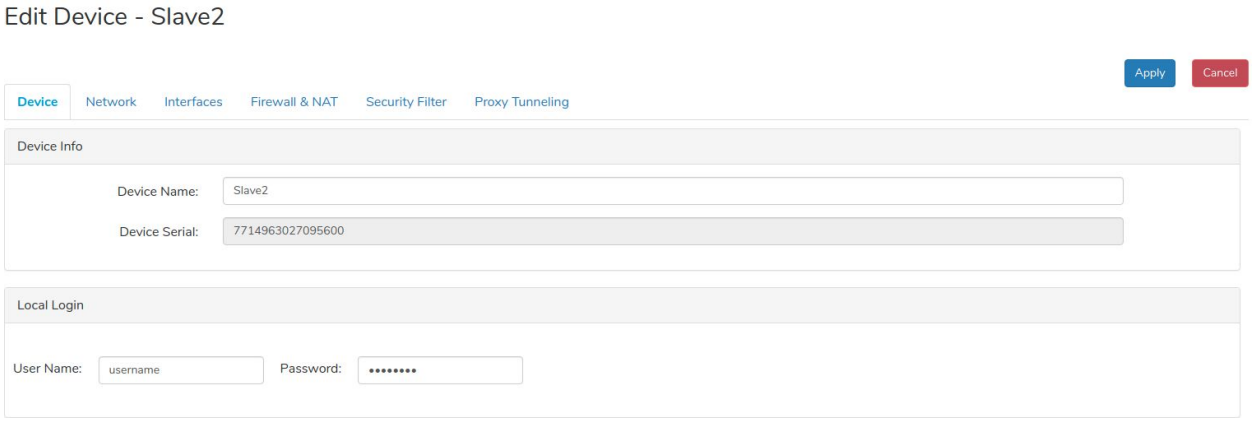
The Thunder gateway devices can also be upgraded over the local UI. To install firmware over the local UI, the firmware image must be downloaded to a PC. To receive a requested firmware image, please contact ThunderNSI.

The local UI can be accessed with a PC connected to the Thunder gateway's LAN network. On the PC web browser, connect to the Thunder gateway's LAN IP on port 5000.



If this page does not load, check if the Thunder gateway is on and the PC is connected to the Thunder gateway's LAN network. By default, the LAN ports are the 3rd and 4th ethernet ports from the left on G20 devices and the 5th - 8th ethernet ports on G100 devices. If there is no issue with the connection and the Thunder gateway is powered but the local UI is not loading, reboot the Thunder gateway by shortly pressing the reset button for 2-3 seconds.
On the user login page, enter the username and password defined in the Local Login section of the Cloud UI

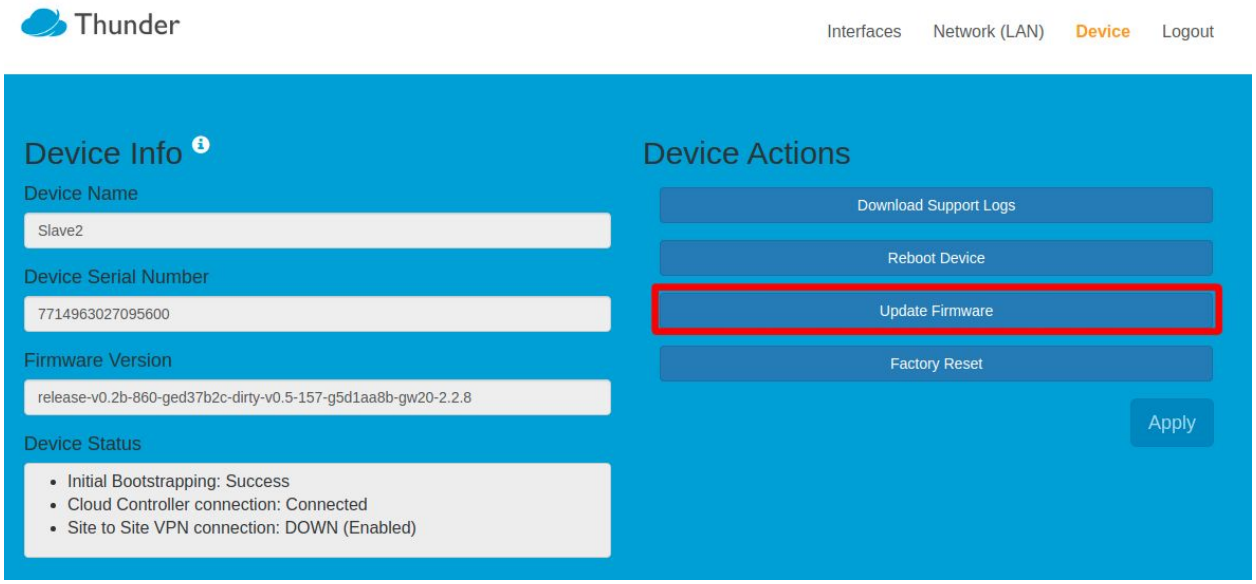
Cloud-> Device->Device>Local Login



If the Thunder gateway has not been connected to the cloud yet, the default username and password are:

- Username: ThunderNSI
- Password: Welcome1!

After logging in, the current firmware version can be found on the main page. In this page under Device Actions, click the Update Firmware button and select the firmware image to be installed.



After the image is selected, the device will download the image from the PC and start the upgrade process. During the upgrade, the device will reboot several times to apply the upgrade and receive the current configuration on the cloud.

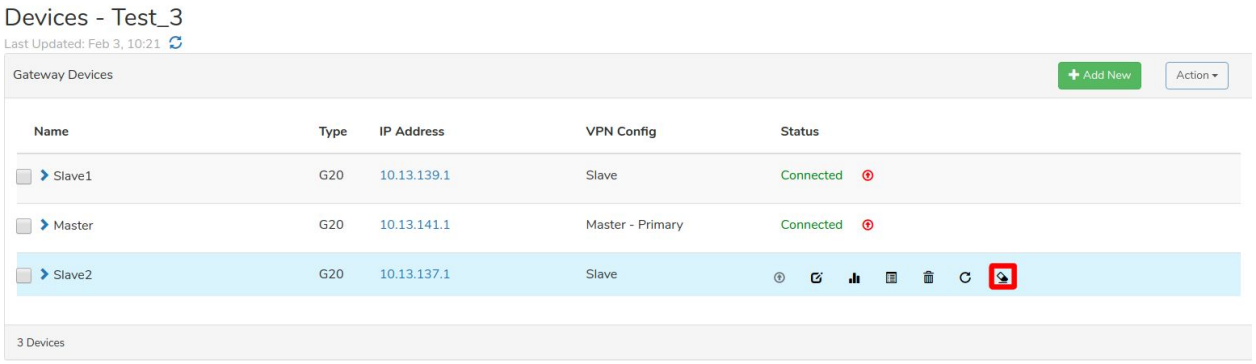
Factory Reset

There are 3 different ways to perform a factory reset on the device.

Cloud

If the device is connected to the cloud, a factory reset can be initiated over the cloud UI. To initiate a factory reset over the cloud UI, navigate to the network summary page. Hover the mouse over the desired Thunder gateway and click on the Factory Reset button.

In addition, multiple devices can be factory reset at the same time by checking the box in the left hand side of the page to select the devices and then clicking on the Action drop down on the right hand side of the page.



The Thunder gateway will perform a factory reset and reboot several times to apply the current cloud configuration.

Local UI

Even if the Thunder gateway is not connected to cloud, a factory reset can be initiated over the local UI by clicking the Factory Reset button on the main page once logged in.

Manual Factory Reset

Gateway 20 or G100

If G20 or G100 is unresponsive to the local UI, a factory reset can be manually initiated by using the end of a paper clip or pin to press and hold the reset button on the Thunder gateway for ~10 seconds or until the cloud light on the center of the device turns off.

LTE & Wi-Fi Kit Assembly

Gateway devices are designed to be modular. Technical professionals can add modules to increase the functionality of the Gateway devices. Both G20 and G100 have expansion slots on its PCBA which can be used to add LTE and Wi-Fi modules. Thunder supports the following modules that work with its devices.
G20 or G100 WiFi - Compex WLE600VX (mini PCIe)
G20 LTE - Quectel EC25 (mini PCIe CAT 4)
G100 LTE - Quectel EM06 (M.2 CAT 6 module)
Installation of the modules should be completed by a professional technician. Contact support@thundernsi.com for access to the full installation guide. The basic installation overview of these modules are outlined below.

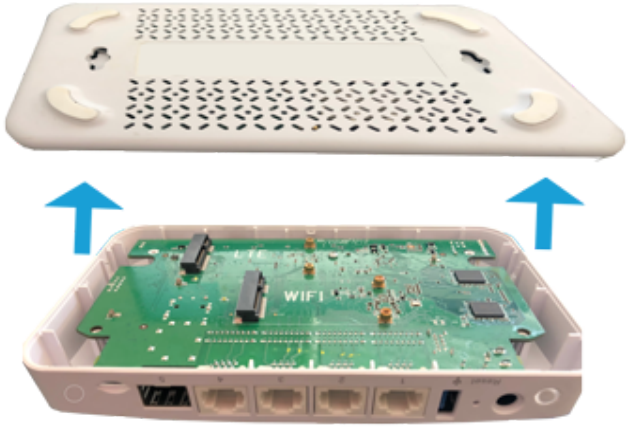
G20

G20 has two mini PCIe slots on the underside of the device.

1. To start the installation, ensure the device is disconnected from power. Flip the device upside down and remove four sticker feet from the bottom panel of the device.

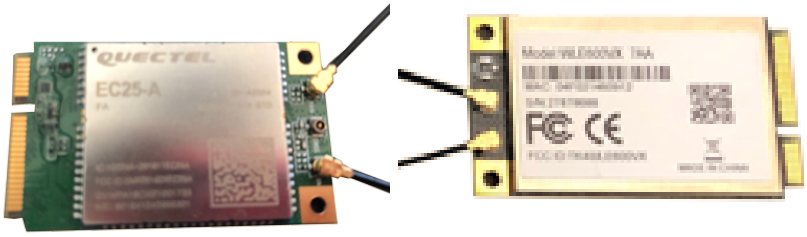
2. Use a size Phillips screwdriver to remove the 4 screws found beneath the four sticker feet.

3. Pry off the bottom panel by separating the bottom panel from the rest of the device. Start the separation of the bottom panel above the Ethernet ports and it should separate easily.

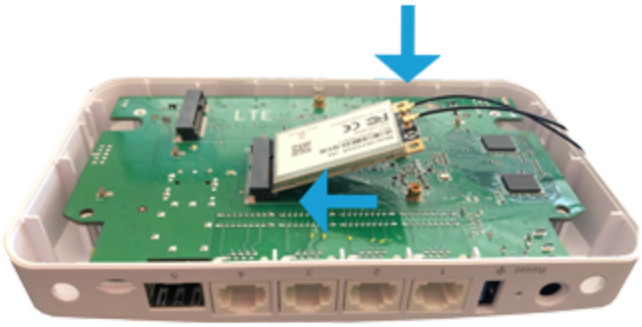


4. Punch out the antenna cover holes from the device enclosure. G20 has 4 locations for antennas. We recommend starting with the two back holes for the first two antennas and using the side holes only when using both Wi-Fi and LTE.

5. Connect SMA cables to the Wi-Fi and/or LTE module. The connectors should be for main & diversity (not GPS). LTE should use cables with female SMA connector cables while Wi-Fi should use cables with male SMA connectors.



6. Remove the mounting screws and insert the Wi-Fi or LTE module



7. Secure the module with mounting screws Screw: M3X0.5XL5 (Ni)(3M/2353) ; Tighten torque: 4~5±0.3kg-cm

8. Route the connected cable and insert the SMA connectors Tighten the SMA connectors so they are secured on the device

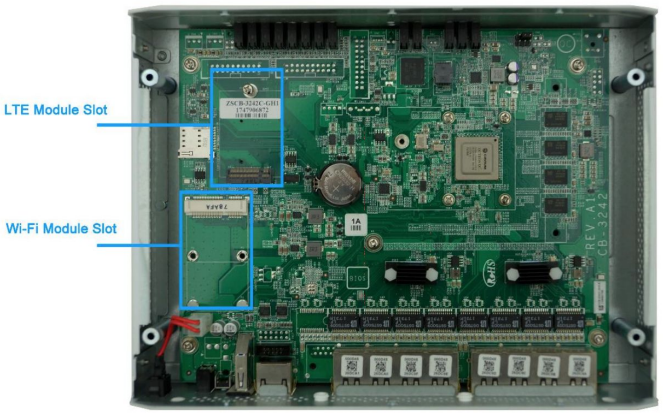
9. Repeat steps 4-8 for a second module (if required). Then secure the cable connectors to the module with a small amount of hot glue.

10. Snap the bottom panel back into place. Screw back in the 4 screws and put the 4 sticker footers back into place

11. Finished

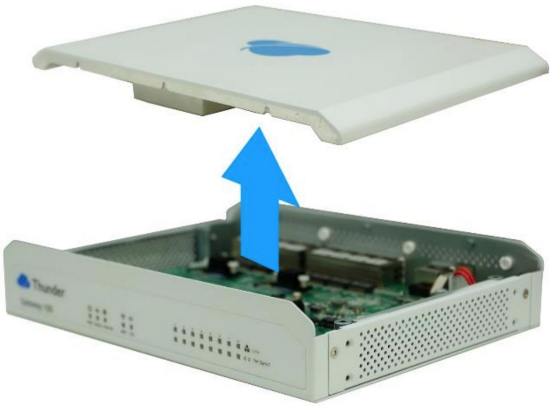
G100

G100 has one mini PCIe slot and one M.2 slot on the top of the PCBA.



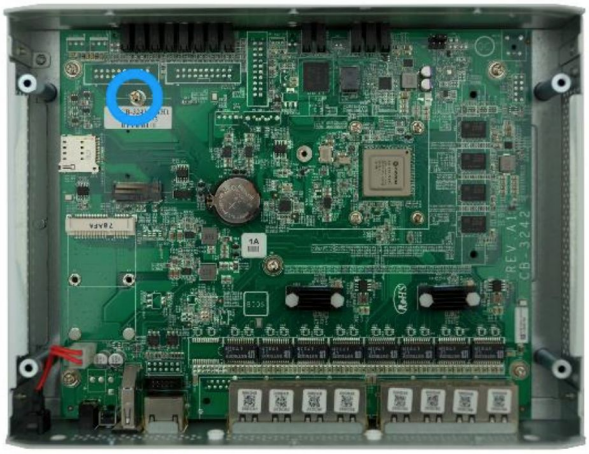
1. Remove four screws from the bottom panel of the device

2. Lift up to remove the top panel

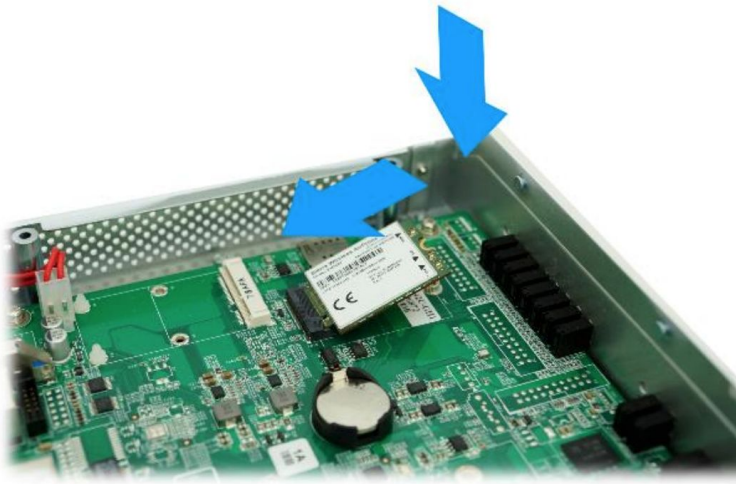


3. Remove plastic covers from SMA holes

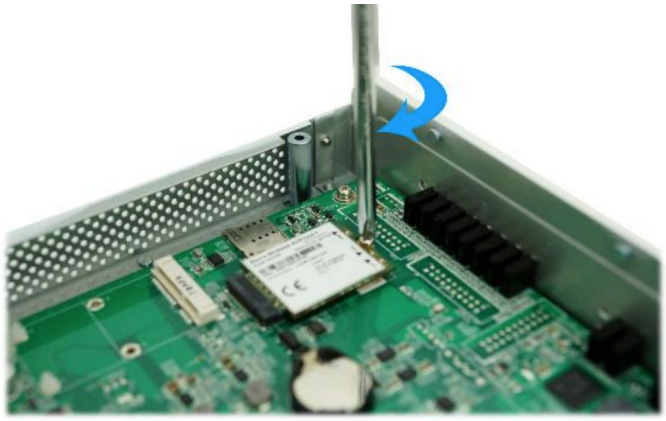
4. Remove the LTE or WiFi mounting screw



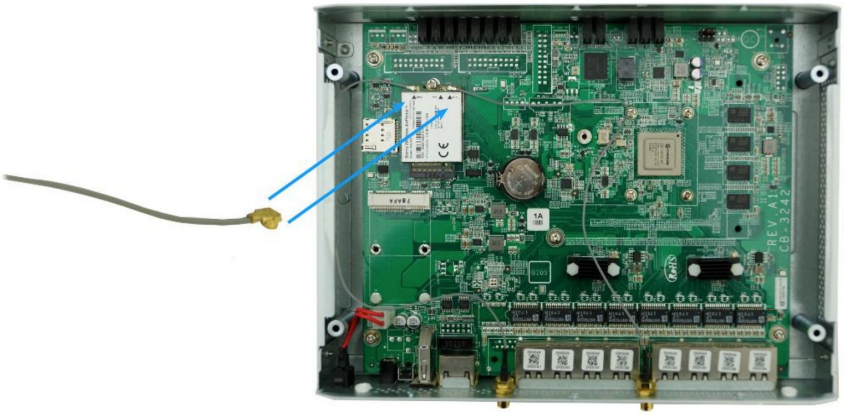
5. Insert the LTE module



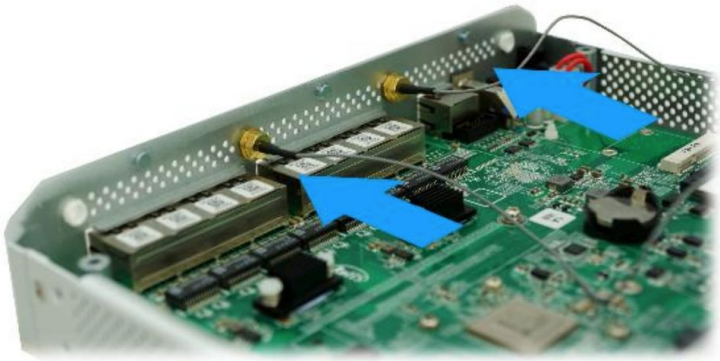
6. Secure LTE module with LTE mounting screw. Screw: M3X0.5XL5 (Ni)(3M/2353) ; Tighten torque: 4~5±0.3kg-cm



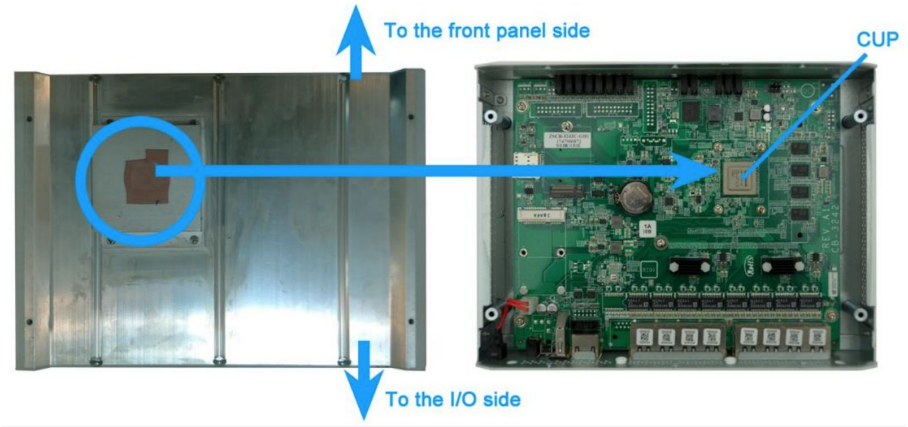
7. Connect the two antenna cables to the MAIN and AUXconnections on the LTE module



8. Route the connected cable and insert the SMA connectors. Tighten the SMA connectors so they are secured on the device. Repeat steps 4-8 for the Wi-Fi module.



9. Orient the thermal pad on the top panel with the CPU on the PCBA. When the top cover is placed correctly, the thermal pad will rest on the CPU.



10. Correctly place top panel back on top of the device and screw on two exterior LTE antennas

11. Screw back in the four screws in the bottom panel. Screw: M3X0.5XL5 (Ni)(3M/2353) ; Tighten torque: 4~5±0.3kg-cm

underside of the device.f the device is connected to the cloud, a factory reset can be initiated over the cloud UI. To initiate a factory reset over the cloud UI, navigate to the network summary page. Hover the mouse over the desired Thunder gateway and click on the Factory Reset button.

LED Status Indicators

Each Gateway device has several LED's on the physical device. The LED's are indicators on the current overall status of the device as well as the individual status of specific ports and features. Below is a chart explaining the meanings of each LED for each Gateway Device.

GW20

	System	White: Solid - Gateway Loading, Blink - Firmware Updating Blue: Solid - Gateway Connected, Blink - No Internet
1	Ethernet 1	White: Solid - LAN 10/100/1000, Blink - LAN 10/100 Blue: Solid - WAN 10/100/1000, Blink - WAN 10/100
2	Ethernet 2	White: Solid - LAN 10/100/1000, Blink - LAN 10/100 Blue: Solid - WAN 10/100/1000, Blink - WAN 10/100
3	Ethernet 3	White: Solid - LAN 10/100/1000, Blink - LAN 10/100 Blue: Solid - WAN 10/100/1000, Blink - WAN 10/100
4	Ethernet 4	White: Solid - LAN 10/100/1000, Blink - LAN 10/100 Blue: Solid - WAN 10/100/1000, Blink - WAN 10/100
5	SFP Cage 5	White: Solid - LAN 10/100/1000 Blue: Solid - WAN 10/100/1000
	VPN	White: Solid - VPN Connected, Blink - VPN Down
	Security	White: Solid - Security Running , Blink - Security Down
	Wi-Fi	White: Solid - Wi-Fi Connected (LAN), Blink - No Wi-Fi Traffic (LAN) Blue: Solid - Wi-Fi Connected (WAN), Blink - No Wi-Fi Traffic (WAN)
	LTE	White: Solid - LTE Connected, Blink - Connected with Low Signal
	USB	White: Solid - LTE Connected, Blink - Connected with Low Signal

GW100

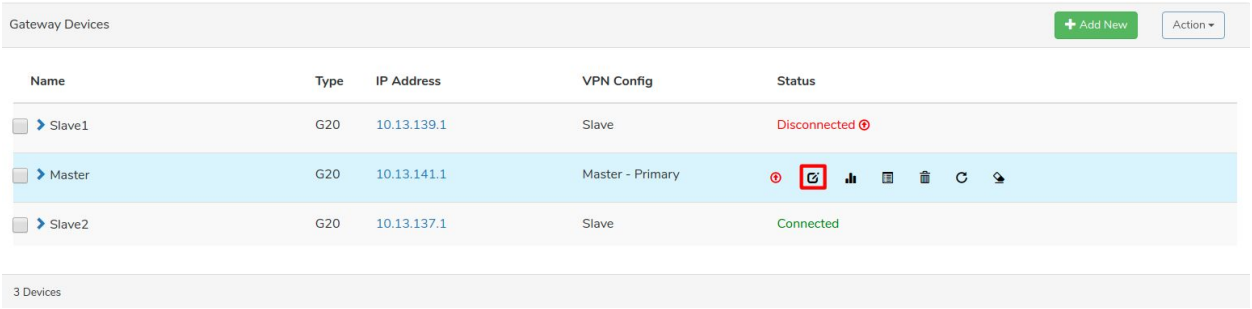
	Power	Solid – Power On, Blink – Firmware Updating
	Status	Solid – Device Running, Blink – Device booting up
	Internet	Solid – Device can access the Internet, Blink – No Internet access
	Wi-Fi	Solid – Wi-Fi module installed and configured
	LTE	Solid – LTE module installed and configured
1	Ethernet 1	Link: Solid – Client device connected Port Speed: Solid – 10/100/1000, Blink – 10/100
2	Ethernet 2	Link: Solid – Client device connected Port Speed: Solid – 10/100/1000, Blink – 10/100
3	Ethernet 3	Link: Solid – Client device connected Port Speed: Solid – 10/100/1000, Blink – 10/100
4	Ethernet 4	Link: Solid – Client device connected Port Speed: Solid – 10/100/1000, Blink – 10/100
5	Ethernet 5	Link: Solid – Client device connected Port Speed: Solid – 10/100/1000, Blink – 10/100
6	Ethernet 6	Link: Solid – Client device connected Port Speed: Solid – 10/100/1000, Blink – 10/100
7	Ethernet 7	Link: Solid – Client device connected Port Speed: Solid – 10/100/1000, Blink – 10/100
8	Ethernet 8	Link: Solid – Client device connected Port Speed: Solid – 10/100/1000, Blink – 10/100

Connectivity

Interface Configuration

By default, G20 ports 1, 2 and 5 configured as WAN interfaces, and ethernet ports 3 and 4 configured as a LAN bridge. By default G100 ports 1-4 are configured as WAN interfaces and 5-8 are configured as a LAN bridge. These default settings can be changed over the Cloud UI or the local UI. However, once the Thunder gateway is assigned to a network on the Cloud UI, the local UI locks interface configurations made over the local UI to ensure cloud configurations are not easily overwritten.

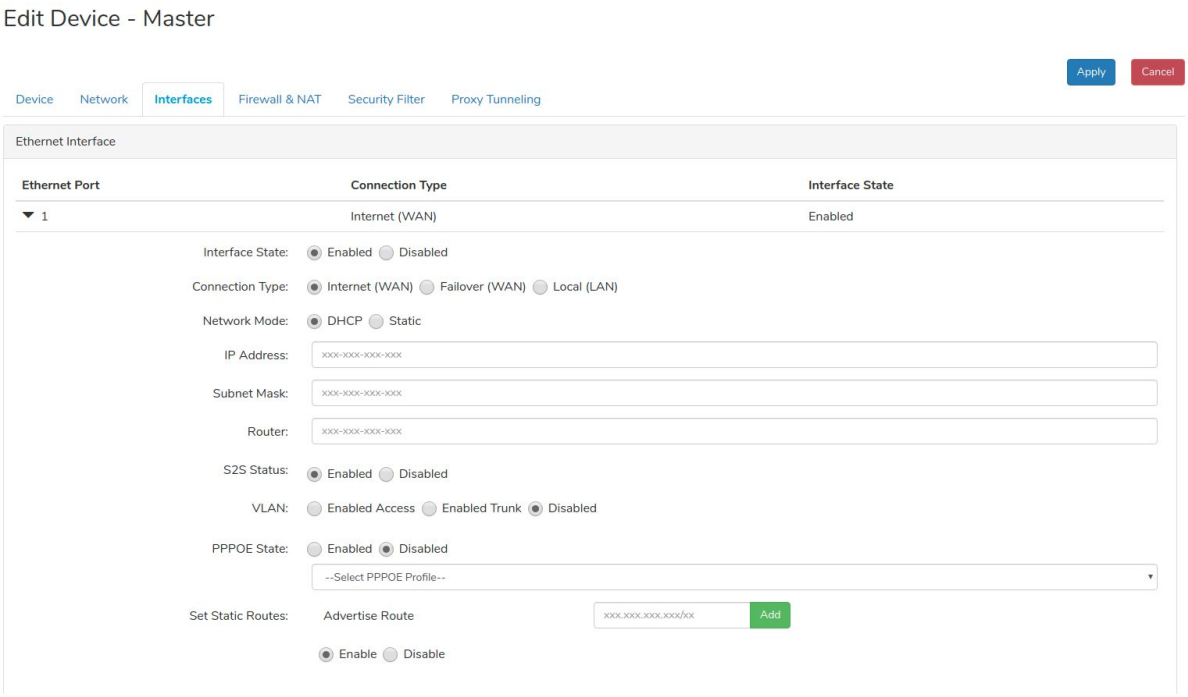
Interface assignments can be made over the Cloud UI in the Interface tab of a selected Thunder gateway. Navigate to the Thunder gateway settings by hovering the mouse over a desired Thunder gateway and click the Edit button.



After getting into the Thunder gateway settings page, navigate to the Interfaces tab. On this tab, after clicking on the desired interface, a list of settings will be available. On this list:

- The selected interface can be enabled/disabled
- The connection type can be set to Load Balance(WAN), Failover(WAN) or Local(LAN)
- The network mode can be selected to be DHCP or static IP
- S2S feature over the interface can be enabled/disabled
- A VLAN can be assigned to the interface
- PPPOE can be enabled/disabled
- Static routes on the interface can be assigned as well as advertisement of the static route over the S2S network can be enabled/disabled

The Thunder gateway will not accept configurations which do not have at least one LAN ethernet port to ensure that the device can be locally accessed.



WAN Configuration

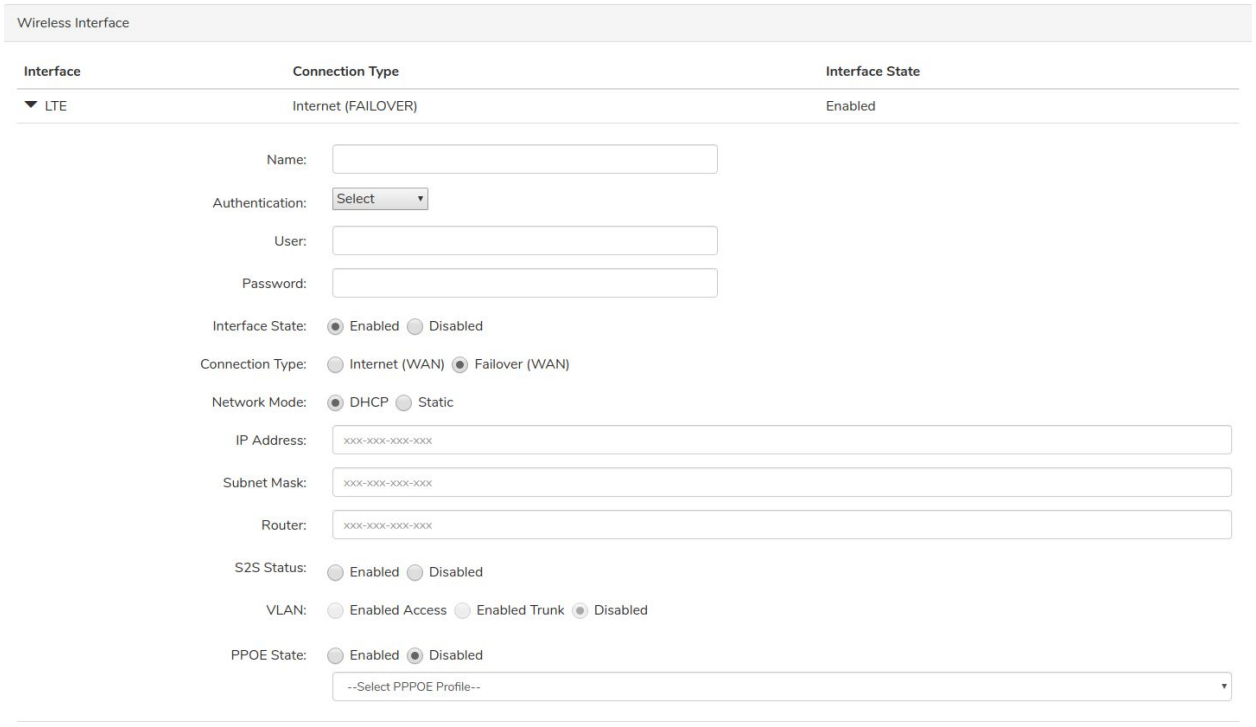
When an interface is assigned to be a WAN interface, the interface can operate as a Load Balance or a Failover interface. Load Balance interfaces will share the traffic amongst themselves. If a Load Balance interface goes down, the other Load Balance interface(s) will take on the failed interface's traffic. Failover interfaces are disabled while there are Load Balance interfaces currently up. When all Load Balance interfaces go down, the Failover interface will go up and provide internet access until at least one of the Load Balance interfaces goes back up.

LTE Configuration

The LTE functionality can be configured in the Wireless Interface field. In addition to the configurations on the Ethernet ports, the LTE configurations have:

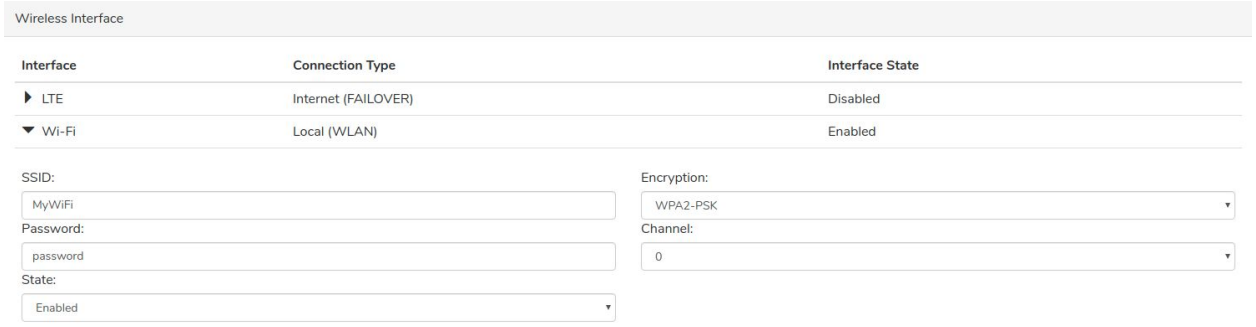
- APN or Name: This field holds the APN given by the mobile providers and must be filled or left blank depending on the mobile provider's instructions.
- Authentication: If the mobile provider requires authentication to access their network, the authentication type as well as username and password must be entered.

By default, the LTE interface is set to Failover mode.



Wi-Fi Configuration

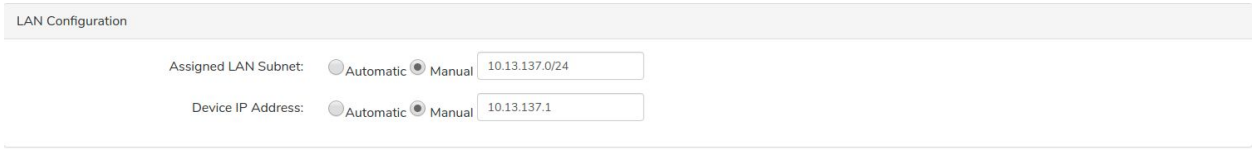
In the Wi-Fi configuration section, the Thunder gateway's Wi-Fi SSID, channel, password and encryption type can be entered.



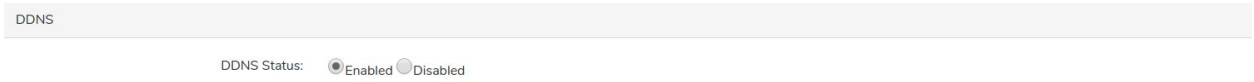
LAN Configuration

Different from the WAN configuration, the LAN configuration is done in two different tabs. On the Interfaces tab, the LAN interface's S2S status, VLAN selection and PPPoE settings can be entered. The network mode and static routes for LAN are configured on the Network tab.

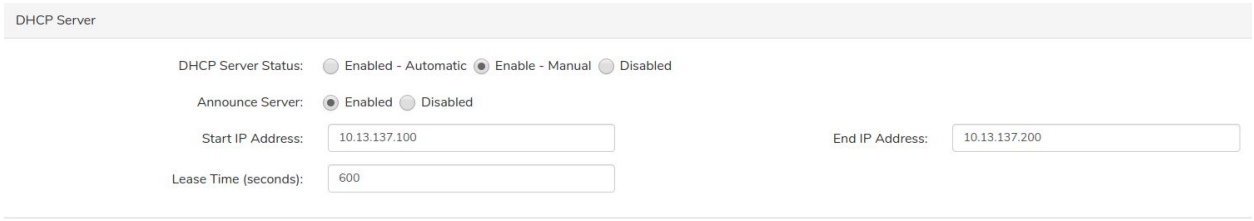
On the Network tab, the user can select the network mode on the LAN Configuration field. The network mode can be automatic or manual IP and subnet assignment.



The DDNS feature is enabled in the DDNS field



The DHCP settings are entered in the DHCP Server field. Here, the DHCP server's IP assignment can be configured along with the lease time and whether or not the subnet will be announced to the S2S network. The Start and End IPs must be compatible with the information entered on the LAN Configuration field.



Static routes can be assigned under the Routes Field. In this field, the network to be routed and the gateway can be entered as well as whether or not the route will be announced to the S2S network.

DHCP IP reservation for the LAN can be configured on the DHCP IP Reservation field. The desired name, device's MAC address and the reserved IP address can be entered in this field.

Failover Modes

The Thunder gateway is commonly used with multiple internet connections to provide a robust internet connection. These multiple internet connections can be configured on the Thunder

gateway as a combination of load balance and failover interfaces. For information on how to configure an interface as load balance or failover mode, please refer to Interface Configuration.

Load Balance WAN with LTE As Failover

One of the most commonly used scenarios is to have the WAN ethernet interfaces on the Thunder gateway configured as load balance interfaces while the LTE interface is configured as a failover interface. With this configuration, the traffic will flow through the WAN ethernet interfaces when there are no connectivity problems with the ethernet connection. If connectivity issues on the WAN ethernet interface arise, the Thunder gateway will direct traffic to the LTE interface to ensure that internet connection is only lost for a short time. Meanwhile, the Thunder gateway will constantly check if the WAN ethernet connection is restored. Once internet connection on the WAN ethernet interface is detected, the LTE interface will be suspended and the traffic will flow again over the WAN ethernet interface.
The LTE interface is always treated as a failover interface as LTE connections are more costly than ethernet connections, causing them to be generally used as a failover.

Load Balance WAN with Another WAN As Failover

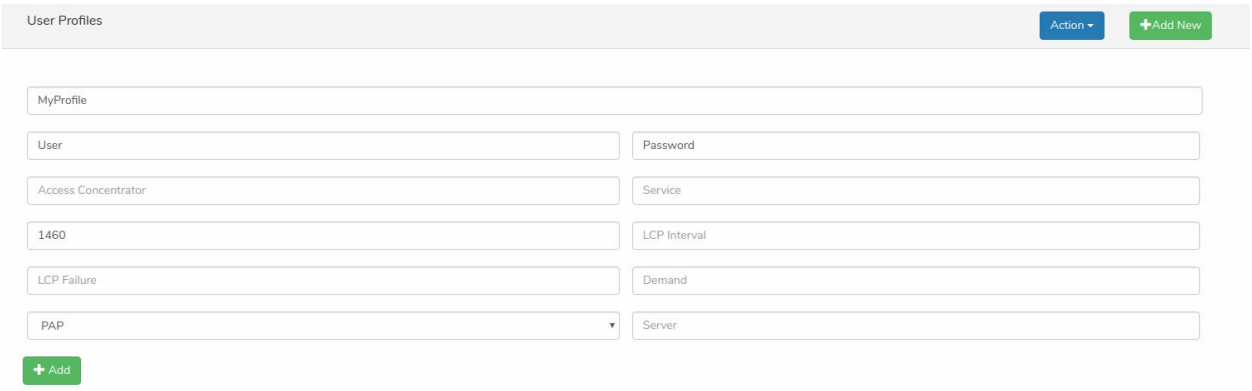
In the case that there are ethernet connections available from multiple different ISPs, the Thunder gateway can be configured to failover to ISP 2's connection whenever ISP 1's connection has connectivity issues. Similar to the use case where LTE is configured as the failover interface, traffic will flow through ISP 2's connection only while ISP 1's connection is lost. This solution is mostly used when a network's downtime must be minimal and the second ISP connection has a data limit. It is recommended to not use connections in the same network for load balance and failover interfaces as the cause of the loss of connection on the load balance interface will result in the failover interface failing as well. Which defeats the purpose of the setup.

Multiple Load Balance WAN

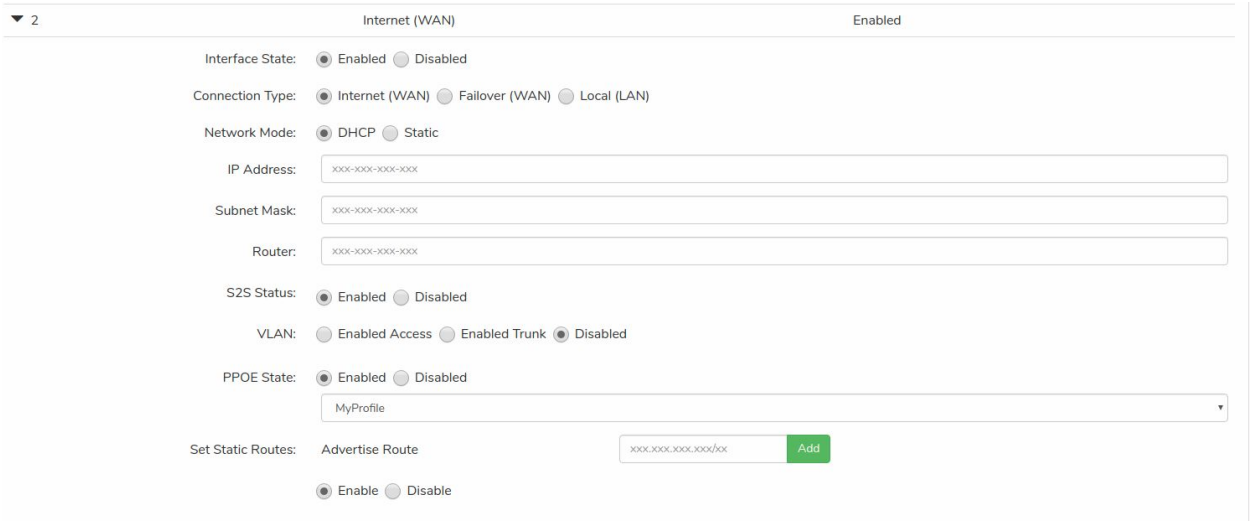
When the gateway has ethernet connection from multiple different ISPs, the Thunder gateway can be configured to balance the traffic load between the multiple connections. The connections will equally share the incoming and outgoing traffic amongst themselves to increase the bandwidth of the internet access.

PPPoE Setup

To set up a PPPoE connection on an interface, navigate to the Interfaces tab on the Cloud UI. Create a PPPoE Profile in the User Profiles field. Enter all required information and click Add.



After adding a profile, click on the desired interface, enable PPPoE State and select the profile.



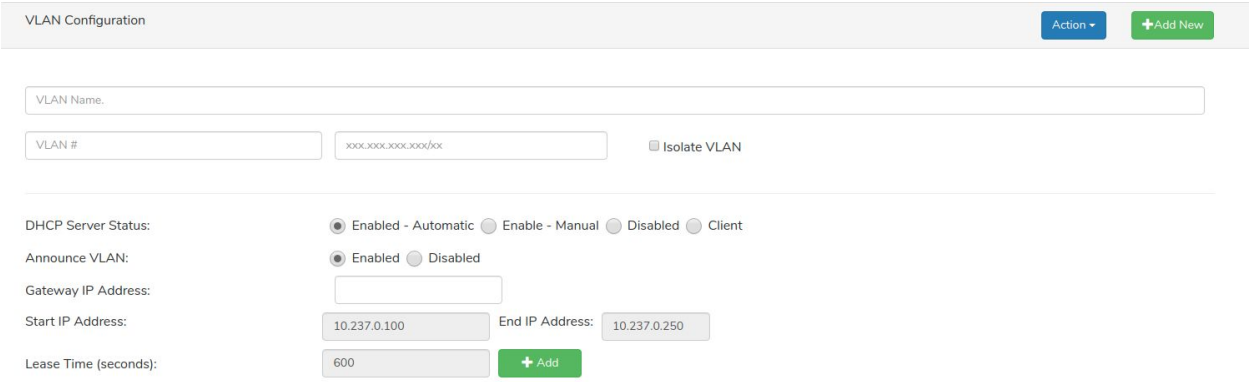
When the configuration is set, click apply to send the configuration to the Thunder gateway.

VLAN Configuration

There are 2 steps to assign a VLAN to a desired interface. Firstly, a VLAN profile must be created. Then, the profile must be applied to the desired interface.

VLAN Profile Creation

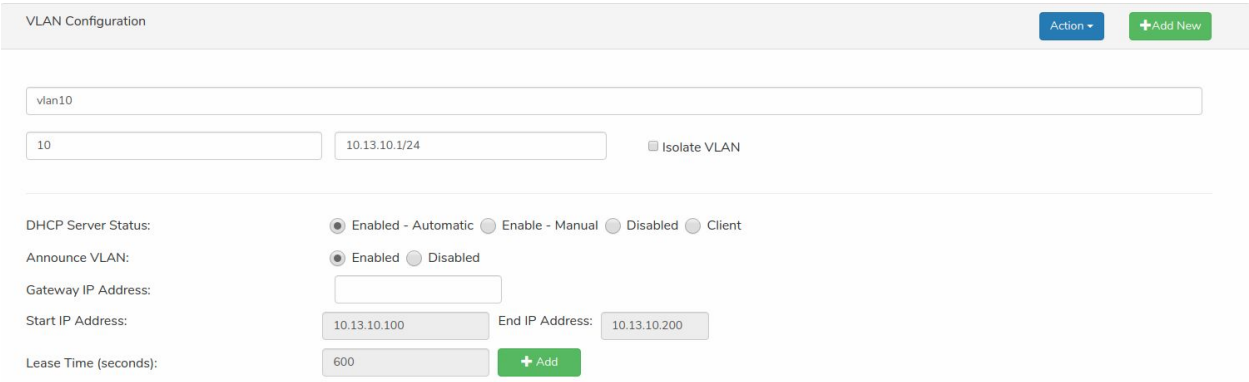
To create a VLAN profile, navigate to the VLAN Configuration field in the Network tab on the Cloud UI. On the VLAN Configuration field, enter the desired VLAN configuration. Multiple VLANs defined on the Thunder gateway can be isolated by clicking the checkbox labeled Isolate VLAN. When VLANs are isolated, any communication between the VLANs are blocked.



Below are some example configurations.

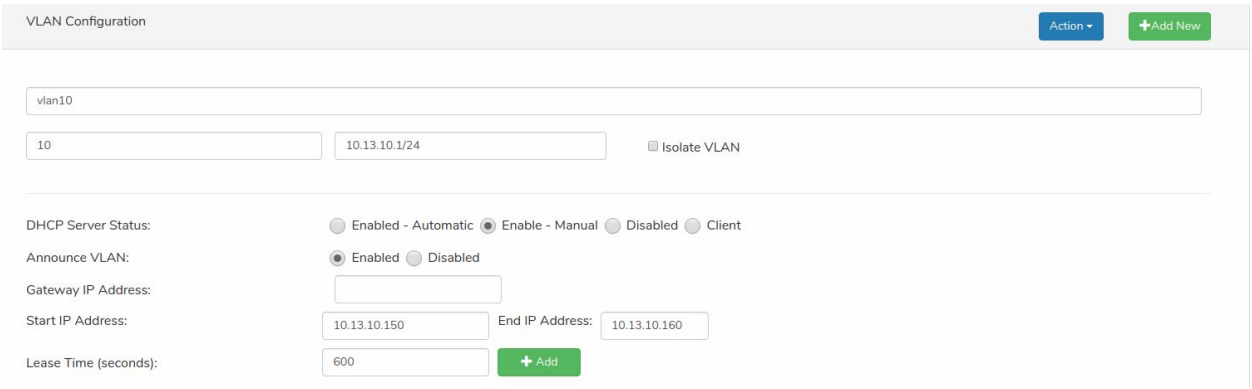
Example 1 : LAN with Automatic DHCP

To create a VLAN for LAN interface with Automatic DHCP, create the VLAN with DHCP Server Status to be “Enabled - Automatic”. To announce the VLAN to the S2S network, enable Announce VLAN. As this VLAN is being created for a LAN interface, the Gateway IP Address field is not filled.



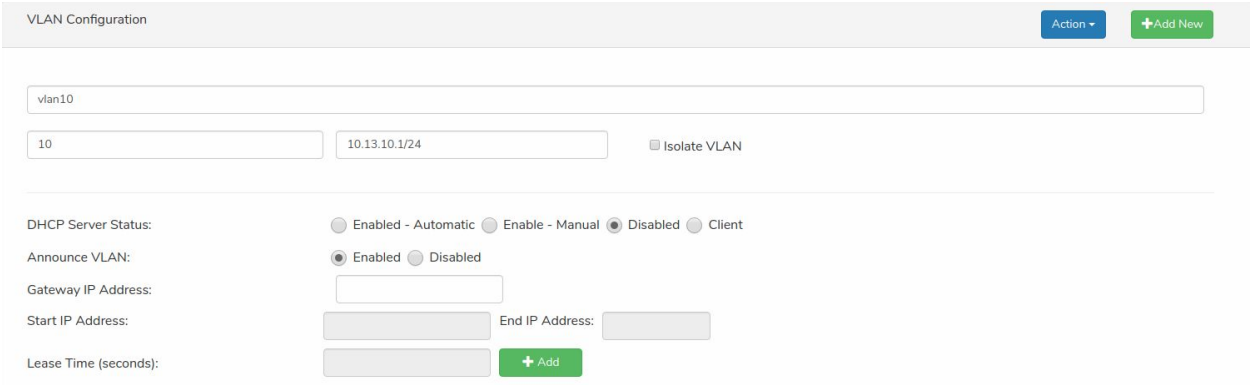
Example 2 : LAN with Manual DHCP

To create a VLAN for LAN interface with Manual DHCP, create the VLAN with DHCP Server Status to be “Enabled - Manual”. To announce the VLAN to the S2S network, enable Announce VLAN. As this VLAN is being created for a LAN interface, the Gateway IP Address field is not filled. The start and end IP addresses as well as the lease time must be defined for manual DHCP configurations.



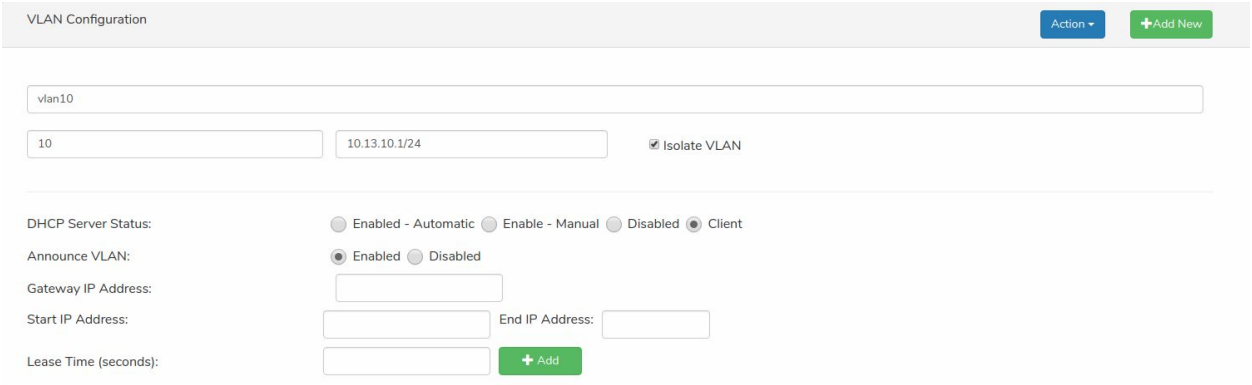
Example 3 : LAN with DHCP Disabled

To create a VLAN for LAN interface with DHCP disabled, create the VLAN with DHCP Server Status to be “Disabled”. To announce the VLAN to the S2S network, enable Announce VLAN. As this VLAN is being created for a LAN interface, the Gateway IP Address field is not filled.



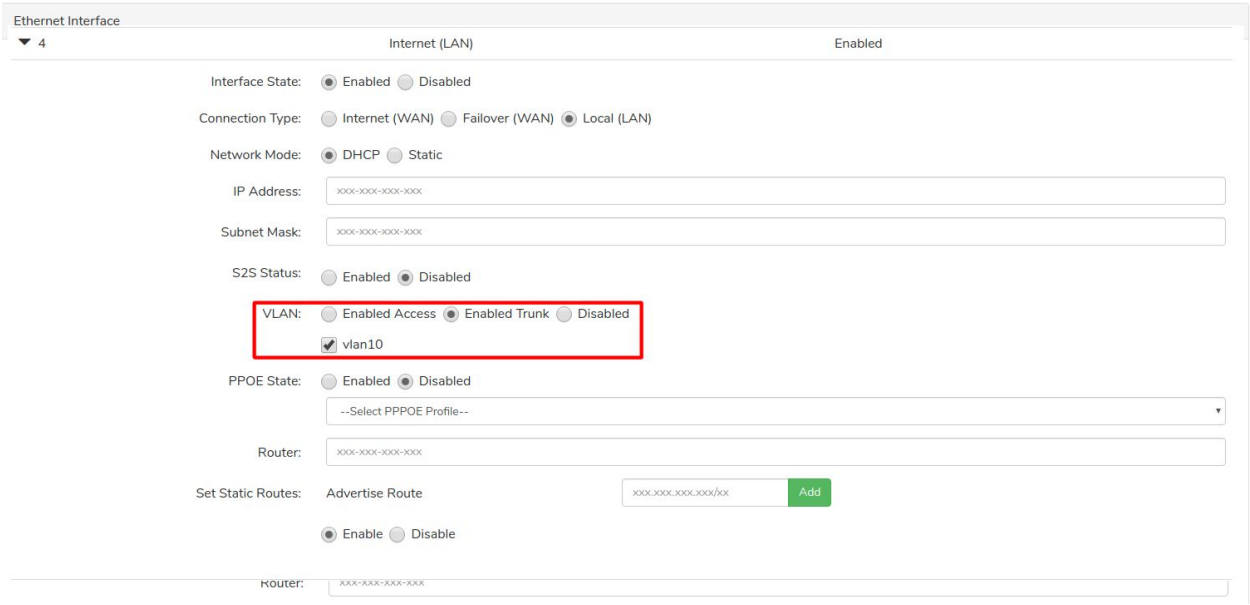
Example 4 : WAN

To create a VLAN for WAN interface, create the VLAN with DHCP Server Status to be “Client”. To announce the VLAN to the S2S network, enable Announce VLAN. As this VLAN is being created for a WAN interface; only the VLAN Name, VLAN # must be entered according to the VLAN DHCP server connected to the Thunder gateway’s WAN port.



VLAN Assignment

To assign the VLAN profiles, navigate to the Interfaces tab on the Cloud UI. Click on the desired interface. If the VLAN will be assigned to a WAN interface, make sure that the VLAN is created with Client as the DHCP Server Status. Enable the VLAN by specifying Access or Trunk mode and select the desired VLAN profile.



After the configuration is done, click apply to send the configuration to the Thunder gateway.

Routing

Default Routing

When Site-to-site VPN is disabled, devices in the Thunder gateway LAN subnets will be disconnected.

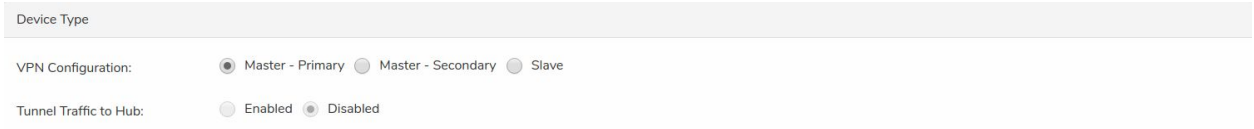
Site-to-Site VPN

To have Site-to-Site VPN on a Thunder gateway network, a Primary Master must be configured and must have a cloud connection. To enable Site-to-Site(S2S) VPN on a Thunder gateway network, first the Primary Master must be configured. Then, Slaves and the Secondary Master can be configured. There can be only one Primary Master and one Secondary Master in a network.

Important: The Master Thunder gateway must have a public IP or the 4500, 500 and 5555 ports must be forwarded to the Master Thunder gateway by the router connected to the Thunder gateway's WAN port.

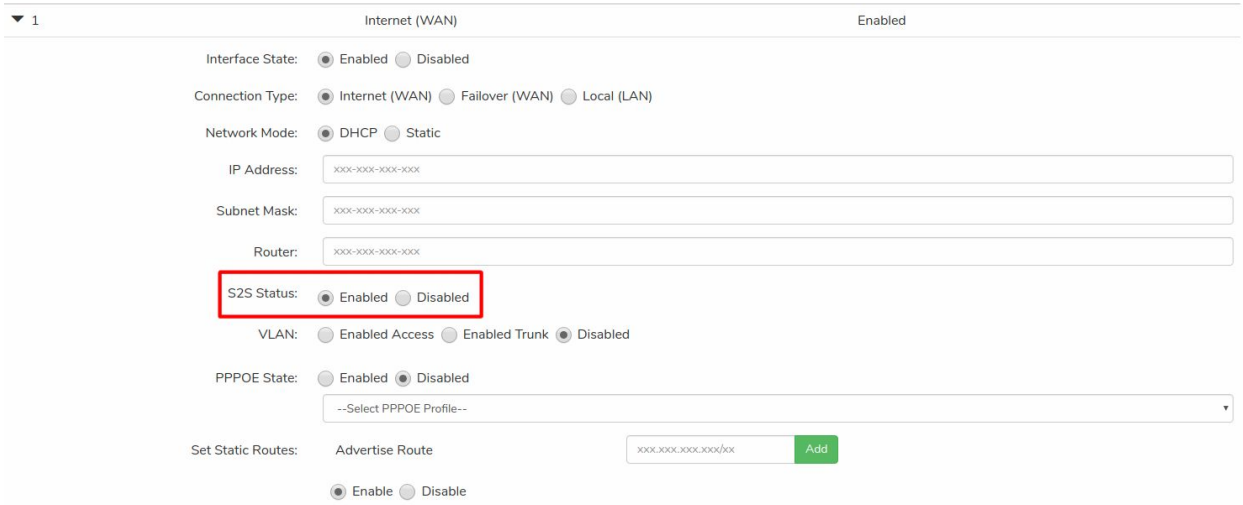
Primary Master Configuration

Navigate to the desired Thunder gateway's settings on the Cloud UI. Under the Device tab, select Primary Master as the VPN Configuration.



On the Network tab, enable Multi-Site VPN.

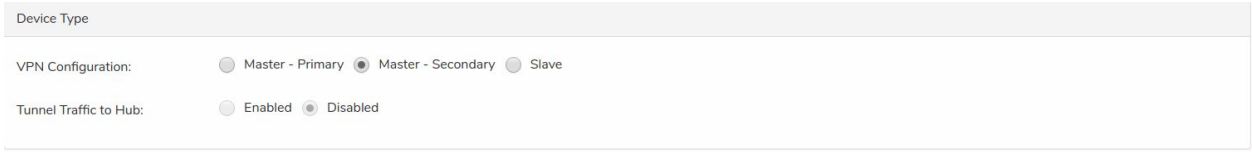
Finally, S2S must be enabled for the interfaces. Generally, the gateways are connected over their WAN interfaces and rarely they are connected over their LAN interfaces. So by default, S2S is disabled for LAN interfaces. If a gateway is on the LAN network of the Primary Master, S2S must be enabled for the LAN interface. If there are no gateways on the LAN network of the Primary Master, S2S for LAN interfaces should be disabled to decrease the S2S connection establishment time.



After the configuration is complete, click Apply to send the configuration to the Thunder gateway.

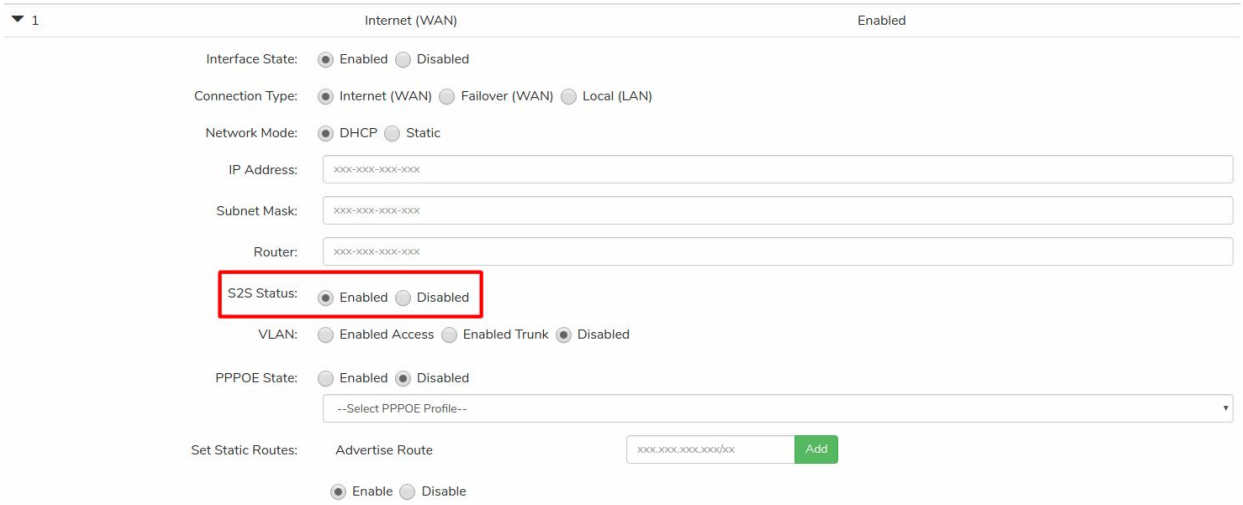
Secondary Master Configuration

In the case where the Primary Master loses connection, the Secondary Master will take on the role as Master to coordinate the S2S network. A Secondary Master is not required for the S2S network to function however, it is recommended to have as a failover system.
Navigate to the desired Thunder gateway's settings on the Cloud UI. Under the Device tab, select Secondary Master as the VPN Configuration.



On the Network tab, enable Multi-Site VPN.

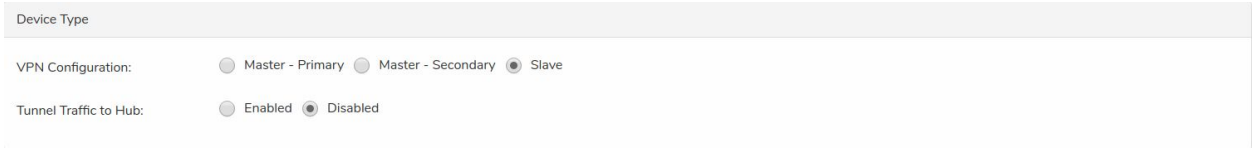
Finally, S2S must be enabled for the interfaces. Generally, the gateways are connected over their WAN interfaces and rarely they are connected over their LAN interfaces. So by default, S2S is disabled for LAN interfaces. If a gateway is on the LAN network of the Secondary Master, S2S must be enabled for the LAN interface. If there are no gateways on the LAN network of the Secondary Master, S2S for LAN interfaces should be disabled to decrease the S2S connection establishment time.



After the configuration is complete, click Apply to send the configuration to the Thunder gateway.

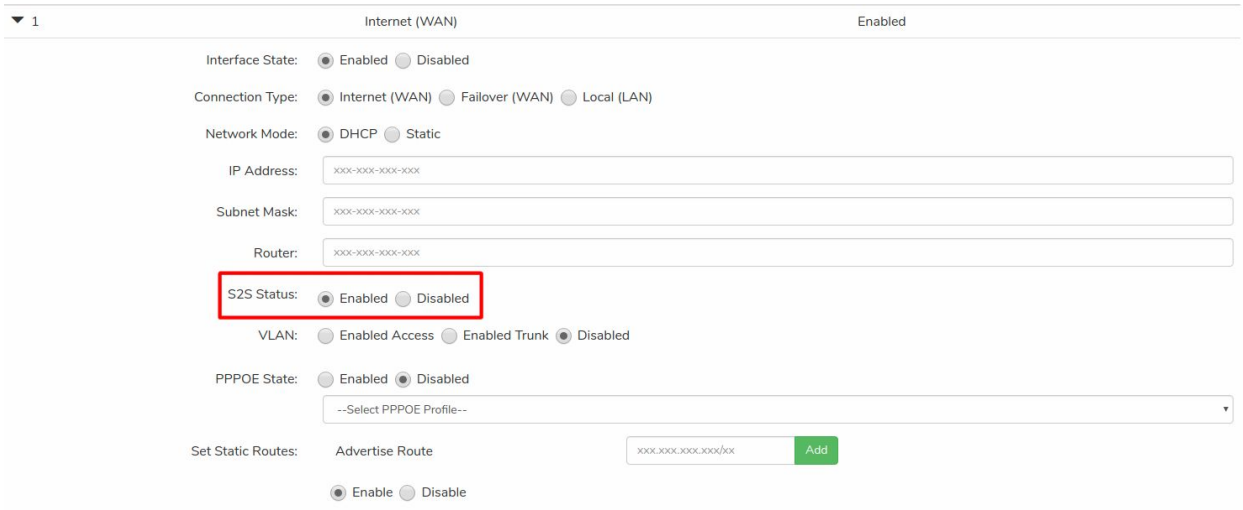
Slave Configuration

Multiple Slaves can be configured for the S2S network. Navigate to the desired Thunder gateway's settings on the Cloud UI. Under the Device tab, select Slave as the VPN Configuration.



On the Network tab, enable Multi-Site VPN.

Finally, S2S must be enabled for the interfaces. Generally, the gateways are connected over their WAN interfaces and rarely they are connected over their LAN interfaces. So by default, S2S is disabled for LAN interfaces. If a gateway is on the LAN network of the Slave, S2S must be enabled for the LAN interface. If there are no gateways on the LAN network of the Slave, S2S for LAN interfaces should be disabled to decrease the S2S connection establishment time.

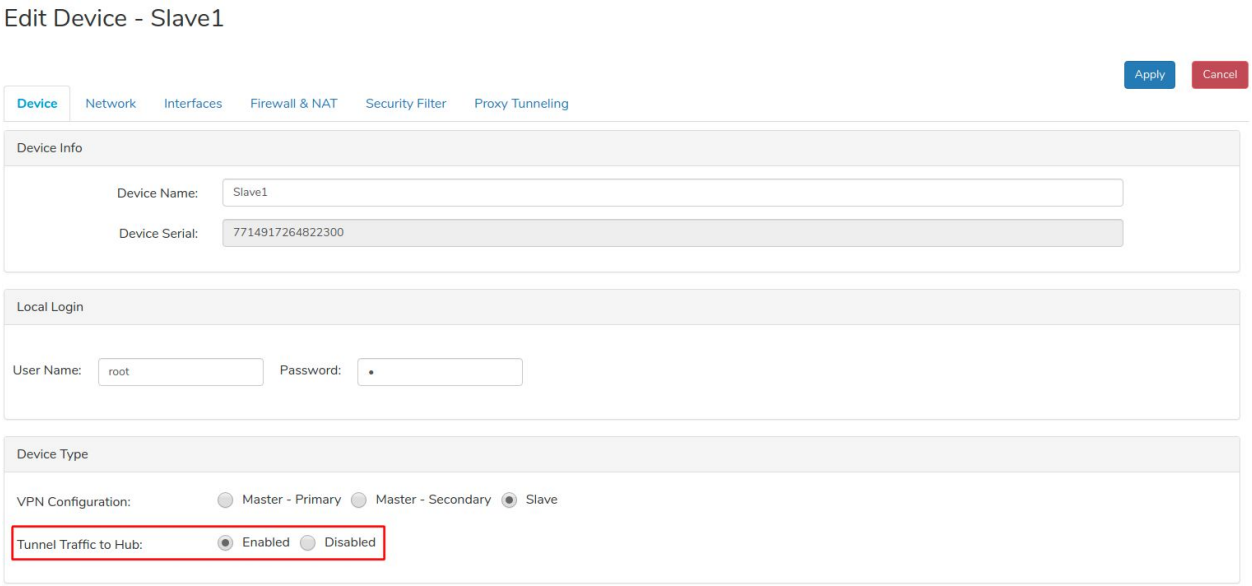


After the configuration is complete, click Apply to send the configuration to the Thunder gateway.

Tunnel Traffic To Master

To route all traffic from a site to the Master, click the edit button for the branch's gateway.

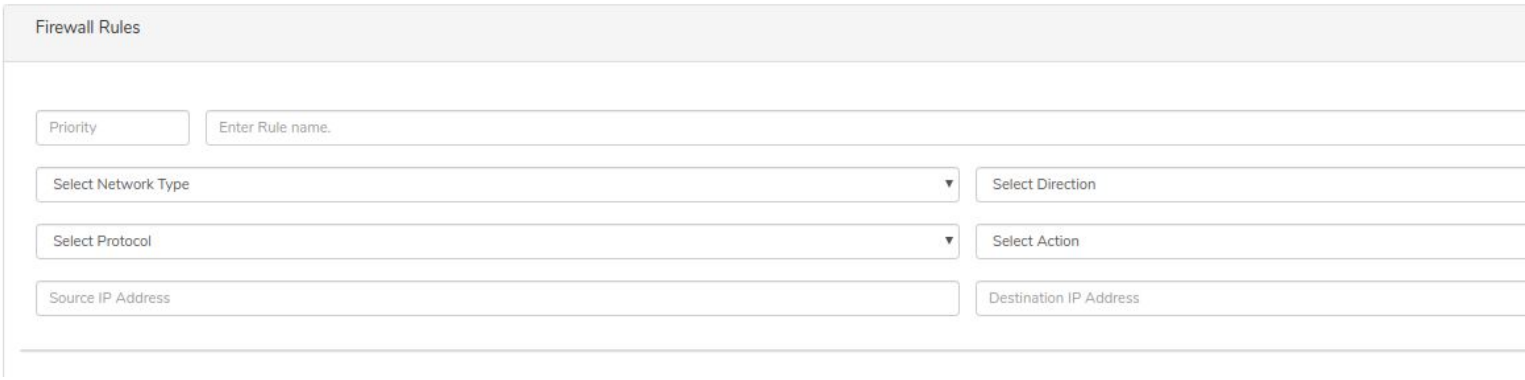
Under the "Device" tab, enable "Tunnel Traffic to Hub" under the Device Type field and click apply.

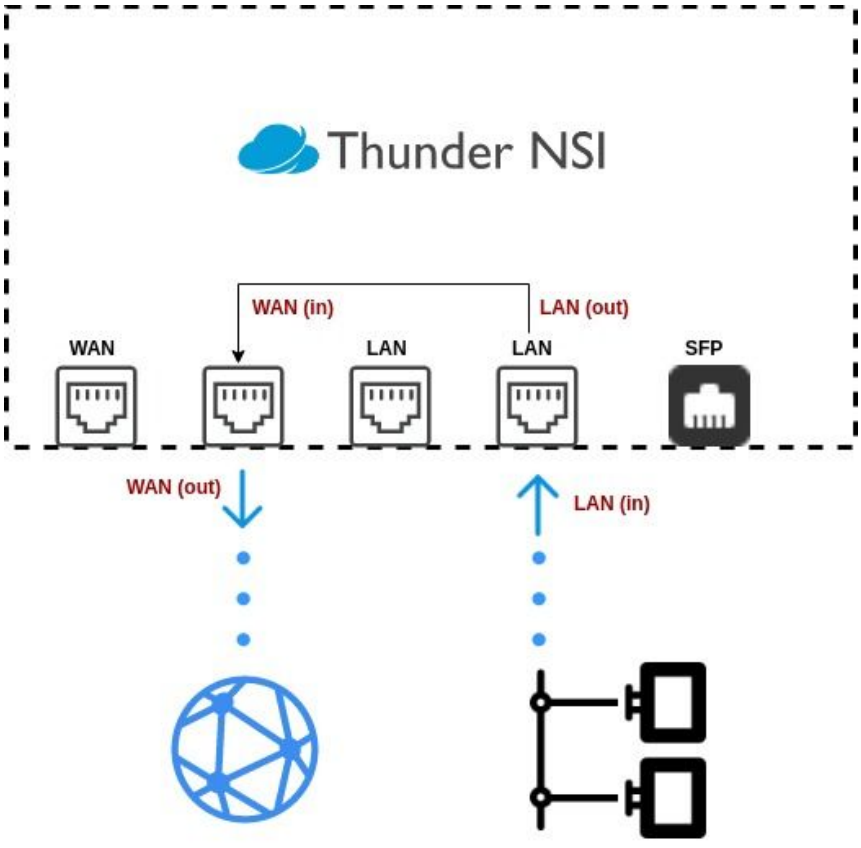


After enabling this feature, all traffic from the branch will be routed to the Master Thunder gateway.

Security

Firewall Rules





Priority : Enter your priority level

Rule Name : Enter your rule name

Network Type :
Aggregate
Private
Tunnel
WAN
LAN

Direction : In
Out

Protocol : All
TCP
UDP

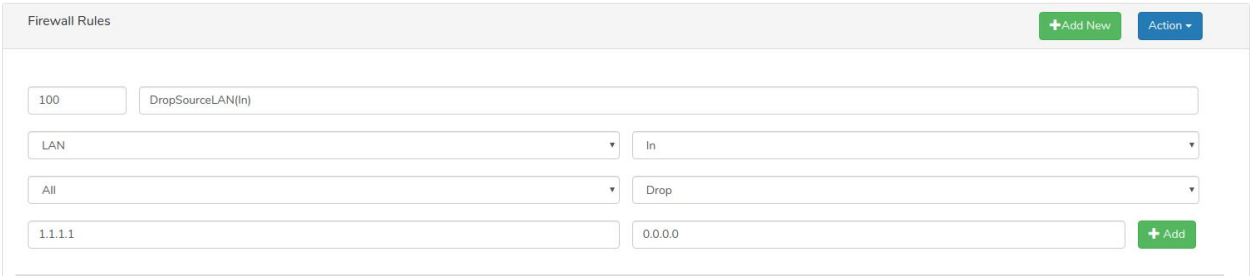
Action :
Accept
Drop

Source NAT
Destination NAT

Source IP : 0.0.0.0:0/0 - (ipv4_address:port/subnet)

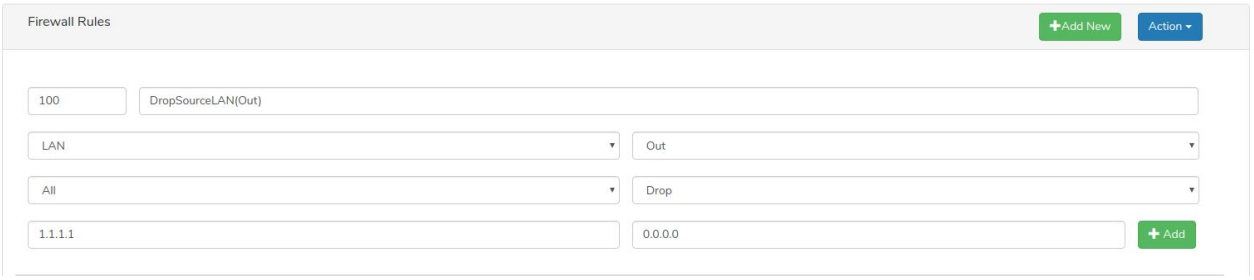
Destination IP : 0.0.0.0:0/0 - (ipv4_address:port/subnet)

Example 1 : Drop to source ip 1.1.1.1 LAN (in)



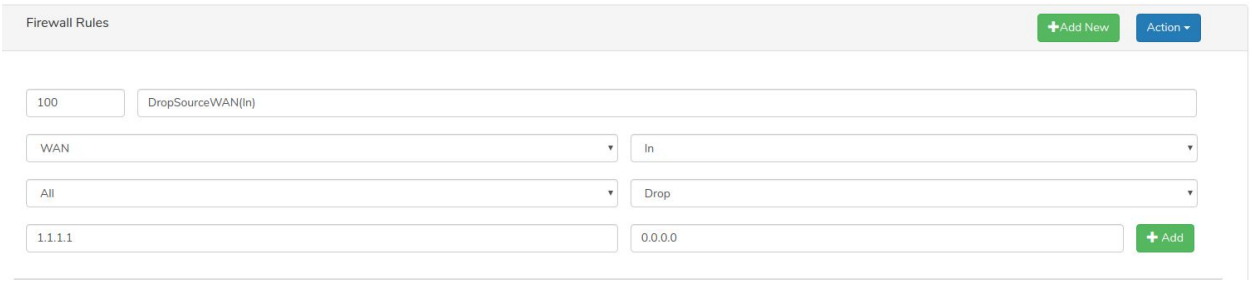
Conf : Priority: ‘Preferred priority’ / Rule Name: ’Preferred Rule Name’ / Network Type: LAN / Direction: In / Protocol: All
/ Action: Drop / Source IP : 1.1.1.1 / Destination IP : 0.0.0.0

Example 2 : Drop to source ip 1.1.1.1 LAN (out) (Dropped according to the source ip of the incoming packet)



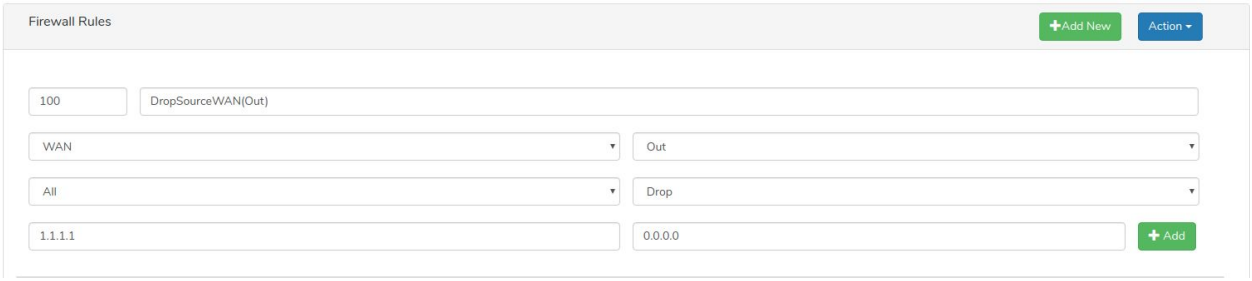
Conf : Priority: ‘Preferred priority’ / Rule Name: ’Preferred Rule Name’ / Network Type: LAN / Direction: Out / Protocol: All
/ Action: Drop / Source IP : 1.1.1.1 / Destination IP : 0.0.0.0

Example 3 : Drop to source ip 1.1.1.1 WAN (in)



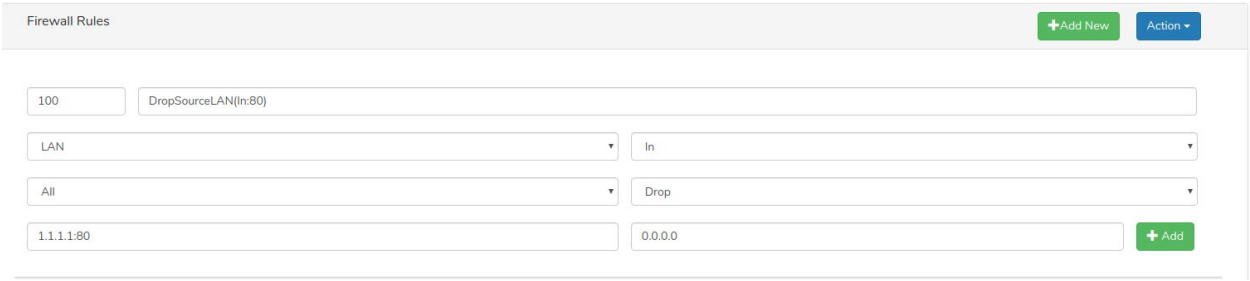
Conf : Priority: ‘Preferred priority’ / Rule Name: ’Preferred Rule Name’ / Network Type: WAN / Direction: In / Protocol: All
/ Action: Drop / Source IP : 1.1.1.1 / Destination IP : 0.0.0.0

Example 4 : Drop to source ip 1.1.1.1 WAN (out) (Dropped according to the source ip of the incoming packet)



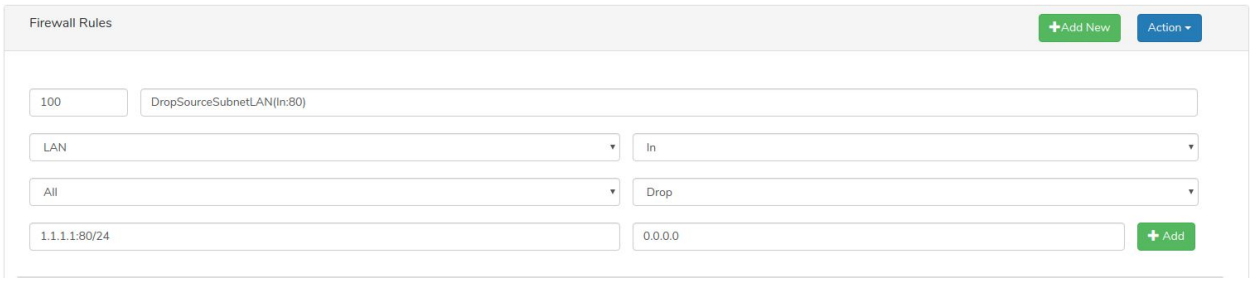
Conf : Priority: 'Preferred priority' / Rule Name: 'Preferred Rule Name' / Network Type: WAN / Direction: Out / Protocol: All
/ Action: Drop / Source IP : 1.1.1.1 / Destination IP : 0.0.0.0

Example 5 : Drop to source ip 1.1.1.1 LAN (in) only 80 port



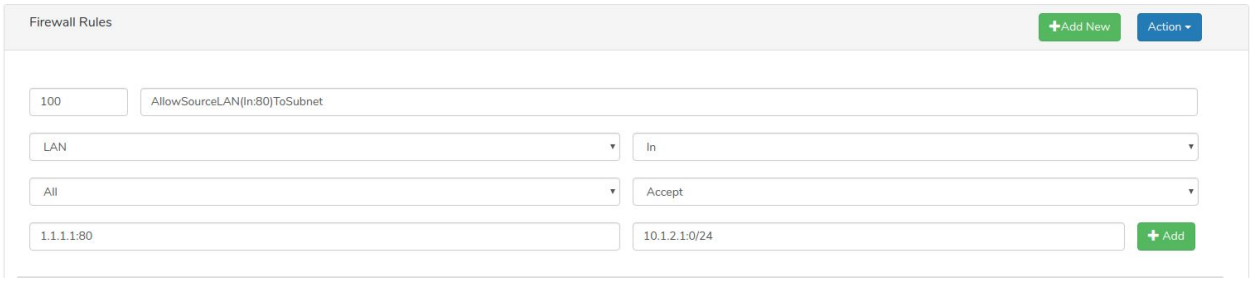
Conf : Priority: 'Preferred priority' / Rule Name: 'Preferred Rule Name' / Network Type: LAN / Direction: In / Protocol: All
/ Action: Drop / Source IP : 1.1.1.1:80 / Destination IP : 0.0.0.0

Example 6 : Drop to source subnet 1.1.1.1/24 LAN (in) only 80 port



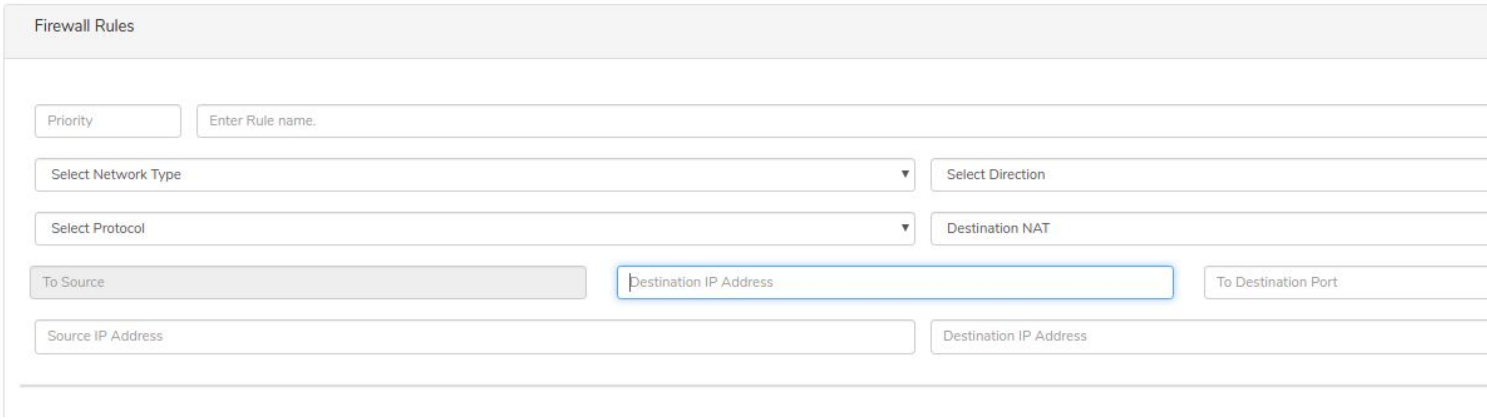
Conf : Priority: 'Preferred priority' / Rule Name: 'Preferred Rule Name' / Network Type: LAN / Direction: In / Protocol: All
/ Action: Drop / Source IP : 1.1.1.1:80/24 / Destination IP : 0.0.0.0

Example 7 : Allow to source ip 1.1.1.1 LAN (in) only 80 port -> destination subnet 10.1.2.1/24 and all port



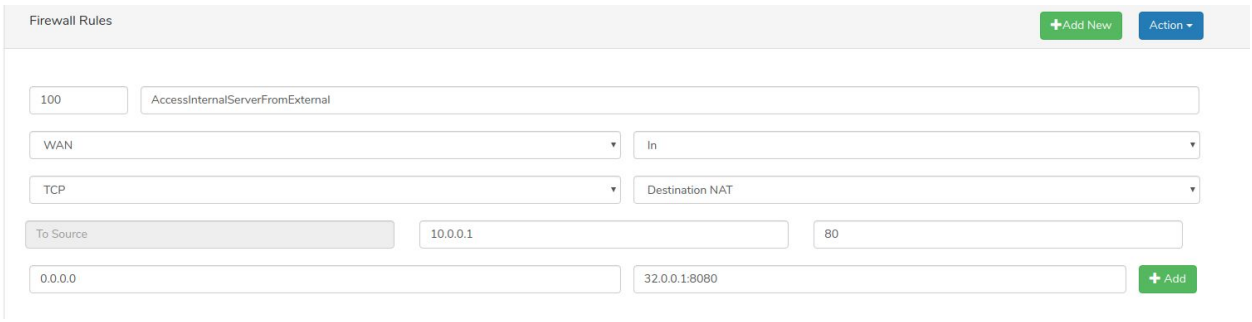
Conf : Priority: 'Preferred priority' / Rule Name: 'Preferred Rule Name' / Network Type: LAN / Direction: In / Protocol: All

/ Action: Allow / Source IP : 1.1.1.1:80 / Destination IP : 10.1.2.1:**0**/24 (zero meaning all ports)



Example 8 : Access an internal server with an internal IP 10.0.0.1 on port 80 through a server with an external IP 32.0.0.1

on port 8080 using TCP.

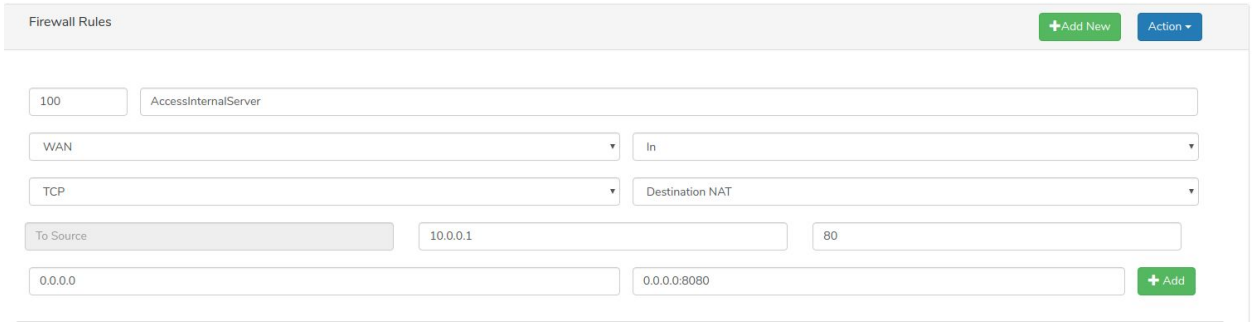


Conf : Priority: 'Preferred priority' / Rule Name: 'Preferred Rule Name' / Network Type: WAN / Direction: In / Protocol: TCP

/ Action: Destination NAT / Destination Ip Address: 10.0.0.1 / To Destination Port: 80 / Source IP : 0.0.0.0 /

Destination IP : 32.0.0.1:8080

Example 9 : Access an internal server with an internal IP 10.0.0.1 on port 80 through a server with on port 8080 using TCP.

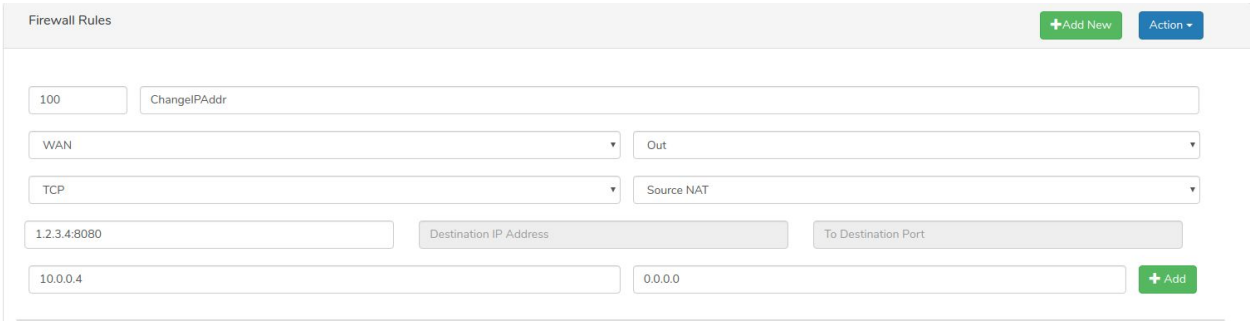


Conf : Priority: 'Preferred priority' / Rule Name: 'Preferred Rule Name' / Network Type: WAN / Direction: In / Protocol: TCP

/ Action: Destination NAT / Destination Ip Address: 10.0.0.1 / To Destination Port: 80 / Source IP : 0.0.0.0 /

Destination IP : 0.0.0.0:8080

Example 10 : Change source ip addresses 10.0.0.4 to 1.2.3.4 on port 8080 using TCP.



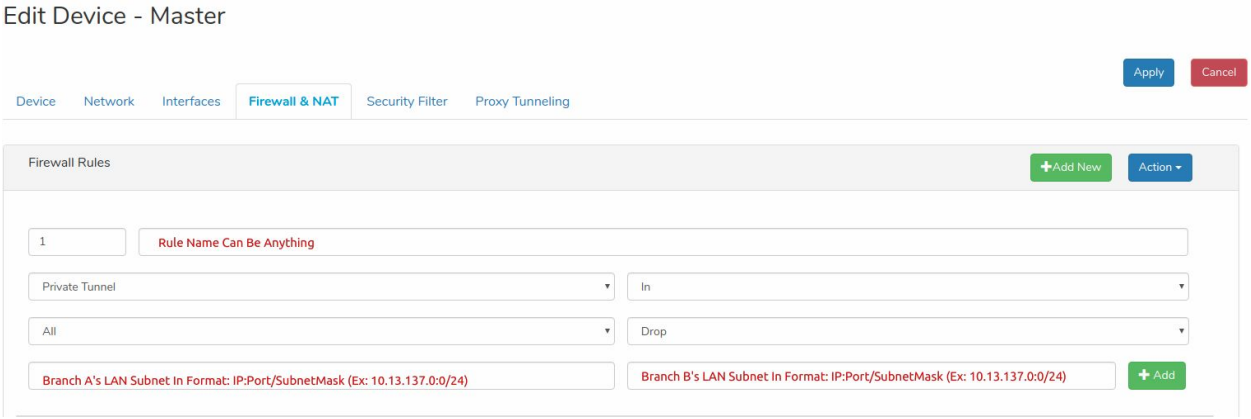
Conf : Priority: 'Preferred priority' / Rule Name: 'Preferred Rule Name' / Network Type: WAN / Direction: Out / Protocol: TCP

/ Action: Source NAT / To Source: 1.2.3.4:8080 / Source IP : 10.0.0.4 / Destination IP : 0.0.0.0

Blocking Communication Between Two Branches

To block communication from Branch A to Branch B a firewall rule must be created on either Branch A or Branch B. For this example, the rule will be added to Branch A however, the rule to be added to Branch B would be the same exact rule. Navigate to Branch A's gateway settings by clicking the edit button for the Branch A gateway.

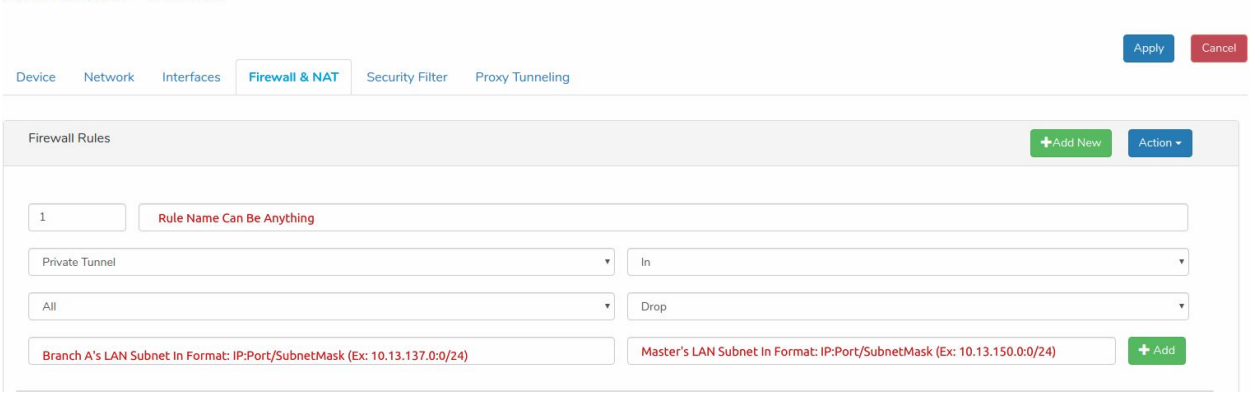
Under the “Firewall & NAT” tab, click the “Add New” button. Enter the rule configuration in this format:



When port is given as 0, the rule is applied to all ports. After applying the rule, Branch A will not be able to communicate to Branch B. To block Branch B from communicating to Branch A, create another rule with Source and Destination fields reversed.

Blocking Communication Between A Branch & Master

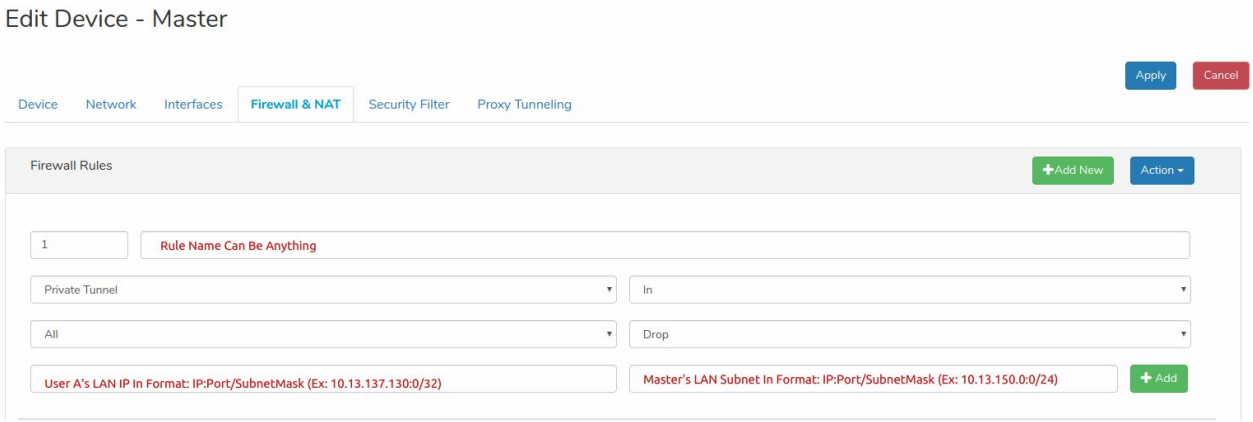
Similarly, a branch can be denied access to resources in the Master’s LAN by entering the Master’s LAN Subnet in the Destination field of the above example like so:



This rule will only block Branch A from accessing the Master’s subnet.

Blocking Specific Users From Accessing Other Sites' Subnets

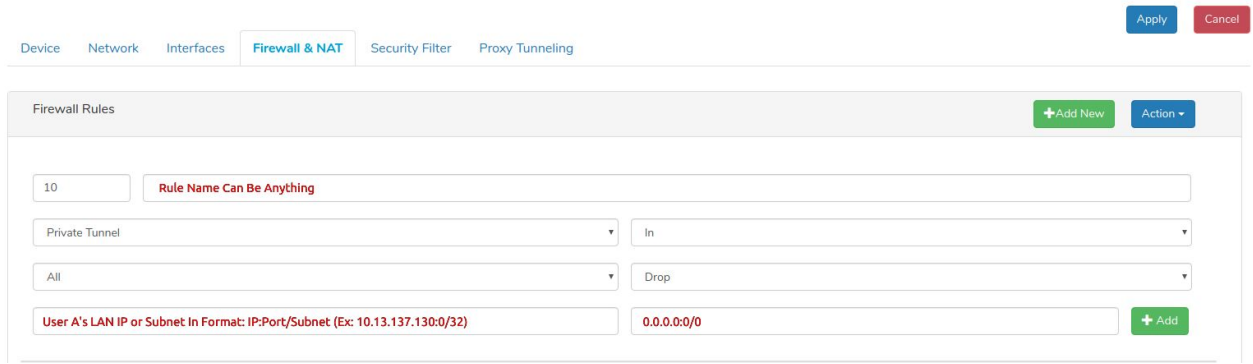
To block User A (which is in Branch A) from accessing Branch B's subnet, add a similar rule where the Source field is the User A's IP in Branch A's Subnet.



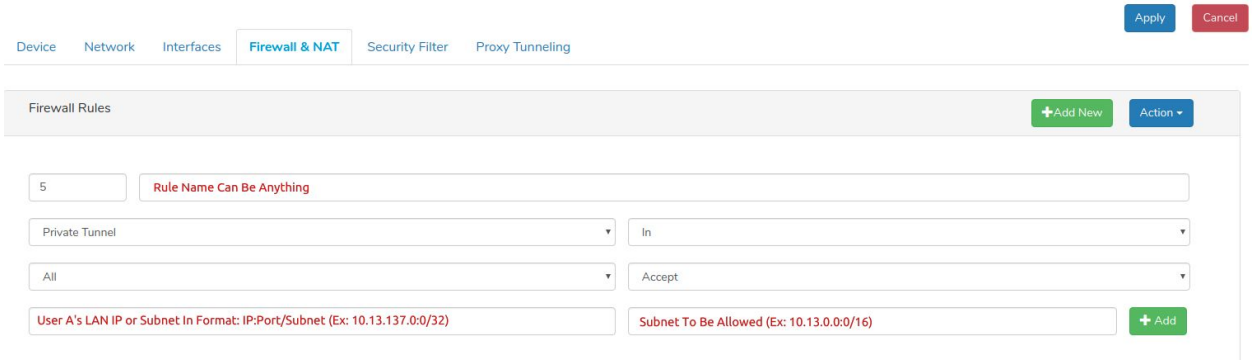
For this rule to work consistently, DHCP IP Reservation for User A is recommended. Navigate to Branch A's gateway settings and under the Network tab, fill in the DHCP IP Reservation field with appropriate settings.

Blocking Internet Access For A Specific User/Subnet

To block internet access for a specific user, add a rule like so:



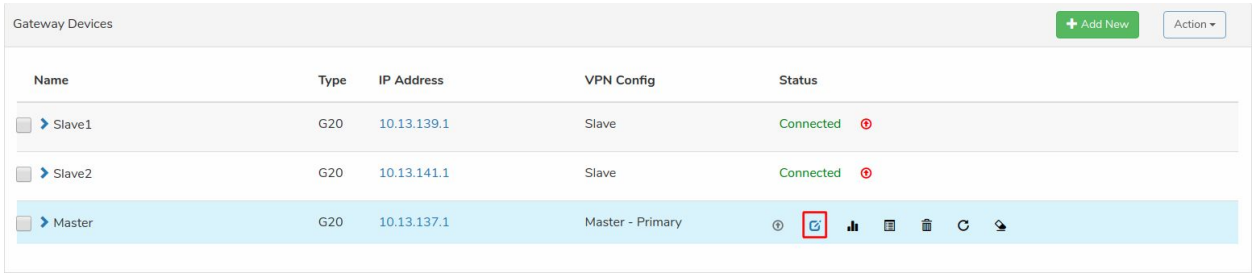
With only this rule, User A will not be able to access the internet as well as any subnet in the S2S network. To allow User A access to Branch B's or Master's subnet, an additional rule with higher priority than this rule must be added as such:



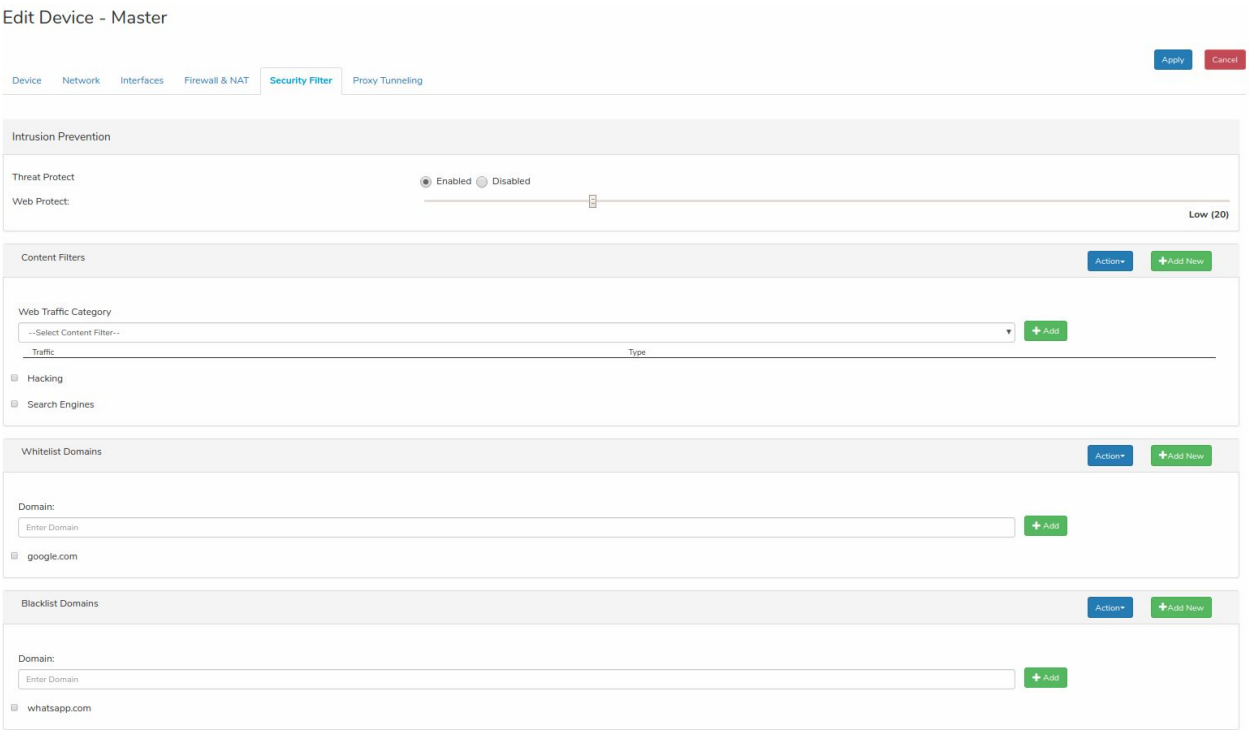
In this example, the LAN subnets in the S2S network are in the 10.13.0.0/16 subnet. So, a single rule to allow all S2S traffic can be made. If the branches are not under a common subnet, rules for each branch subnet must be added.

DNS Based Security

To setup a filter for a Thunder gateway's LAN network, navigate to the desired gateway settings by clicking the edit button for the gateway.



Under the "Security Filter" tab the desired blacklist, whitelist, blocked categories and reputation filter for the Thunder gateway can be input.
The blacklist field will block domains for the LAN users. Additionally to block a group of domains, a category filter can be selected for example to block all domains categorized as Search Engine domains. If a couple of domains which are in the selected category filter are wanted to be accessible, these domains must be added to the whitelist. In addition to these filters, the Thunder gateway also has a reputation filter which blocks domains having a lower score than desired. This minimum score should be selected with caution as cloud.thundernsi.com may be blocked if the minimum score is set too high. For this reason, it is recommended to keep this value below 75. Below is an example filter setup.



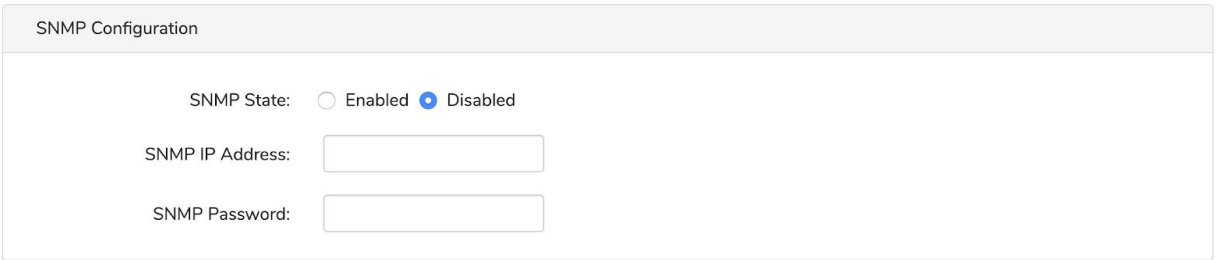
Device Monitoring

Thunder gateway devices can be monitored using SNMP and also using cloud.

SNMP

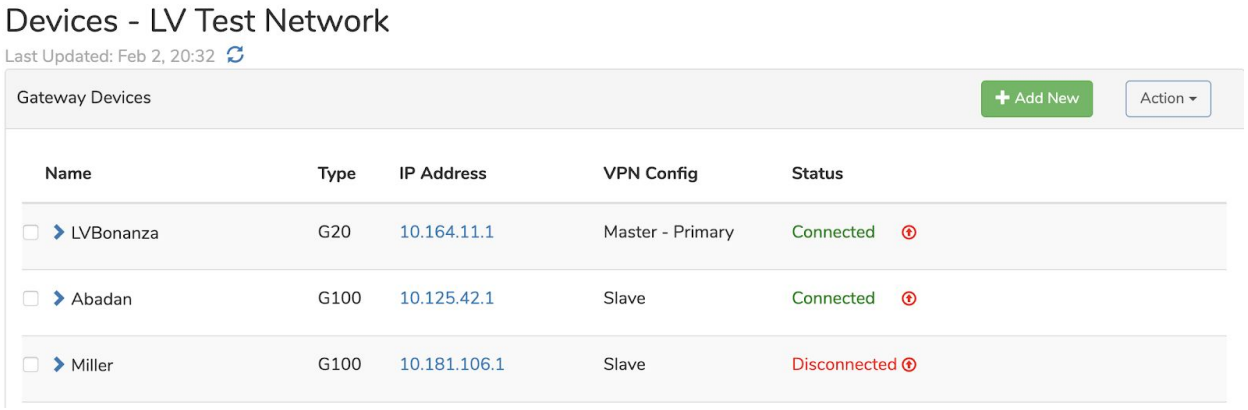
Thunder Gateway devices support only SNMP V2, SNMP v1 is disabled for security reasons. Also it requires IP address of the SNMP server that will query and also SNMP Password (String). This is configured from cloud per device under Network section

Cloud-> Device->Network->SNMPConfiguration

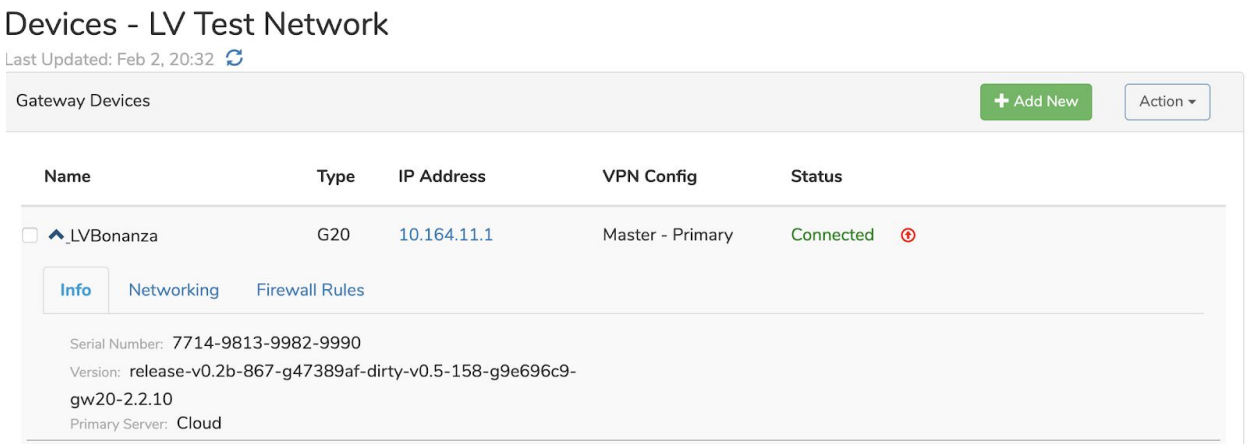


Monitoring Over Cloud

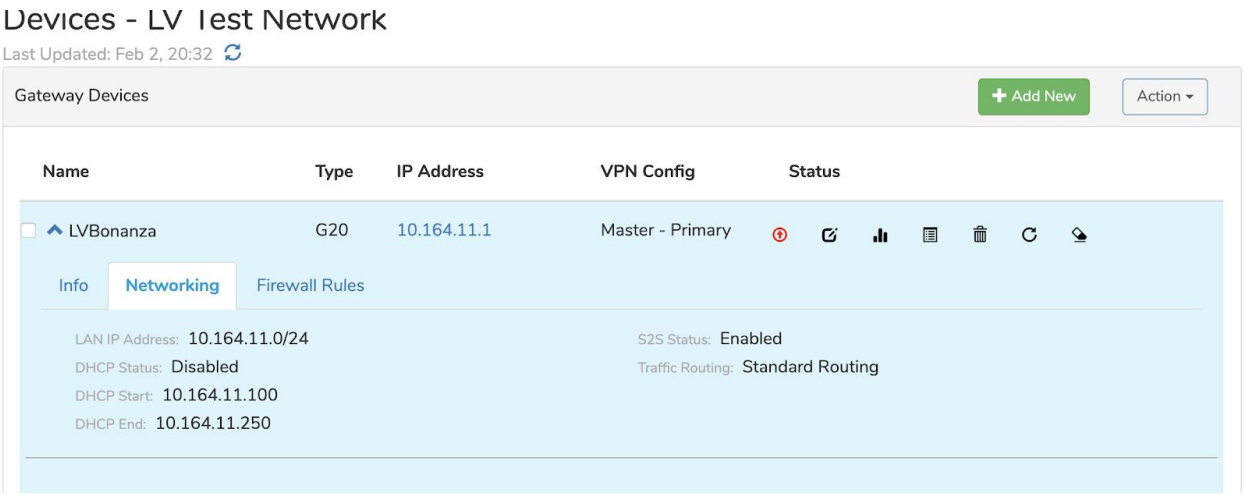
Cloud monitores each device continuously, when a user logs onto the cloud it shows if a device is connected to the cloud via the status on the summary page as shown in below picture. A device connected to cloud doesn't guarantee a device is up/down. Reason for this being, the operator can device to block cloud connection to thunder cloud but still use the device local UI for configuration. Note local UI doesn't not have all rich features as on cloud. So if the device shows as disconnected, most probably it is a network connection on the operator end or thunder cloud issue.



User can get quick information on the current S/W version and serial number by clicking the device name under the summary page as shown below.



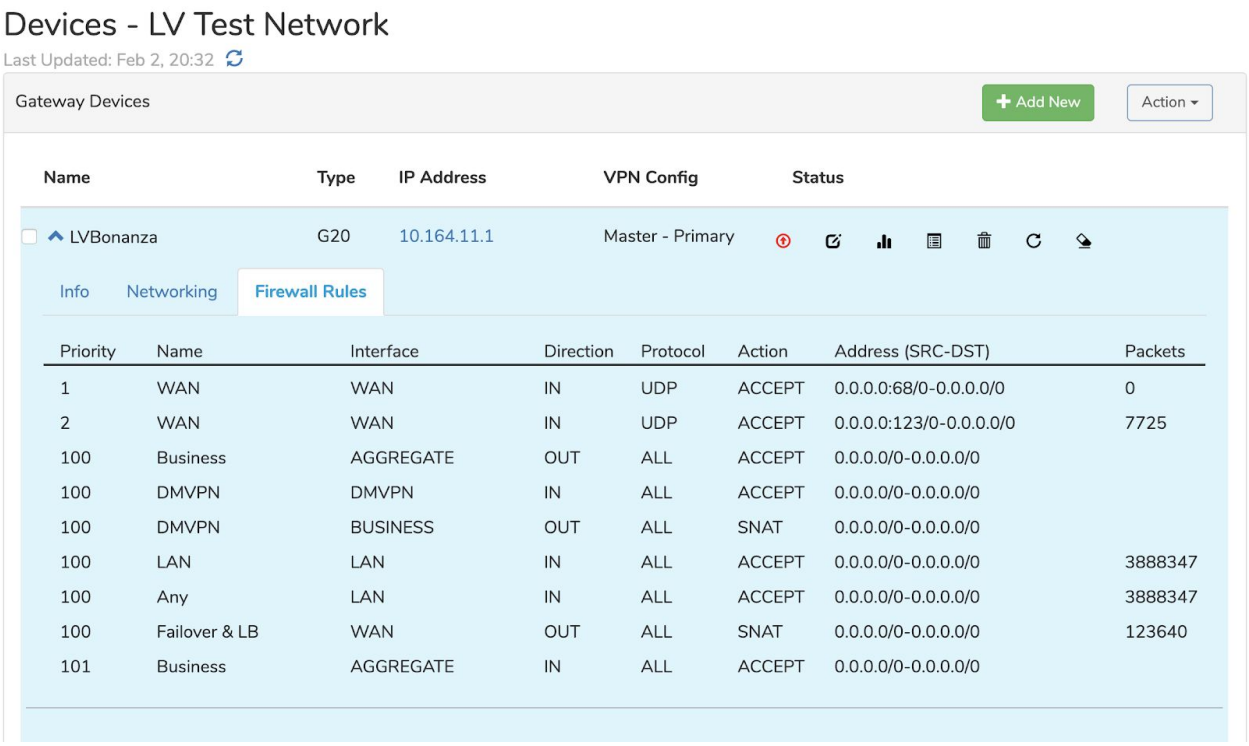
Quick network status can be obtained under the networking tab of quick view



This view provides LAN configuration, S2S (Site -Site) status and how the traffic will be routed to the internet. Standard Routing means all internet traffic will be routed via local internet, while Aggregate means the traffic will be sent to the master/HUB.

Firewall Quick View

Thunder Gateway devices come with preinstalled firewall rules, such as all inbound traffic on WAN will be blocked etc… more information can be found under the Security section of the guide. Under the Firewall quick view we can find number of packets matched by each rules.

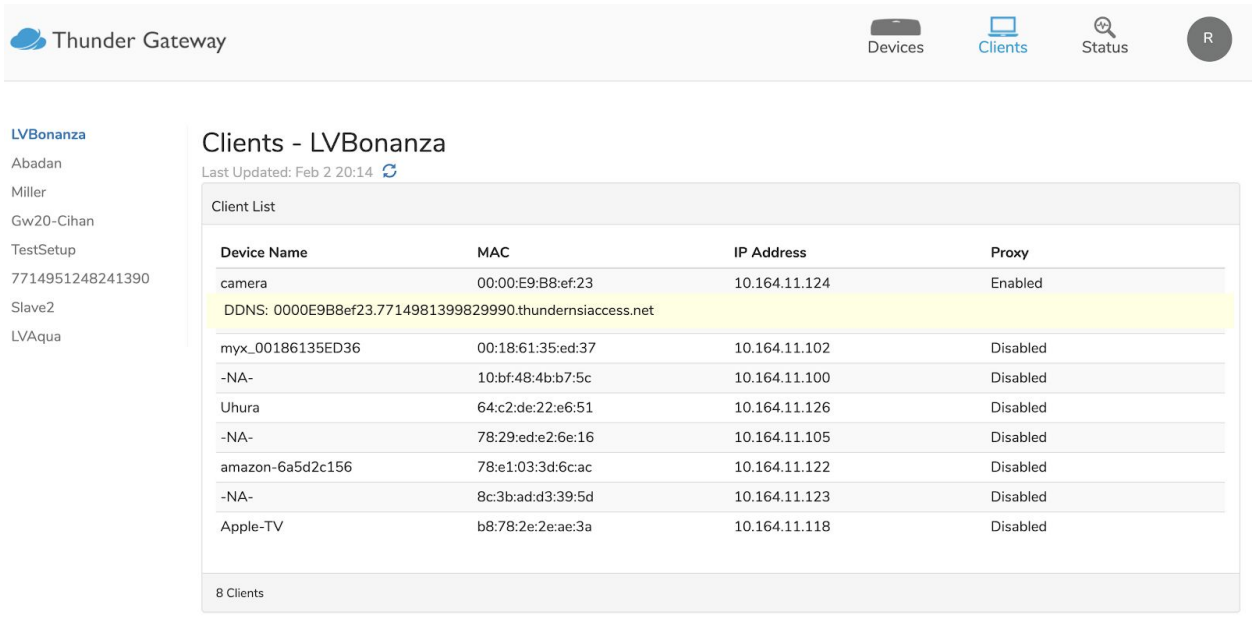


These rules are updated when a user logs in, and there can be a delay upto 2 mins for these counters to get updated.

Clients Section

When logged into Thunder cloud and navigate to Clients section, it provides all DHCP lease information from the devices. If a Gateway does not have DHCP server enabled on LAN or clients (laptops, desktops or phones) does not require DHCP from gateway then they won't appear here in the list.

ThunderCloud->Clients->Device



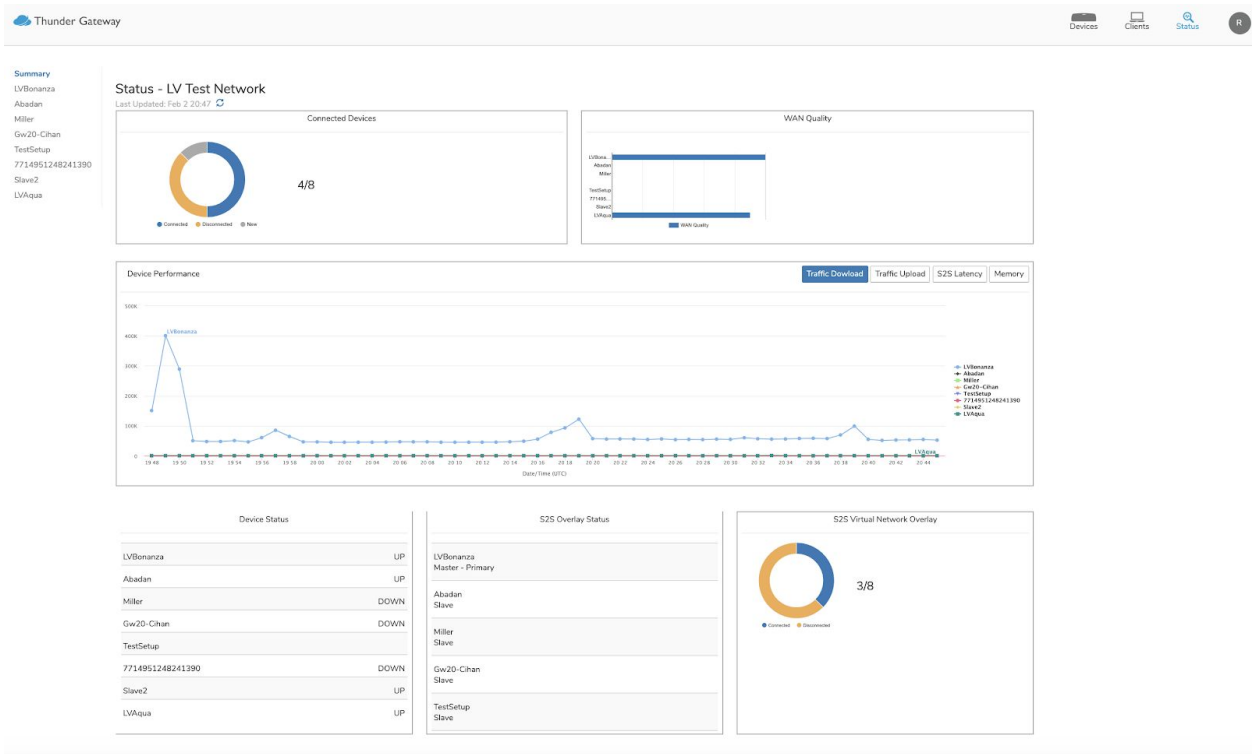
This table provides

- Clients name - These are names configured manually under the DHCP lease segment or what the clients advertises when DHCP is requested
- MAC address - Clients Mac address
- IP address - IP address assigned by Gateway to the Client as part of DHCP request
- Proxy - This is for Service proxy configuration

Device Status

Cloud collects information on device performance, navigating to Status sections provides this information. This information is collected in real-time. The stats are collected in real time and only when a user logs in, reduces the b/w cost for user, cloud cost and also provides relevant information in time. This page has two views Summary and device specific view.

Summary view is shown below



The page displays the last update to show when the data was last collected from device and also has an option to request latest information.The page will keep refreshing every few minutes while logged in to get the real time data from devices.

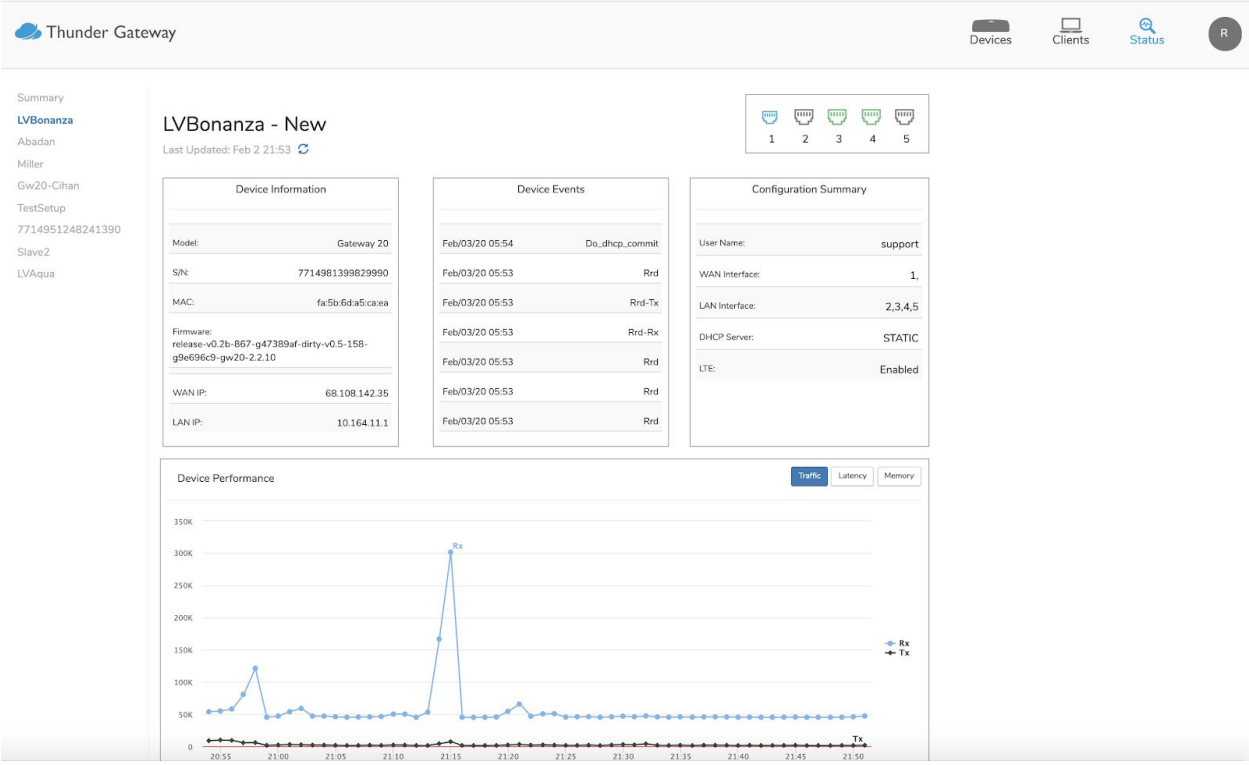
Below are the sections on the page with quick summary on what information they provide

- Connected Devices
- WAN quality
- Device Performance - This Graph shows different performance metrics for all devices, this view helps to view the performance in comparison to
- Device status - This provides consolidated status of all devices in that network devices can be one of two states UP/DOwn
- S2S Overlay status - This view provides role of each device on S2S
- S2S Virtual overlay status - Pictorial representation of number of devices connected via S2S

Device Level Stats

Individual device level stats can be obtained by selecting the device from the left navigation plane

Below is a screenshot of individual device stats

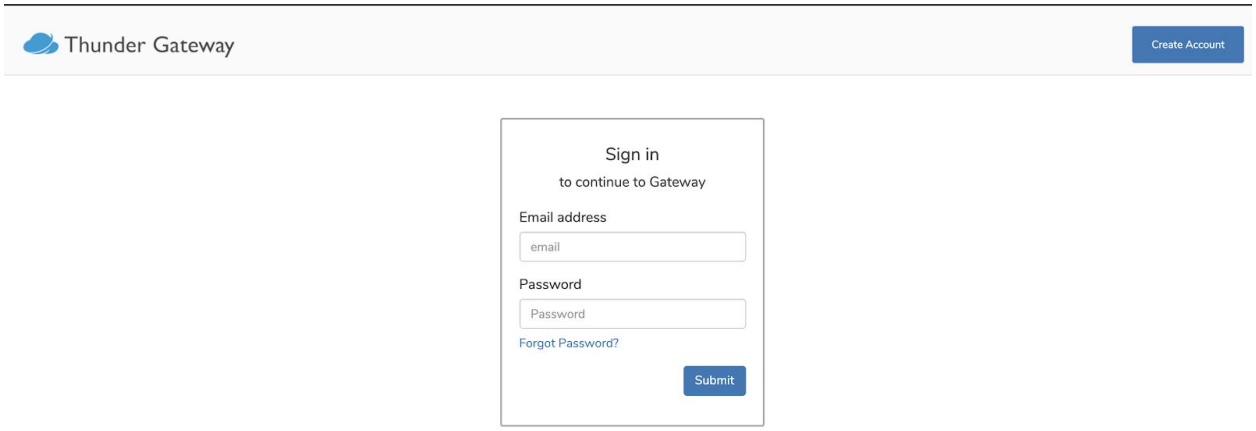


This view provides following information

- Last update time - This shows when the stats were last received from the device and the refresh button lets users request for updated information. The page updates every few minutes.
- Port status and Port mode - This Visual chart provides LAN/WAN and UP/DOWN status for quick status. GW20 provides status for 4 interface and GW100 provides status for 8 interfaces
- Device information - This provides information on Model, Serial number, WAN IP, LAN IP, MAC and S/W version.
- Device Events: Last few events of the device, such as image upgrade etc..
- Configuration Summary: Which interfaces are set to WAN, LAN and also if LTE is enabled or not
- Device summary : this provides a set of graphs on device performance.

Cloud UI

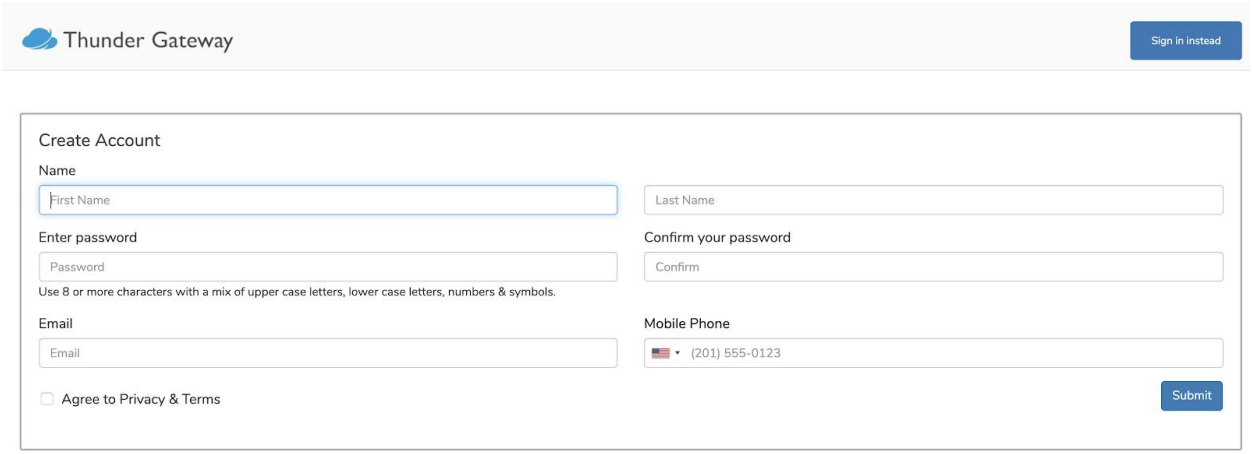
Thunder gateway devices used thunder nsi cloud for monitoring, management and orchestration. Thunder cloud can be accessed via https://cloud.thundernsi.com url



User Accounts

User account creation

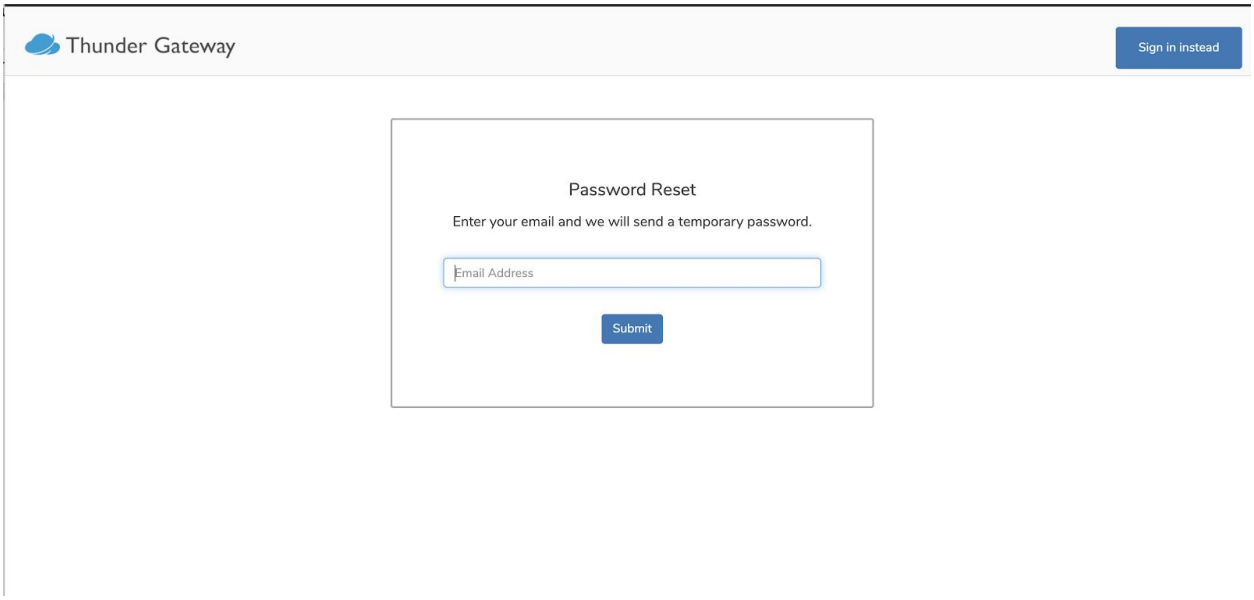
User account can be created by clicking “Create Account”



Once the form is successfully submitted a validation email will be sent from the user registered email address. Accounts will be active only after the user clicks on the validation email., Validation email is valid only for 24 hours. Also a valid mobile number is required. Mobile number will be used to send TXT messages in future and to enable two factor validation soon.

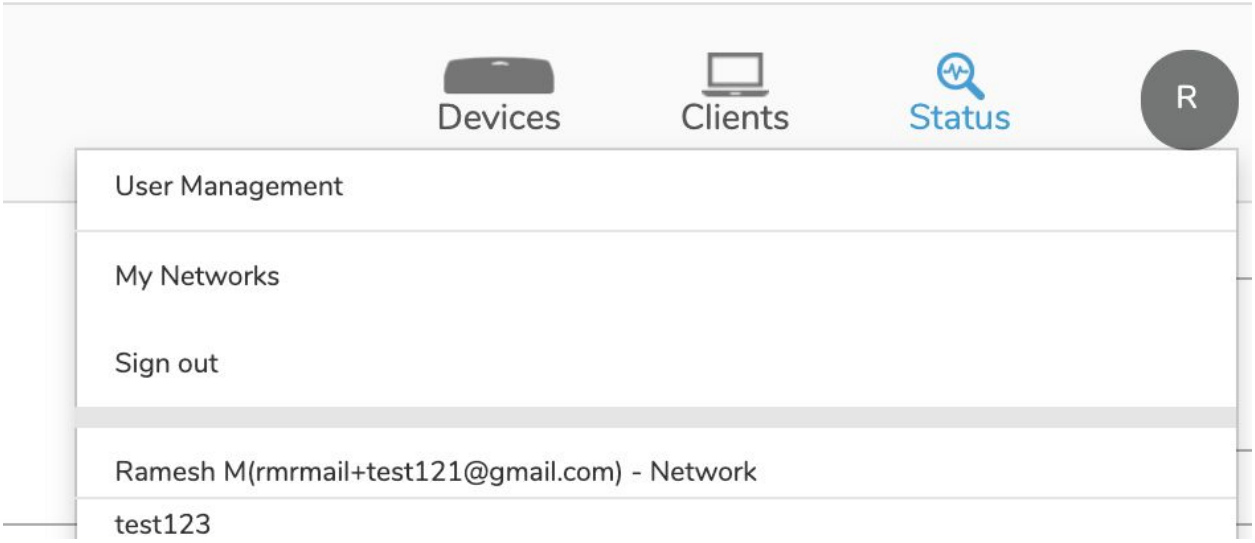
Password Reset

Users who forgot their password or need to reset password or change password should follow Password reset flow. This could be accessed from the login screen and submitting the password reset form.



Network

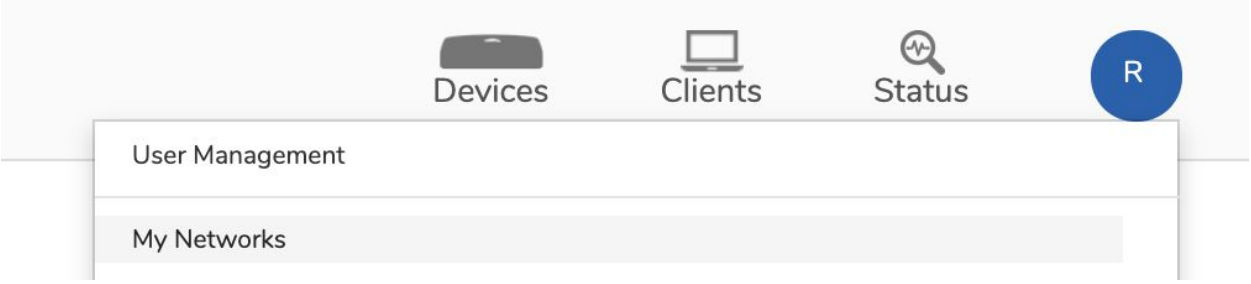
Gateway devices are organized under a network., when a user account is created by a user a network is created under the username. Users can use this default network or can create a new network and add devices to the new network. Users might opt to create a new network so it can be shared with others as well. One can view the network by clicking the Initial shown on the right most corner as shown in the below picture



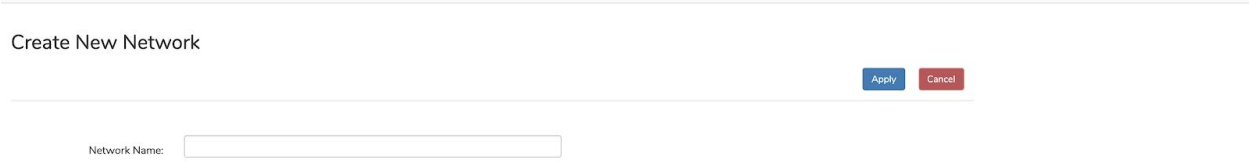
Users can change networks by selecting the appropriate network from the drop down.

Creating a New Network

New networks can be created by navigating to the network management section on the cloud by clicking on “My Networks” sections as shown below



New network can be created by clicking on “Add New” button under Network management page



Setting Default Network

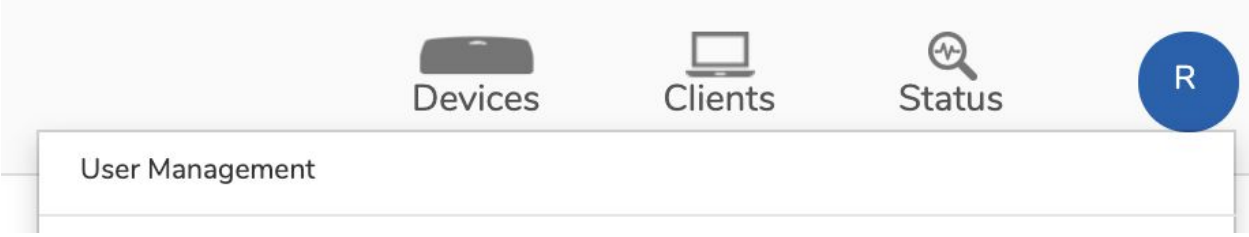
When a user has multiple networks, the user can set what the default network should be when he logs in. This avoids the user from having to change to a network every time he logs in. This can be set from Network Management section as shown below

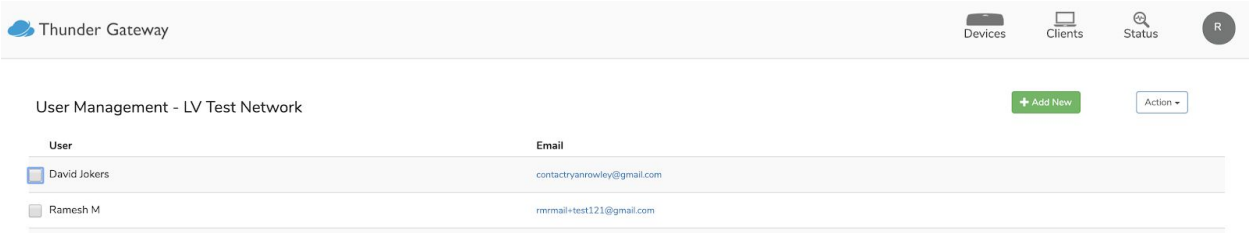
Also users can decide to delete a network when not in use by selecting the “Delete Network” option from the Action button in Network management page. Network can be deleted only if it doesn't have any devices in that network.

User Management

ThunderNSI cloud allows Network operators to control access to the devices in the to multiple users. All users should have a valid thundernsi account.

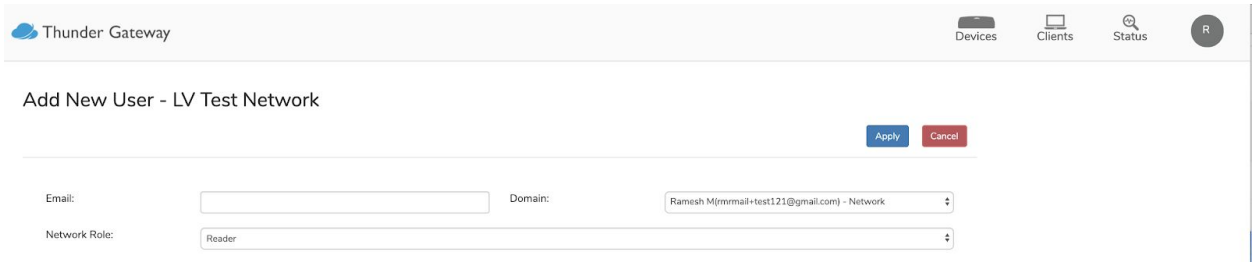
All user management functionalities can be access under user management page, this can be accessed by clicking user name on the right most part of the page and selecting “User Management”





Invite User

A User can invite a new user to any of the network that the current user control, this page be accessed by clicking on “Add New”

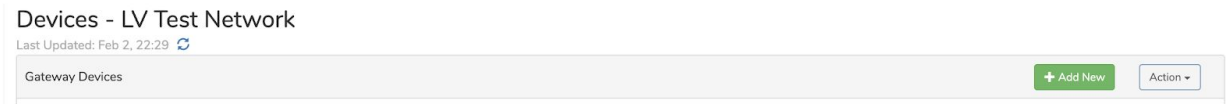


Revoke User

Also a access to a user can be revoked by clicking on the user name and selecting “Remove User”

Add Device To Network

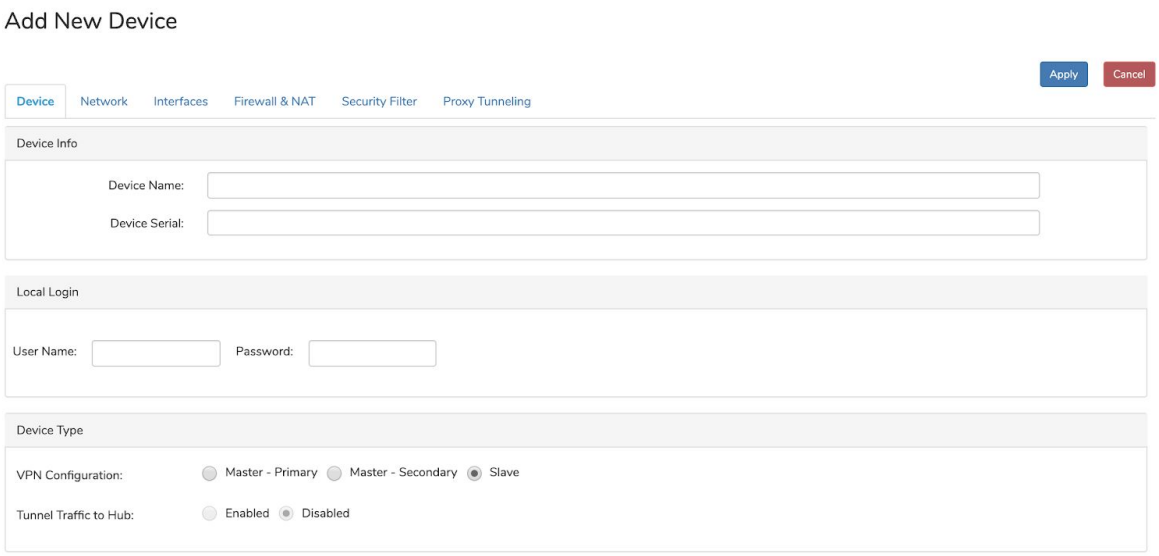
A new device can be add to a network by a user by selecting “Add New”



To add a new device user needs two things

1. Valid thundernsi user account
2. Device Serial number

The serial number of the device can be found under the Thunder gateway.



On the Add New Device page, the Thunder gateway's serial number must be added to the Device Serial field. After the Thunder gateway is given a name, all necessary configurations must be entered. For details on the configurations refer to Connectivity, Routing, Security and Device Monitoring.

Troubleshooting

Cloud and local UI

Local UI has minimal configuration to get the device connected to the internet setting and cloud provides all configurations.

Why is Local UI read only

When a device is cloud connected, configuration changes or disabled on local UI. This is done because, cloud makes sure the device has the updated configuration and assumes cloud configuration as the truth. SO any configuration on a local device will be overwritten. Tio avoid user confusion local UI configuration is disabled when the device is connected to the cloud.

Internet Connectivity

Ping test

User can initiate Ping test from local UI to make sure there is internet connectivity.

S2S Connectivity

Led Status

To observe if the Thunder gateway's S2S connection is up, examine the  LED on the gateway. If the LED is solid, it means that the S2S connection is up. If the LED is blinking, the S2S connection is currently down. For further information, refer to LED Decode

Ping Test

To test if a branch's S2S connection is up, a PC connected to the Thunder gateway's network on the branch can ping a PC in the Master's LAN subnet. If pings are successful, the branch's S2S connection is up. However if the pings fail and the Master's S2S connection is known to be up, the branch's S2S connection is currently down.

Fix

1. Check if the Thunder gateways have internet connection
    a. If it does not, check if the interface settings are correctly configured. Refer to Interface Configuration. Once internet connection is established, it may take a couple of minutes for the gateway to establish S2S connection.
2. Check if S2S is enabled for the branch and Master Thunder gateway
    a. If it is not, refer to Site-to-Site VPN to enable S2S
3. Check if the Master is connected to the cloud.
    a. If it is not connected, refer to Internet Connectivity
4. Check if the PC on the branch network can ping the Master's LAN IP
    a. If it can, there could be a subnet announcement issue with the Master Thunder gateway. Refer to Interface Configuration to find a possible issue with the configuration. The LAN interfaces settings should have announcements enabled.
5. If the Master is behind a router performing NAT, check if port forwarding rules are in place on the router for port 4500, 500 and 5555.

Security

Firewall Rule

To test if the firewall rule is correctly applied, send a packet which should be blocked by the firewall, using netcat or similar tools from a device on the source subnet and read the packet on the destination end.

If a firewall rule is not being applied to the Thunder gateway, check if the rule's configuration is correct. For example firewall rules, refer to Firewall Rules. Additionally, check if the Thunder gateway is connected to the Cloud. If the device is disconnected, changes to the Cloud UI configurations will take effect when the Thunder gateway is reconnected to the Cloud.

If the firewall configuration is correct and the rule is still not applied, check if there is a conflicting rule on the firewall. For example if there is a rule with priority 20 which drops all packets from 192.168.189.130 and another rule with priority 50 which accepts packets from 192.168.189.130's 80 port, the rule with higher priority(lower number on the priority field) will be applied first and packets from 192.168.189.130's 80 port will be dropped. To avoid this issue, plan the firewall with the priority field in mind.