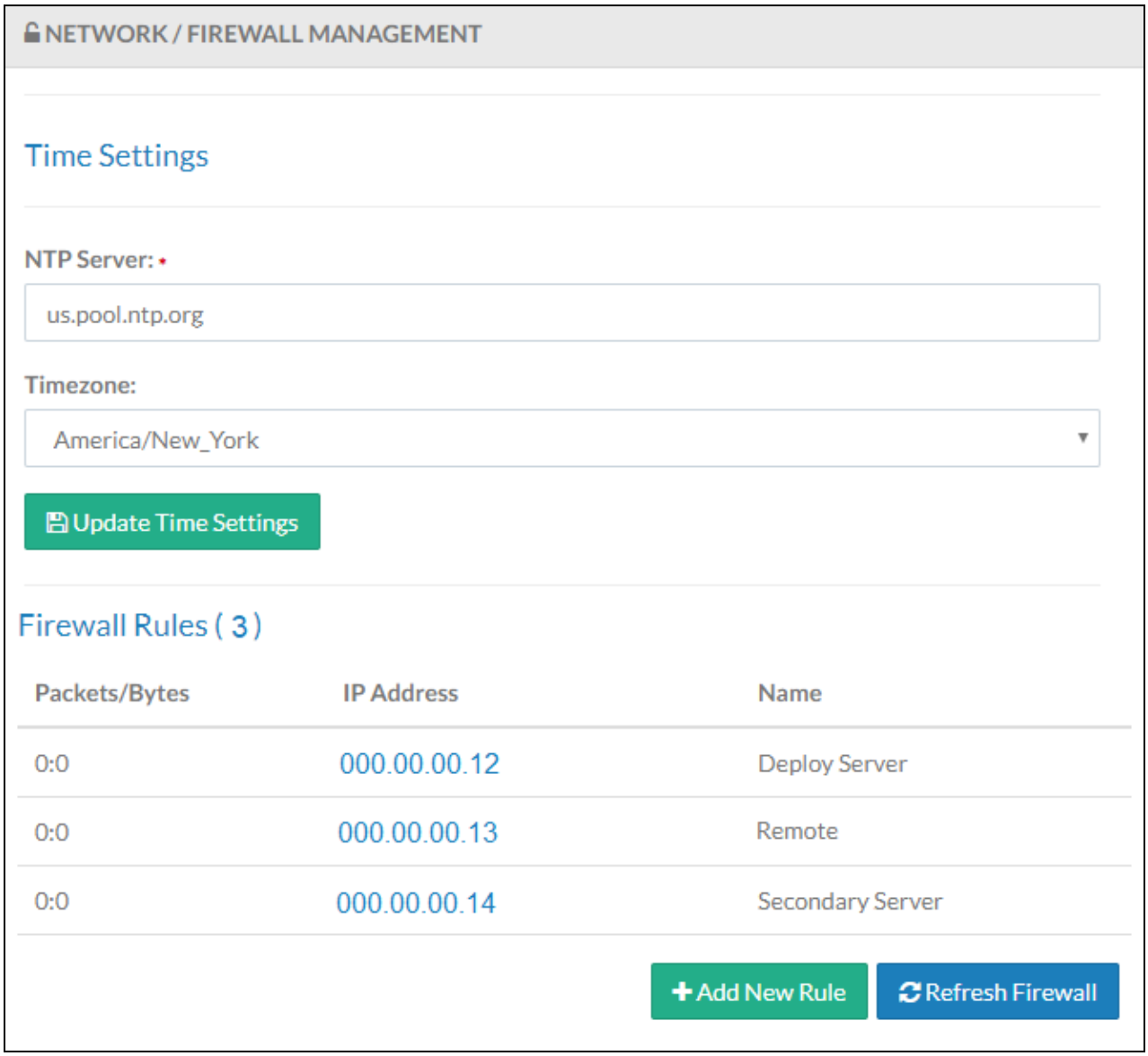
Firewall Rules & Time Zone - GENERAL USERS

Last Modified on 11/22/2019 1:12 pm EST

From the main menu, navigate to **System Admin > Network & Firewall**.

General users can view and manage Time Settings and Firewall Rules. Installers can manage additional options including Interface Routing and HTTPS.

Main Menu:

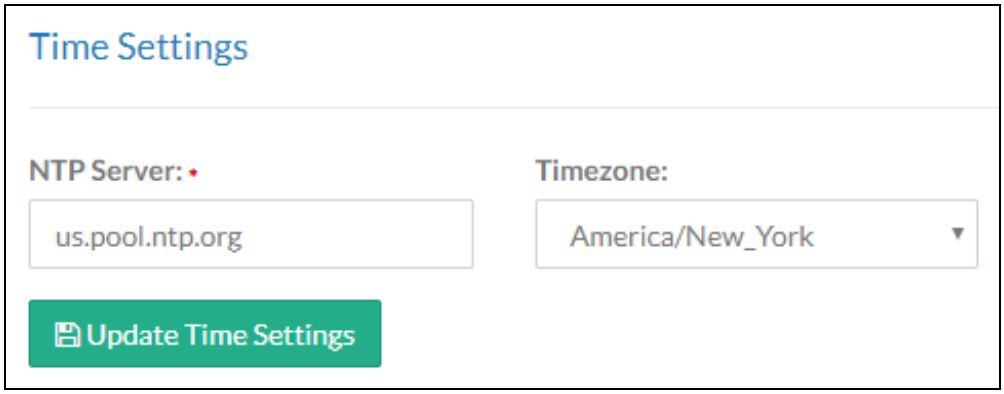


Time Settings

The NTP Server name and Time Zone can be edited from this screen.

NTP Server: The NTP server regulates the internal time clock in Kerauno. The default NTP server is us.pool.ntp.org – a public NTP service.

Timezone: Time zone for the internal time of Kerauno. Note: Individual time zones can be set for each extension under Users & Devices when employees are dispersed geographically across various time zones.



Firewall Rules

An installer has permission to manage Firewall Rules. Communication traffic to Kerauno is blocked by default, with the exception of the Kerauno Management network and any trunks set up in the System & Settings > Trunks menu.

Firewall Rules allow specific IP addresses to be white listed to pass through Kerauno unobstructed. The firewall tool is particularly useful when setting up phones for remote users who are utilizing their own home internet connections.

When accessing Kerauno via the web GUI, an installer must white list the public IP address of the network or PC in order to gain access to the Kerauno Presence module. Also, devices cannot properly register to Kerauno until the IP address is white listed.

To find your public IP address, go to https://www.google.com/#q=my+ip+address.

Active Firewall Rules appear on the main screen. Only IP addresses saved here are able to send traffic to and from Kerauno. The Packets/Bytes column represents the number of incoming packets from each IP address, as well as how many total bytes of data were transferred through those packets.

Add Firewall Rule

To add a new firewall rule, click **+ Add New Rule**. Populate the **IP Address** or Hostname the traffic originates from. Ensure all phone system users are configured with a static public IP address. When configured with a dynamic IP address the firewall must be modified each time the dynamic IP address changes. When a static IP is not an option, enter a DNS hostname when creating a firewall rule.

Provide an easily recognizable name for the firewall rule. Then click **+Add Firewall Rule** to save the changes.

Delete Firewall Rule

Delete a Firewall Rule to revoke access to send and receive data from Kerauno. Click the corresponding rule on the main menu. Then click **Delete Firewall Rule** on the resulting screen.