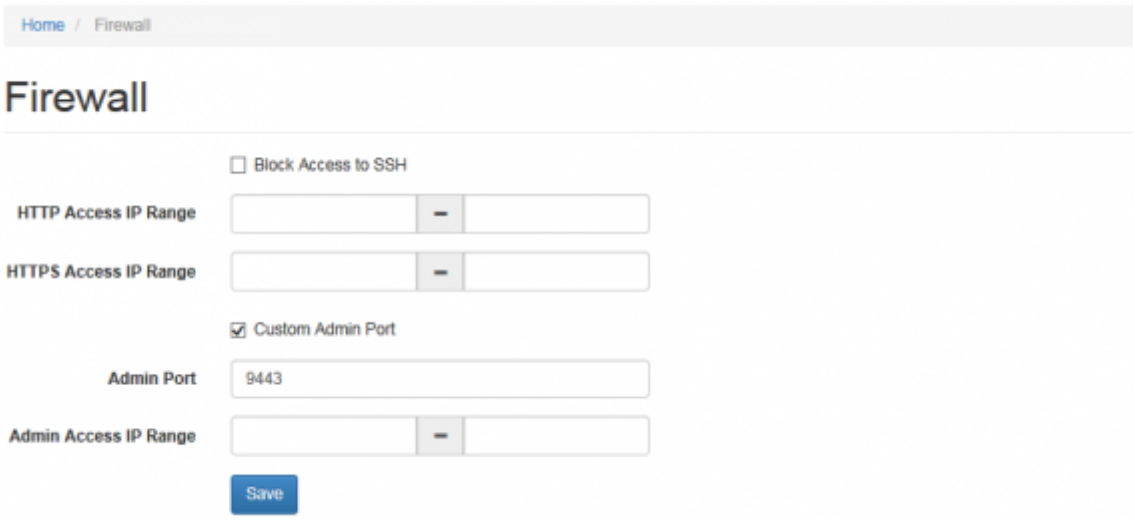
Within the Firewall settings (you find them under setting in (/admin/settings/firewall) you can define the following settings:

- **Block Access to SSH**: Click this, if you want to disable SSH access completely
- **HTTP & HTTPS Access Range**: You can define the IP Ranges, from which the HTTP or HTTPS service will be reachable. Please note, that your users won't be able to access the phishing simulations if you don't include their IP range. If you only want to block access to the administrative admin GUI you will need to run the campaigns on HTTP only and then restrict the access to HTTPS.
- **Custom Admin Port**: define here the port, under which the administrative LUCY access (web-based) will be accessible (do not change the admin port if you have a docker based installation and use LUCY < 4.4!)
- **Admin Access IP Range**: You can define the IP Ranges, from which access to the Lucy admin panel is allowed.



From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=firewall_security_settings

Last update: **2019/07/25 12:49**