How to configure ClearOS to only permit management from a specific IP address

2021-07-20: WikiSuite will now support all major Linux distros. Thus, the information below is no longer updated. It may still be valid, or not. It will be eventually removed from this site, so anything relevant should be moved to the appropriate site. For anything related to ClearOS, please search among the following: ClearOS site, code base, Developer docs, Wiki or forum.

Please contact us if you would like to help out.

ClearOS offers Attack Detector but if you have a fixed IP address, you can restrict SSH and / or Webconfig (the web-based admin panel) to a specific IP address.

Below is an example to remove SSH (usually port 22) and Webconfig (port 81) access from default Incoming Firewall (https://example.org:81/app/incoming_firewall) and replace by rules in the Custom Firewall

Be careful not to lock yourself out!

Blanket block of SSH access on port 22

```
$IPTABLES -I INPUT -p tcp --dport 22 -j DROP
```

Accept connections from 203.0.113.0 (replace with your IP)

```
$IPTABLES -I INPUT -p tcp --source 203.0.113.0 --dport 22 -j ACCEPT
```

Blanket block of ClearOS Webconfig

```
$IPTABLES -I INPUT -p tcp --dport 81 -j DROP
```

Accept connections from 203.0.113.0 (replace with your IP)

```
$IPTABLES -I INPUT -p tcp --source 203.0.113.0 --dport 81 -j ACCEPT
```

Notes

- In the Custom Firewall use "$IPTABLES" and not "iptables, but test the rules first at the command line with "iptables". If there are no errors, put the rule in the Custom Firewall.
- The order of the rules is important, so in this case, it's block everything, and after, add an exception.
- Make sure you have activated the rules on the Custom Firewall (you disable a rule instead of deleting)
- The DROP rule will drop traffic from every interface including LAN and VPN. If you want to drop traffic from your external interface add the "-i External_IF" switch to the DROP rules where "External_IF" is the name of your external interface from the IP Settings webconfig screen (e.g ppp0, enp2s0 etc). Repeat the rule for each interface you want to apply the rule to.
- You can also use ClearOS as a gateway and VPN server, and thus, you would VPN in to your office, and access the server from there.

- The same idea could be used to restrict a web-based intranet (with port 80 / 443)
- Webconfig (port 81) also offers phpMyAdmin so it's one more reason to restrict access