**Change Firewall Settings of Linux VM**

Overview: <https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands>

<https://www.rosehosting.com/blog/how-to-open-ports-in-ubuntu-and-centos-using-iptables/>

What done when configuring Linux VM:

* Allow all incoming HTTP (port 80) connections:

sudo iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

* Allow all incoming HTTPS (port 443) connections:

sudo iptables -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

* Allow connections via Port 12800 for RServer:

sudo iptables -A INPUT -p tcp --dport 12800 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

* Allow connections via Port 8000 for plumber:

sudo iptables -A INPUT -p tcp --dport 8000 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

* Allow connections via Port 8080 for plumber in Docker:

sudo iptables -A INPUT -p tcp --dport 8080 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

* Allow connections via Port 8004 for other:

sudo iptables -A INPUT -p tcp --dport 8004 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

* Save the established rules:

sudo apt-get install iptables-persistent

* Y, Yes

The following are not necessary:

* Allow traffic on your loopback interface (localhost)

sudo iptables -A INPUT -i lo -j ACCEPT

sudo iptables -A OUTPUT -o lo -j ACCEPT

* Outgoing of Ports above:

sudo iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT

sudo iptables -A OUTPUT -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED -j ACCEPT

sudo iptables -A OUTPUT -p tcp --sport 12800 -m conntrack --ctstate ESTABLISHED -j ACCEPT

sudo iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT (not necessary)

* Allow all incoming SSH connections

sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT