Strong SSH Security on Centos 7

Prerequisites:

A Centos 7 server with root access and public key SSH authentication.

Run Updates and Install Packages:

```
yum update
yum install firewalld policycoreutils-python libpcap wget
```

Add Non-Root SSH User and Copy SSH Keys:

```
adduser ssh_user
passwd
usermod -aG wheel ssh_user
mkdir /home/ssh_user/.ssh
cp ~/.ssh/authorized_keys /home/ssh_user/.ssh
chown -R ssh_user:ssh_user /home/ssh_user/.ssh
```

Start FirewallD

```
systemctl start firewalld
systemctl enable firewalld
```

Change SSH Port (Use Your Own Port)

```
firewall-cmd --add-port=2662/tcp --permanent
firewall-cmd --reload
semanage port -a -t ssh_port_t -p tcp 2662
```

Update SSHD Config

```
vi /etc/ssh/sshd_config
     PermitRootLogin no
     Port 2662
     LoginGraceTime 1m
     MaxAuthTries 5
     PasswordAuthentication no
     PermitEmptyPasswords no
```

Block SSH on Port 22

```
firewall-cmd --remove-service=ssh --permanent
firewall-cmd --reload
```

Install KnockD

```
wget http://li.nux.ro/download/nux/misc/el7/x86_64//knock-server-0.7-
1.el7.nux.x86_64.rpm
rpm -ivh knock-server-0.7-1.el7.nux.x86_64.rpm
```

Configure /etc/knockd.conf

```
vi /etc/knockd.conf
      3141:udp,1684:udp,9797:udp  #Example ports
      start_command = /usr/bin/firewall-cmd --add-port=2662/tcp
      stop_command  = /usr/bin/firewall-cmd --remove-port=2662/tcp

systemctl enable knockd
systemctl start knockd
firewall-cmd --remove-port=2662/tcp
```

Configure Google Authenticator

```
sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
sudo yum install google-authenticator
google-authenticator

sudo vi /etc/pam/d/sshd
    ADD TO END: auth required pam_google_authenticator.so nullok
    COMMENT OUT: #auth substack password-auth

sudo vi /etc/ssh/sshd_config
      CHANGE: ChallengeResponseAuthentication yes
       ADD TO END: AuthenticationMethods publickey,keyboard-interactive

sudo systemctl reload sshd

sudo vi /etc/pam/d/sshd
    REMOVE nullok: auth required pam_google_authenticator.so ~~nullok~~
```