Fwknop Tutorial with Single Packet Authorization (SPA)

source: https://www.cipherdyne.org/fwknop/docs/fwknop-tutorial.html

on server:
install fwknop server:
```
sudo apt-cache search fwknop
sudo apt-get install fwknop-server
```

if necessary, install openssh server:
```
sudo netstat -alnp | grep ' LISTEN '
sudo apt-cache search openssh
sudo apt-get install openssh-server
```

get server IP:
```
ifconfig
```

on client:
install fwknop client:
```
sudo apt-cache search fwknop
sudo apt-get install fwknop-client
```

get client IP:
```
ifconfig
```

generate fwknop key:
```
client=138.47.128.35
server=138.47.134.184
ssh_port=22
fwknop -A tcp/$ssh_port -a $client -D $server --key-gen --use-hmac
--save-rc-stanza
grep KEY ~/.fwknoprc
```

copy fwknop key to server:
```
scp ~/.fwknoprc $server:~/access.conf
```

on server:
replace keys in fwknop config:
```
sudo vim ~/access.conf /etc/fwknop/access.conf
```
note the format of access.conf should be as follows (make sure to comment [default]):

SOURCE	**<ip>**
OPEN_PORTS	**<prot>/<port>**
KEY_BASE64	**<key>**
HMAC_KEY_BASE64	**<key>**

```
rm ~/access.conf
```

enable fwknop (so that it can actually start):
```
sudo vim /etc/default/fwknop-server
```
change **START_DAEMON="no"** to **START_DAEMON="yes"**

specify the listening interface:
```
sudo vim /etc/fwknop/fwknopd.conf
```
make sure that the interface is correct: PCAP_INTF <interface>
you may need to uncomment this line

restart fwknop server:
```
sudo service fwknop-server restart
```

check the logs:
```
tail /var/log/syslog
```
check fwknop's status:
```
sudo service fwknop-server status
```

on client:
test SSH (should work):
```
ssh $server
```

on server:
get interface:
```
ifconfig
```

add firewall rule(s) to block incoming SSH:
```
sudo iptables -L -nv
int=enp0s3
ssh_port=22
sudo iptables -A INPUT -i $int -p tcp --dport $ssh_port -j DROP
sudo iptables -L -nv
```

on client:
test SSH now (shouldn't work):
```
ssh $server
```

install nmap (if necessary):
```
sudo apt-get install nmap
```

check if SSH is visible on server (should be filtered):
```
sudo nmap -sS -p $ssh_port $server
```

send a valid SPA packet to the server:
```
fwknop -n $server
```

on server:
check firewall rules:
```
sudo iptables -L -nv
```

on client:
check if SSH is visible on server (should be open):
```
sudo nmap -sS -p $ssh_port $server
```

test SSH now (should work):

```
ssh $server
```

NOTE: may need to resend SPA packet to the server (if the above takes too long)

on a different machine:

test SSH now (shouldn't work):

```
server=138.47.134.184
ssh $server
```

on server:

we still get locked out once the knocking window closes; so, allow related and established connections in iptables:

```
sudo iptables -D INPUT -i $int -p tcp --dport $ssh_port -j DROP
sudo iptables -A INPUT -i $int -p tcp --dport $ssh_port -m state
--state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -i $int -p tcp --dport $ssh_port -j DROP
```