1. Install conntrack

```
sudo apt-get install conntrack
```

2. (1) modify **/usr/bin/rmtrack**

```
nano /usr/bin/rmtrack
```

(2) edit：

```
#!/bin/bash
/usr/sbin/conntrack -L |grep $1 |grep ESTAB |grep 'dport=80' |awk
"{ system("conntrack -D --orig-src $1 --orig-dst " substr($6,5) " -p
tcp --orig-port-src " substr($7,7) " --orig-port-dst 80"); }"
```

(3) justify permissions

```
chmod 755 /usr/bin/rmtrack
```

3. Allow web server users to execute sudo command

(1) `sudo visudo`

(2) insert following code（Assume www-data as web server users）

```
www-data ALL=NOPASSWD: /usr/sbin/arp
www-data ALL=NOPASSWD: /sbin/iptables
www-data ALL=NOPASSWD: /usr/bin/rmtrack [0-9]*.[0-9]*.[0-9]*.[0-9]*
```

4. Add Iptables rules in rc.local

`nano /etc/rc.local`（100.64.0.1 as Access point，172.31.254.100 as Web Portal server，eth0 as LAN interface name）

```
#####################################################################
#add portal chain
/sbin/iptables -t mangle -N portal
/sbin/iptables -t mangle -A PREROUTING -i eth0 -p tcp -m tcp --dport 1:65534
-j portal
/sbin/iptables -t mangle -A PREROUTING -i eth0 -p udp -m udp --dport 1:65534
-j portal
/sbin/iptables -t nat -A PREROUTING -i eth0 -p tcp -m mark --mark 99 -m tcp
--dport 1:65534 -j DNAT --to-destination 100.64.0.1
/sbin/iptables -t mangle -A portal -j MARK --set-mark 99
/sbin/iptables -t mangle -I portal 1 -d 172.31.254.100 -p tcp -m tcp -j
RETURN
/sbin/iptables -t mangle -I portal 1 -d 100.64.0.1 -p tcp -m tcp -j RETURN
/sbin/iptables -t mangle -I portal 1 -d 100.64.0.1 -p udp --dport 1:52 -j
DROP
/sbin/iptables -t mangle -I portal 1 -d 100.64.0.1 -p udp --dport 54:65534 -
j DROP
#deny access of unauthenticated users
/sbin/iptables -t filter -A FORWARD -m mark --mark 99 -j DROP
/sbin/iptables -t filter -A FORWARD -m mark --mark 99 -d 172.31.254.100 -j
ACCEPT
/sbin/iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
/sbin/iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT
/sbin/iptables -t filter -A INPUT -m mark --mark 99 -j DROP
/sbin/iptables -t filter -A INPUT -m mark --mark 99 -d 172.31.254.100 -j
ACCEPT
#####################################################################
```