# README FILE

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

## controller:

# Become root
sudo su -

# Install packages

```
yum install MySQL-python python-netaddr
```

# Install MySQL

```
yum install mysql-server
/usr/bin/mysql_secure_installation
/sbin/chkconfig --level 35 mysqld on
/sbin/service mysqld start
```

# After you have finished installing MySQL log in as root:

```
mysql -u root -p <password-you-just-created>
create database nac;
grant all on nac.* to nac identified by 'nacnacwh053dar3?';
flush privileges;
use nac;
CREATE TABLE `tbl_nac_session` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NOT NULL DEFAULT '',
  `ip_address` varchar(255) NOT NULL DEFAULT '',
  `mac_address` varchar(255) NOT NULL DEFAULT '',
  `start_dt` datetime NOT NULL,
  `end_dt` datetime DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM;
```

# Configure iptables (/sbin/service iptables restart when complete)

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 6633 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8000 -j ACCEPT
-A INPUT -s <your-subnet/24> -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

# Prepare local installation directories

```
mkdir /local
mkdir /local/python
mkdir /local/pox
```

# Install Python 2.7.5

```
cd /tmp
wget http://www.python.org/ftp/python/2.7.5/Python-2.7.5.tgz
tar -zxvf Python-2.7.5.tgz
cd Python-2.7.5
./configure --prefix=/local/python
make && make altinstall
```

# Link CentOS/RedHat Python site-packages to this local install (ugly, but it works)

```
cd /local/python/lib/python2.7
/bin/rm -rf site-packages

ln -s /usr/lib/python2.6/site-packages site-packages
```

# Create the following file to help set the path

```
vi /local/path.sh
        PATH=/local/python/bin/$PATH
        export PATH

# Install the POX controller (version betta)
cd /local
wget https://github.com/noxrepo/pox/archive/betta.zip
unzip betta.zip
mv pox-betta pox
```

# At the end your /local should look as follows:

```
ls /local
path.sh  pox  python
```

# Download and extract NCSU-Internet2-SDN-NAC-Code.tar.gz

```
tar -zxvf NCSU-Internet2-SDN-NaC-Code.tar.gz
```

# You should have the following directory layout:

```
cd NCSU-Internet2-SDN-NAC-Code
NCSU-Internet2-SDN-NAC-Code
|-- CONTROLLER
|   |-- path.sh
|   `-- pox
|       `-- ext
|           |-- nac.py
|           `-- nac-readme.txt
`-- PORTAL
    |-- .htaccess
    |-- index.php
    |-- lib.php
    `-- nac
```

```
|-- .htaccess
|-- .htpasswd
`-- index.php
```

# Install the nac.py NAC controller engine

```
cp CONTROLLER/path.sh /local
cp CONTROLLER/pox/ext/nac.py /local/pox/ext/
cp CONTROLLER/pox/ext/nac-readme.txt /local/pox/ext/
```

# Configure POX - nac.py

Note that within /local/pox/ext/nac.py there are a number of comments and configuration variables at the top of the file. You will need to configure the following variables with values that make sense for your environment.

```
#####################################################
# CONFIGURATION - update these values to match
# your environment as required.
#####################################################
# dpid of the openflow switch in your environment
dpid = "00-01-e8-8b-95-24|1"

# openflow switch supports matching ARP messages
dp_supports_arp_match = False

# openflow switch supports matching IP addresses
dp_supports_l3_match = True

# network configuration
networks = {
   '10.0.0.0/24'  : {'untrusted' : 250, 'trusted' : 1250, 'portal' : 2250},
   '10.0.1.0/24' : {'untrusted' : 251, 'trusted' : 1251, 'portal' : 2251},
}

# the Router MAC address
router = EthAddr("00:1b:d4:70:7b:d8")
# the Portal MAC address (recommend that this be set to the Router MAC)
# note: this means you should CHANGE the MAC address on the portal interfaces
# note: facing clients via MACADDR="00:1b:d4:70:7b:d8", etc
portal = router
# ports on OpenFlow switch facing the client
# Note: If only a single port is used on OpenFlow switch (if capable)
# use of.OFPP_IN_PORT as the action
client_port_match = 2
client_port_action = 2
# number of seconds that authenticated clients can be idle before timing out their session
client_idle_timeout = 30
# ports on OpenFlow switch facing infrastructure (router,portal)
# Note: If only a single port is used on OpenFlow switch (if capable)
# use of.OFPP_IN_PORT as the action
router_port_match = 1
router_port_action = 1
portal_port_match = 1
portal_port_action = 1
#
```

```
# MySQL database connection parameters
db_host = "localhost"
db_user = "nac"
db_pass = "nacnacwh053dar3?"
db_name = "nac"
#####################################################
```

# Start the POX controller with the NAC engine

```
source /local/path.sh
python2.7 /local/pox/pox.py log.level --DEBUG nac
```

**##########################################################################**

**captive portal:**

# Become root
sudo su -

# Install packages

```
yum install httpd php php-mysql php-xmlrpc
```

## /etc/sysconfig/network-scripts/ifcfg-eth0

```
# whatever management L3 configuration you require
```

## /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE="eth1"
BOOTPROTO="static"
IPADDR="192.168.200.10"
NETMASK="255.255.255.0"
# override mac address - this should match client router MAC in VL250
MACADDR="00:1b:d4:70:7b:d8"
NM_CONTROLLED="yes"
ONBOOT="yes"
TYPE="Ethernet"
```

## /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE="eth2"
BOOTPROTO="static"
IPADDR="192.168.201.10"
NETMASK="255.255.255.0"
# override mac address - this should match client router MAC in VL251
MACADDR="00:1b:d4:70:7b:d8"
NM_CONTROLLED="yes"
ONBOOT="yes"
TYPE="Ethernet"
```

## /etc/sysconfig/network-scripts/route-eth1

```
# equivalent to route add -net 10.0.0.0/24 dev eth1
10.0.0.0/24 via 192.168.200.10 dev eth1
```

## /etc/sysconfig/network-scripts/route-eth2

```
# equivalent to route add -net 10.0.1.0/24 dev eth2
10.0.1.0/24 via 192.168.201.10 dev eth2
```

## /etc/sysconfig/iptables (/sbin/service iptables restart when complete)

```
# equivalent to /sbin/iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.200.10:80
# equivalent to /sbin/iptables -t nat -A PREROUTING -i eth2 -p tcp --dport 80 -j DNAT --to 192.168.201.10:80
# Generated by iptables-save v1.4.7 on Mon Sep 30 23:39:25 2013
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A PREROUTING -i eth1 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.200.10:80
-A PREROUTING -i eth2 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.201.10:80
COMMIT
# Completed on Mon Sep 30 23:39:25 2013
# Note: this is the default CentOS configuration file from this point forward
# Generated by iptables-save v1.4.7 on Mon Sep 30 23:39:25 2013
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Mon Sep 30 23:39:25 2013
```

## /etc/sysctl.conf  (append the following)

```
# equivalent to sysctl -w net.ipv4.ip_forward=1
# equivalent to echo 1 > /proc/sys/net/ipv4/ip_forward
net.ipv4.ip_forward = 1
net.ipv4.conf.eth1.proxy_arp = 1
net.ipv4.conf.eth1.proxy_arp_pvlan = 1
net.ipv4.conf.eth2.proxy_arp = 1
net.ipv4.conf.eth2.proxy_arp_pvlan = 1
```

## /etc/sysconfig/selinux

```
# disable SELINUX because we have a lot of odd things going on with this portal server that it blocks.
# note: You must reboot the box after making this change
SELINUX=disabled
```

## # Download and extract NCSU-Internet2-SDN-NAC-Code.tar.gz

```
tar -zxvf NCSU-Internet2-SDN-NaC-Code.tar.gz
```

# You should have the following directory layout:

```
cd NCSU-Internet2-SDN-NAC-Code
NCSU-Internet2-SDN-NAC-Code
|-- CONTROLLER
|   |-- path.sh
|   `-- pox
|       `-- ext
|           |-- nac.py
|           `-- nac-readme.txt
`-- PORTAL
    |-- .htaccess
    |-- index.php
    |-- lib.php
    `-- nac
        |-- .htaccess
        |-- .htpasswd
        `-- index.php
```

# Install the portal files

```
mkdir /var/www/html/nac
cp PORTAL/index.php /var/www/html/
cp PORTAL/lib.php /var/www/html/
cp PORTAL/.haccess /var/www/html/
cp PORTAL/nac/index.php /var/www/html/nac/
cp PORTAL/nac/.htaccess /var/www/html/nac/
cp PORTAL/nac/.htpasswd /var/www/html/nac/
```

# Make sure Apache will honor the .htaccess files

```
vi /etc/httpd/conf/httpd.conf
<Directory “/var/www/html”>
        # Replace AllowOverride None with AllowOverride All
/sbin/service httpd restart
```

# Make sure Apache will start at system boot time

```
/sbin/chkconfig --level 35 httpd on
```