Subject: Setting up a HN-based firewall
Posted by raenk on Tue, 30 Apr 2013 18:53:07 GMT
View Forum Message <> Reply to Message

Hi,

I'm following the article on the wiki for setting up a HN firewall:
openvz.org/Setting_up_an_iptables_firewall

But the script does not consider ICMP thus are being blocked.

I managed to insert rule to accept requests on the HN, but can't figure it out for the containers. I'm sure this is going to be an easy one, but i'm not that good for scripting + iptables.

Here's my the modified script:

```
#!/bin/sh
# firewall      Start iptables firewall
# chkconfig: 2345 97 87
# description:  Starts, stops and saves iptables firewall
# This script sets up the firewall for the INPUT chain (which is for
# the HN itself) and then processes the config files under
# /etc/firewall.d to set up additional rules in the FORWARD chain
# to allow access to containers' services.
# wiki.openvz.org/Setting_up_an_iptables_firewall

. /etc/init.d/functions

# the IP block allocated to this server
SEGMENT="*.*.*.64/27"
# the IP used by the hosting server itself
THISHOST="*.*.*.210"
# services that should be allowed to the HN;
# services for containers are configured in /etc/firewall.d/*
OKPORTS="1234"
# hosts allowed full access through the firewall,
# to all containers and to this server
DMZS=""

purge() {
  echo -n "Firewall: Purging and allowing all traffic"
  iptables -P OUTPUT ACCEPT
  iptables -P FORWARD ACCEPT
  iptables -P INPUT ACCEPT
  iptables -F
  success ; echo
}
```

```
setup() {
  echo -n "Firewall: Setting default policies to DROP"
  iptables -P INPUT DROP
  iptables -P FORWARD DROP
  iptables -I INPUT   -j ACCEPT -m state --state ESTABLISHED,RELATED
  iptables -I FORWARD -j ACCEPT -m state --state ESTABLISHED,RELATED
  iptables -I INPUT -j ACCEPT -i lo
  iptables -I FORWARD -j ACCEPT --source $SEGMENT
  success ; echo

  echo "Firewall: Allowing access to HN"
  for port in $OKPORTS ; do
    echo -n "         port $port"
    iptables -I INPUT -j ACCEPT -d $THISHOST --protocol tcp --destination-port $port
    iptables -I INPUT -j ACCEPT -d $THISHOST --protocol udp --destination-port $port
    success ; echo
  done
  for ip in $DMZS ; do
    echo -n "         DMZ $ip"
    iptables -I INPUT   -i eth0 -j ACCEPT -s $ip
    iptables -I FORWARD -i eth0 -j ACCEPT -s $ip
    success ; echo
  done

  echo "Firewall: Allowing ICMP incoming and outgoing requests (Ping) for HN"
  iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -d $THISHOST -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
  iptables -A OUTPUT -p icmp --icmp-type 0 -s $THISHOST -d 0/0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
  iptables -A OUTPUT -p icmp --icmp-type 8 -s $THISHOST -d 0/0 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
  iptables -A INPUT -p icmp --icmp-type 0 -s 0/0 -d $THISHOST -m state --state
ESTABLISHED,RELATED -j ACCEPT
  success ; echo

  CTSETUPS=`echo /etc/firewall.d/*`
  if [ "$CTSETUPS" != "/etc/firewall.d/*" ] ; then
  echo "Firewall: Setting up container firewalls"
  for i in $CTSETUPS ; do
    . $i
    echo -n "$CTNAME CT$CTID"
    if [ -n "$BANNED" ]; then
      for source in $BANNED ; do iptables -I FORWARD -j DROP --destination $CTIP --source
$source ; done
    fi
    if [ -n "$OPENPORTS" ]; then
      for port in $OPENPORTS ; do iptables -I FORWARD -j ACCEPT --protocol tcp --destination
```

```
$CTIP --destination-port $port ; done
      for port in $OPENPORTS ; do iptables -I FORWARD -j ACCEPT --protocol udp --destination
$CTIP --destination-port $port ; done
    fi
    if [ -n "$DMZS" ]; then
      for source in $DMZS ; do iptables -I FORWARD -j ACCEPT --protocol tcp --destination $CTIP
--source $source ; done
      for source in $DMZS ; do iptables -I FORWARD -j ACCEPT --protocol udp --destination $CTIP
--source $source ; done
    fi
    [ $? -eq 0 ] && success || failure
    echo
  done
  fi

  echo "Firewall: Allowing ICMP incoming and outgoing requests (Ping) for Containers"
  iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -d $SEGMENT -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
  iptables -A OUTPUT -p icmp --icmp-type 0 -s $SEGMENT -d 0/0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
  iptables -A OUTPUT -p icmp --icmp-type 8 -s $SEGMENT -d 0/0 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
  iptables -A INPUT -p icmp --icmp-type 0 -s 0/0 -d $SEGMENT -m state --state
ESTABLISHED,RELATED -j ACCEPT
  success ; echo

}

case "$1" in
  start)
    echo "Starting firewall..."
    purge
    setup
    ;;
  stop)
    echo "Stopping firewall..."
    purge
    ;;
  restart)
    $0 stop
    $0 start
    ;;
  status)
    iptables -n -L
    ;;
  *)
    echo "Usage: $0 <start|stop|restart|status>"
    ;;
```

esac