Subject: Firewall
Posted by rcraig114 on Mon, 03 Feb 2014 01:23:50 GMT
View Forum Message <> Reply to Message

I followed one of the recommended firewall guides that involves creating a "firewall" service instead of just plain ole IPTABLES. It works great, but there are a few customizations that I am having trouble with. Below is my code, sanitized of course. My first goal is to allow access to the Host Node via port 22 (secure shell). The only way I can figure out how to get it working right now is to add the IP I am coming from in the DMZ section. How can I add a statement (and where do I add it) to permit secure shell from a single host? Any help is appreciated.

```
#!/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.

. /etc/init.d/functions

# the IP block allocated to this server
SEGMENT="63.141.X.X/X"
# the IP used by the hosting server itself
THISHOST="63.141.X.X"
# services that should be allowed to the HN;
# services for containers are configured in /etc/firewall.d/*
OKPORTS="53 22 3000 80"
# hosts allowed full access through the firewall,
# to all containers and to this server
DMZS="192.168.4.0/24 70.122.X.X 208.110.X.X 10.0.0.1 10.1.1.1 10.254.254.0/30"

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 -s $SEGMENT -d $THISHOST --protocol tcp --destination-port
$port
    iptables -I INPUT -j ACCEPT -s $SEGMENT -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

  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
      for port in $OPENPORTS ; do iptables -I FORWARD -j ACCEPT --protocol udp --destination
$CTIP --destination-port 5060:5080 ; done
      for port in $OPENPORTS ; do iptables -I FORWARD -j ACCEPT --protocol udp --destination
$CTIP --destination-port 10000:20000 ; done
    fi
    if [ -n "$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
}

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>"
    ;;
```

Subject: Re: Firewall
Posted by rcraig114 on Mon, 03 Feb 2014 23:42:31 GMT
View Forum Message <> Reply to Message

OK, I've been able to figure out how to add individual rules. I just insert them at the bottom if need be or even in the beginning. My next problem is NAT. In order to conserve IP space, I created a container with a private IP address. The configuration for NAT is fairly straight forward,

iptables -t nat -A POSTROUTING -s 10.254.253.0/24 -o eth0 -j SNAT --to 63.141.X.X
iptables -A INPUT -s 10.254.253.0/24 -j ACCEPT
iptables -A FORWARD -d 10.254.253.0/24 -j ACCEPT

And it works just fine. However, I've tried a million different ways of integrating it into my above firewall config and it doesn't work. Anyone have any suggestions? Or does anyone have a different way of doing a firewall for the VZ host?