Subject: Firewall issues...kinda
Posted by detz on Sat, 21 Jun 2008 14:28:10 GMT
View Forum Message <> Reply to Message

I used the firewall scripts to setup a firewall on the HT and the VM's and it seems to work but I have issues/questions. I can't ping/access anything from the servers but I can access the servers from outsite(web, ssh). Also, I have three VM's setup and one of them can ping but the other two can't.

```
#!/bin/sh
# firewall      Start iptables firewall
# chkconfig: 2345 08 92
# 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="216.245.192.138/216.245.192.142"

# the IP used by the hosting server itself
THISHOST="216.245.192.138"

# services that should be allowed to the HN;
# services for containers are configured in /etc/firewall.d/*
OKPORTS="6022"

OUTPORTS="8888 8889 6022"

# hosts allowed full access through the firewall,
# to all containers and to this server
DMZS="209.130.152.0/209.130.152.28"

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

  echo "Firewall: Allowing access to HN from outside"
  for port in $OUTPORTS ; do
    echo -n "         port $port"
    iptables -A INPUT -p tcp --dport $port -j ACCEPT
    iptables -A INPUT -p udp --dport $port -j ACCEPT
    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
```

```
    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>"
    ;;
esac
```

And each of the VM's have a conf file...

```
CTID="110"                  # the container's ID#
CTNAME="Production"         # A human-friendly label for the container
CTIP="216.245.192.139"      # the IP address for this container
OPENPORTS="80 443 6022"       # ports that should be universally opened
DMZS="209.130.152.0/28"       # IPs and blocks that should have full access
```

Subject: Re: Firewall issues...kinda

Posted by detz on Sun, 22 Jun 2008 19:17:04 GMT
View Forum Message <> Reply to Message

No one knows?

Subject: Re: Firewall issues...kinda
Posted by detz on Mon, 23 Jun 2008 21:11:44 GMT
View Forum Message <> Reply to Message

I'm an idiot...well, I didn't know better I guess. In case does something similar the SEGMENT should have been
SEGMENT="216.245.192.138/5"
and now everything works!

Subject: Re: Firewall issues...kinda
Posted by klearvue on Sat, 26 Sep 2009 10:16:55 GMT
View Forum Message <> Reply to Message

Hi Razz,

Could you help:

I have 3 IP addresses:

xx.xx.197.35
xx.xx.197.79
xx.xx.197.80

What would my SEGMENT= be?