Subject: Firewall-Script
Posted by michl13 on Tue, 18 Mar 2008 08:16:18 GMT
View Forum Message <> Reply to Message

Hallo!

Ich habe folgendes Problem:
Wenn ich beim booten die Firewall starte, habe ich keinen Zugriff mehr auf den Host.
Ich verwende CentOS5 und iptables ist in allen runlevels deaktiviert.
Was stimmt mit diesem Script nicht? (IP-Adressen wurden geändert)

```
#!/bin/sh
. /etc/init.d/functions
# the IP block allocated to this server
SEGMENT="7X.4X.1XX.147/25"
# the IP used by the hosting server itself
THISHOST="7X.4X.1XX.147"
# services that should be allowed to the HN; services for VEs areconfigured in /etc/firewall.d/*
TCPPORTS="80 10000"
UDPPORTS="4520 4569 5038 5060"
# hosts allowed full access through the firewall, to all VEs 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
 iptables -I INPUT -j ACCEPT -p icmp --icmp-type echo-request
 success ; echo
 echo "Firewall: Allowing access to HN"
 for port in $TCPPORTS ; do
   echo -n "          port $port"
   iptables -I INPUT -j ACCEPT -s $SEGMENT -d $THISHOST --protocol tcp --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

 VESETUPS=`echo /etc/firewall.d/*`
 if [ "$VESETUPS" != "/etc/firewall.d/*" ] ; then
 echo "Firewall: Setting up VE firewalls"
 for i in $VESETUPS ; do
   . $i
   echo -n "          $VENAME VE$VEID"
iptables -I FORWARD -j ACCEPT -p icmp --icmp-type echo-request --destination $VEIP
  if [ -n "$BANNED" ]; then
for source in $BANNED ;  do iptables -I FORWARD -j DROP --destination $VEIP --source
$source ; done
   fi
   if [ -n "$OPENTCPPORTS" ]; then
for port in $OPENTCPPORTS ; do iptables -I FORWARD -j ACCEPT --protocol tcp --destination
$VEIP --destination-port $port ; d$
   fi
   if [ -n "$OPENUDPPORTS" ]; then
for port in $OPENUDPPORTS ; do iptables -I FORWARD -j ACCEPT --protocol udp --destination
$VEIP --destination-port $port ; d$
   fi
   if [ -n "$DMZS" ]; then
for source in $DMZS ; do iptables -I FORWARD -j ACCEPT --protocol tcp --destination $VEIP
--source $source ; done
for source in $DMZS ; do iptables -I FORWARD -j ACCEPT --protocol udp --destination $VEIP
--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
```

Bitte um Hilfe!

DANKE!
