Subject: Re: Host firewall
Posted by ferp2 on Wed, 10 May 2006 13:03:18 GMT
View Forum Message <> Reply to Message

vps:
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Tried the following:

set host input policy to accept and output policy to deny = vps can ping host, host cannot ping vps.

set host output policy to accept and input policy to deny = vps cannot ping host, host can ping vps.

Here are the host iptables rules:

```
# Path to executable
IPT="/sbin/iptables"

# Enable OVZ kernel conntracks in host system
/sbin/modprobe ip_conntrack "ip_conntrack_enable_ve0=1"

# Enable FTP connection tracking
#/sbin/modprobe ip_conntrack_ftp

# Open ports for limited access
OPENPORTS="22"

# INTERFACES
INTERFACE="eth0"                    # Internet-connected interface
LOOPBACK_INTERFACE="lo"                 # Loopback interface
IPADDR="192.168.0.7"

# NETWORKS
LOOPBACK="127.0.0.0/8"              # reserved loopback address range
CLASS_A="10.0.0.0/8"                # class A private networks
CLASS_B="172.16.0.0/12"             # class B private networks
CLASS_C="192.168.0.0/16"            # class C private networks
CLASS_D_MULTICAST="224.0.0.0/4"         # class D multicast addresses
CLASS_E_RESERVED_NET="240.0.0.0/5"      # class E reserved addresses
```

```
BROADCAST_SRC="0.0.0.0"                 # broadcast source address
BROADCAST_DEST="255.255.255.255"        # broadcast destination address

# SUBNET
LAN="192.168.0.0/24"

# PORTS
PRIVPORTS="0:1023"                      # privileged port range
UNPRIVPORTS="1024:65535"                # unprivileged port range

# ============================
# Reset chains and set policies
# ============================

# Remove any existing rules from all chains
$IPT -t filter --flush
$IPT -t nat --flush
$IPT -t mangle --flush

# Set default policy for all chains
# filter
$IPT --policy INPUT DROP
$IPT --policy OUTPUT DROP
$IPT --policy FORWARD ACCEPT

# Don't set nat and mangle tables to DROP unless
# you know what you're doing
# nat
#$IPT -t nat --policy PREROUTING DROP
#$IPT -t nat --policy OUTPUT DROP
#$IPT -t nat --policy POSTROUTING DROP

# mangle
#$IPT -t mangle --policy PREROUTING DROP
#$IPT -t mangle --policy OUTPUT DROP

# Remove any pre-existing user-defined chains
$IPT -t filter --delete-chain
#$IPT -t nat --delete-chain
#$IPT -t mangle --delete-chain

# ============================================
# Using connection state to by-pass rule checking
# ============================================

# Using the state module alone, INVALID will break protocols that use
# bi-directional connections or multiple connections or exchanges,
# unless an ALG is provided for the protocol. At this time, FTP and
```

```
# IRC are the only protocols with ALG support.

$IPT -I INPUT 1 -p ALL -m state --state RELATED,ESTABLISHED -j ACCEPT
$IPT -I OUTPUT 1 -p ALL -m state --state RELATED,ESTABLISHED -j ACCEPT
#$IPT -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#$IPT -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# above 2 rules allow response to future rules using --state NEW

# Give this computer unrestricted access to the internet
$IPT -A OUTPUT -p ALL -o $INTERFACE -j ACCEPT

# Set traffic on the loopback interface to unrestricted
$IPT -A INPUT -i $LOOPBACK_INTERFACE -j ACCEPT
$IPT -A OUTPUT -o $LOOPBACK_INTERFACE -j ACCEPT

# ================================
# Allow lan to ping host
#$IPT -A INPUT -i $INTERFACE -p icmp \
#--icmp-type echo-request -s $LAN \
#-d $IPADDR -m state --state NEW -j ACCEPT

# Allow LAN/PORTA to ping host
$IPT -A INPUT -i $INTERFACE -p icmp -s $LAN \
--icmp-type echo-request -d $IPADDR -j ACCEPT

$IPT -A OUTPUT -o $INTERFACE -p icmp -s $IPADDR \
--icmp-type echo-reply -d $LAN -j ACCEPT
# ================================

# Allow limited access to host
for f in $OPENPORTS; do
        $IPT -A INPUT -i $INTERFACE -p tcp \
        -s $LAN -d $IPADDR --dport $f \
        -m state --state NEW -j ACCEPT
done
```

Hope this helps.