soundtraining.net
Box 1321 Seahurst, WA 98062-1321
v) 206.988.5858 f) 206.892.0499
w) www.soundtraining.net

How-To Guide: Configuring a Basic NAT Firewall in Linux

Network Address Translation

Network Address Translation (NAT) is used to isolate a private network (say, 192.168.0.0/24) from the public Internet. Inexpensive cable modem and DSL routers use NAT to create a simple, yet effective firewall. Hosts on the private network share a single IP address on the public network. Port numbers are assigned to each connection to ensure that each connection has a unique identifier. This simple lab will show you how to configure NAT on a gateway device. Modern Linux systems use iptables to access the netfilter infrastructure of the kernel to implement firewalling.

Configuring the Firewall

1. Use the following command to enable routing:
   `echo "1" > /proc/sys/net/ipv4/ip_forward`
2. Use this command to enable IP masquerading (where your internal (private) hosts all share the same public IP address:
   `iptables -t nat -A POSTROUTING -o [external address] -j MASQUERADE`
3. View the filter with this command:
   `iptables -t nat -n -L -v`
4. To flush a filter, use the following command:
   `iptables -t nat -F POSTROUTING`
   (This command specifies the NAT table and tells iptables to flush the POSTROUTING chain, thus removing the previously configured rule.)
5. Reset the system to disable IP forwarding with this command:
   `echo "0" > /proc/sys/net/ipv4/ip_forward`

Additional Resources

There is more information about iptables at www.netfilter.org. You can download customizable scripts at these locations:

www.e-infomax.com/ipmasq

www.malibyte.net/iptables/scripts/fwscripts.html

We also recommend these books:

Running Linux, 4th Edition, by Matt Welsh, Lar Kaufman, Matthias Kalle Dalheimer, Terry Dawson, O'Reilly

Linux Server Hacks, 1st Edition, by Rob Flickenger, O'Reilly

soundtraining.net is the Seattle, Washington-based firm that specializes in accelerated, short-form training for Information Technology professionals who work with Linux, Microsoft, and Cisco products. soundtraining.net offers both public seminars and workshops and "onsite" training programs in which the training is conducted at your location (or the location of your choosing) and at the time and date of your choosing.

For more information about soundtraining.net, visit www.soundtraining.net or call 206.988.5858.