socat: Linux / UNIX TCP Port Forwarder

Article Number: 637 | Rating: Unrated | Last Updated: Tue, Aug 6, 2019 3:32 PM

socat: Linux / UNIX TCP Port Forwarder

last updated March 15, 2010 in Categories Linux, Networking, UNIX

How do I configure UNIX or Linux system to act as TCP port forwarder without using firewall? How do I install socat (SOcket CAT) multipurpose relay for bidirectional data transfer under Linux?

You can use the utility called socat (SOcket CAT). This is just like the **Netcat but with security** in mind (e.g., it support chrooting) and works over various protocols and through a files, pipes, devices, TCP sockets, Unix sockets, a client for SOCKS4, proxy CONNECT, or SSL etc.

From the man page:

> Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them. Because the streams can be constructed from a large set of different types of data sinks and sources (see address types), and because lots of address options may be applied to the streams, socat can be used for many different purposes.

socat Usage:

1. TCP port forwarder
2. External socksifier
3. Attacking weak firewalls (security testing)
4. A shell interface to UNIX sockets
5. IP6 relay
6. For redirecting TCP oriented programs to a serial line
7. Logically connect serial lines on different computers
8. Security testing and research
9. Establish a relatively secure environment (su and chroot) for running client or server shell scripts with network connections etc

WARNING! These examples may open your computer ports and sockets to other Internet users.

> You must have a good understanding of TCP/IP and UNIX networking to use this tool.

Install socat Under Debian / Ubuntu Linux

Type the following command:
$ sudo apt-get update && sudo apt-get install socat

Source Code Installation

Visit the official website and grab the latest version:
cd /opt
wget http://www.dest-unreach.org/socat/download/socat-1.7.1.2.tar.gz
Untar and install the same:
tar -zxvf socat-1.7.1.2.tar.gz
cd socat-1.7.1.2
./configure
make
make install

Examples

To redirect all port 80 conenctions to ip 202.54.1.5, enter:
socat TCP-LISTEN:80,fork TCP:202.54.1.5:80
All TCP4 connections to port 80 will be redirected to 202.54.1.5. This is just like netcat. You can terminate connection by pressing [CTRL+C] i.e. ^C.

Connect To Remote SSH Server

You can connect to the remote ssh server called server1 and use pty for communication between socat and ssh, makes it ssh's controlling tty (ctty), and makes this pty the owner of a new process group (setsid), so ssh accepts the password from socat.
$ (sleep 5; echo YOURSSHPASSWORDHERE; sleep 5; echo date; sleep 1) |socat - EXEC:'ssh -l userName server1.nixcraft.net.in',pty,setsid,ctty

Get Information About Haproxy

The following will give you information about the running HAProxy process such as pid, uptime and much more:
echo "show info" | socat unix-connect:/var/tmp/haproxy stdio

TCP port forwarder, each side bound to another local IP address (bind)

This example handles an almost arbitrary number of parallel or consecutive connections by fork'ing a new process after each accept() . It provides a little security by su'ing to user nobody after forking; it only permits connections from the private 10 network (range); due to reuseaddr, it allows immediate restart after master process's termination, even if some child sockets are not completely shut down. With -lmlocal2, socat logs to stderr until successfully reaching the accept loop. Further logging is directed to syslog with facility local2:
socat -d -d -lmlocal2
TCP4-LISTEN:80,bind=myaddr1,su=nobody,fork,range=10.0.0.0/8,reuseaddr
TCP4:www.nixcraft.net.in:80,bind=myaddr2