NAME

torsocks.conf — Configuration file for torsocks(8)

SUMMARY

By default, torsocks will assume that it should connect to the Tor SOCKS proxy running at 127.0.0.1 on port 9050. This is the default address and port for Tor's socks server on most installations. If you are running a normal Tor installation and have no special requirements, then you should not need to create, edit or invoke a configuration file when using torsocks.

Your installation of torsocks includes a default configuration file that contains values sensible for use with most Tor installations. The installation location for your default configuration file is:

/etc/tor/torsocks.conf

In order to use a configuration file, you must set the environment variable TORSOCKS_CONF_FILE with the location of the file.

If TORSOCKS_CONF_FILE is not set, torsocks will attempt to read the configuration file at /etc/tor/torsocks.conf. If that file cannot be read, torsocks will use sensible defaults for most Tor installations, i.e. it will assume that you want to use a SOCKS proxy running at 127.0.0.1 (localhost) on port 9050.

CONFIGURATION

SYNTAX

The basic structure of all lines in the configuration file is:

<directive> <parameters>

Empty lines are ignored and all input on a line after a '#' character is ignored.

DIRECTIVES

The following directives are used in the torsocks configuration file:

TorAddress ip_addr

The IP address of the Tor SOCKS server (e.g "server = 10.1.4.253"). Only one server may be specified. Currently, torsocks does NOT support hostname. (default: 127.0.0.1)

TorPort port

The port on which the Tor SOCKS server receives requests. (default: 9050)

OnionAddrRange subnet/mask

Tor hidden sites do not have real IP addresses. This specifies what range of IP addresses will be handed to the application as "cookies" for .onion names. Of course, you should pick a block of addresses which you aren't going to ever need to actually connect to. This is similar to the MapAddress feature of the main tor daemon. (default: 127.42.42.0/24)

SOCKS5Username username

Username to use for SOCKS5 authentication method that makes the connections to Tor to use a different circuit from other existing streams. If set, the SOCKS5Password must be specified also. (Default: none).

SOCKS5Password password

Password to use for SOCKS5 authentication method that makes the connections to Tor to use a different circuit from other existing streams. If set, the SOCKS5Username must be specified also. (Default: none).

AllowInbound 0|1

Allow inbound connections meaning that listen() and accept()/accept4() will be allowed for non localhost address so the applicaton can handle incoming connection. Note that Unix socket are allowed. (Default: 0)

AllowOutboundLocalhost 0|1|2

Allow outbound connections to the loopback interface meaning that connect() will be allowed to connect to localhost addresses bypassing Tor. If set to 1, TCP connections will be allowed. If set to 2, both TCP/IP and UDP connections will be allowed. This option should not be used by most users. (Default: 0)

IsolatePID 0|1

Set Torsocks to use an automatically generated SOCKS5 username/password based on the process ID and current time, that makes the connections to Tor use a different circuit from other existing streams in Tor on a per-process basis. If set, the SOCKS5Username and SOCKS5Password options must not be set. (Default: 0)

EXAMPLE

```
$ export TORSOCKS_CONF_FILE=$PWD/torsocks.conf
$ torsocks ssh account@sshserver.com
```

SEE ALSO

torsocks(1), torsocks(8),

AUTHOR

David Goulet <dgoulet@ev0ke.net>