GNU/Linux Administration - Support #852

Setup a Transparent TOR System Proxy on Arch Linux

09/25/2016 07:07 PM - Daniel Curtis

Status:	Closed	**Start date:**	09/25/2016
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	The Onion Router (TOR)	**Estimated time:**	1.00 hour
Target version:	Arch Linux	**Spent time:**	1.00 hour

Description

This is a guide on setting up a transparent system proxy over TOR on Arch Linux.

Prepare the Environment

- Make sure the system is up to date:

```
pacman -Syu
```

Install TOR

- Install TOR:

```
pacman -S tor
```

- Edit the tor config file:

```
nano /etc/tor/torrc
```

  - And add/modify the following values:

```
SocksPort 9050
DNSPort 5353
TransPort 9040
```

- Start and enable tor at boot:

```
systemctl enable tor
systemctl start tor
```

Configure IPTables

- Install iptables:

```
pacman -S iptables
```

- Enable the required kernel modules:

```
modprobe ip_tables
modprobe iptable_nat
```

```
modprobe ip_conntrack
modprobe iptable-filter
modprobe ipt_state
```

- Create the iptables rules file:

```
sudo nano /etc/iptables/iptables.rules
```

  - And add the following:

```
*nat
:PREROUTING ACCEPT [6:2126]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [17:6239]
:POSTROUTING ACCEPT [6:408]

-A PREROUTING ! -i lo -p udp -m udp --dport 53 -j REDIRECT --to-ports 5353
-A PREROUTING ! -i lo -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REDIRECT --to-ports
 9040
-A OUTPUT -o lo -j RETURN
--ipv4 -A OUTPUT -d 192.168.0.0/16 -j RETURN
-A OUTPUT -m owner --uid-owner "tor" -j RETURN
-A OUTPUT -p udp -m udp --dport 53 -j REDIRECT --to-ports 5353
-A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j REDIRECT --to-ports 9040
COMMIT

*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]

-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
--ipv4 -A INPUT -p tcp -j REJECT --reject-with tcp-reset
--ipv4 -A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
--ipv4 -A INPUT -j REJECT --reject-with icmp-proto-unreachable
--ipv6 -A INPUT -j REJECT
--ipv4 -A OUTPUT -d 127.0.0.0/8 -j ACCEPT
--ipv4 -A OUTPUT -d 192.168.0.0/16 -j ACCEPT
--ipv6 -A OUTPUT -d ::1/8 -j ACCEPT
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m owner --uid-owner "tor" -j ACCEPT
--ipv4 -A OUTPUT -j REJECT --reject-with icmp-port-unreachable
--ipv6 -A OUTPUT -j REJECT
COMMIT
```

    NOTE: Make sure to change the network address in the iptables rule file to the appropriate network address.

- Create a link to enable the rules for IPv6:

```
ln -s /etc/iptables/iptables.rules /etc/iptables/ip6tables.rules
```

- Start and enable the iptables rules at boot:

```
systemctl start iptables
systemctl start ip6tables
systemctl enable iptables
systemctl enable ip6tables
```

Autostart

- Edit the display-manager systemd unit file:

```
nano /etc/systemd/system/display-manager.service
```

  - And add the Requires=iptables.service and Requires=ip6tables.service at the end of the [Unit] tag:

```
[Unit]
Description=LXDE Display Manager
Conflicts=getty@tty1.service plymouth-quit.service
After=systemd-user-sessions.service getty@tty1.service plymouth-quit.service
Requires=iptables.service
Requires=ip6tables.service

[Service]
ExecStart=/usr/sbin/lxdm
Restart=always
IgnoreSIGPIPE=no

[Install]
Alias=display-manager.service
```

- Reload systemd:

```
sudo systemctl --system daemon-reload
```

- Reboot:

```
reboot
```

Resources

- https://wiki.archlinux.org/index.php/tor#Transparent_Torification

History

#1 - 09/25/2016 07:07 PM - Daniel Curtis

- Status changed from New to Resolved

- % Done changed from 0 to 100

#2 - 12/03/2016 12:48 PM - Daniel Curtis

- Status changed from Resolved to Closed