Mandrivauser.de

anwendung:internet:tor

Einrichten von Tor

Tor ist eine freie Software und ein offenes Netzwerk, dass dir hilft, dich gegen eine Analyse der Verbindungsdaten zu schützen.

Hier soll eine Möglichkeit beschrieben werden, wie man Tor unter Mandriva einrichtet.

Was Tor kann

Tor verschleiert in erster Linie deine IP-Adresse in den Verbindungsinformationen. Wenn du wirklich anonym sein willst nutzt dir das alleine wenig solange dein Browser oder dein IM munter weiterhin Informationen (und das kann wider die IP-Adresse sein) über dich preisgibt. Du musst deswegen auch diese “ruhigstellen”. Das lässt sich im Normalfall in den Einstellungen der einzelnen Programme bewerkstelligen. Im Allgemeinen gilt, je besser du dich auskennst desto besser kannst du dich gegen Lücken in Tor schützen deswegen ist die beste Möglichkeit dich zu schützen dich zu informieren.

Des weiteren verschlüsselt Tor deine Daten nur im inneren des Netzwerkes. Am Ende können sie deshalb immer noch abgehört oder manipuliert werden. Es ist sogar eher einfacher. Deshalb musst du dich selbst um die Verschlüsselung deines Verkehrs kümmern. Üblicherweise geht das am einfachsten mit SSL. (Das erkennt ihr daran, das im Browser https: am Anfang der Adresszeile steht und in anderen Programmen der Port 443 ausgewählt ist.) Damit ihr merkt, dass eure Daten nicht manipuliert wurden, solltet ihr natürlich immer auf die Signaturen der heruntergeladenen Programme und Mails achten. (Für Programme macht das urpmi bzw. der rpmdrake automatisch, für Mails solltet ihr euch den Artikel über pgp anschauen.)

Die dritte große Lücke von Tor ist, dass bei der hier beschriebenen Konfiguration die DNS-Anfragen nicht über Tor geleitet werden. (Das Domain Name System ist dafür zuständig, dass die menschenverständlichen Web-Adressen (wie z.B www.mandrivauser.de [http://www.mandrivauser.de]) in computerverständliche Adressen (in unserem Beispiel 62.141.52.97), die zum Erreichen der Site nötig sind, umgewandelt werden.) Wenn also befürchtet wird, dass abgehört wird oder der DNS-Server (standardmäßig ist das der vom ISP (z.B. die 1&1 oder der mit dem T)) die Verbindungsdaten mitloggt, solltet ihr den DNS-Server wechseln oder auch die DNS-Abfragen verschlüsselt über Tor leiten.

Gefahren im Browser

Für den Browser sind die typischsten Gefahrenstellen Java, Javascript, Flash und alles was sonst noch bunt ist und krach-bum macht. Außerdem sind Plugins und Add-ons aller Art gefährlich. Hier ist z.B. die Google-Toolbar zu erwähnen. Aber dass man nicht einfach Software installiert, von der man nicht weiß was sie macht, sollte eigentlich klar sein.

Der zweite Punkt sind Cookies. Sie werden von zahlreichen Sites missbraucht, um Informationen über dich auf deinem Computer zu speichern und später wieder abzurufen. Für den Browser sollte es deshalb strikte Regeln für Cookies geben. Am besten ist es natürlich, sie gar nicht erst zuzulassen. Da Cookies aber auch für durchaus sinnvolle Dinge gebraucht werden (z.B. überall dort, wo eine Anmeldung nötig ist), ist es ein durchaus kontroverses Thema, welche Cookies man von welchen Seiten zulässt.

Einige Arbeit beim richtigen Einstellen des Browsers können Plugins wie der der Torbutton [https://addons.mozilla.org/en-US/firefox/addon/2275] abnehmen.

"Grundinstallation" von Tor

1. Tor installieren und einrichten

1.1 Tor installieren

Am besten wird Tor aus den Mandriva-Quellen installiert. Das geht entweder mit

```
su
urpmi tor
```

oder mit dem rpmdrake.

1.2 Tor konfigurieren

Die Konfiguration von Tor steht im Normalfall in der Datei ”/etc/tor/torrc”. Diese Datei kann prinzipiell nur root ändern. Dazu holt ihr euch in der Konsole root-Rechte und öffnet die Datei mit einem Editor eurer Wahl. (In meinem Fall ist das nano.):

```
su -
Passwort:
nano /etc/tor/torrc
```

In dieser Datei stehen schon viele Beispiele mit einer Beschreibung ihrer Wirkung: Texte hinter einer Doppelraute (**##**) sind nur Kommentare.

Texte hinter einer Raute (**#**) sind Beispielkonfigurationen. Sie werden ebenfalls von Tor ignoriert. Durch Entfernen der Raute wird dieser Text Teil der Konfiguration, so dass im Normalfall nur dies gemacht werden muss.

Die unten aufgeführten Zeilen gewährleisten, dass Tor funktioniert:

```
SocksPort 9050
SocksListenAddress 127.0.0.1
```

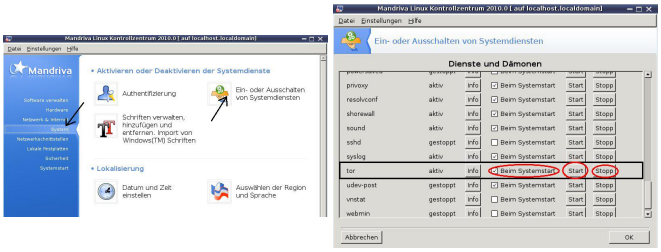
Die erste Zeile besagt, dass Tor auf dem Port 9050 läuft und die zweite, dass niemand von außerhalb direkt auf Tor zugreifen kann. Wenn gewünscht wird, dass auch andere Computer über diesen PC auf Tor zugreifen können, wird das am besten mit privoxy realisiert.

Wenn Tor manuell gestartet werden soll, müssen auch noch folgende Zeilen in die Datei geschrieben oder die Raute vor ihnen entfernt werden. Wenn man sich nicht sicher ist, schadet es auch nicht, wenn sie dastehen obwohl man sie nicht braucht:

```
Log notice file /var/log/tor/notices.log #optional
DataDirectory /var/lib/tor
User toruser
```

1.3 Tor Starten

Tor kann man im MCC unter System → Ein- oder Ausschalten von Systemdiensten suchen und ein und ausschalten. Am besten setzt man ein Häkchen bei “Beim Systemstart” dann braucht man sich in Zukunft um nichts mehr kümmern.



2. privoxy installieren und konfigurieren

Tor stellt auf Port 9050 einen SOCKS-Proxy zur Verfügung. Da die meisten Anwendungen nicht damit umgehen können, wird einfach privoxy, der als gewöhnlicher HTTP-Proxy arbeitet und den Verkehr zu Tor umleitet, installiert.

2.1 privoxy installieren

Am besten installiert man auch privoxy aus den Quellen. Das geht wieder mit

```
su -
Passwort:
urpmi privoxy
```

oder mit dem rpmdrake.

2.2 privoxy konfigurieren

Die Konfiguration von privoxy steht im Normalfall in der Datei ”/etc/privoxy/config”. Auch sie lässt sich nur als root editieren.

Hier sollten folgende Zeilen hinzugefügt werden (bzw die # vor ihnen entfern werden): (Achtung! Der Punkt hinter der 0 und dem Leerzeichen ist wichtig.)

```
listen-address  127.0.0.1:8118
forward-socks4a   /      localhost:9050 .
```

Und falls vorhanden müssen folgende Zeilen mit einer # wirkungslos gemacht oder entfernt werden:

```
jarfile jarfile
logfile logfile
```

2.3 privoxy Starten

Wie schon Tor, kann man privoxy im MCC starten und beenden und gegebenenfalls beim Systemstart starten lassen.

3. Die Anwendungen anpassen.

Jetzt wird in den Anwendungen, die Tor nutzen sollen, die eigene IP-Adresse (127.0.0.1) und der Port 8118 (viele Anwendungen verlangen das ganz, dann so dargestellt: 127.0.0.1:8118.) als HTTP-Proxy bzw. HTTPS-Proxy eingetragen und schon wird Tor benutzt. Ob euer Browser tatsächlich Tor benutzt, könnt ihr hier [http://check.torproject.org/] testen.

Wenn ihr auch die DNS-Abfragen durch Tor leiten wollt, müsst ihr stattdessen direkt Tor (127.0.0.1:9050 bzw. IP-Adresse 127.0.0.1 und Port 9050) als SOCKSv5 Proxy eintragen. Prinzipiell könnt ihr dann Schritt 2 weglassen. Allerdings bieten die wenigsten Anwendungen die Möglichkeit, einen SOCKS-Proxy zu nutzen. Außerdem verlangsamt dies das Surfen noch einmal erheblich, da erst mit Laden der Seite angefangen werden kann, wenn die DNS-Abfrage, die wegen der langen ping-Zeiten im Tor Netz sehr lange dauert, beendet wurde. Anmerkung: Sowohl ein SOCKS-Proxy, wie auch ein HTTP-Proxy einzutragen ist sinnlos, da immer nur einer genutzt werden kann.

Aber Vorsicht: Guckt euch nochmal den Abschnitt “Was Tor kann” an. Damit ihr wisst, was Tor macht und vor allem was Tor nicht macht.

Tor hinter Filtersystemen

Firewall auf Layer 4

Die meisten Firewalls arbeiten auf Layer 4 (Sie sperren bestimmte Ports.). Wenn man hinter einer solchen Firewall sitzt, kann man die Konfigurationsdatei (/etc/tor/torrc) um folgende Zeilen erweitern:

```
FascistFirewall 1
FirewallPorts 80, 443
```

Wobei in die durch Kommas getrennte Liste mit Ports hinter “FirewallPorts” natürlich Ports kommen, die die Firewall freigibt. Wobei 80 (HTTP) und 443 (SSL bzw. HTTPS) von den meisten Firewalls erlaubt werden. Wenn genau diese beiden Ports benutzt werden sollen, kann die zweite Zeile auch weggelassen werden.

Einen Server einrichten

Da Tor den Internet-Traffic, um ihn zu anonymisieren, über viele Server (sie werden Nodes genannt) umleitet, ist Tor darauf angewiesen, dass es Leute gibt, die diese Nodes aufstellen. Hier wird erklärt, wie man einen solchen Node aufstellen und so das Tor-Projekt unterstützen kann.

Es gibt drei Arten von Servern: Bridges, Middle-Nodes und Exit-Nodes. Am dringendsten werden Exit-Nodes gebraucht. Die Eindeckung mit Bridges ist, obwohl es gerade von denen nicht genug geben kann, am besten. Was allerdings daran liegt, dass sie recht selten gebraucht werden.

Um heraus zu finden, was für ein Server am besten betrieben wird, lest ihr euch am besten die Einleitungen zu den einzelnen Serverarten durch. Aber hier mal eine kleine Übersicht:

Wenn wenig Upload-Bandbreite zur Verfügung steht sollte eine Bridge betrieben werden. Ansonsten ist es hier in Deutschland zu empfehlen, einen Middle-Node zu betreiben, da es bei Exit-Node Betreibern wohl recht gerne mal zu Hausdurchsuchungen und ähnlichem kommt, wenn mal wieder jemand Tor für illegale Zwecke missbraucht. (Vor Gericht wurde aber meines Wissens noch keiner für schuldig befunden.) Mutige, die sich mit der Rechtslage auskennen, können einen Exit-Node (gegebenenfalls mit gewissen Einschränkungen) betreiben.

Fix Me! Währe toll wenn der Abschnitt um die Rechtslage in anderen Ländern (vor allem der in Österreich und der in der Schweiz) erweitert würde.

Eine Bridge betreiben

Was ist eine Bridge?

Eine Bridge ist ein Node dessen Adresse nicht veröffentlicht wird. Da es keine öffentliche Liste mit ihnen gibt, kann niemand den Zugriff auf sie verhindern. Über sie können dann auch Menschen, denen der Zugriff auf das Tor-Netzwerk eigentlich blockiert wird (zum Beispiel von ihrem ISP, ihrem Land aber auch ihrem Arbeitgeber), auf Tor zugreifen. Da die Adresse dann aber auch nur an wenige Leute über E-Mail [mailto:bridges@torproject.org], Social-Networks und eine Website [https://bridges.torproject.org/], die immer nur 3 Bridges preisgibt, verteilt werden, profitieren auch nur entsprechend wenige Leute von diesem Node.

Eine Bridge einrichten

Um eine Bridge einzurichten, muss zu erst folgende Zeile aus der Datei /etc/tor/torrc wieder entfernt werden. (Oder durch eine # am Anfang wirkungslos gemacht werden):

```
SocksListenAddress 127.0.0.1
```

Damit wird der Zugriff von außen auf Tor erlaubt.

Und dann folgende Zeilen hinzugefügt werden oder die # vor ihnen entfernt werden, falls sie schon vorhanden sind:

```
ORPort 443
BridgeRelay 1
Exitpolicy reject *:*
```

Der erste Eintrag gibt an, dass die Bridge auf Port 443 (HTTPS) läuft, der zweite, dass es sich um eine Bridge handelt und der dritte, dass hier kein Exit-Node betrieben wird.

Wenn Port 443 schon von einem anderen Dienst besetzt wird (sas ist im Normalfall beim Betreiben eines Webservers mit SSL Zugang der Fall) oder dieser Port von einer Firewall, die nicht verändert werden kann, gesperrt wird, kann ein anderer Port gewählt werden. Dabei sollte allerdings bedacht werden, dass die Leute die eine Bridge nutzen müssen, meistens hinter starken Filtersystemen sitzen, die mit hoher Wahrscheinlichkeit nur auf wenigen Ports verschlüsselten Verkehr erlauben. Gute andere Möglichkeiten sind zum Beispiel 80 (HTTP), 995(pop3s), 110(pop3), 143(IMAP) oder 8080(HTTP Alternative). Anmerkung: Viele Firewalls erlauben nur hohe Ports (>1024 oder sogar >6000).

Da jetzt nur die bridgespezifischen Änderungen vorgenommen wurden, müsst ihr mit dem Punkt Schritte für alle Arten von Servern weiter machen.

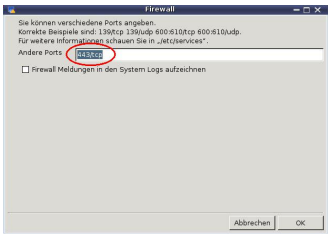
Schritte für alle Arten von Servern

Da die Konfigurationen der verschiedenen Server recht ähnlich sind, habe ich, um nicht alles mehrfach schreiben zu müssen die Schritte, die für die Konfiguration aller Arten von Servern notwendig sind, zusammengefasst.

Mandriva Firewall anpassen

Da für gewöhnlich der Zugriff von außen von der Firewall geblockt wird, muss der Zugriff auf den Tor-Server erlaubt werden. Dazu wird im MCC unter *"Sicherheit" → "Einstellungen für die Firewall" → "Fortgeschrittene Optionen"* der ORPort eingetragen. Wenn alles wie hier beschrieben gemacht wurde ist das 443/tcp.

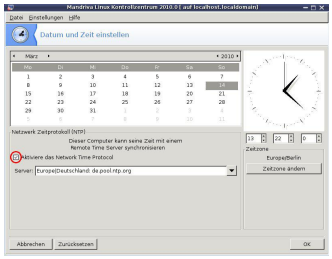
mccfriewall.jpeg



Anmerkung: Die Interaktive Firewall wird euch jetzt regelmäßig darüber informieren, dass sich jemand mit dem HTTPS-Dienst verbindet. Aber dass euer Node von anderen genutzt wird, ist ja ihr Sinn. Und deswegen sind die Meldungen nicht bedenklich.

ntp aktivieren

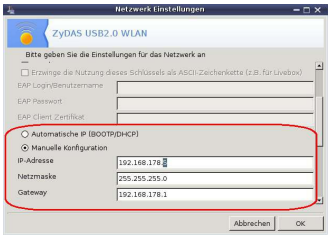
Es scheint für den Betrieb von Tor-Servern nötig zu sein, eine relativ genaue Uhr zu haben. (Ich weiß selbst nicht warum.) Deswegen sollte dafür gesorgt werden, dass sich die Uhr regelmäßig über ntp aktualisiert. Das geht recht einfach über das MCC. Dazu wird ein Häkchen im MCC unter *"System" → "Zeit und Datum einstellen" → "Aktiviere Network Time Protocol"* gesetzt. Welcher Server ausgewählt wird, ist mehr oder weniger egal. Aber am besten nehmt wir einen aus der Nähe.



Ein Tor-Server hinter einem Router

Wenn der Computer mit dem Tor-Node hinter einem Router steht, muss die Anfragen an den Node auch vom Router an den Computer mit dem Node weitergeleitet werden.

Dazu wird am besten am Computer eine feste IP vergeben. (Im Netzwerkcenter unter "Konfigurieren" → "Manuelle Konfiguration" eine bestimmte IP einstellen) Wenn ihr keine Ahnung habt tragt ihr unter Gateway die IP-Adresse eures Routers und unter Netzmaske 255.255.255.0 ein. Und unter IP-Adresse werden die ersten 3 Zahlen gleich wie beim Router eingetragen und an die letze Stelle schriebt ihr irgend eine Zahl, die größer als 1 und kleiner als 255 ist (nicht gleich!). Dabei trennt ihr die Zahlen durch Punkte.



Dann muss im Router eingestellt werden, dass der ORPort (443 im hiesigen Beispiel) an den gleichen Port(wider 443) an der Adresse, die vergeben wurde (im Bild 192.168.178.5) weiter geleitet wird. Die meisten Router nennen diesen Vorgang (Port)forwarding, Virtualserver, oder (Destiantion) NAT. Wenn ich nicht weiter kommt, sucht mal nach dem Namen eures Routers und den oben genannten Begriffen im Internet oder wendet auch an den Hersteller eures Routers.

Überprüfen, ob der Tor-Node läuft

Wenn alles eingerichtet wurde, kann anhand der Logs überprüft werden, ob der Tor-Node funktioniert. Die Logs sind nur als root lesbar können am besten so eingesehen werden:

```
su -
Passwort:
cat /var/log/tor/tor.log
```

Wenn die folgende Meldung erscheint, ist alles bestens:

```
[notice] Self-testing indicates your ORPort is reachable from the outside. Excellent. Publishing server descriptor.
```

Bei diesen Meldungen ist vermutlich noch irgendeine Firewall im Weg und/oder der Router leitet die Anfragen noch nicht richtig weiter:

```
[warn] Your server (XXX.XXX.XXX.XXX:443) has not managed to confirm that its ORPort is reachable. Please check your firewalls, ports, address, /etc/hosts file, etc.
```

Wenn diese Meldung erscheint, ist die Wahrscheinlichkeit für solche Problem auch recht groß:

```
[notice] Now checking whether ORPort XXX.XXX.XXX.XXX:443 is reachable... (this may take up to 20 minutes -- look for log messages indicating success)
```

Links

https://www.torproject.org/ [https://www.torproject.org/] Offizielle Website des Tor-Projekts

http://wiki.bsdforen.de/howto/tor_und_privoxy [http://wiki.bsdforen.de/howto/tor_und_privoxy] Eine Webseite von der ich einiges, wenn auch nicht wörtlich, übernommen habe.

— *Fabian Wannenmacher [mailto:fabiwanne@yahoo.de] 2010/03/02 22:50*

anwendung/internet/tor.txt · Last modified: 2012/12/20 16:16 (external edit)