Nutzung des TOR-Browsers in TightGate-Pro

TOR ist ein Overlay-Netzwerk zur Anonymisierung von Verbindungsdaten. Es wird für TCP-Verbindungen eingesetzt und kann im TightGate-Pro für ein anonymes Surfen im Internet verwendet werden. Tor schützt seine Nutzer vor der Analyse des Datenverkehrs. Es basiert auf der Idee des Onion-Routings. **TOR** war ursprünglich ein Akronym für **The Onion Routing**.

Im TightGate-Pro bietet die m-privacy GmbH den TOR-Browser als optionales Paket an. In diesem optionalen Paket enthält der TOR-Browser einen TOR-Proxy und die vom TOR-Projekt vorkonfigurierte Version des TOR-Browsers (Mozilla Firefox ESR). Die Details zum Design des TOR-Browsers können Sie auf der Webseite des Tor-Projektes nachlesen unter folgendem Link:
https://2019.www.torproject.org/projects/torbrowser/design/ (in Englisch)

Architektur

Der TOR-Browser hat auf Grund seiner Architektur und Funktionsweise einige Besonderheiten, welche bei der Vorbereitung der Nutzung des TOR-Browsers auf TightGate-Pro zu beachten sind. Eine Beschreibung, wie das TOR-Netzwerk funktioniert, findet sich beim TOR-Projekt unter folgendem Link:
https://tb-manual.torproject.org/de/about/

Vorbereitungen

Aus der Architektur des TOR-Browsers ergibt sich, dass TightGate-Pro bei der Nutzung des TOR-Browsers entweder einen freien Zugang Richtung Internet (Port 443 TCP) bekommt oder es muss als Uplink-Proxy ein SSL/https-fähiger Proxy am TightGate-Pro eingestellt sein.

Bitte stellen Sie sicher, dass:

- TightGate-Pro sich entweder direkt mit dem Internet (Port 443 Protokoll TCP) verbinden kann oder das für TightGate-Pro ein SSL fähiger Proxy verwendet wird –> Link zum setzen der Proxy-Einstellungen in TightGate-Pro.
  Sofern sich TightGate-Pro frei in Richtung Internet verbinden kann, kann als Proxy in TightGate-Pro auch ein nicht SSL fähiger Proxy eingetragen sein. Dann wird der Proxy für alle Verbindungen mit Firefox und Chrome verwendet und der TOR-Browser verbindet sich direkt mit dem TOR-Netzwerk über den freien Internetzugang.
- TightGate-Pro sich auf einem aktuellen Update-Stand befindet.

Installation

Zur Installation des TOR-Browser im TightGate-Pro gehen Sie bitte folgendermaßen vor:

- Anmeldung als Administrator ***update***
- Aufruf des Menüpunktes **Optionale Pakete hinzufügen**
- Auswahl des Paketes **tor-browser**

Nach der Installation steht der TOR-Browser zur Verfügung.

Nutzung

Damit der Tor-Browser genutzt werden kann, muss er zunächst aktiviert werden. Danach kann der TOR-Browser einzelnen Kennungen zugewiesen werden.

TOR-Browser global aktivieren

- Anmeldung als Administrator ***config***
- Auswahl des Menüpunkts **System-Vorgaben > Tor-Browser-Unterstützung:** und dort den Wert auf **Ja** ändern
- **Speichen** und **Anwenden** durchführen.

Zuweisung des TOR-Browsers zu Kennungen

Der TOR-Browser im TightGate-Pro kann auf zwei verschiedenen Arten aufgerufen werden. Zum einen kann der Browser direkt über das **Startmenü** im Verzeichnis **Internet** gestartet werden oder Sie können einzelnen Benutzern oder Benutzergruppen ein neues Icon auf die Menüleiste legen, über den der TOR-Browser zu starten ist.

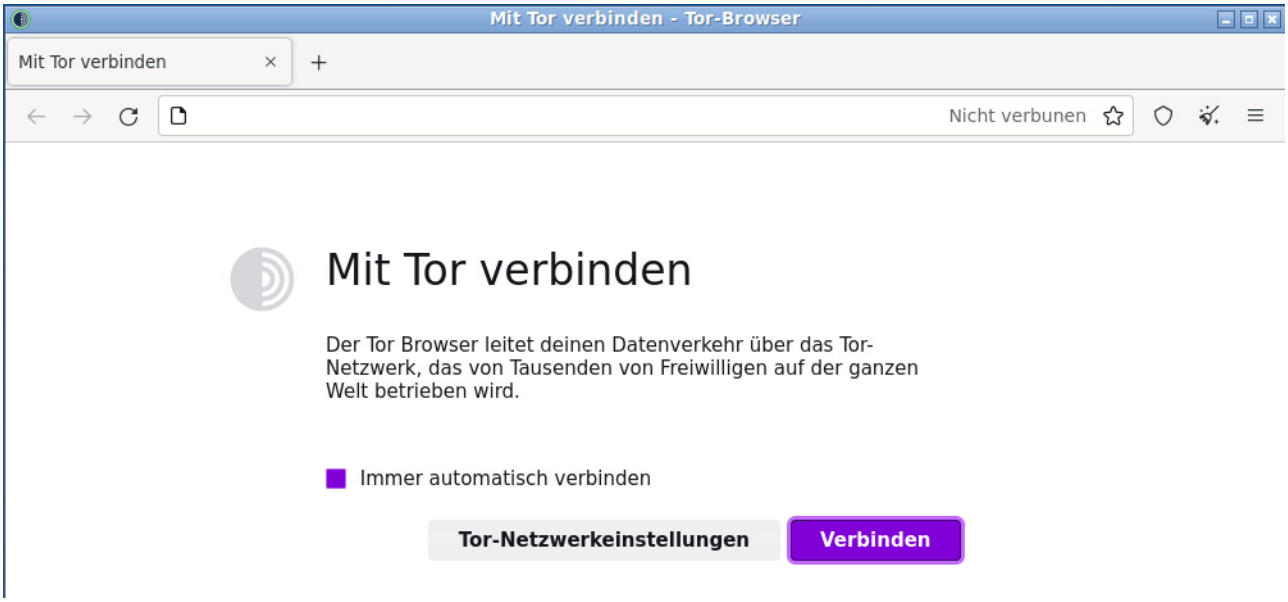
- Anmeldung als Administrator ***maint***
- Auswahl des Menüpunktes **Benutzerverwaltung → Menü-Optionen:**
- Wählen Sie dort bitte die Kennung oder Gruppe aus, der sie das TOR-Browser Icon zuweisen wollen.
- Wählen Sie in den Oberflächen-Menü-Optionen **tor** aus. Die Auswahl erfolgt mit der **Leertaste**.
- Nach der Auswahl ist das neue Icon  nutzbar und erscheint bei der nächsten Anmeldung über den TightGate-Viewer auf der Menüleiste.

Hinweis

Sofern die Benutzerauthentifizierung per Active-Directory erfolgt, sind aller Benutzerkennungen die den TOR-Browser nutzen sollen in die AD-Sicherheitsgruppe **TGtoricon** aufzunehmen. Eine Übersicht über alle AD-Sicherheitsgruppen findet sich hier: Übersicht AD-Sicherheitsgruppen für TightGate-Pro.

Starten und erste Verbindung

- Der Start des TOR-Browsers erfolgt durch Anklicken des neuen Icons  auf der Menüleiste.
- Es öffnet sich danach der TOR-Browser mit folgendem Startbildschirm:



- Obwohl der Startbildschirm dazu auffordert sich zu verbinden oder sich ein Pop-up-Fenster öffnet, welches auf eine unerwartete Unterbrechung hinweist, ist es nicht notwendig Tor neu zu starten oder sich neu zu verbinden. Bitte ignorieren Sie diese Meldungen, im Hintergrund hat TightGate-Pro schon alle notwendigen Verbindungen aufgebaut und die benötigte Proxy-Verbindung erstellt. Es kann wie gewohnt in der Adresszeile des Browsers eine gewünschte URL eingeben werden.

Weitergehende Anleitungen zur Nutzung des TOR Browsers finden sich beim TOR-Projekt unter folgendem Link: https://support.torproject.org/de/

Achtung

Es sollten keine zusätzlichen Add-ons für den TOR-Browser installiert werden, da dies einige seiner Datenschutzfunktionen beeinträchtigen kann.