Proxy

TightGate-Pro kann mit vorgeschalteten Proxys zusammenarbeiten. Die nachfolgende Übersicht erläutert die Konfiguration.

Proxy-Einstellungen

Menüpunkt	Beschreibung
HTTP-Proxy*	IPv4-Adresse(n) oder DNS-Namen der HTTP-Proxy-Server, über die alle Internetzugriffe der Benutzer geleitet werden. Es können mehrere Proxys eingetragen werden, diese sind durch ein Leerzeichen bei der Eingabe zu trennen. **Achtung:** Werden Proxys mit einem DNS-Namen eingetragen, muss der Menüpunkt HTTP-Proxy-Netz spezifiziert werden. Weiterhin muss ein DNS-Server eingetragen sein, der den DNS-Namen des Proxys auflösen kann.
HTTP-Proxy-Reihenfolge*	Falls mehrere Proxys eingetragen wurden, ist hier das Verfahren festzulegen, in welcher Reihenfolge die Proxys verwendet werden sollen. Es stehen folgende Verfahren zur Auswahl: **Round-Robin:** Proxys werden zufällig abwechseln genutzt, es gibt keine bestimmte Reihenfolge. **Geordnet:** Die Proxys werden der Reihenfolge wie sie eingetragen wurden verwendet. **CARP:** Bei diesem Verfahren wird für eine aufgerufene URL immer der gleiche Proxy verwendet (–> Wikipedia: CARP). **Hinweis:** Wird nur ein Proxy-Server eingetragen, wird diese Menüoption nicht angezeigt.
HTTP-Proxy-Port*	Angabe des Ports, der zum Kontakt mit den eingetragenen HTTP-Proxys zu verwenden ist. Es muss für alle referenzierten HTTP-Proxys der gleiche Proxy-Port verwendet werden.
HTTP-Proxy-Netz*	Falls Proxys mit DNS-Namen eingetragen wurden, benötigt das System unbedingt die Information über die IP-Adressen, die sich dahinter verbergen. Die IP-Adressen sind in der Form [IP-Adresse/Valid Bits] anzugeben.
HTTP-Proxy SSL/https*	Auswahl, ob die Proxys über HTTPS oder HTTP angesprochen werden.
HTTP-Proxy-Login*	Sofern die eingetragenen Proxys eine Benutzerauthentifizierung mit Benutzername und Passwort erfordern, kann hier der Benutzername hinterlegt werden.
HTTP-Proxy-Passwort*	Sofern die eingetragenen Proxys eine Benutzerauthentifizierung mit Benutzername und Passwort erfordern, kann hier das Passwort hinterlegt werden.
Aktiviere HTTP-Pipelining*	HTTP-Pipelining ist eine Technik, bei der mehrere HTTP-Anfragen einem einzigen Socket übergeben werden, ohne auf eine Antwort zu warten. Besonders bei Verbindungen mit hohen Latenzzeiten, kann dies eine erhebliche Verkürzung der Seitenladezeiten bedeuten. Das Abschalten kann helfen, wenn das Laden von HTTPS-Seiten über den Uplink-Proxy wiederholt hängt.
AD/Kerberos-Proxy-Anmeldung	Ja/Nein - aktiviert AD-Benutzerauthentisierung Proxy. Eine Anleitung zur Proxy-Authtentisierung per Active Directory gibt es hier

Menüpunkt	Beschreibung
AD/Kerberos Proxy-Servis	Dieser Menüpunkt erscheint nur, wenn der Menüpunkt **AD/Kerberos-Proxy-Anmeldung** auf **Ja** gesetzt ist. Eine Anleitung zur Proxy-Authtentisierung per Active Directory gibt es hier
AD/Kerberos Proxy REALM	Dieser Menüpunkt erscheint nur, wenn der Menüpunkt **AD/Kerberos-Proxy-Anmeldung** auf **Ja** gesetzt ist. Eine Anleitung zur Proxy-Authtentisierung per Active Directory gibt es hier

Proxy-Ausnahmen

Über den Menüpunkt **Proxy > Proxy-Ausnahmen** können IP-Adressen oder URLs von Websites hinterlegt werden, die nicht über den externen Proxy geleitet werden sollen. Die Ausnahmen werden den TightGate-Pro Benutzern im Browser bei jeder Anmeldung eingetragen. Alle Proxy-Ausnahmen die hier eingetragen werden, müssen auch im Menü unter **Netzwerk > HTTP-Server** eingetragen werden.

Proxy-Filter (Webfilter)

Neben der Darstellung von Inhalten aus dem Internet bietet TightGate-Pro auch die Möglichkeit zur inhaltlichen Kontrolle und Beschränkung der Internetnutzung. Der Webfilter von TightGate-Pro arbeitet als Zwangsproxy und filtert die aus dem Internet abgerufenen Daten anhand definierbarer Kriterien. Folgende Kategorien werden dabei berücksichtigt:

- Vordefinierte Blacklisten für URLs und Domänen
- Manuell definierte Black- und Whitelisten für URLs und Domänen

Allgemeines zum Webfilter

Die Funktionsweise des Webfilters ist ähnlich der eines Malwarefilters. Es bestehen vordefinierte Listen von unerwünschten Inhalten (Blacklisten), die unterschiedlichen Kategorien zugeordnet sind. Ist der Webfilter aktiv und Kategorien als unerwünschter Inhalt ausgewählt, so übergibt TightGate-Pro bei jeder Anfrage nach einer Webseite diese zur Prüfung vorab an den internen Webfilter. Dieser prüft, ob die Seite auf einer Liste (Blackliste) mit unerwünschten Inhalt steht. Ist dies der Fall, liefert der Webfilter statt des Inhalts der Seite einen Hinweis, dass der Zugriff auf die entsprechende Seite unterbunden wurde. Grundsätzlich erfolgt die Prüfung auf Zulässigkeit einer Seite nach dem Prinzip "Whitelist vor Blacklist". Ist eine Domäne oder URLs im System auf der Whitelist vermerkt, so wird der Zugriff immer gestattet.

Grenzen des Webfilters: Ein Inhaltsfilter ist nur so treffsicher wie seine Listen. Diese haben einen begrenzten Umfang und bedürfen der regelmäßigen Pflege. Die m-privacy GmbH bietet eine Liste an, die von dritter Seite gepflegt wird. Die m-privacy GmbH übernimmt daher keine Haftung für die Vollständigkeit und den Inhalt der Liste.

Exkurs zur Webfilterung von HTTPS-verschlüsselten Seiten
Im Zuge der Webfilterung können HTTPS-Verbindung auf TightGate-Pro aufgebrochen werden. Nur so ist die URL-genaue Filterung der abgerufenen Web-Inhalte auch bei HTTPS-Zugriffen möglich. Wird ein

Aufbrechen von HTTPS-Verbindungen durch den in TightGate-Pro integrierten Proxyfilter nicht gewünscht, ist lediglich eine domänenbasierte Filterung verschlüsselt abgerufener Web-Inhalte möglich. Die m-privacy GmbH empfiehlt, vor Aktivierung des Leistungsmerkmals den jeweils zuständigen Datenschutzbeauftragten beziehungsweise IT-Sicherheitsbeauftragten zu konsultieren.

Konfiguration des zentralen Webfilters

Zum Anschalten und Konfigurieren des Webfilters sind folgende Schritte zu befolgen:

So geht's:

- Anmeldung als Administrator ***config***
- Den Menüpunkt **Proxy > Proxy Filter** auswählen und den Webfilter über die Auswahl **Ja** anschalten. Damit wird der Webfilter aktiviert und es stehen weitere Menüpunkte zur Verfügung.
- Prüfen, ob die HTTPS-Verbindungen aufgebrochen werden sollen, damit die Webfilterung nicht nur Domänen, sondern auch URLs umfasst. Sofern dies der Fall ist, den Menüpunkt **HTTPS-Verbindungen aufbrechen** auswählen und mit **Ja** bestätigen.
  Hinweis: Bitte beachten Sie obenstehende Ausführungen zum Aufbrechen von HTTPS-Verbindungen und besprechen Sie diese Funktion vorab mit Ihrem internen Datenschutz- bzw. Sicherheitsbeauftragten.
  Achtung: Wird TightGate-Pro mit einem vorgeschalteten Proxy betrieben, so funktioniert die Webfilterung von HTTPS-verschlüsselten Seiten nicht!
- Über den Menüpunkt **Zugriff-Verweigert-Text** lässt sich ein Individueller Text hinterlegen, der Benutzern angezeigt wird, sofern ein Zugriff verweigert wird.
  Hinweis: Der Text wird bei HTTPS verschlüsselten Webseiten nur ausgegeben, sofern HTTPS-Verbindungen aufgebrochen werden.
- Über den Menüpunkt **Anzahl Filter-Gruppen**, kann festgelegt werden, wie viele unterschiedliche Gruppen es für den Webfilter geben soll. Den Gruppen werden jeweils eigene Kategorien zugeordnet. Es können bis zu 99 Gruppen definiert werden.
- Im letzten Schritt sind die jeweiligen Filter-Gruppen mit Kategorien zu versehen. Zur Auswahl stehen folgende Optionen:
  Nur Weißlisten: Diese Option verbietet den Zugriff auf alle Inhalte, die nicht explizit freigegeben sind. Freigaben erstellt der Administrator ***maint*** unter den Menüpunkten **Webseiten-Filter > Domänen freischalten** und **Webseiten-Filter > URLs freischalten**.
  Kategorien (Sperrliste): Es wird eine Liste von Kategorien angezeigt, die nicht erlaubt werden sollen. Zusätzlich zu den ausgewählten Kategorien werden alle Einstellungen des Administrators ***maint*** unter den Menüpunkt **Webseiten-Filter** berücksichtigt. Die Einstellungen unter **Webseiten-Filter** haben dabei Vorrang vor den Kategorien.
  Blockiere IP- und IPv6-Adressen: Auswahl, ob der direkte Aufruf von IP-Adressen (IPv4 und IPv6) im Browser verboten werden soll. Bei **Ja**, ist es nicht möglich IP-Adressen direkt anzusprechen. Ausnahmen davon bilden die explizit erlaubten IPs, welche der Administrator **maint** unter dem Menüpunkt **Webseiten-Filter > Domänen freischalten** freigegeben hat.
- Die Einstellungen im Hauptmenü **Speichern** und **Anwenden**.
- Anmeldung als Administrator ***maint*** und Zuweisung einer Filter-Gruppe zu Benutzern oder Gruppen über dem Menüpunkt **Benutzerverwaltung > Gefiltertes Web**.

Achtung

Bei der initialen Nutzung des Proxy-Filters ist in jedem Fall einen **Speichen** und **Anwenden** notwendig, bevor den einzelnen Filtergruppen Kategorien zugeordnet werden können.

Konfiguration des Webseiten-Filters

Zusätzlich oder alternativ zur Verwendung der zentralen Kategorien des Proxy-Filters ist es möglich im TightGate-Pro selber Domänen und URLs zu eigenen Black- und Whitelisten hinzuzufügen.

Das wird benötigt: → Als ***config*** aktivierter Proxy-Filter (Webfilter)

So geht's:

- Anmeldung als Administrator ***maint.***
- Auswahl des Menüpunkts **Webseiten-Filter**.
- Auswahl der Gruppe, für die Sperrungen oder Freigaben erfolgen sollen. Es stehen alle als ***config*** unter **Proxy > Proxyfilter > GRUPPE** definierten Gruppen zur Verfügung. Gibt es nur eine Filtergruppe, so geht es direkt mit den nachfolgenden Einstellungen weiter.
- Es stehen folgende Möglichkeiten der Konfiguration zur Verfügung:
  Domänen sperren: Eingabe der Domänen, welche vom Inhaltsfilter gesperrt werden sollen. Sollen IP-Adressen (IPv4 oder IPv6) gesperrt werden, so sind diese ebenfalls hier einzutragen.
  URLs sperren: Eingabe der URL, welche gesperrt werden soll. Es werden nur exakt die Seiten gesperrt, die hinterlegt werden. Diese Option ist zur Sperrung kompletter Domänen nicht geeignet.
  Domänen freischalten und **URLs freischalten**: Diese Einstellungen funktionieren analog zur Einstellung für die Sperrung von Domänen und definiert die Whiteliste für TightGate-Pro.
- Die Einstellungen müssen über den Menüpunkt **Anwenden** aktiviert werden.
- Sind die Einstellungen angewendet, so kann über den Menüpunkt **Benutzerverwaltung > Benutzer ändern > BENUTZER > Gefiltertes Web = Ja** die Proxy-Filterung für einzelne Kennungen angeschaltet werden. Über den Menüpunkt **Benutzerverwaltung > Benutzer ändern > BENUTZER > Proxy-Filter-Gruppe** kann einer Kennung die gewünschte Filtergruppe zugewiesen werden. Die Einstellungen zum **Gefilterten Web** und zur **Filtergruppe** werden bei der Benutzerkennung bei deren nächsten Anmeldung mit dem TightGate-Viewer aktiv.

Hinweis

Unter dem Menüpunkt **Webseiten-Filter**, kann man nicht das Wildcard-Symbol (*) nutzen, um alle Webseiten zu sperren. Verwenden Sie stattdessen **config > Proxy > Proxyfilter > GRUPPE > Nur Weißlisten**.

Inhaltsfilter für einzelne Benutzer umgehen

TightGate-Pro bietet die Möglichkeit, die Inhaltskontrolle für einzelne Benutzer zu umgehen. Der Inhaltsfilters für einzelne Benutzer oder Gruppen kann durch den Administrator ***maint*** unter dem

Menüpunkt **Benutzerverwaltung > Gefiltertes Web** ausgeschaltet werden.

Hinweis

Bei der Umstellung vom gefilterten zum ungefilterten Web (oder umgekehrt), muss sich die Kennung erneut an TightGate-Pro anmelden, damit die Einstellung aktiv wird. Ein Neustart des Browsers reicht nicht aus.

Protokollierung des Webzugriffs

TightGate-Pro bietet die Möglichkeit, Webzugriffe von Benutzern zu protokollieren. Zu Wahrung des Datenschutzes sind Anonymisierungs-, bzw. Pseudonymisierungs-Funktionen bei der Protokollierung bereits implementiert.

So geht's:

- Anmeldung als Administrator ***config.***
- Unter dem Menüpunkt **System-Vorgaben > Pseudomyisierung** ist festzulegen, ob die Protokollierung den Klarnamen der Benutzer enthält oder ob stattdessen Pseudonyme verwendet werden. Soll die Protokollierung in anonymisierter Form erfolgen, so ist hier keine Auswahl notwendig.
- Es ist unter dem Menüpunkt **Proxy > Protokollierung** die Protokollierung anzuschalten und festzulegen, ob ein anonymes oder mit Kennungen (Klarname oder Pseudonym) versehenes Proxy-Protokoll erstellt werden soll.
- Weiterhin ist zwingend notwendig, eine Lebensdauer für das Proxy-Protokoll festzulegen, da sonst die Protokollierung nicht aktiviert wird. Die Festlegung der Protokoll-Lebensdauer erfolgt über den Menüpunkt **Proxy > Protokoll-Lebensdauer** und wird in Tagen angegeben. Nach Ablauf der Speicherdauer werden die Protokolle gelöscht und können nicht rekonstruiert werden. Wird eine 0 eingetragen, findet keine Protokollierung statt.
- Die Einstellungen im Hauptmenü **Speichern** und **Anwenden**.