Proxy

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

Einstellungen für Uplink-Proxys

Menüpunkt	Beschreibung
HTTP-Proxy*	IPv4-Adresse(n) der HTTP-Proxy-Server, über die alle HTTP-Zugriffe in das Internet geleitet werden. Der verwendete Port muss für alle eingetragenen HTTP-Proxy-Server gleich sein und wird über eine gesonderte Menüoption festgelegt. Werden mehrere Server eingetragen, werden diese wahlweise per Rundlauf-Verfahren (Round Robin) oder in einer bestimmten Reihenfolge automatisch angesprochen. Dabei werden die Zugriffe nach Zugriffsgeschwindigkeit gewichtet, nicht erreichbare Server automatisch übersprungen. **Achtung:** In den meisten Fällen gibt es nur Server im Netzwerk, die mit expliziter IPv4-Adresse an dieser Stelle einzutragen sind. Für den Ausnahmefall, in dem hier auflösbare DNS-Namen referenziert werden, muss das betreffende Netzwerk im Menüpunkt HTTP-Proxy-Netz genau spezifiziert werden. Weiterhin muss ein DNS-Server eingetragen sein, der den Proxy-Namen auflösen kann. Andernfalls ist eine korrekte Verbindung zu den jeweiligen Proxyservern nicht möglich.
HTTP-Proxy-Reihenfolge*	Falls mehrere Proxy-Server eingetragen wurden, kann mit dieser Option das Auswahlverfahren festgelegt werden. Es steht das Rundlauf-Verfahren (Round-Robin) und die Ansprache nach bestimmter Reihenfolge zur Verfügung. **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-Proxy-Servern zu verwenden ist. Muss für alle referenzierten HTTP-Proxy-Server gleich sein.
HTTP-Proxy-Netz*	Falls ein auflösbarer DNS-Name als Proxyserver eingetragen wird, benötigt das System unbedingt die Information über die IPv4-Adressen, die sich dahinter verbergen. Die IPv4-Adresse ist 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 Proxy-Anmeldung eine Benutzerauthentifizierung mit Benutzername und Passwort erfordert, kann hier der Benutzername hinterlegt werden.
HTTP-Proxy-Passwort*	Sofern die Proxy-Anmeldung eine Benutzerauthentifizierung mit Benutzername und Passwort erfordert, 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.

Menüpunkt	Beschreibung
AD/Kerberos-Proxy-Anmeldung	Ja/Nein - aktiviert AD-Benutzerauthentisierung Proxy. Eine Anleitung zur Proxy-Authtentisierung per Active Directory gibt es hier
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 IPv4-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.
- Im letzten Schritt sind die jeweiligen Webfiltergruppen mit Kategorien zu versehen. Zur Auswahl stehen **3** Optionen:
  1) Alles verbieten und nur die Inhalte der Weißliste erlauben (erstellt als ***maint*** unter **Webseiten-Filter > Domänen freischalten** und **Webseiten-Filter > URLs freischalten**; Menüpunkt **Nur Weißlisten**).
  2) Alles erlauben und nur unerwünschte Inhalte per Kategorie zu verbieten (Menüpunkt **Kategorien (Sperrliste)**).
  3) Aufruf von Webseiten per IP-Adresse im Browser verbieten (Vorgabe verrboten). Ausnahme sind IPs, die in der Weißliste (Domäne freischalten) eingetragen sind.
- 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 sowie bei jedem Wechsel der **SquidGuard-Blacklist-URL**

ist in jedem Fall einen **Speichen** und **Anwenden** notwendig, bevor den einzelnen Filtergruppen Kategorien zugeordnet werden können. Nach jedem Wechsel der **SquidGuard-Blacklist-URL** ist immer auch eine Neuauswahl und neue Zuordnung der Kategorien notwendig.
Bei der Verwendung des Proxy-Filters in einen Cluster-System können bis zu 10 Minuten vergehen, ehe die Filtergruppen clusterweit verfügbar sind.

Konfiguration des Individuellen Webfilters

Neben der Verwendung der zentralen White- und Blacklisten lässt sich TightGate-Pro mit individuellen Einstellungen erweitern. So ist es möglich, individuell Domänen und URLs zu eigenen Black- und Whitelisten hinzuzufügen.

Das wird benötigt:
→ Aktivierter Proxy-Filter (Webfilter)
→ Zuordnung der Benutzer zum gefilterten Web

So geht's:

- Anmeldung als Administrator ***maint.***
- Auswahl des Menüpunkts **Webseiten-Filter**. Es stehen folgende Möglichkeiten der Konfiguration zur Verfügung:
  Domänen sperren: Eingabe der Domänen, welche vom Inhaltsfilter gesperrt werden sollen. Die Domäne kann dabei auch unter Zuhilfenahme von Wildcards (*) angegeben werden. Beispiel: Die Domäne von EBAY kann für alle Länder mit www.ebay.* komplett verboten werden.
  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.

Hinweis: Unter **Webseiten Filter**, kann man nicht mehr Wildcards (*) 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. Die Umgehung des Inhaltsfilters für einzelne Benutzer oder Gruppen wird durch den Administrator ***maint*** unter dem Menüpunkt **Benutzerverwaltung > Gefiltertes Web** eingerichtet.

Hinweis: Ist für einen Benutzer der ungefilterte Zugriff auf das Web eingestellt, so erfolgt für diesen Benutzer keinerlei Inhaltskontrolle. Bei der Umstellung eines Benutzers von gefiltertem zu ungefiltertem Web (oder umgekehrt), muss sich dieser 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.***
- Sofern die Protokollierung nicht in anonymisierter Form stattfinden soll, ist unter dem Menüpunkt **System-Vorgaben > Pseudomyisierung** festzulegen, ob die Protokollierung den Klarnamen der Benutzer enthält oder ob stattdessen Pseudonyme verwendet werden.
- Im nächsten Schritt 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 Protokoll-Dateien gelöscht und können nicht rekonstruiert werden. Wird eine 0 eingetragen, findet keine Protokollierung statt.
  Hinweis: Ist die Proxy-Protokollierung abgeschaltet, wird diese Menüoption nicht angezeigt.
- Die Einstellungen im Hauptmenü **Speichern** und **Anwenden**.