

TrutzBox® Kompendium

Teil 2: Funktionen und Architektur

Version 13.73 · Ausgabe November 2026

Autor: Hermann Sauer, Dipl.-Informatiker

Comidio GmbH · Eltville am Rhein · www.trutzbox.de

Rechtliche Hinweise

Sorgfalt und Gewähr. Dieses Kompendium wurde mit größter Sorgfalt erstellt. Für Vollständigkeit, Richtigkeit und Aktualität der Inhalte, insbesondere der Angaben zu Produkten, Diensten und Praktiken Dritter, übernehmen die Comidio GmbH und der Autor keine Gewähr. Alle Angaben geben den Kenntnisstand zum Redaktionsschluss (September 2026) wieder; Menüpfade, Bildschirmkopien und Standardwerte entsprechen dem Softwarestand zum Redaktionsschluss; spätere Versionen können abweichen. Unternehmen und Produkte können ihre Praktiken seither geändert haben.

Meinungen. Bewertungen und Einschätzungen geben die Auffassung des Autors wieder und sind als solche zu verstehen. Die rechtliche Bewertung einzelner Sachverhalte obliegt den zuständigen Behörden und Gerichten. Die Inhalte stellen keine Rechts- oder Sicherheitsberatung im Einzelfall dar.

Haftung. Comidio haftet uneingeschränkt für Vorsatz und grobe Fahrlässigkeit sowie nach den gesetzlichen Bestimmungen für Schäden aus der Verletzung von Leben, Körper oder Gesundheit; die Haftung nach dem Produkthaftungsgesetz bleibt unberührt. Bei einfach fahrlässiger Verletzung wesentlicher Vertragspflichten ist die Haftung auf den vorhersehbaren, vertragstypischen Schaden beschränkt; im Übrigen ist die Haftung ausgeschlossen.

Marken. TrutzBox® ist eine eingetragene Marke der Comidio GmbH. Alle weiteren genannten Marken, Firmen- und Produktnamen sind Eigentum ihrer jeweiligen Inhaber und werden ausschließlich beschreibend verwendet.

Nutzung für Dritte. Wer den Datenverkehr Dritter (etwa von Mitarbeitern, Bewohnern, Patienten oder Gästen) filtert oder einsehbar macht, benötigt dafür eine Rechtsgrundlage, in der Regel die informierte Einwilligung der Betroffenen oder eine entsprechende dienstliche bzw. vertragliche Regelung; das Fernmeldegeheimnis und die Mitbestimmungsrechte sind zu beachten. Die Verantwortung hierfür liegt beim Betreiber der TrutzBox.

Urheberrecht. © Comidio GmbH 2026. Alle Rechte vorbehalten. Abbildungen Dritter sind mit Quellenangabe wiedergegeben; die Rechte verbleiben bei den Urhebern. Vervielfältigung und Weitergabe nur mit Zustimmung der Comidio GmbH.

Impressum. Comidio GmbH, Eichendorffweg 2, 65343 Eltville. Vertreten durch: Hermann Sauer, Geschäftsführer. Registergericht: Amtsgericht Wiesbaden, Handelsregister B, Registernummer 27951. Umsatzsteuer-Identifikationsnummer gemäß § 27a UStG: DE296578929. Verantwortlich im Sinne von § 18 Abs. 2 MStV: Hermann Sauer, Eichendorffweg 2, 65343 Eltville. Kontakt: Telefon +49 6123 9748802, E-Mail info@comidio.de, Web www.trutzbox.de und www.comidio.de.

Inhaltsverzeichnis

1 Comidio TrutzBox Funktionen und Architektur....8
2 TrutzBox Setup....12
2.1 Schritt 1: Verkabelung....12
2.2 Schritt 2: TrutzBox Setup....13
2.3 Schritt 3: Benutzer-Geräte an der TrutzBox anschließen....15
Möglichkeit 1: Internet-Gerät wird an TrutzBox Netzwerk angeschlossen (Transparent-Modus)....16
Möglichkeit 2: Internet-Gerät bleibt am angeschlossenen Internet-Router angeschlossen (Proxy-Modus)....17
Möglichkeit 3: Internet-Gerät per VPN (Fernverbindung) mit der TrutzBox verbinden....18
3 TrutzBox-Dashboard....19
4 Monitor....21
4.1 Eingebaute Hilfe: geführte Touren....22
4.2 Die Steuerleiste: Zeitraum, Darstellung, Verbindungstypen und Gruppierung....24
Anzeigezeitraum: welcher Ausschnitt zu sehen ist....25
Speicherdauer: wie weit zurück überhaupt Daten vorliegen....25
Darstellungen: vier Sichten auf dieselben Daten....25
Verbindungstypen: welche Zeilen und Linien erscheinen....26
Gruppierungen: aus vielen Servern wenige Einträge....27
Weitere Schalter der Kopfleiste....27
4.3 Voreinstellungen beim ersten Aufruf....29
4.4 Vier Darstellungen....29
Liste....30
Verbindungen....31
Datendurchsatz....34
Blasendiagramm....35
4.5 Warum wurde geblockt? Drilldown auf eine Verbindung....36
4.6 Wie der Monitor die Daten vorhält....38
4.7 Server gruppieren: von Anbieter bis Protokoll/Port....39
4.8 Sperren und Freischalten direkt aus dem Monitor....44
5 Geräte....47
5.1 Geräte-Übersicht....47
5.2 Geräte-Detaileinstellungen....49
Diese Ausnahmen zulassen....51
Nur Ausnahmen erlauben....52
Gerätetyp festlegen....52
Standardposition Slider....52
Tor-Netzwerk verwenden....52
Was genau ist der Unterschied, wenn TrutzBrowse ein- oder ausgeschaltet ist?....53
TrutzBurg-Symbol anzeigen....53
6 Benutzer....54
6.1 Arten von Benutzer-Accounts....54
6.2 Benutzer-Übersicht....54
6.3 Benutzer hinzufügen....55
6.4 Detail-Einstellungen eines Benutzers....56
7 TrutzBox-Proxy: Funktion und interner Aufbau....58

7.1 TrutzContent und TrutzBrowse: neben der Firewall zwei weitere Schutzebenen....60
7.2 TrutzBox-Proxy: interner Aufbau....61
8 TrutzContent....62
8.1 Filtergruppen....64
8.2 Filterlisten....65
TrutzBox Filterlisten....66
Filterlisten aus dem Internet importieren (automatische Aktualisierung)....68
Drei Standard TrutzBox Filterlisten....69
8.3 Eigene Sperren und Ausnahmen....70
8.4 Was der Anwender bei einer gesperrten Seite sieht....71
9 TrutzBrowse....73
9.1 TrutzBrowse: verräterische Daten aus der Internet-Kommunikation herausfiltern....73
Woran man TrutzBrowse im Monitor erkennt....73
HTTP-Header korrigieren....74
9.2 TrutzBrowse: die zusätzliche Tiefenfilterung....75
TrutzBrowse: Vorteile....75
TrutzBrowse: Nachteile....75
9.3 Slider-Positionen....76
Intelligenter SecuritySlider....77
Der SecuritySlider gilt auch für alle TrutzBrowse Folgeaufrufe....80
Verschiedene Blockinglisten für TrutzBrowse und TrutzContent....81
9.4 TrutzBrowse-Blacklists....82
9.5 TrutzBurg-Symbol im Browser....82
9.6 Die Spalte „TrutzBrowse“ in der Liste des Monitors....84
9.7 TrutzBrowse HTTP-Header-Filter....84
9.8 Verschlüsselte (SSL/TLS)-Verbindungen....88
Was muss auf Client- bzw. auf Geräte-Seite sichergestellt werden, damit die TrutzBox verschlüsselten Datenverkehr analysieren kann (TrutzBrowse)?....90
9.9 Die optimale TrutzBrowse- und TrutzContent-Einstellung....92
9.10 Kann die TrutzBox auch zu viel filtern?....93
9.11 Vergleich auf einen Blick....95
10 Statistiken....97
11 Allgemeine Einstellungen....100
12 E-Mail (TrutzMail)....103
12.1 Austausch von sicheren E-Mails über die TrutzBox....106
12.2 Maximalgröße einer TrutzMail....107
12.3 Technische TrutzMail Implementierung....108
E-Mails senden....110
E-Mails empfangen....110
12.4 Austausch von E-Mails mit (Standard) Mail-Servern (mit jemandem, der keine TrutzBox besitzt)....111
Öffentlichen Schlüssel eines Empfängers hinterlegen....111
Empfangen von Standard-E-Mails....113
Senden von PGP-verschlüsselten E-Mails an Standard-E-Mail-Accounts....113
12.5 Austausch von sicheren TrutzMails zwischen TrutzBoxen....115
12.6 Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen....116
Was passiert, wenn der Empfänger seinen Schlüssel gewechselt hat?....116
12.7 Mail-Austausch über die TrutzBox: Zusammenfassung....117
12.8 Neue TrutzMail-Adresse registrieren....118
12.9 TrutzMail-Zertifikat Updates....119

12.10 TrutzMail-Adressen löschen und wiederverwenden....120
12.11 TrutzMail Ein- und Ausgang kontrollieren....120
12.12 Schlüsselverwaltung....122
TrutzMail-Schlüssel Detail-Ansicht....124
12.13 Mail-Programme einrichten....125
13 TrutzDynDNS: Erreichbarkeit aus dem Internet....127
13.1 Wozu TrutzDynDNS dient....127
13.2 Der Name und seine Vergabe....127
13.3 Wie die TrutzBox ihre Adressen meldet....128
13.4 Der Weg zum Server von Comidio....128
13.5 Welche Anschlüsse von außen erreichbar sind....129
13.6 Prüfung der Erreichbarkeit von außen....129
13.7 Nur IPv6 oder nur IPv4 veröffentlichen....130
13.8 Zertifikat für den TrutzDynDNS-Namen....131
13.9 Eigener Name neben TrutzDynDNS....131
13.10 Was Comidio speichert und protokolliert....133
14 Videokonferenz und Chat (TrutzRTC)....134
14.1 Videokonferenz einrichten und starten....135
14.2 TrutzRTC: Messaging/Chat-Verbindungen (XMPP-Server)....136
Die Karteikarte „TrutzChat“....136
TrutzChat im Browser....140
Externe Verbindungen zu TrutzRTC....145
Einrichtung und Nutzung von Chat-Räumen....145
Sicherheit und Anonymität bei der Nutzung des XMPP-Servers....146
14.3 TrutzRTC Videokonferenz Server....147
Sicherheit und Anonymität bei der Nutzung des Videokonferenz-Servers....150
Leistungsgrenzen des Konferenz-Servers....150
Externe Verbindungen zum TrutzRTC-Konferenz-Server....151
Telefonverbindung von und zum Videokonferenzserver....152
Interne TrutzRTC Architektur....152
15 Mehrschichtiger Netzwerk-Schutz (TrutzBase)....154
15.1 Drei Methoden, Netzwerk-Verkehr zu erkennen und zu blockieren....155
DNS-Blockierung (am Nameserver)....156
IP-Blockierung (im Netzwerk)....156
Proxy- bzw. URL-Filterung (im Anwendungsprotokoll)....156
Warum die TrutzBox kombiniert....157
16 Netzwerk....158
16.1 Das TrutzBox externe (unsichere) Netzwerk....158
16.2 Das TrutzBox interne (sichere) Netzwerk....159
Die TrutzBox im Netz finden: trutzbox.local (mDNS)....161
16.3 Status (Netzwerk)....161
Erreichbarkeit von außen....163
16.4 Firewall....164
16.5 IP-Blocklisten-Verwaltung....167
16.6 Firewall-Ausnahmen....169
16.7 Blockierte IP-Adressen....169
16.8 Angriffsschutz....170
Wie Erkennung und Sperre intern zusammenspielen....174
16.9 Verkehr ohne sichtbaren Domain-Namen....176

16.10 Firewall-Monitor....176
Blockierte Verbindungen im Detail....178
16.11 DNS-Auflösung....179
16.12 Zeitserver....183
16.13 WLAN....185
Funkeinstellungen....186
5-GHz-Kanäle und Funkregulierung....186
Verbundene WLAN-Geräte....186
Zeit-Steuerung....187
Andere WLANs in der Umgebung....187
16.14 Fernzugriff: VPN (Virtual Private Network)....187
TrutzBox auf Fernzugriff vorbereiten und Internet-Router freischalten....189
Die Fernzugriff-Seite im Detail....190
Zweiter Tunnel: WireGuard....193
Sonderfall: VPN aus dem eigenen Netz heraus....196
Mobiles Gerät für den Fernzugriff vorbereiten....197
IPv6 Unterstützung....197
16.15 Portübersicht: was der Internet-Router durchlassen muss....201
17 Systemeinstellungen....204
17.1 TrutzBox-Betriebszustand....204
Zustand der Box....205
TrutzBox-Funktionen....206
Internet-Anschluss: der stille Wächter....208
DNS für Geräte: die zweite stille Karte....209
Systemgrenzen: stille Engpässe früh erkennen....210
Verlauf der letzten 30 Tage....212
Ereignis-Protokoll....213
17.2 Vertrag und Pakete....213
17.3 Rechtliche Hinweise....215
17.4 System-Logs....216
Proxy debuggen....217
Systemmails....218
17.5 Webmin....218
Über Webmin den Systemstatus der TrutzBox auf den eigenen PC laden....221
TrutzBox mit Hilfe von Webmin auf Werkseinstellung zurücksetzen....221
17.6 Die Kommandozeile: Terminal und SSH....221
Anmeldung an der Kommandozeile (SSH)....221
Terminal im Browser....222
18 Aktualität und Pflege der TrutzBox....223
18.1 Drei Arten von Updates im Überblick....223
18.2 Voraussetzung: gültiger TrutzServices-Vertrag....224
18.3 Software-Paket-Updates....224
Comidio-eigene Pakete....224
Debian-System-Pakete....224
Updates beim TrutzBox-Setup....224
Automatische tägliche Auslieferung im Betrieb....225
Aktuelle Paketübersicht für den Administrator....225
18.4 Filter- und Sperrlisten-Updates....226
TrutzContent- und TrutzBrowse-Filterlisten....226
TrutzMail-Adress-Blacklist....226

TrutzMail-Zertifikat-Updates....226
IP-Blocklisten....226
18.5 Komplette TrutzBox-Image-Updates....227
Zwei Wege zum neuen Image....227
18.6 Sichere Voreinstellungen....227
18.7 Schwachstellen melden....228
18.8 Was der Anwender tun (bzw. nicht tun) muss....228
19 TrutzBox Betriebssystem....229
20 TrutzBox zurücksetzen....231
20.1 TrutzMail-Adressen bleiben reserviert nach Zurücksetzen der TrutzBox....236
20.2 Was vor einem Besitzerwechsel zu tun ist....237
21 TrutzBox Hardware....239
21.1 LED-Anzeigen an der Gerätefront....241
21.2 Austausch der Hardware....242
22 Anhang: Zertifikate und Schlüssel....243
23 Anhang: Comidio BSS/OSS und TrutzLegitimation....247
23.1 TrutzServices....247
23.2 Die TrutzLegitimation aus Anwendungssicht....248
23.3 Die TrutzLegitimation aus System-Sicht....250
24 Index....251

1 Comidio TrutzBox Funktionen und Architektur

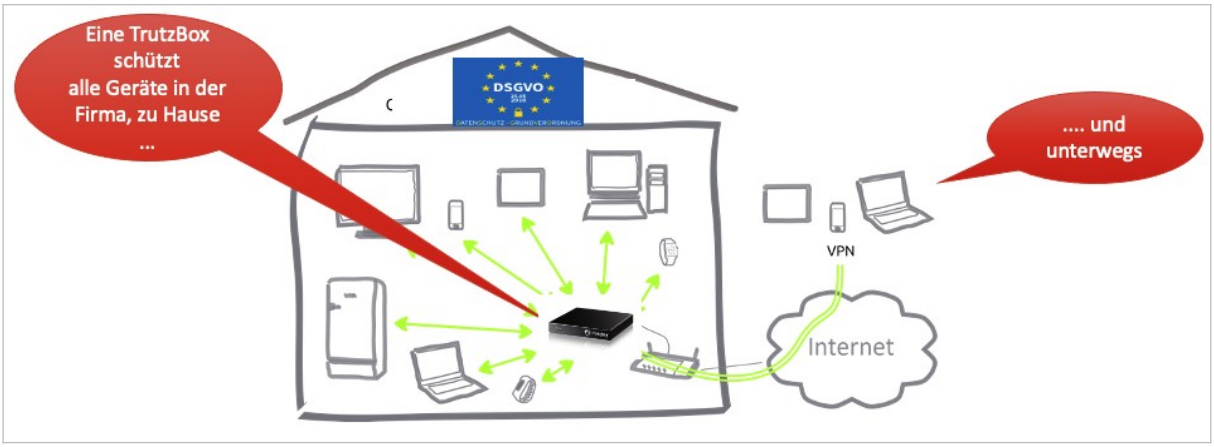
Dieses Dokument, Teil 2 des TrutzBox-Kompendiums, beschreibt die Funktionsweise und interne Implementierung der Comidio TrutzBox. Der Aufbau folgt dem Menübaum der TrutzBox-Bedienoberfläche: Jeder Screen wird einzeln vorgestellt, und seine Bedienung sowie technische Umsetzung werden erläutert.
Zielgruppe sind TrutzBox-Administratoren, Integratoren und technisch interessierte Anwender, die die internen Abläufe der TrutzBox nachvollziehen möchten. Eine allgemeine Einführung in Konzept, Zielsetzung und Nutzen der TrutzBox findet sich in Teil 1 des Kompendiums sowie im TrutzBox-Handbuch.
Das Dokument folgt dem Aufbau der TrutzBox-Bedienoberfläche und gliedert sich in folgende Bereiche:

- **Inbetriebnahme (Setup):** Verkabelung, Ersteinrichtung und Anschluss der Geräte.
- **TrutzBox-Dashboard:** die Startseite mit dem Überblick.
- **Monitor:** die Live-Sicht auf den Netzwerkverkehr aller Geräte.
- **Geräte und Benutzer:** Verwaltung und Einstellungen je Gerät und Konto.
- **TrutzBox-Proxy:** der Anonymisierungs-Proxy mit TrutzContent und TrutzBrowse.
- **Statistiken und Allgemeine Einstellungen:** Auswertungen und Grundeinstellungen der Box.
- **E-Mail (TrutzMail):** sichere E-Mail zwischen TrutzBoxen und zu Standard-Postfächern.
- **Videokonferenz und Chat (TrutzRTC):** TrutzMeeting und TrutzChat.
- **Mehrschichtiger Netzwerk-Schutz (TrutzBase):** die drei Filtermethoden im Zusammenspiel.
- **Netzwerk:** Firewall, Angriffsschutz, DNS-Auflösung, Zeitserver, WLAN und Fernzugriff per VPN.
- **Systemeinstellungen:** Betriebszustand, Vertrag und Pakete, System-Logs, Terminal und Webmin.
- **Aktualität und Pflege:** Updates von Software, Filterlisten und Image.
- **Betriebssystem, Zurücksetzen und Hardware:** Debian-Basis, Werksreset und Hardware.
- **Anhänge:** Zertifikate und Schlüssel sowie die Comidio BSS/OSS-Architektur mit der TrutzLegitimation.

Die TrutzBox ist ein Werkzeug zur „Digitalen Selbstverteidigung“. Mit Hilfe der TrutzBox können digitale Angriffe erschwert und es kann vermieden werden, dass unnötig Daten herausgegeben werden, die für den Betrieb nicht notwendig sind. Die TrutzBox ist eine Hardware/Software-Kombination, die in das interne Netzwerk eines Haushalts oder einer Firma installiert wird und die alle Geräte schützt, die

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Zugriff auf das Internet haben. Auf diesen zu schützenden Geräten muss keine zusätzliche Software installiert werden. Die TrutzBox kann auch sicher von unterwegs genutzt werden.



Eine TrutzBox schützt alle Geräte zu Hause, in der Firma und unterwegs.
(© 2026 Comidio GmbH)

Dadurch gibt die TrutzBox die Kontrolle über die Daten an den Benutzer zurück.
Sie bietet folgende Sicherheits- und Anonymisierungsvorteile:

- **Kontrolle über alle Internet-Zugriffe:** TrutzContent entscheidet für jedes Gerät im Netzwerk, welche Server kontaktiert werden dürfen.
- **Anonymisierung:** TrutzBrowse entfernt verräterische Daten aus der Internet-Kommunikation auf Geräten, auf denen das TrutzBox-Stammzertifikat importiert wurde.
- **Zugriffskontrolle pro Gerät oder Benutzer (TrutzContent):** flexible Filtergruppen legen fest, welche Server kontaktiert werden dürfen, nützlich u. a. als Inhaltsfilter für Kinder und Jugendliche, zum Schutz vor Kostenfallen (z. B. in Seniorenheimen), Einschränkung von IoT-Geräten (Kamera, Fernseher, Heizung) sowie Kontrolle der Telemetrie von Smartphones und Betriebssystemen.
- **Eigenhosting:** Der Nutzer ist nicht mehr auf Dienstleister im Internet angewiesen, die ihm nicht die erforderliche Sicherheit und Anonymität bieten.
- **Verschlüsselte E-Mail (TrutzMail):** E-Mails sind bei der Übertragung zwischen TrutzBoxen gegen Mitlesen und Manipulation geschützt; die Absender-Adresse wird innerhalb des TrutzMail-Verbunds verifiziert.
- **Videokonferenz und Chat (TrutzRTC):** TrutzMeeting und TrutzChat laufen auf der eigenen Box. Der Nutzer ist nicht auf zentrale Cloud-Dienste angewiesen, bei denen Meta- und Nutzungsdaten beim Anbieter verarbeitet werden.
- **Netzwerk-Schutz (TrutzBase):** Firewall und Angriffserkennung schützen das lokale Netzwerk vor Einbrechern.

- **Transparenz (Monitor):** Für jedes Gerät wird sichtbar, mit wem es im Internet kommuniziert.

Somit kann der Internet-Nutzer mit Hilfe der TrutzBox kontrollieren, welche Daten er wem geben möchte. Ein wesentliches Merkmal der TrutzBox ist, dass der Benutzer ihre Funktionen mit allen seinen internetfähigen Geräten zu Hause oder in seinem Unternehmen nutzen kann. So können nicht nur PC, Mac und mobile Geräte wie iPhone, iPad oder Android-Geräte, sondern auch Fernseher sowie vorhandene oder zukünftige „Smart Home"-Geräte wie Heizung, Zahnbürste oder Fitness-Armband kontrolliert und geschützt werden.
Bei der Architektur der TrutzBox wurden viele der bisher hier erwähnten Bedrohungen und Abwehrmöglichkeiten berücksichtigt. Es wird jedoch nie möglich sein, sich gegen alle dieser Bedrohungen vollständig zu schützen. Hundertprozentige Sicherheit gibt es nicht, auch nicht mit der TrutzBox. In der Praxis muss immer ein Kompromiss zwischen diesen vier Anforderungen gefunden werden:

- **Marktreife:** man kann endlos den Bedrohungen hinterherlaufen und Zug um Zug Lösungen in das Produkt einbauen. Aber die Lösung kommt nie auf den Markt,
- dem Grad des Schutzes,
- den Kosten für Entwicklung und Betrieb (somit auch der Preis, den der Kunde zu zahlen hat) und
- der Bedienbarkeit für den Anwender.

Die TrutzBox ist ein Kompromiss zwischen diesen vier Anforderungen.
Die folgenden Kapitel beschreiben die TrutzBox Funktionen und ihre technische Umsetzung.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2



Die TrutzBox als Hardware: ein lüfterloses Gerät für den Dauerbetrieb.
(© 2026 Comidio GmbH)

2 TrutzBox Setup

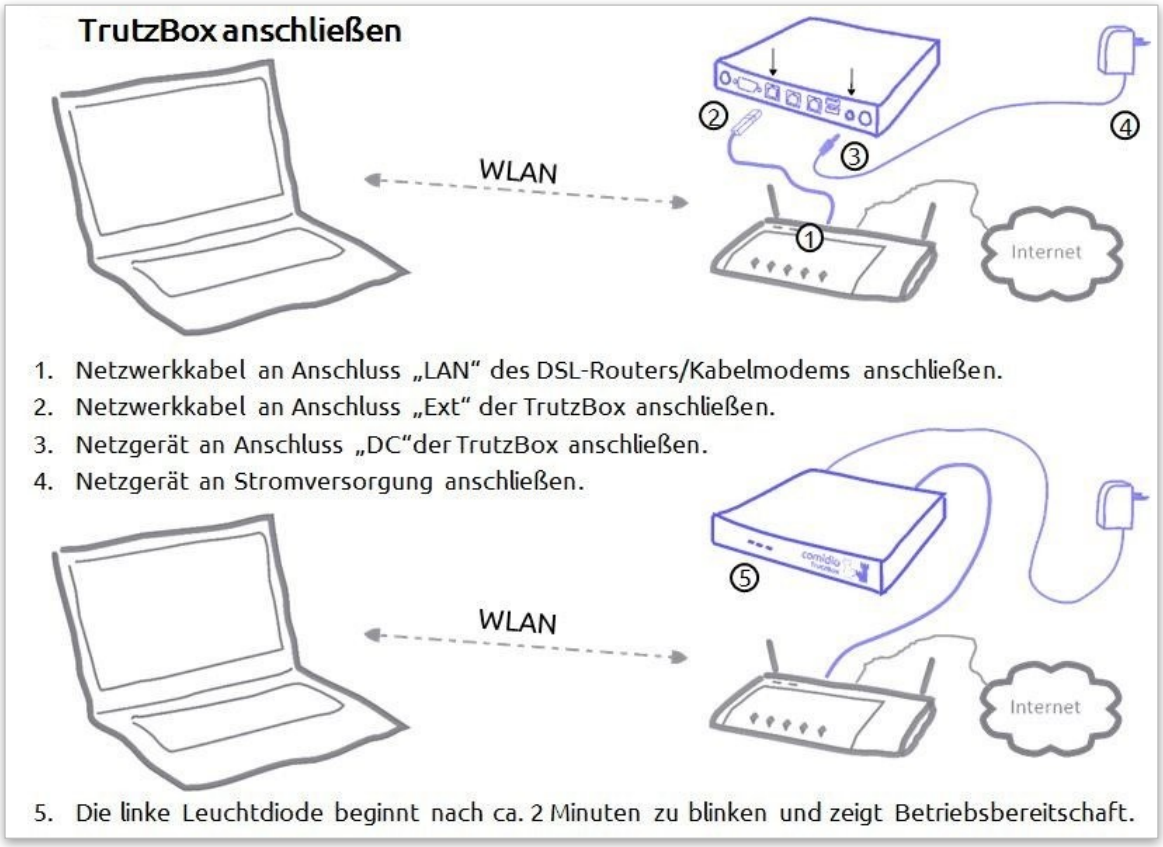
Die TrutzBox ist so ausgelegt, dass sie ohne spezielle technische Kenntnisse in Betrieb genommen werden kann. Aus diesem Grund wurde bei der Architektur der TrutzBox sehr viel Wert auf eine einfache Setup-Funktion gelegt. Da die TrutzBox speziellen Sicherheitskriterien genügen muss, ist es leider nicht möglich, die TrutzBox nur durch einfaches Verkabeln in Betrieb zu nehmen. Die Inbetriebnahme besteht aus drei Schritten:

2.1 Schritt 1: Verkabelung

Die Verkabelung ist recht einfach, da die TrutzBox lediglich mit einem mitgelieferten LAN-Kabel an den Internet-Router angeschlossen werden muss.
Nach dem Anstecken des Stromkabels zeigt die linke LED an der Gerätefront den Startfortschritt:

- **Dauerleuchten:** Die TrutzBox bootet.
- **Langsames, gleichmäßiges Blinken:** Das Betriebssystem läuft, die Bedienoberfläche startet noch. Beim allerersten Start und nach Updates kann diese Phase mehrere Minuten dauern.
- **Schnelles Blinken im Herzschlag-Rhythmus (Doppelpuls):** Die Bedienoberfläche antwortet, die TrutzBox ist bereit, es kann mit Schritt 2 weitergehen. Im laufenden Betrieb blinkt die LED dauerhaft in diesem Rhythmus und zeigt so, dass die Box arbeitet; dunkel wird sie im Betrieb nie.
- **Dauerhaft langsames Blinken:** Die Bedienoberfläche konnte nicht starten.

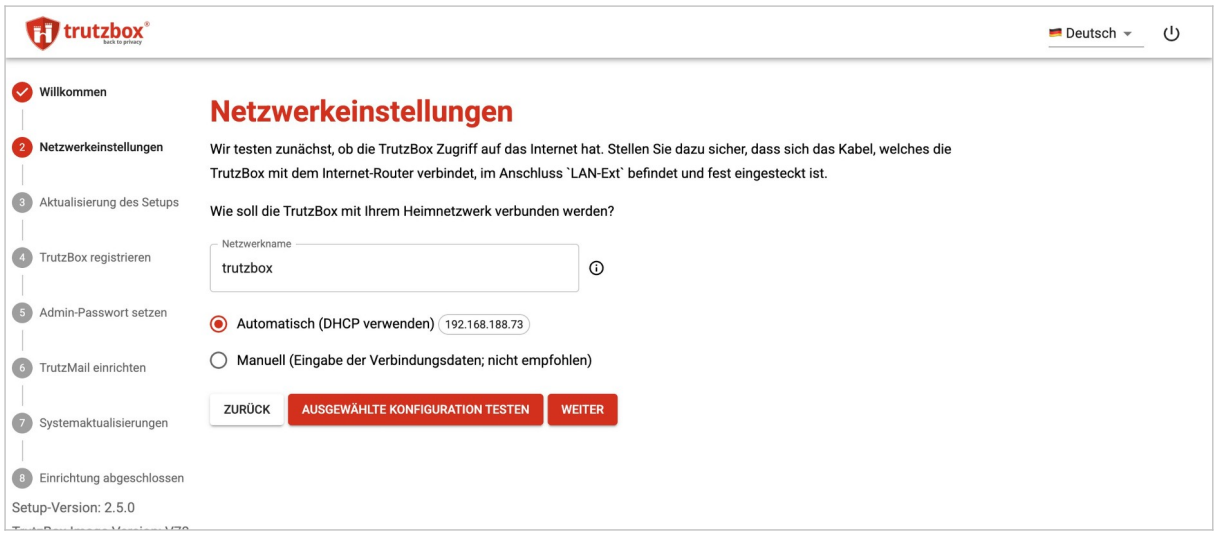
Auf dem NanoPi R5C zeigt die rote Leuchtdiode dieselben drei Stufen. Die ganze Abfolge für APU2 und NanoPi R5C vom Einschalten bis zum Setup steht als Tabelle im Abschnitt „Was die Leuchtdioden während des Zurücksetzens anzeigen“.



TrutzBox anschließen: Kabel zum Internet-Router, Kabel ins eigene Netz, Netzteil; nach etwa zwei Minuten meldet die linke Leuchtdiode die Betriebsbereitschaft.
(© 2026 Comidio GmbH)

2.2 Schritt 2: TrutzBox Setup

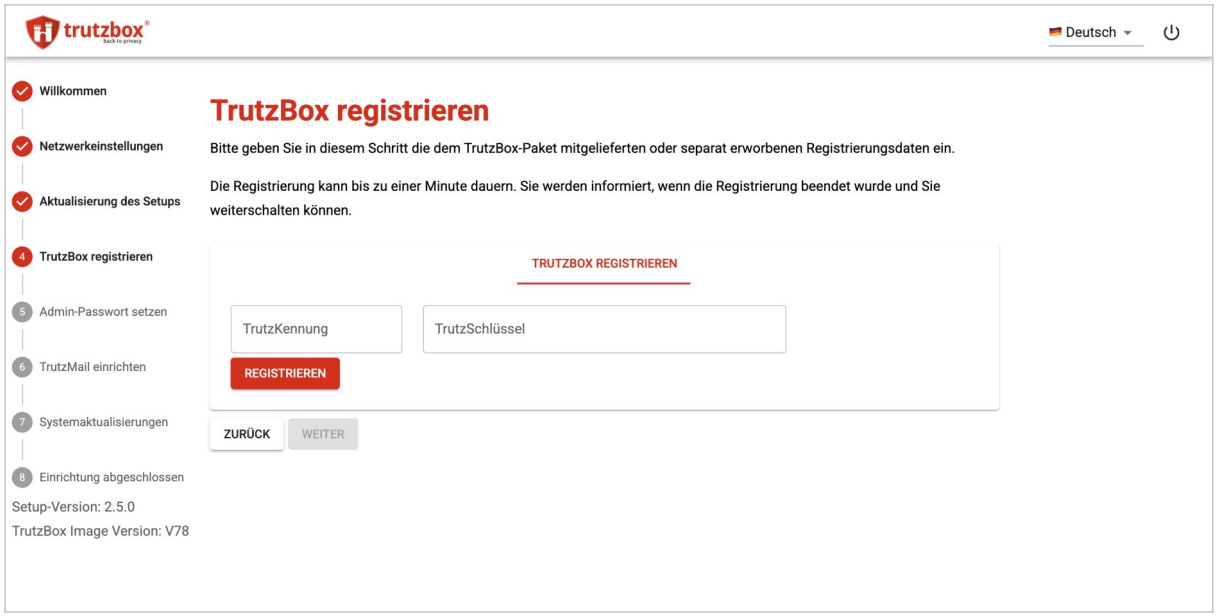
Die Einrichtung der TrutzBox (Setup) kann nun über einen PC ausgeführt werden, der am Internet-Router angeschlossen sein muss. Dazu wird am PC ein Browser gestartet. Durch die Eingabe des Links http://trutzbox/ gelangt man in das Setup-Menü der TrutzBox. Kennt der Internet-Router diesen Namen nicht, führt http://trutzbox.local/ ebenfalls dorthin (Abschnitt „Die TrutzBox im Netz finden: trutzbox.local (mDNS)“).
Nach kurzem Begrüßungstext und Bestätigung der Lizenzbedingungen, prüft die TrutzBox, ob es mittlerweile ein neues Setup-Programm gibt. Wenn ja, wird das neue Setup-Programm automatisch geladen.
Danach prüft die TrutzBox, ob sie Zugriff auf das Internet hat. Hier kann auch eingestellt werden, ob die TrutzBox die IP-Adresse automatisch bezieht (DHCP) oder man eine eigene feste IP-Adresse einstellen möchte (eine feste IP-Adresse wird nicht empfohlen).



Setup-Schritt 2: Die TrutzBox prüft die Internet-Verbindung und lässt die Adressvergabe wählen. (© 2026 Comidio GmbH)

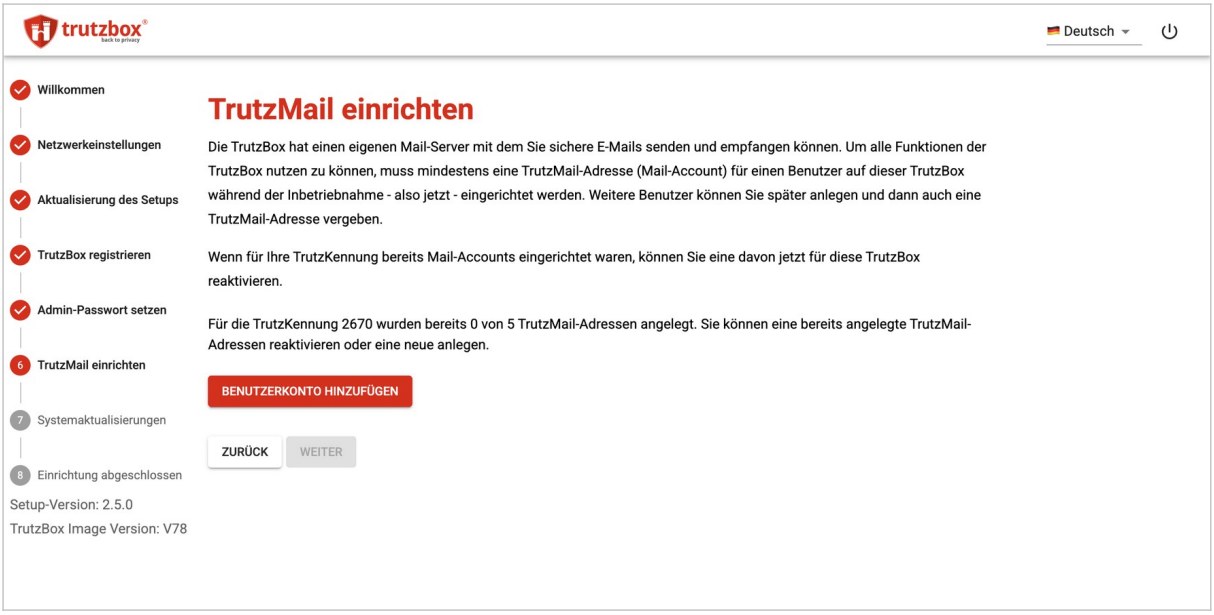
Falls der Internet-Zugriff misslingt, sollte die Verkabelung oder Netzwerk-Einstellung des Internet-Routers überprüft werden.

Als nächstes muss die TrutzBox registriert werden. Dazu muss die mitgelieferte TrutzLegitimation eingegeben werden.



Setup-Schritt 2: Eingabe der mitgelieferten TrutzLegitimation zur Registrierung der Box.(© 2026 Comidio GmbH)

Nach dem Setzen eines Admin-Passworts, wird mindestens ein TrutzMail-Account auf der TrutzBox eingerichtet. Dazu kann man einen zuvor registrierten TrutzMail-Account reaktivieren, oder einen neuen TrutzMail-Account anlegen.



Setup-Schritt 2: Anlegen oder Reaktivieren einer TrutzMail-Adresse.
(© 2026 Comidio GmbH)

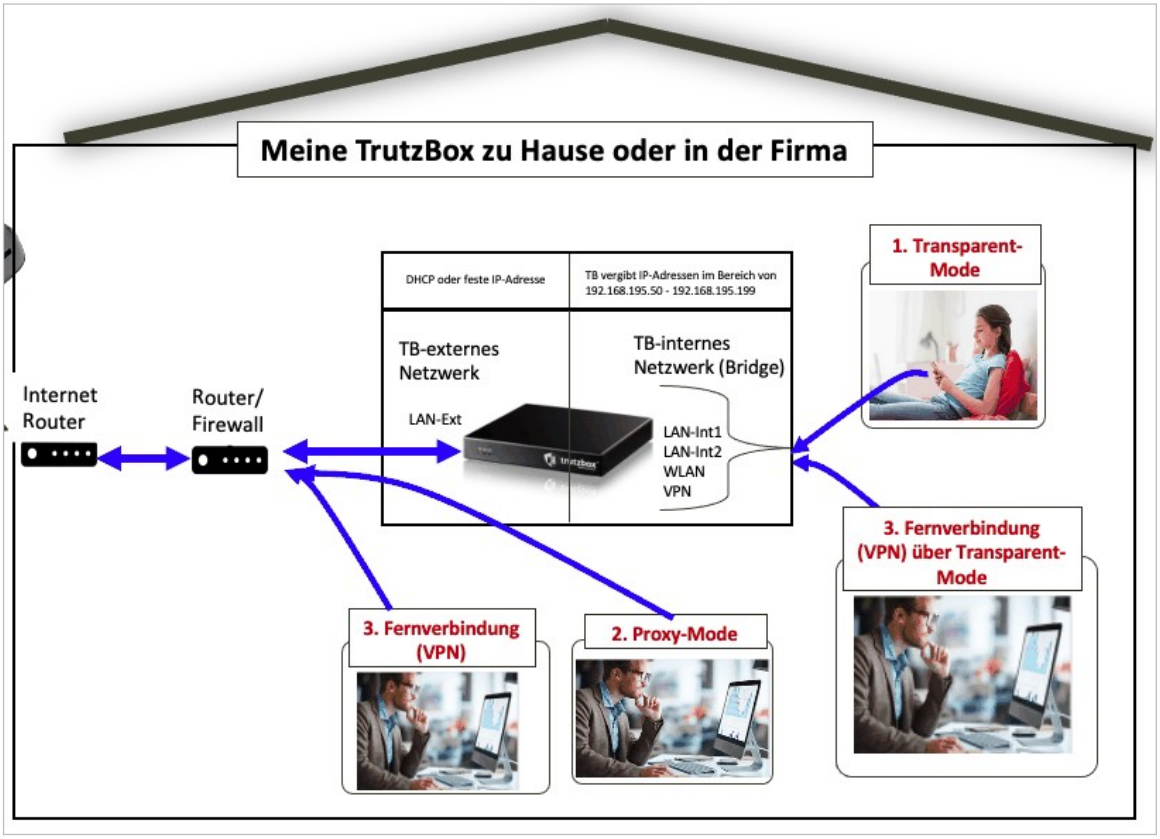
Nachdem das Setup noch Updates der TrutzBox eingespielt hat, ist das Setup abgeschlossen.

Mit erneutem Aufruf von http://trutzbox/ kann nun die Administrator-Oberfläche der TrutzBox aufgerufen werden. In seltenen Fällen ist es notwendig, den Browser-Cache zuvor zu löschen.

2.3 Schritt 3: Benutzer-Geräte an der TrutzBox anschließen

Es gibt drei Möglichkeiten, ein Gerät (z. B. PC, mobiles Gerät, Fernseher ...) an die TrutzBox anzuschließen:

- im Transparent-Modus. Dabei wird das Gerät direkt an das interne Netzwerk der TrutzBox angeschlossen. Das kann per LAN-Anschluss (RJ45) oder mit dem optional erhältlichen WLAN-Modul geschehen
- über einen Proxy-Eintrag im Browser des Geräts oder in den Netzwerk-Einstellungen des Geräts
- Oder über eine VPN-Verbindung zur TrutzBox. Diese Möglichkeit empfehlen wir vor allem für mobile Geräte (Smartphone oder Laptop), da dann die TrutzBox auch unterwegs genutzt werden kann..



Die drei Wege, ein Gerät mit der TrutzBox zu verbinden: Transparent-Modus, Proxy-Modus und Fernverbindung über VPN.
(© 2026 Comidio GmbH)

Für jedes Gerät kann individuell entschieden werden, über welche Anschlussmöglichkeiten das Gerät die TrutzBrowse und TrutzContent Funktionen der TrutzBox nutzen soll. Um erste Erfahrungen mit der TrutzBox zu sammeln empfiehlt Comidio zunächst nur ein Gerät an die TrutzBox anzuschließen.

Möglichkeit 1: Internet-Gerät wird an TrutzBox Netzwerk angeschlossen (Transparent-Modus)

Bei Nutzung des Inhaltsfilters für Kinder und Jugendliche sollte man die zu schützenden Geräte im Transparent-Modus anschließen, da es in den anderen Anschluss-Alternativen mit etwas technischem Know-how möglich ist, die Konfiguration im Endgerät wieder zu ändern und so den Filter zu umgehen. Die TrutzBox ist kein anerkanntes Jugendschutzprogramm im Sinne des JMStV und ersetzt keine Aufsicht.
Um Geräte im Transparent-Modus an die TrutzBox anzuschließen, werden die Geräte netzwerkmäßig direkt per WLAN (optional bestellbar) oder LAN-Kabel an der TrutzBox angeschlossen. In diesem Fall sollte kein Proxy in dem Endgerät konfiguriert sein. Es müssen in diesem Fall keine Einstellungen auf dem Endgerät vorgenommen werden. Da in diesem Betriebs-Modus die gesamte Datenkommunikation über die TrutzBox geleitet wird, ist weder der Benutzer noch eine Applikation in der Lage, sich der Kontrolle der TrutzBox zu entziehen.

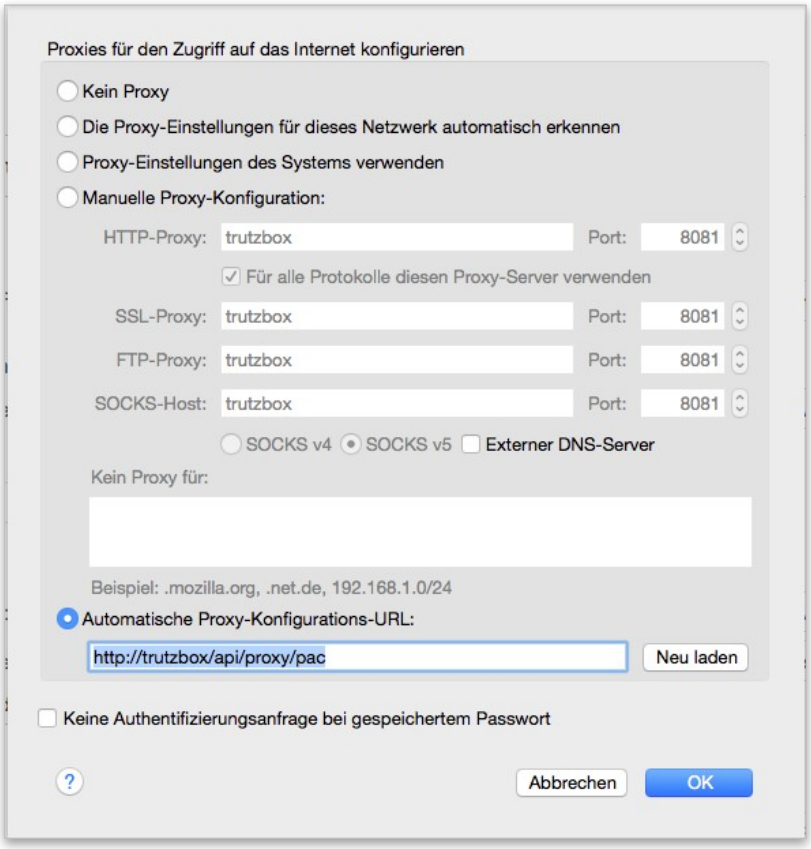
Beim Anschluss per LAN-Kabel wird einer der beiden freien LAN-Int-Anschlüsse (LAN-Intern) an der TrutzBox genutzt. Sollen mehr als zwei Geräte per LAN-Kabel angeschlossen werden, können die Anschlüsse durch einen zusätzlichen Hub, Switch oder Router erweitert werden (nicht im Lieferumfang enthalten).
Geräte, die direkt per Netzwerk an die TrutzBox angeschlossen sind, werden im TrutzBox-Administrator-Menü mit der Endung .sec aufgeführt.
Sollen alle Ihre Geräte die TrutzBox nutzen, könnte das WLAN des Internet-Routers sogar abgeschaltet werden.
Für den Anschluss von IoT-Geräten, also Geräten wie Fernseher, Überwachungskamera usw., bei denen man weder einen Proxy einstellen, noch einen VPN-Client installieren kann, ist der Transparent-Modus (Möglichkeit 1) die einzige Möglichkeit, den Datenverkehr über die TrutzBox zu leiten.

Möglichkeit 2: Internet-Gerät bleibt am angeschlossenen Internet-Router angeschlossen (Proxy-Modus)

Wir empfehlen zunächst nichts am vorhandenen internen Netzwerk zu ändern und erste Erfahrungen mit dieser Konfiguration für einen PC zu sammeln. Damit der Netzwerk-Verkehr per Proxy-Eintrag über die TrutzBox geleitet wird, gibt es zwei Wege zu unterscheiden:

- in Firefox die TrutzBox als Proxy eintragen. Der Firefox-Browser kann eine eigene Proxy-Konfiguration verwenden, die unabhängig von den Systemeinstellungen gilt. Wenn man im Firefox-Browser die TrutzBox als Proxy einträgt, dann geht nur der Firefox-Browser über die TrutzBox. Andere Programme gehen weiter ungehindert ins Internet. Diese Möglichkeit bietet unter den verbreiteten Browsern vor allem der Firefox-Browser
- **in den Netzwerk-Einstellungen des Endgeräts die TrutzBox als Proxy eintragen**. Dann geht der gesamte Netzwerk-Verkehr, der über dieses Netzwerk läuft durch die TrutzBox. Das entspricht so ziemlich dem Transparent-Modus. Das geht bei allen Betriebssystemen, inkl. iOS, macOS, Linux, Windows, Android und auch bei vielen, aber nicht allen IoT-Geräten (Fernseher, Video-Überwachungskamera, Heizungsregler …).

Um einen Proxy in Firefox oder im Netzwerk einzutragen, wird im Browser unter Netzwerkeinstellungen, Proxy-Einstellung entweder für alle Netzwerke der Proxy „trutzbox“ mit der Portnummer 8081 eingetragen oder dort unter automatische-Proxy-Konfiguration das PAC-Script http://trutzbox/api/proxy/pac eingetragen.
Hier die Einstellung für Firefox:



Proxy-Einstellung im Firefox: Die automatische Konfigurations-Adresse der TrutzBox eintragen. (Bildschirmfoto: Mozilla Firefox)

Möglichkeit 3: Internet-Gerät per VPN (Fernverbindung) mit der TrutzBox verbinden

Für mobile Geräte empfehlen wir diese Alternative. Sie hat den Vorteil, dass die TrutzBox sowohl aus dem eigenen Netzwerk heraus, als auch unterwegs genutzt werden kann.
Dazu wird auf der TrutzBox unter „Netzwerk“ -> „Fernzugriff“ ein Domain-Name (TrutzDynDNS) eingerichtet und der VPN-Server aktiviert, am Internet-Router der Port 1194 (UDP) zur TrutzBox weitergeleitet und in der Benutzereinstellung der VPN-Zugriff je Benutzer freigeschaltet; die dabei erzeugte Konfigurationsdatei (.ovpn) wird in die VPN-App des Endgeräts importiert. Einzelheiten im Kapitel „Fernzugriff: VPN (Virtual Private Network)“.
Dies ist hier nur verkürzt dargestellt; die vollständige Beschreibung (inklusive TrutzDynDNS, Erreichbarkeitstest und erweiterten Optionen) findet sich im Kapitel „Fernzugriff: VPN (Virtual Private Network)“.

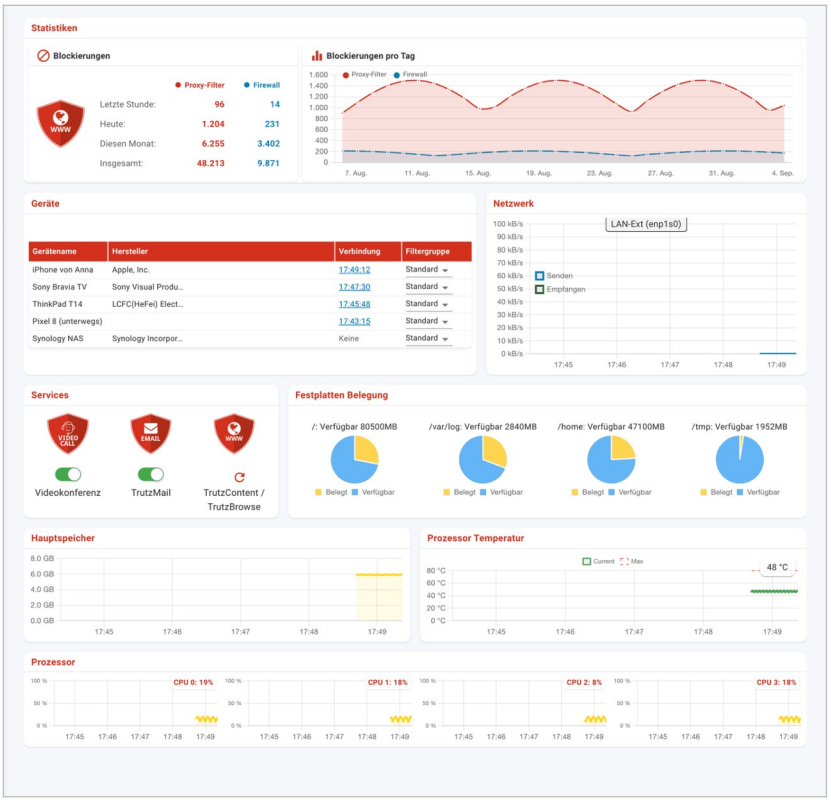
Der Vorteil von Möglichkeit 2 und 3 ist, dass man im Gegensatz zu Möglichkeit 1, einfach auch mal mit einem Schalter die TrutzBox umgehen kann. Das könnte gelegentlich hilfreich sein, falls die TrutzBox in ihrer Standard-Einstellung zu viel filtert und es dadurch Probleme mit einer Anwendung gibt. Natürlich kann man solche Probleme einer Anwendung auch durch Anpassung der Filter in der TrutzBox lösen.

3 TrutzBox-Dashboard

Die TrutzBox Bedministrator Oberfläche wird im Browser mit http://trutzbox/ aufgerufen. Hier werden alle administrativen Einstellungen der TrutzBox durchgeführt. In diesem Kapitel werden wir lediglich auf die wichtigsten Funktionen eingehen. Eine genaue Beschreibung kann man online im TrutzBox-Handbuch finden.

Nachdem die TrutzBox-Oberfläche aufgerufen wurde, wird das Dashboard angezeigt. Es bietet einen sofortigen Überblick über Systemstatus, aktive Services und Netzwerkaktivität.

Menüpfad: Übersicht



Das Dashboard nach dem Anmelden: Systemzustand, Dienste und Netzwerkaktivität auf einen Blick. (© 2026 Comidio GmbH)

Das Dashboard zeigt folgende Bereiche:

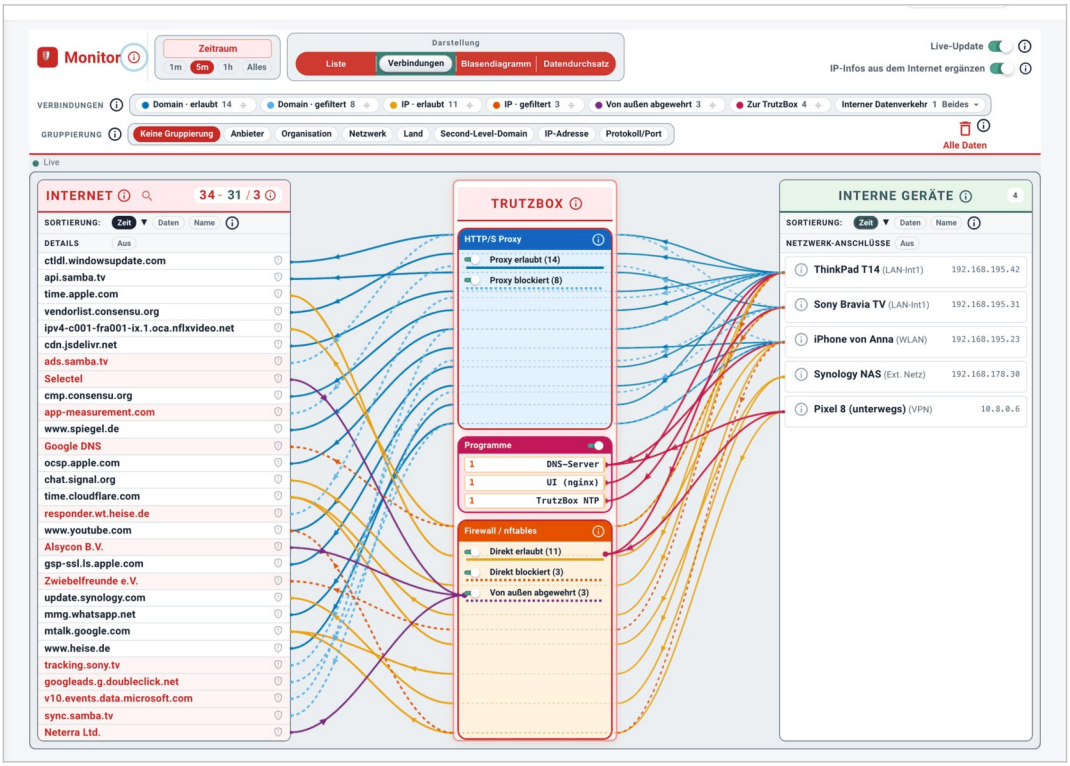
- **Blockierungsstatistik:** Oben links die Anzahl geblockter Verbindungen, nach letzter Stunde, heute, diesem Monat und insgesamt. Daneben ein Zeitdiagramm der geblockten Verbindungen pro Tag.
- **Geräteliste:** Alle mit der TrutzBox verbundenen Geräte mit Gerätename, Hersteller, letzter Verbindungszeit, TrutzBrowse-Status und zugewiesener Filtergruppe. Ein Klick auf die Verbindungszeit öffnet das Verbindungsprotokoll des Geräts im Monitor (Darstellung „Liste“).

- **Netzwerk:** Ein Live-Diagramm des aktuellen Netzwerkverkehrs. „LAN-Ext (enp2s0)“ zeigt den externen WAN-Anschluss Richtung Internet-Router.
- **Services:** Drei Icons zeigen den Status von TrutzMeeting (Videokonferenz), TrutzMail und TrutzContent/TrutzBrowse. Rotes Symbol = aktiv, graues Symbol = inaktiv. Per Klick auf ein Icon kann der jeweilige Service direkt ein- oder ausgeschaltet werden.
- **Festplatten-Belegung:** Vier Donut-Diagramme zeigen den freien Speicherplatz der Partitionen / (Root-Partition), /var/log (Logdateien), /home (Nutzerdaten) und /tmp (temporäre Daten). Ein Klick auf ein Diagramm öffnet eine Liste der größten Dateien der jeweiligen Partition, die sich zur Analyse als Datei herunterladen lässt.
- **Hauptspeicher:** Zeitdiagramm der RAM-Auslastung. Die gelbe Linie markiert den aktuell belegten Speicher; die y-Achse den maximal verfügbaren.
- **Prozessor-Temperatur:** Zeitdiagramm der aktuellen CPU-Temperatur; zusätzlich wird der vom Sensor gemeldete Maximalwert angezeigt. (Zum Schutz der Hardware schaltet sich die TrutzBox bei zu hoher Temperatur selbsttätig ab.)
- **Prozessor-Auslastung:** Je ein separates Diagramm pro Prozessorkern (Anzahl abhängig von der Hardware, z. B. vier Kerne 0 bis 3).
- **Abmelden / TrutzBox steuern:** Das Symbol oben rechts ermöglicht Abmelden, Herunterfahren oder Neustart der TrutzBox.

4 Monitor

Mit dem Monitor stellt die TrutzBox eine zentrale Live-Sicht auf alle Internetverbindungen aller Geräte im eigenen Netzwerk bereit. Er ist eine interaktive, filter- und gruppierbare Visualisierung des Datenverkehrs zwischen eigenem Netz und Internet mit Drilldown bis zur einzelnen Verbindung.
Der Monitor zieht seine Daten aus den beiden Filterstufen, die jede Verbindung durchläuft: dem HTTP/S-Proxy (TrutzContent / TrutzBrowse) für Verbindungen auf Anwendungsebene und der nftables-Firewall für Verbindungen auf Netzwerkebene. Beide Stufen sind im zentralen Bedienfeld als eigene Stationen sichtbar, sodass sich auf einen Blick erkennen lässt, welche Filterstufe eine Verbindung erlaubt, blockiert oder durchgereicht hat. Die nftables-Firewall ist dabei die im Linux-Kernel verankerte Paketfilter-Firewall, die den Datenverkehr auf Netzwerkebene (IP-Adressen und Ports) prüft.

Menüpfad: Monitor



Der Monitor in der Darstellung „Verbindungen“: links die Internet-Server, in der Mitte die TrutzBox, rechts die eigenen Geräte.
(© 2026 Comidio GmbH)

Wichtig für die Privatsphäre: Der Monitor wertet ausschließlich lokale Daten der TrutzBox aus, die Verbindungsverfolgung des Linux-Kernels (conntrack) und das Protokoll der Firewall (nftables). Nach außen fragt er nur, wenn der Schalter „IP-Infos aus dem Internet ergänzen“ eingeschaltet ist; dann holt die Box zu den angezeigten Adressen Angaben aus den öffentlichen Registrierungsdiensten. Steht der Schalter aus, verlässt keine Anfrage die Box. Aufgezeichnet wird laufend, unabhängig davon, ob gerade jemand den Monitor geöffnet hat: Firewall-Ereignisse und die Zugriffe über den Proxy schreibt die TrutzBox mit, solange eine Speicherdauer eingestellt ist. Nur die zusätzlichen Momentaufnahmen des

Monitors, also die laufende Abfrage von conntrack und der Zähler an den Netzwerk-Anschlüssen, arbeiten während einer geöffneten Monitor-Ansicht. Ohne gesetzte Speicherdauer bleibt eine Live-Ansicht der letzten rund zehn Minuten im Arbeitsspeicher, mit gewählter Speicherdauer lassen sich ältere Daten mit dem Zeit-Regler durchblättern (Einzelheiten im Abschnitt „Die Steuerleiste“). Datenquelle ist dabei conntrack: Sie führt für jede aktive Verbindung Quelle, Ziel und Status mit, sodass der Monitor das aktuelle Geschehen ohne zusätzliche Messung ablesen kann.

Was sich mit dem Monitor beantworten lässt

Folgende typische Fragen lassen sich ohne zusätzliche Werkzeuge direkt im Monitor klären:

- Welche Tracker hat ein bestimmtes Gerät heute kontaktiert? Filter auf „Proxy: Blockiert“ und Sortierung nach dem betreffenden Gerät zeigt, welche Werbe- oder Tracking-Server TrutzContent abgewiesen hat. Gruppierung nach Anbieter macht zusätzlich sichtbar, welche Konzerne dahinterstehen.
- Mit welchen Servern verbindet sich ein neues IoT- oder Smart-Home-Gerät? Nach Zuordnung des Geräts zu einer Filtergruppe genügt ein Blick auf die ausgehenden Verbindungslinien. Auffällig sind regelmäßige Verbindungen in Länder, die für die Gerätefunktion nicht plausibel sind.
- Warum wurde diese Verbindung blockiert? Klick auf eine rote Verbindungslinie öffnet einen Detail-Dialog mit Klartext-Erklärung, betroffener Filterregel, WHOIS-Information zum Zielserver und Empfehlung, ob Handlungsbedarf besteht.
- Welche Geräte verursachen den meisten Datenverkehr? Sortierung nach „Daten“ stellt die Server bzw. Geräte mit der höchsten übertragenen Datenmenge an die Spitze.
- Treten Anomalien im normalen Verbindungsmuster auf? IoT-Geräte und Smartphones haben relativ stabile Verbindungsmuster. Plötzlich auftretende Verbindungsversuche zu unbekannten Servern oder ungewöhnlichen Ländern können auf Schadsoftware oder kompromittierte Geräte hindeuten. Die TrutzBox markiert auffälliges Verhalten zudem mit einem Hinweis (z. B. „Scan-Versuch erkannt“).

4.1 Eingebaute Hilfe: geführte Touren

Neben der Überschrift „Monitor“ sitzt ein Info-Symbol („i“). Beim ersten Aufruf und nach Updates, die die Bedienung ändern, pulsiert ein blauer Ring darum. Ein Klick öffnet die Hilfe: eine Themenliste, die nach Aufgaben gegliedert ist („Erste Schritte“, „Geräte untersuchen“, „Internet-Ziele untersuchen“, „Sperren und freigeben“, „Übersicht behalten“) und nicht nach Bedienelementen. Derzeit gibt es 16 Themen in fünf Abschnitten, von „Wie der Monitor aufgebaut ist“ über „Eine Verbindung sperren oder freigeben“ bis „Reihenfolge der Liste ändern“.

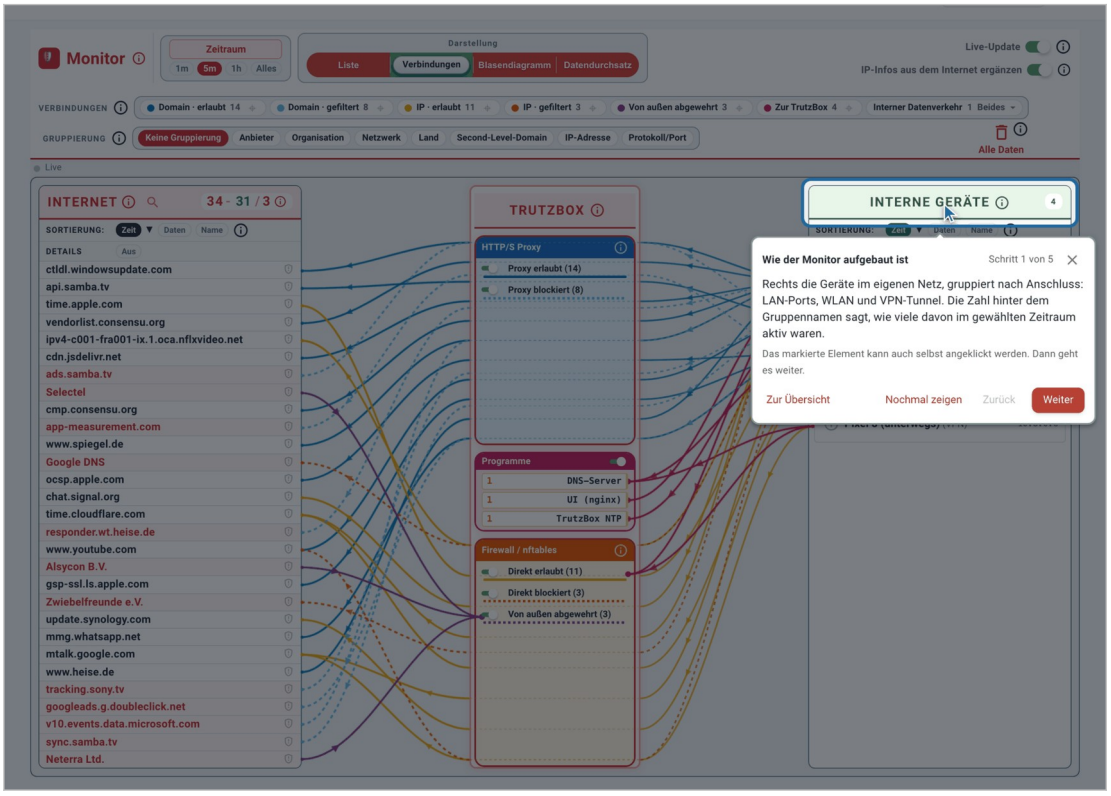
Jedes Thema startet eine geführte Tour auf dem echten Bildschirminhalt: Die Seite wird abgedunkelt, das jeweilige Bedienelement bleibt hell markiert, ein gezeichneter Mauszeiger fährt dorthin, und eine Sprechblase erklärt in ein bis zwei Sätzen, was dort passiert. Wer das markierte Element selbst anklickt, springt automatisch zum nächsten Schritt. Gehört ein Thema zu einer anderen

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Darstellung, fragt die Hilfe vor dem Start („Dorthin wechseln und starten?“) und schaltet erst nach Bestätigung um.

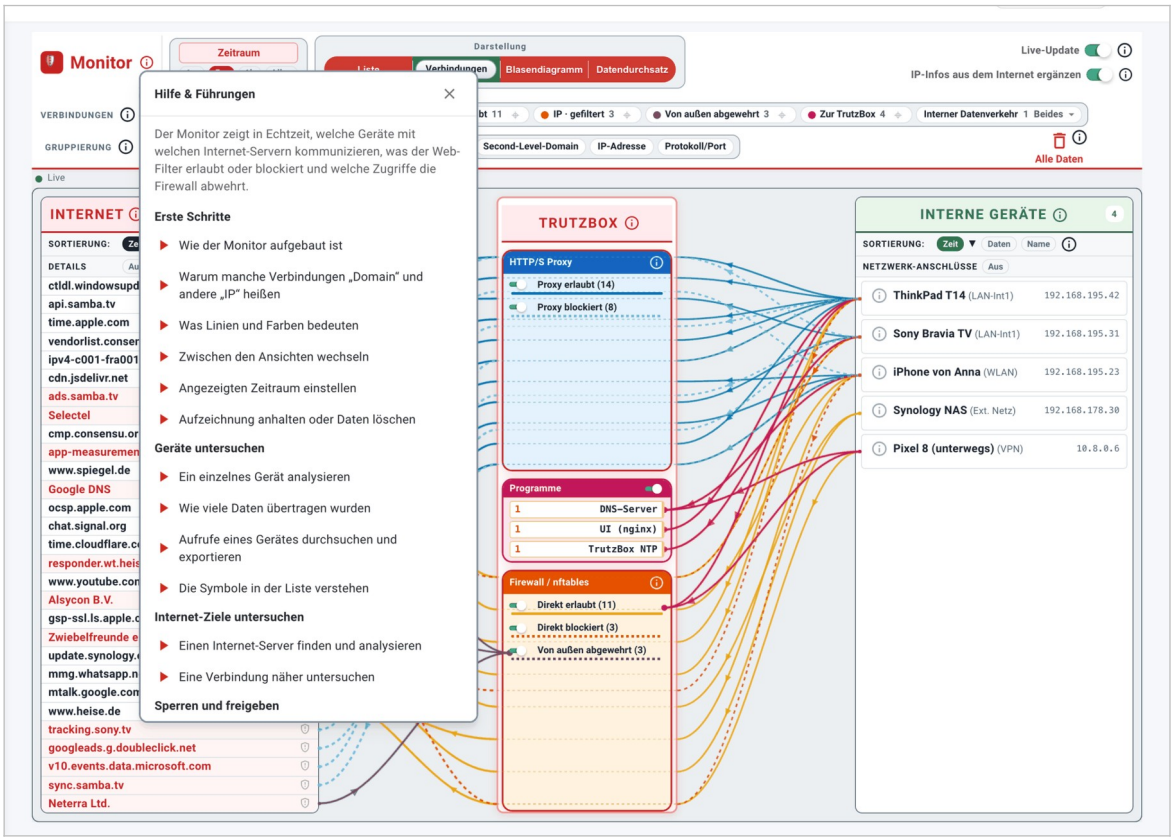
Eine Tour lässt sich jederzeit beenden: über das Schließkreuz der Sprechblase, mit der Esc-Taste oder mit einem Klick neben die Markierung. Zugeklappte Bereiche wie die Zeitraum-Einstellung öffnet die Tour bei Bedarf selbst, damit Text und Bild zusammenpassen. Da die Touren auf die tatsächlichen Bedienelemente zeigen, bleiben sie auch nach Oberflächen-Updates aktuell.

Menüpfad: Monitor



Das Hilfe-Fenster des Monitors mit den geführten Touren.
(© 2026 Comidio GmbH)

Menüpfad: Monitor



Erster Schritt einer Tour: Die Sprechblase erklärt den gerade hervorgehobenen Bereich.
(© 2026 Comidio GmbH)

4.2 Die Steuerleiste: Zeitraum, Darstellung, Verbindungstypen und Gruppierung

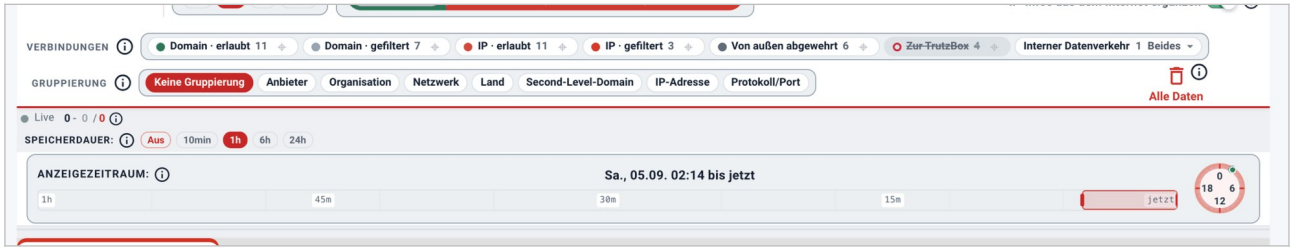
Die Kopfleiste des Monitors bündelt fünf Einstellungen. Vier davon ändern nur die Sicht auf dieselben aufgezeichneten Daten: der Anzeigezeitraum, die Darstellung, die Verbindungstypen und die Gruppierung. Die fünfte, die Speicherdauer, greift tiefer, denn sie entscheidet, wie viel die TrutzBox überhaupt aufhebt. Diese fünf Einstellungen lohnen sich zu verstehen, bevor es an die Einzelheiten geht.



Die Steuerleiste des Monitors: Zeitraum, Darstellung, Schalter für Live-Update und IP-Infos, darunter die Chip-Zeilen „Verbindungen" und „Gruppierung".
(© 2026 Comidio GmbH)

Anzeigezeitraum: welcher Ausschnitt zu sehen ist

Der Anzeigezeitraum bestimmt, welchen Ausschnitt der Aufzeichnung die Box gerade darstellt. Die Schnellwahl bietet 1 Minute, 5 Minuten, 1 Stunde und „Alles“. Der Knopf „Zeitraum“ klappt die genaue Einstellung auf: Dort lässt sich der Ausschnitt mit zwei Griffen breiter oder schmaler ziehen und mit der Fläche dazwischen in die Vergangenheit schieben. Rechts außen liegt immer der aktuelle Zeitpunkt.



Der Knopf „Zeitraum“ klappt beides auf: oben die Speicherdauer, darunter der Regler für den Anzeigezeitraum.
(© 2026 Comidio GmbH)

Wann welche Wahl: Für den Blick auf das, was gerade passiert, sind 1 oder 5 Minuten richtig, weil wenige Zeilen und Linien ein ruhiges Bild ergeben. Wer einem Verdacht nachgeht, etwa einem Gerät, das nachts Daten sendet, wählt 1 Stunde oder „Alles“ und schiebt den Ausschnitt zurück. Die Wahl gilt in allen vier Darstellungen und bleibt beim Wechsel erhalten.
Der Schalter „Live-Update“ friert das Bild ein, ohne die Aufzeichnung anzuhalten. Das ist nützlich, wenn eine Zeile in Ruhe angesehen werden soll und sonst ständig neue Einträge nachrücken.

Speicherdauer: wie weit zurück überhaupt Daten vorliegen

Die Speicherdauer legt fest, wie lange die TrutzBox die Verkehrsdaten des Monitors aufhebt, bevor sie automatisch gelöscht werden. Zur Wahl stehen „Aus“, 10 Minuten, 1 Stunde, 6 Stunden und 24 Stunden. Bei „Aus“ bleibt nur die Live-Ansicht im Arbeitsspeicher, dauerhaft mitgeschrieben wird nichts. Solange für den Monitor eine Speicherdauer eingestellt ist, hebt sie die Aufbewahrung von Zugriffsprotokoll und Firewall-Protokoll mindestens auf denselben Wert an.
Der häufigste Irrtum: Anzeigezeitraum und Speicherdauer werden leicht verwechselt. Weiter zurückschauen, als die Speicherdauer reicht, ist nicht möglich, weil dort nichts mehr vorhanden ist. Wer länger zurückblicken möchte, stellt zuerst die Speicherdauer höher. Das kostet Platz auf der TrutzBox, deshalb ist sie ab Werk knapp eingestellt.
Achtung beim Verkleinern: Eine kürzere Speicherdauer löscht die älteren Daten sofort und unwiderruflich. Die TrutzBox fragt vorher nach.

Darstellungen: vier Sichten auf dieselben Daten

Der Umschalter „Darstellung“ wechselt zwischen „Liste“, „Verbindungen“, „Blasendiagramm“ und „Datendurchsatz“. Alle vier greifen auf denselben Datenbestand zu und bereiten ihn nur anders auf; der gewählte Zeitraum bleibt beim Wechsel erhalten.
Wann welche Darstellung: Die „Liste“ ist das Protokoll Zeile für Zeile und die Wahl, wenn ein bestimmter Aufruf gesucht oder eine Domain nachgeschlagen wird. „Verbindungen“ zeichnet die Wege

zwischen Geräten, TrutzBox und Internet-Servern und zeigt damit, welchen Weg ein Zugriff genommen hat und wo er gestoppt wurde. Das „Blasendiagramm“ ordnet die Gegenstellen nach Größe und macht Ausreißer sichtbar. „Datendurchsatz“ beantwortet die Frage, wohin die Datenmenge geflossen ist. Der folgende Abschnitt beschreibt die vier Darstellungen einzeln.

Verbindungstypen: welche Zeilen und Linien erscheinen

Die Zeile „Verbindungen“ enthält für jede Art von Verbindung einen Chip mit der zugehörigen Anzahl. Damit lässt sich die Anzeige auf genau das eingrenzen, worum es gerade geht. Sieben Arten werden unterschieden:



Die Chip-Zeile „Verbindungen“ mit den sieben Arten und der Zahl der Zeilen je Art, ganz rechts der graue Punkt „Interner Datenverkehr“.
(© 2026 Comidio GmbH)

- **Domain · erlaubt:** Verbindung zu einer Domain, vom Inhaltsfilter der TrutzBox geprüft und durchgelassen.
- **Domain · gefiltert:** Verbindung zu einer Domain, vom Inhaltsfilter blockiert.
- **IP · erlaubt:** direkte Verbindung zu einer IP-Adresse ohne Domain-Filterung, erlaubt.
- **IP · gefiltert:** direkte Verbindung zu einer IP-Adresse, von der Firewall blockiert.
- **Von außen abgewehrt:** ein aus dem Internet eingehender Verbindungsversuch, den die Firewall verworfen hat.
- **Zur TrutzBox:** ein Gerät spricht mit einem Programm der Box selbst, etwa Namensauflösung, Verwaltung oder Mail, oder die Box geht selbst ins Internet.
- **Interner Datenverkehr:** Verbindungen zwischen zwei Geräten im eigenen Netz, dargestellt mit einem grauen Punkt.

Wann man sie braucht: Wer wissen möchte, was die Filter tatsächlich stoppen, lässt nur „Domain · gefiltert“ und „IP · gefiltert“ stehen. Wer prüfen möchte, was am Web-Filter vorbei direkt ins Internet geht, wählt „IP · erlaubt“. Und wer Angriffsversuche aus dem Internet sehen möchte, schaltet auf „Von außen abgewehrt“.

- **Chip-Leiste:** Die farbigen Punkte sind zweifach bedienbar. Ein Klick auf die Beschriftung zeigt nur Verbindungen dieser Art (nochmaliges Klicken hebt die Auswahl auf), ein Klick auf den Farbpunkt blendet die Art ein oder aus; ein Hinweistext erklärt jede Verbindungsart einzeln.

Interner Datenverkehr: Verbindungen zwischen zwei Geräten im eigenen Netz hatten bis September 2026 eine eigene Menü-Kachel mit drei Stufen. Seit Oktober 2026 stehen sie als grauer Punkt am Ende der Chip-Zeile und verhalten sich wie jede andere Art:

- **Immer mitgeschrieben:** Die TrutzBox zeichnet internen Verkehr auf, solange der Monitor geöffnet ist, genau wie die übrigen Arten. Der Punkt blendet die Zeilen nur ein und aus, die Zahl dahinter nennt ihre Anzahl, der Hinweis am Punkt erklärt die Art. „Nur intern“ ergibt sich, indem die übrigen Punkte ausgeschaltet werden.
- **Was als intern gilt:** Beide Enden der Verbindung liegen in einem Netz der TrutzBox, also im internen Netz oder im Tunnelnetz von TrutzVPN: etwa ein Notebook im WLAN, das auf den Speicher am Kabel zugreift, oder ein Gerät, das über TrutzVPN auf das interne Netz zugreift.
- **Zur TrutzBox:** Verbindungen zur TrutzBox selbst (Namensauflösung, Verwaltung, Mail) stehen getrennt davon unter „Zur TrutzBox“.
- **Gerät zu Gerät innerhalb der Brücke:** Bis September 2026 blieb unsichtbar, was zwei Geräte am selben Anschluss direkt miteinander sprachen, denn dieser Verkehr durchlief die Netzwerkbrücke der TrutzBox ohne Umweg über die Firewall. Seit der Firewall-Fassung vom Oktober 2026 (trutz-network, Kernelmodul br_netfilter) laufen auch diese Pakete durch Verbindungsverfolgung und Firewall. Die TrutzBox sieht damit auch Gerät zu Gerät innerhalb der Brücke, WLAN zu Kabel eingeschlossen, und der Monitor zeigt je Fluss eine Verbindung. Gemessen am 01.10.2026 in einer virtuellen ARM-Maschine: Durchsatz unverändert, Rechenlast ein bis vier Prozentpunkte höher.
- **Eigenes Netz nie behindert:** Die Firewall lässt Verkehr zwischen Geräten des eigenen Netzes immer durch; Sperrlisten und Umleitungen zielen auf das Internet. Ein in der Geräteliste getrenntes Gerät verliert nur das Internet und erreicht Drucker, NAS und TrutzVPN-Teilnehmer weiter.
- **Alle Protokolle:** Der Monitor erfasst alle Protokolle, nicht nur TCP und UDP. Auch Verbindungsarten ohne Portnummer wie ICMP erscheinen in der Liste, und eine eigene Zeile „DNS unverschlüsselt“ zeigt die unverschlüsselte Namensauflösung der TrutzBox (Port 53).

Gruppierungen: aus vielen Servern wenige Einträge

Ohne Gruppierung steht jeder Server für sich, und schon der Aufruf einer einzigen großen Nachrichtenseite füllt den Bildschirm. Die Gruppierung fasst die Einträge nach einer Eigenschaft des Ziels zusammen: in der Liste als aufklappbare Gruppenzeilen, im Blasendiagramm als gemeinsame Blase, in der Darstellung „Verbindungen“ als Gruppenzeile der Internet-Spalte. Die Zahl in Klammern nennt, wie viele Einträge dahinterstecken. An den Daten ändert sich dabei nichts, nur an der Darstellung. **Wann welche Gruppierung:** „Second-Level-Domain“ ist der schnellste Weg zu vertrauten Namen wie google.com. „Anbieter“ und „Organisation“ zeigen, welche Konzerne hinter den vielen Adressen stecken. „Land“ macht ungewöhnliche Ziele sichtbar. „Protokoll/Port“ beantwortet die Frage, welcher Verkehr am Web-Filter vorbeiläuft. Der Abschnitt „Server gruppieren“ weiter unten beschreibt alle acht Möglichkeiten einzeln.

Weitere Schalter der Kopfleiste

- **IP-Infos aus dem Internet ergänzen:** ergänzt zu jedem Server Land, Anbieter, Organisation und Netzbereich aus den öffentlichen Registrierungsdiensten (RIPE, ARIN, APNIC, LACNIC,

AFRINIC). Übertragen werden nur die IP-Adressen der gerade angezeigten Server, die Ergebnisse werden auf der TrutzBox zwischengespeichert; die Einstellung bleibt gespeichert und ist Teil der Sicherung:

- **Reverse-DNS:** Für Server, die noch keinen Namen aus dem Datenverkehr gezeigt haben, ermittelt die TrutzBox den registrierten Namen zusätzlich per Reverse-DNS (PTR).
- **Bestätigungsdialog:** Er erklärt vorab, welche Daten dabei abgefragt werden, und weist darauf hin, ob die DNS-Auflösung der Box verschlüsselt läuft (dann sind auch diese Namensabfragen verschlüsselt). Andernfalls empfiehlt er, unter „Netzwerk → DNS-Auflösung“ die verschlüsselte Weiterleitung (DoT) zu aktivieren.
- **Anbietername statt IP:** Ist zu einem Ziel nur die IP-Adresse bekannt, setzt die Liste an ihre Stelle den Namen des Anbieters aus der Katalog-Auskunft. Ein Mauszeiger darüber nennt die Quelle des Namens (Rückwärts-Auflösung des Namens, WHOIS-Eintrag oder der im Datenverkehr gesehene Servername).
- **Fehlende Angaben:** Fehlt zu einem Zugriff die Server-Adresse oder das Herkunftsland, steht dort der Grund, etwa dass der Zugriff nur über einen Namen lief und nie eine Adresse zugeordnet wurde.
- **Zähler der Internet-Server:** Über der Server-Spalte steht in allen vier Darstellungen, wie viele Internet-Ziele der gewählte Zeitraum enthält, aufgeteilt in insgesamt, durchgelassen (grün) und blockiert (rot). Ein Klick auf die grüne Zahl bietet an, alle derzeit durchgelassenen Adressen in einem Schritt zu sperren. Kleine Info-Symbole an Legende, Zählern und Gruppierung erklären jeweils, was genau gezählt wird und warum sich zwei Zahlen unterscheiden können, etwa weil gezählt wird, wie viele verschiedene IP-Adressen im Zeitraum vorkamen: Eine Domain mit vier Adressen zählt viermal. Die Zahl stammt aus den Verbindungsdaten und kann deshalb von den Zahlen der Liste abweichen, in der auch Proxy-Zugriffe mitzählen, die keine eigene Verbindungszeile haben.
- **Symbole:** Jeder Internet-Server in der Internet-Spalte der Darstellungen „Verbindungen“ und „Datendurchsatz“ sowie jede Server-Blase im Blasendiagramm trägt seit Oktober 2026 ein Bildzeichen für die Art seines Dienstes. Der mitgelieferte Katalog kennt 19 Arten: Plattform, Video und Streaming, Musik und Podcasts, Soziale Netze, Chat und Telefonie, Handel und Essen, Werbung und Messung, Spiele, KI, Finanzen und Zahlung, Cloud und Speicher, Auslieferung (CDN), Nachrichten und Wissen, Entwicklung, Sicherheit und VPN, Reisen und Mobilität, Haustechnik und Geräte, E-Mail sowie TrutzBox; Server der TrutzBox-Dienste von Comidio (etwa mytrutzbox.de) tragen das TrutzBox-Logo, Markenlogos gibt es nicht. Der Name des Dienstes steht im Hinweis am Server („Dienst: …“). Der Schalter „Symbole“ im Kopf der Internet-Spalte ist ab Werk eingeschaltet, ausgeschaltet erscheint das bisherige Zeichen; die Stellung merkt sich der Browser. Quelle ist der Dienste-Katalog dienste.json, den das Paket trutz-blacklists unter /usr/share/trutz-blacklists/ ausliefert: zusammengestellt aus den Diensten von NextDNS und der domain-list-community von v2fly (beide unter MIT-Lizenz, mit Namensnennung im Paket) sowie eigenen Einträgen von Comidio, Stand Ende September 2026 rund 1.600 Dienste mit knapp 25.000 Domains.

Die Oberfläche lädt ihn einmal je Aufruf über GET /api/traffic/dienste, gepackt (rund 150 KB) und mit ETag, und ordnet jeden Servernamen durch Kürzen von links Label für Label dem längsten passenden Domain-Eintrag zu; IP-Adressen ohne Namen bleiben ohne Symbol.

- **Alle Daten löschen:** leert die aufgezeichneten Verbindungs- und Block-Protokolle vollständig, einschließlich der Firewall-Block-Historie und in allen Darstellungen, auch in der Liste.

4.3 Voreinstellungen beim ersten Aufruf

Solange noch keine eigenen Einstellungen gespeichert wurden, startet der Monitor mit Voreinstellungen, die sich jederzeit ändern lassen und dann erhalten bleiben:

- **Voreinstellungen:** die Ansicht „Liste“, keine Gruppierung, Sortierung nach Zeit, ein Anzeigezeitraum von 5 Minuten und die Speicherdauer „Aus“.
- **Speicherdauer:** Ohne Speicherdauer schreibt die Box nichts dauerhaft mit. Wer zurückblättern möchte, wählt eine Speicherdauer selbst.
- **TrutzBox-eigene Programme:** Proxy, DNS, NTP usw. sind zunächst ausgeblendet, damit der Blick auf dem tatsächlichen Geräte-Verkehr liegt. Sie lassen sich mit einem Klick einblenden.
- **Gruppierung:** Sie wählt der Anwender selbst. Nur das Blasendiagramm fasst ab 500 Servern von sich aus nach Domain (SLD) zusammen, damit die Darstellung lesbar bleibt.
- **Anzeigezeitraum:** Der gewählte Zeitraum gilt in allen Darstellungen, auch in der Liste, und bleibt beim Wechsel der Darstellung erhalten.
- **Leerer Bildschirm:** Liegt der Zeitraum vor dem Beginn der Aufzeichnung, erklärt eine orangefarbene Statuszeile den leeren Bildschirm (etwa „Für diesen Zeitraum gibt es keine Aufzeichnungen. Gespeichert wird seit … Uhr.“).

Die Sortierung nach Zeit verhält sich wie die Liste: Neue Server und Geräte erscheinen oben, alles andere rückt ruhig nach unten. Dafür merkt sich der Monitor für jeden Eintrag den Zeitpunkt, zu dem er erstmals in der Ansicht auftaucht, und behält ihn bei. Die letzte Aktivität eines Servers spielt für die Reihenfolge keine Rolle, deshalb springen die Spalten im Betrieb nicht um. Bei gleichem Zeitpunkt entscheidet die Reihenfolge des Eintreffens. Verschwindet ein Server kurz aus dem Zeitfenster und kehrt innerhalb von 300 Sekunden zurück, behält er seinen Platz; taucht er nach längerer Pause wieder auf, steht er oben. Erst ein Wechsel des Anzeigezeitraums oder der Darstellung setzt die Reihenfolge neu; das Ziehen im Zeitstrahl tut das bewusst nicht.

4.4 Vier Darstellungen

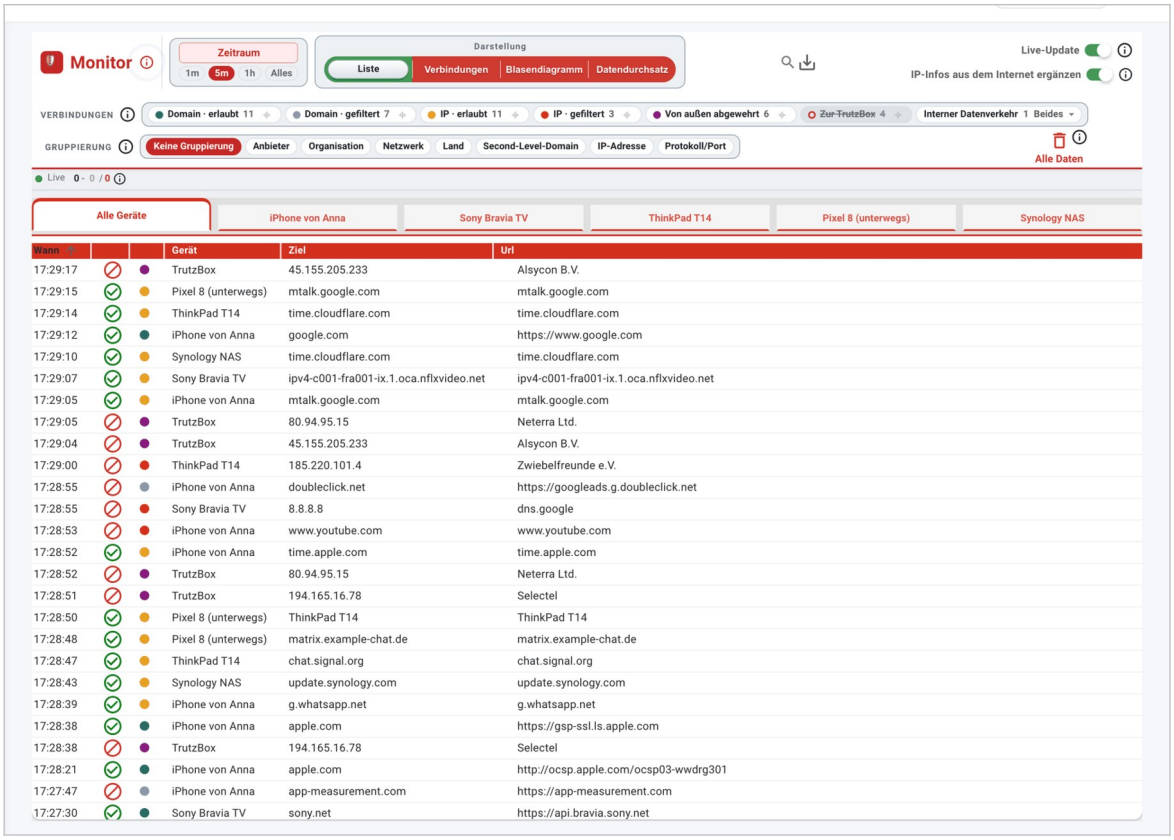
Über den Umschalter „Darstellung“ in der Kopfleiste lässt sich zwischen vier Sichten auf dieselben Daten wechseln: Liste, Verbindungen, Datendurchsatz und Blasendiagramm. Alle vier greifen auf denselben aufgezeichneten Datenbestand zu und reagieren auf die gleichen Filter- und Zeiteinstellungen.

Sie unterscheiden sich nur darin, wie sie die Verbindungen aufbereiten. Der eingestellte Anzeigezeitraum bleibt beim Umschalten der Darstellung erhalten.

Liste

Die Darstellung „Liste“ ist das tabellarische Protokoll aller Verbindungen. Sie vereint die Zugriffe über den Proxy mit den Firewall-Ereignissen: Jede Zeile ist ein Server-Kontakt über den HTTP/S-Proxy oder eine direkt an der Firewall behandelte Verbindung. Welche Zeilenarten angezeigt werden, steuern die Verbindungs-Chips der Kopfleiste.

Menüpfad: Monitor



Die Darstellung „Liste“ ohne Gruppierung: je Zeile ein Server-Kontakt mit Uhrzeit, Gerät, Ziel und Adresse; das Symbol links zeigt das Urteil von TrutzContent.
(© 2026 Comidio GmbH)

Die Liste hat sechs Spalten, zwei davon führen kein Wort in der Kopfzeile, sondern nur ein Symbol:

- **Wann:** Zeitpunkt des Server-Kontakts. Wiederholte Zugriffe auf dasselbe Ziel fasst die Liste zu einer Zeile mit Zähler zusammen, etwa „2×“; der Pfeil am Zeilenanfang klappt die einzelnen Zeitpunkte auf. Ein Klick auf die Uhrzeit öffnet die Verbindungs-Details.
- **Ergebnis (Symbol):** Das erste Symbol zeigt, wie der Proxy den Kontakt behandelt hat. Die Einzelheiten dazu stehen im nächsten Absatz.

- **Art der Verbindung (Farbpunkt):** Der farbige Punkt daneben nennt die Art der Verbindung. Es sind dieselben sieben Arten und dieselben Farben wie in der Chip-Zeile „Verbindungen“ der Kopfleiste, beschrieben im Abschnitt „Verbindungstypen“. Der Mauszeiger nennt die Art im Klartext, ein Klick öffnet die vollständigen Verbindungs-Details.
- **Gerät:** Das Gerät im eigenen Netz, von dem der Zugriff ausging. Die Spalte erscheint nur im Reiter „Alle Geräte“; in einem Geräte-Reiter wäre sie überflüssig.
- **Ziel:** Der Server, mit dem das Gerät gesprochen hat. Ein Klick öffnet die Angaben zu diesem Server, der Mauszeiger nennt die Herkunft des Namens.
- **Url:** Die vollständige Adresse, soweit die TrutzBox sie kennt. Bei verschlüsselten Verbindungen sieht sie ohne TrutzBrowse nur den Server-Namen, nicht den Pfad dahinter; bei unverschlüsselten Aufrufen steht die ganze Adresse.

Ein Klick auf eine freie Stelle der Kopfzeile öffnet das Spaltenmenü „Spalten anzeigen“, über das sich zusätzliche Spalten einblenden lassen (Land, Protokoll/Port, IP, HTTP-Methode, Anbieter, Organisation, Netzwerk, Anzahl, Seitentitel); „Alle anzeigen“ und „Grundeinstellung“ setzen die Auswahl gesammelt, gemerkt wird sie je Gruppierung. Bei großen Datenmengen zeigt die Liste zunächst die neuesten Zeilen („Neueste … von … angezeigt“); „Alle laden“ lädt den Rest, warnt aber vorab, wenn das Sortieren sehr vieler Zeilen die Oberfläche spürbar anhalten würde. Blockierte Zeilen öffnen per Klick denselben Detail-Dialog wie in der Darstellung „Verbindungen“. Nackte IP-Adressen ohne Domain ergänzt die Liste, wo möglich, um einen Namen aus dem lokalen Server-Katalog. Die Liste lädt beim Herunterscrollen von selbst nach. Die Suche sitzt platzsparend hinter dem Lupen-Symbol, und die Sortierung nach Zeit bleibt dabei stabil. Abgerufen wird nur der gerade angezeigte Zeitraum, wodurch die Liste auch bei großen Datenmengen zügig erscheint.
Die Spalte „TrutzContent“ zeigt je Zeile als Symbol, wie der Proxy den Server-Kontakt behandelt hat: durchgelassen, blockiert, ohne HTTPS-Entschlüsselung (SecuritySlider auf L10) oder mit Verbindungsfehler. Mit einem Klick auf das Symbol lässt sich eine blockierte Verbindung für künftige Zugriffe freischalten bzw. eine erlaubte blockieren; ein Dialog erlaubt dabei, die betroffene Domain genauer einzugrenzen.
Ist auf einem Gerät zusätzlich TrutzBrowse eingeschaltet, kommt in der Liste eine weitere Spalte hinzu. Sie ist im Kapitel „TrutzBrowse“ beschrieben, zusammen mit allem, was zu dieser Zusatzstufe gehört.

Verbindungen

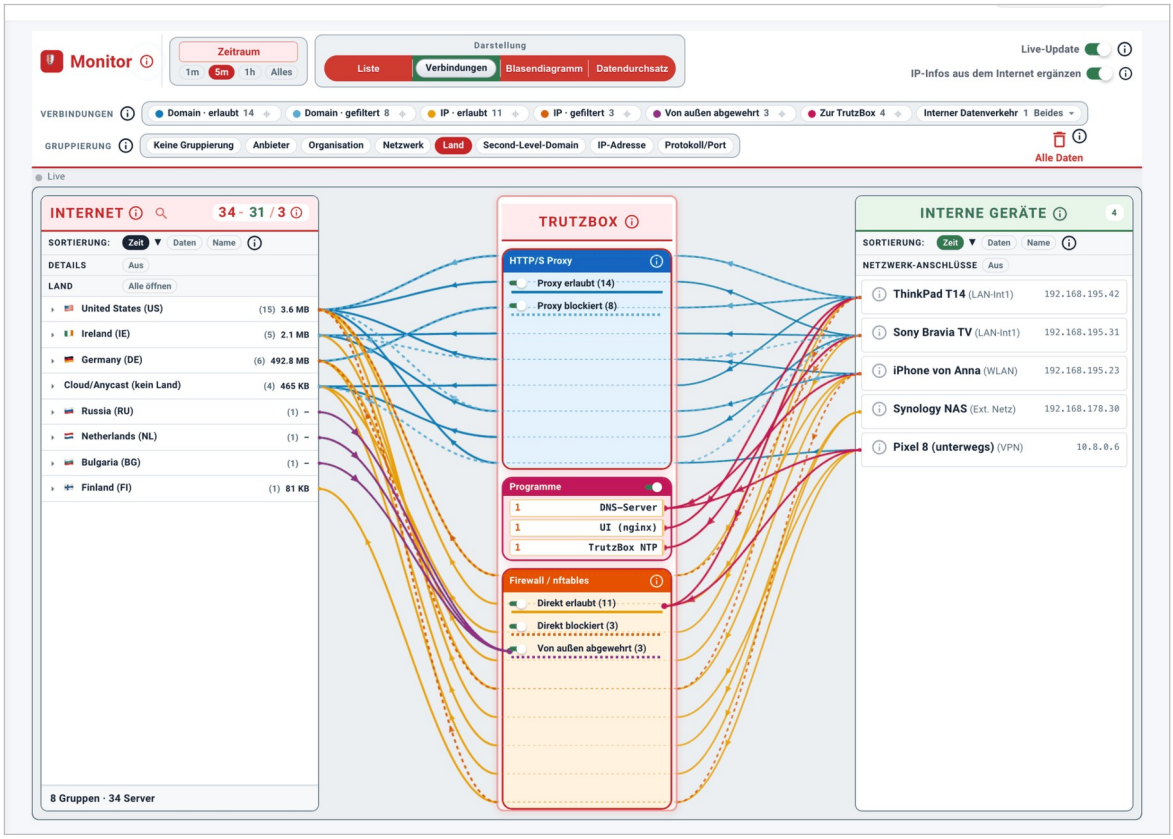
Die Darstellung „Verbindungen“ ist die ausführlichste Sicht. Sie gliedert sich in drei Spalten: links die kontaktierten Internet-Server, in der Mitte die TrutzBox selbst mit ihren Stationen (HTTP/S-Proxy, interne Programme/Dienste und nftables-Firewall), rechts die internen Geräte des eigenen Netzwerks, gruppiert nach Netzwerksegment (VPN, WLAN, LAN, externes Netz). Jede Spalte zeigt zusätzlich die übertragene Datenmenge und die Anzahl von Servern bzw. Geräten. Geräte, die hinter dem Internet-Router geroutet sind und sich dessen MAC-Adresse teilen (etwa VPN-Clients einer FRITZ!Box), erhalten in der Spalte „Ext. Netz“ eine eigene Karte je IP-Adresse mit dem Zusatz „hinter … (geroutet)“;

benannt werden sie, soweit möglich, über die Namensauflösung des Routers oder selbst vergebene Namen.
Geräte im Tunnel des Fernzugriffs tragen den Namen ihres Zugangs mit der Endung .vpn.sec, etwa iphone.vpn.sec. Die TrutzBox schreibt dazu alle 30 Sekunden die Namen der WireGuard-Zugänge und der gerade verbundenen OpenVPN-Clients in eine Datei, die ihr Namensdienst (dnsmasq) mitliest; die Rückwärts-Auflösung der Tunneladresse liefert so den Namen. Private Adressen, die die TrutzBox nur über ihre Standardroute erreicht, also weder in einem eigenen Netz noch im Netz des Routers noch über eine eingetragene statische Route, gelten dagegen nicht als Geräte. Sie stehen in der Internet-Spalte, denn sie liegen wie jedes Ziel im Internet hinter dem Router. Beispiele sind der Telefonie-Server (SIP) des Internetanbieters unter einer Adresse wie 10.199.27.29 oder die Suchanfragen einer App, die private Adressbereiche nach Geräten abtastet. Der Kontakt bleibt so sichtbar, und die Geräteliste füllt sich nicht mit Adressen, hinter denen kein eigenes Gerät steht.
Zwischen den Spalten werden Bögen gezogen: jede Linie steht für eine konkrete Verbindung zwischen einem Internet-Server und einem internen Gerät, geführt durch eine der Stationen in der Mitte. Dabei kodiert die Farbe die Station, die eine Verbindung durchlaufen hat (blau für den HTTP/S-Proxy, orange für die nftables-Firewall), und der Strich-Stil das Ergebnis: durchgezogene Linien stehen für durchgereichte, gestrichelte für blockierte Verbindungen:

- **Blau, durchgezogen:** Die Verbindung lief über den HTTP/S-Proxy und wurde durchgereicht.
- **Blau, gestrichelt:** Die Verbindung wurde am Proxy blockiert, durch TrutzContent oder TrutzBrowse.
- **Orange, durchgezogen:** Direkt über die nftables-Firewall durchgereicht, ohne dass der Proxy im Pfad war (z. B. UDP, Nicht-HTTP-Ports oder VPN-Verkehr).
- **Rot-orange, gestrichelt:** Direkt von der nftables-Firewall blockiert.
- **Magenta-Pink:** An der Verbindung ist die TrutzBox selbst beteiligt, etwa ihre eigenen Dienste wie DNS, NTP oder der Mailserver. Auch kurzlebige Wartungsvorgänge erscheinen hier, etwa die regelmäßige DynDNS-Aktualisierung („TrutzBox DynDNS“). Diese Farbe hat Vorrang vor der Lane-Farbe.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Menüpfad: Monitor



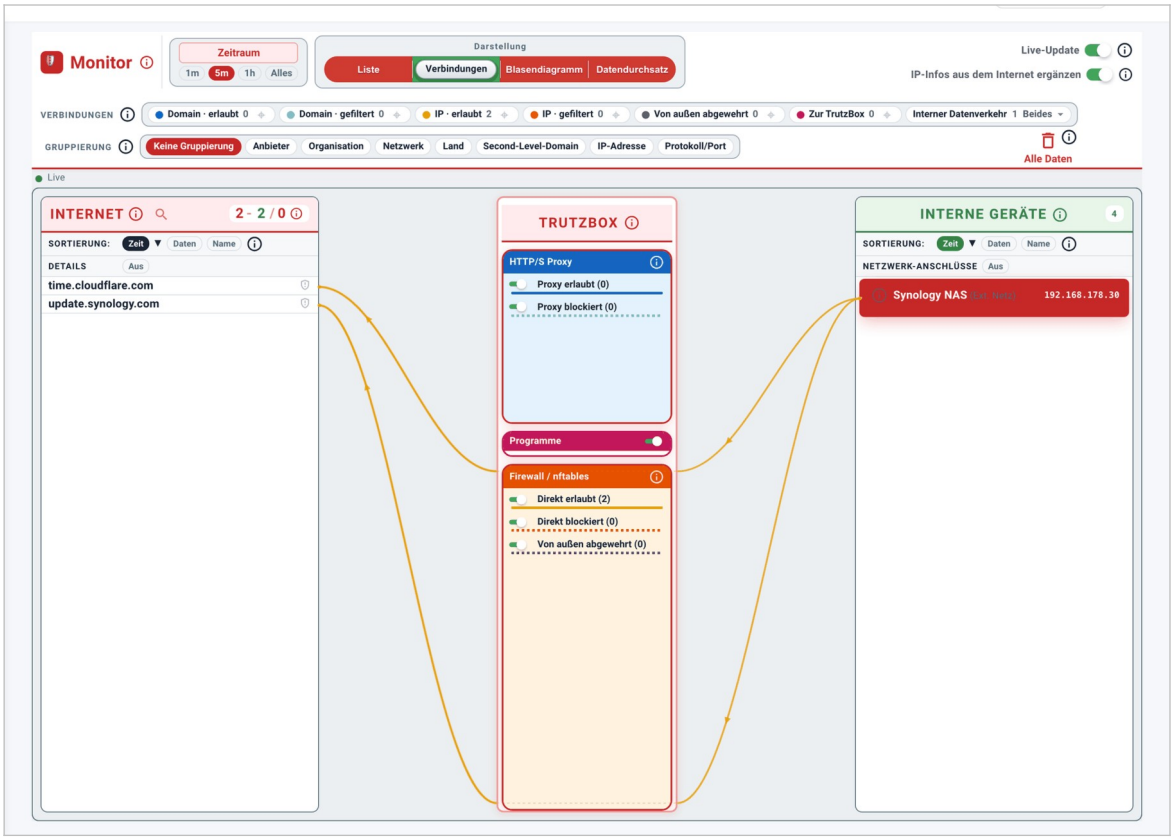
Darstellung „Verbindungen“ mit Gruppierung nach Land: links die Internet-Server, in der Mitte Proxy, Programme und Firewall der TrutzBox, rechts die internen Geräte.
(© 2026 Comidio GmbH)

Ein Mauszeiger über einer Verbindung blendet einen Tooltip mit Klartext-Erklärung ein („Eine Verbindung von … zu … wurde von … blockiert“), Schweregrad, WHOIS-Information des Zielservers und den Hinweis „Klick für Details“. Bei Verbindungen, die die TrutzBox selbst aufbaut, nennt der Tooltip zusätzlich den Zweck (etwa „Software-Updates“, „Zeitabgleich (NTP)“ oder „TrutzVPN-Einwahl“); die box-eigenen Programme erscheinen dabei unter verständlichen Namen, etwa „TrutzVPN“ statt openvpn oder „DNS-Server“ statt dnsmasq. Bei direkt blockierten Verbindungen zeigt der Tooltip außerdem die auslösende Firewall-Regel.

Die Anzeige lässt sich auf einzelne Verbindungstypen reduzieren: Die Beschriftungen in den Kästen „HTTP/S Proxy“ (Proxy erlaubt / Proxy blockiert) und „Firewall / nftables“ (Direkt erlaubt / Direkt blockiert / Von außen abgewehrt) sind anklickbar und blenden den jeweiligen Verbindungstyp ein oder aus. So lässt sich die Visualisierung z. B. auf reine Firewall-Blockierungen reduzieren. Die Magenta-Pink-Linien der TrutzBox-eigenen Programme blendet der separate Schalter „Programme“ ein und aus. Neben den Schaltern steht jeweils die Anzahl der zugehörigen Verbindungen in Klammern. Eine Bildschirmkopie dieser Darstellung findet sich am Kapitelanfang. Die Chip-Zeile „Verbindungen“ der Kopfleiste wird in dieser Darstellung nicht angezeigt; ihre Rolle übernehmen die genannten Schalter. Die Serverzeilen der Internet-Spalte sind kompakt gehalten; ein Schalter je Zeile klappt die Details auf (IP-Adresse, Port und übertragene Datenmenge). Je Ziel gibt es genau eine Sperr- oder Freigabe-Aktion.

Liegen auf derselben Adresse eine erlaubte und eine gesperrte Domain, wie es bei Google-Diensten häufig vorkommt, zeichnet der Monitor zwei getrennte Linien, eine grüne und eine rote, statt den Server pauschal rot einzufärben. Der Verkehr der TrutzBox selbst ist vom Geräteverkehr getrennt: Er trägt keinen Gerätenamen und lässt sich über die Chip-Leiste vollständig ausblenden.

Menüpfad: Monitor

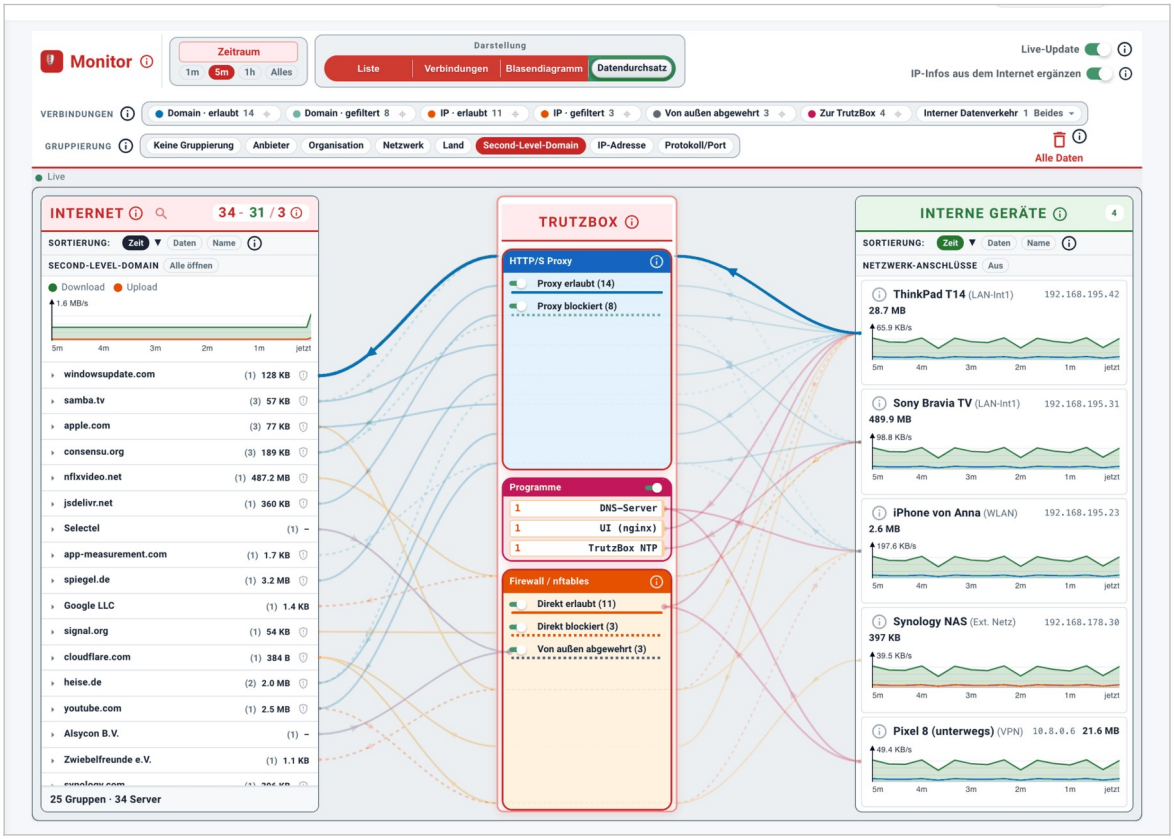


Verbindungen eines Geräts am externen Netz, das die TrutzBox als Proxy nutzt.
(© 2026 Comidio GmbH)

Datendurchsatz

Die Darstellung „Datendurchsatz“ rückt die übertragene Datenmenge in den Vordergrund. Für jede Servergruppe (links) und jedes Gerät (rechts) zeigt sie eine Verlaufsgrafik für Download und Upload über den gewählten Zeitraum sowie die aktuelle Bandbreite in KB/s. So lässt sich auf einen Blick erkennen, wer wann wie viel Datenverkehr verursacht. Das ist nützlich, um Geräte mit besonders hohem Datenverbrauch, unerwartete Cloud-Backups oder ungewöhnliche Aktivität außerhalb der Nutzungszeiten aufzuspüren. Auch diese Darstellung zeigt die Verbindungslinien und die mittlere TrutzBox-Spalte mit ihren Stationen (Proxy, interne Programme, Firewall), sodass gleichzeitig erkennbar ist, wie viel fließt und auf welchem Weg. Die kleinen Verlaufsdiagramme in den Gerätezeilen zeigen dabei fest die letzten fünf Minuten, unabhängig vom gewählten Anzeigezeitraum: In einem großen Zeitfenster wäre ein kurzer Übertragungsschub sonst unsichtbar. Das Summendiagramm der Internet-Spalte zählt nur den Verkehr der Geräte, nicht den, den die Box selbst verursacht (allen voran der geöffnete Monitor).

Menüpfad: Monitor



Die Darstellung „Datendurchsatz“ mit Verlaufsgrafik je Server und je Gerät.
(© 2026 Comidio GmbH)

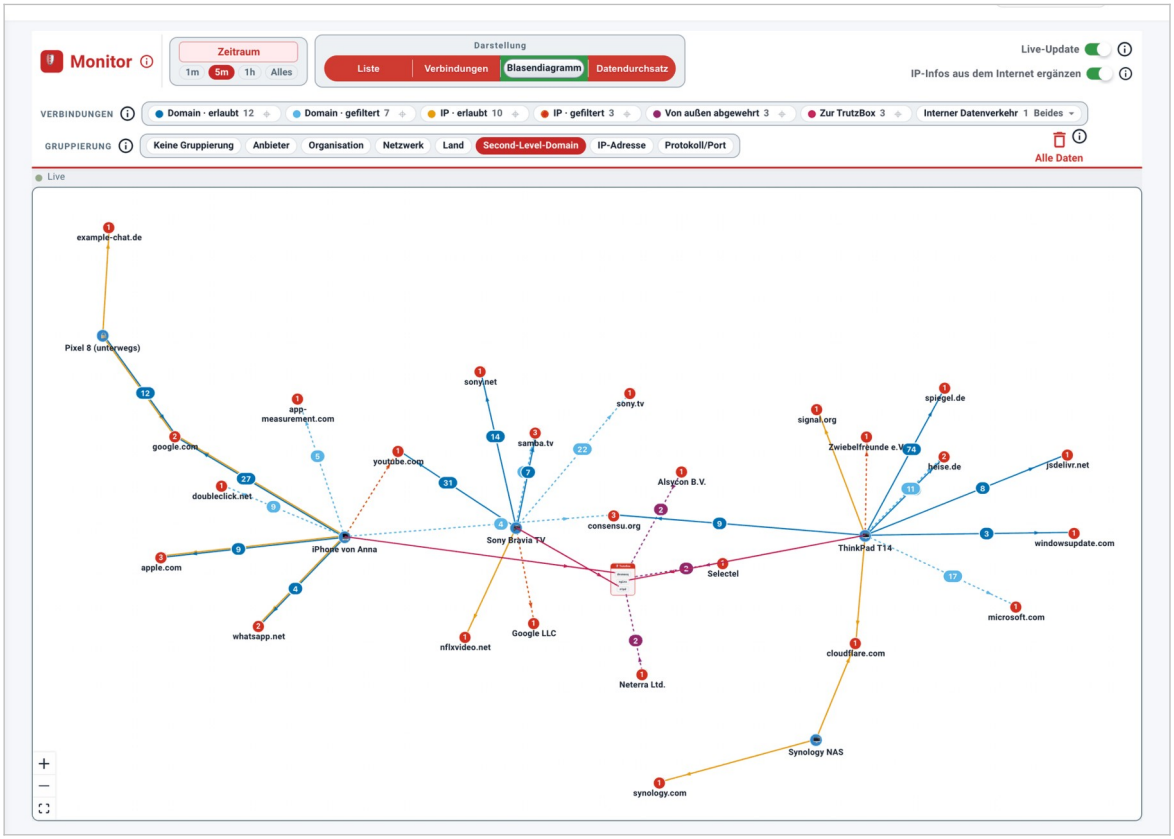
Blasendiagramm

Das „Blasendiagramm“ stellt die Verbindungen als Netzdiagramm dar:

- **Aufbau:** In der Mitte steht das jeweilige Gerät, von dem aus Linien zu den kontaktierten Zielen führen. Die Ziele sind je nach Gruppierung z. B. nach Land zusammengefasst, und eine Zahl an jeder Blase nennt die Anzahl der Verbindungen.
- **Einsatz:** Diese Sicht eignet sich besonders, um schnell zu erfassen, mit wie vielen und welchen Zielen ein einzelnes Gerät kommuniziert, und um Ausreißer (z. B. einen Smart-TV, der Verbindungen in viele verschiedene Länder aufbaut) sofort zu erkennen.
- **Linien:** Wiederholte Zugriffe auf dasselbe Ziel tragen einen Zähler an der Linie, und die Linienstärke richtet sich nach der Zahl der gezeichneten Linien.
- **Zoom:** Beim Zoomen behalten Blasen und Linien ihre Größe, und die Ansicht passt sich stets vollständig ins Fenster ein.
- **Zeitraum:** Wie die anderen Darstellungen lädt sie den gewählten Anzeigezeitraum und nicht nur den Live-Stand.

- **Hinweisfenster:** Im Hinweisfenster einer Blase steht der Servername aus der Verbindung selbst, auch wenn die Adresse sonst namenlos bliebe.

Menüpfad: Monitor



Das Blasendiagramm: Jede Blase ist ein Server, ihre Größe steht für die Datenmenge. (© 2026 Comidio GmbH)

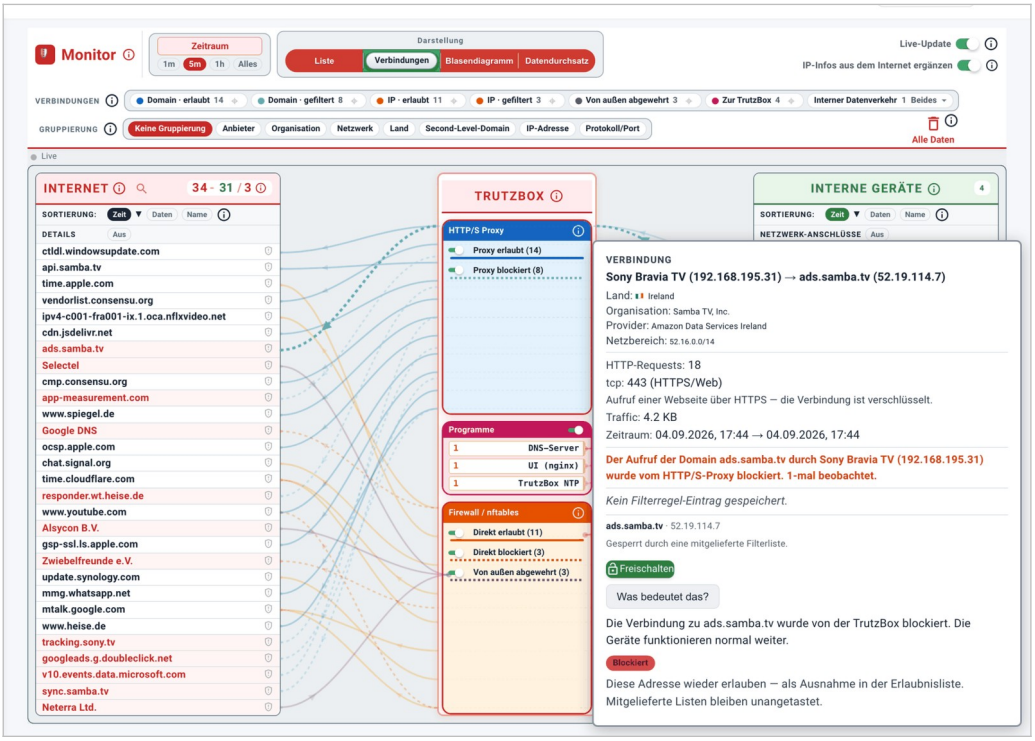
4.5 Warum wurde geblockt? Drilldown auf eine Verbindung

Klick auf eine blockierte Verbindung öffnet einen Detail-Dialog:

- **Zusammenfassung:** Der Dialog fasst in einem Satz zusammen, was passiert ist (z. B. „Eine Verbindung von 10.8.0.6 zu 35.241.186.140 wurde vom HTTP/S-Proxy blockiert“).
- **Technische Details:** Darunter stehen für Administratoren Quell- und Ziel-IP, Protokoll, Port, ausführende Filterregel sowie WHOIS-Informationen zum Zielserver inklusive Missbrauchskontakt.
- **Empfehlung:** Eine farblich abgesetzte Empfehlung weist auf die zugehörige Filterliste, Gruppe und Regel hin, sodass bei Bedarf direkt eine Ausnahme erstellt werden kann.
- **WHOIS:** Das ist das öffentliche Register der regionalen IP-Vergabestellen (etwa RIPE für Europa). Es nennt zu einer IP-Adresse den Betreiber, den zugehörigen Netzbereich und einen Missbrauchskontakt.

- **Passende Aktion:** Über „Was bedeutet das?“ bietet der Dialog bei Proxy-Verbindungen „Domain sperren“ bzw. „Domain erlauben“ an (wahlweise die ganze Domain oder nur die konkrete Adresse), bei direkten Verbindungen „IP blockieren“ (Eintrag in die IP-Blockliste). Der Dialog nennt dabei immer ausdrücklich die Adresse, die eingetragen wird.
- **Geteilte Server-IP:** Teilen sich mehrere Domains dieselbe Server-IP (häufig bei CDNs), listet das Server-Detail sie einzeln unter „Domains (N)“, jede mit eigener Bewertung („erlaubt“ oder „gesperrt“, zuletzt aktive zuerst).
- **Bewertung:** Eine Domain gilt nur dann als gesperrt, wenn jede Verbindung zu ihr blockiert wurde. Als Name der Verbindung zeigt der Monitor bevorzugt eine erlaubte Domain, damit ein einzelner gesperrter Mitbewohner den Server nicht falsch einfärbt.

Menüpfad: Monitor



Der Erklär-Dialog zu einer Verbindung nennt Grund und Filterregel der Sperre.
(© 2026 Comidio GmbH)

Bei DNS-Servern ergänzt das Detail die Zeile „DNS-Verschlüsselung“ (über TLS verschlüsselt, über HTTPS verschlüsselt oder unverschlüsselt über Port 53), sodass sich prüfen lässt, ob die eingestellte Verschlüsselung tatsächlich greift; eine vom Schutz vor DNS-Umgehung abgefangene Anfrage erscheint folgerichtig als Verbindung zur TrutzBox. Einzelheiten im Kapitel „DNS-Auflösung“. Zu jedem Port nennt das Detailfenster den zugehörigen Dienst und eine kurze Erklärung, wofür er üblicherweise verwendet wird; das gilt auch für die Ports, die die TrutzBox selbst bedient.
Für ein Gerät im eigenen Netz zeigt das Detailfenster zusätzlich, was die TrutzBox aus dessen DHCP-Anfrage ableitet:

- **Grundlage:** Jedes Gerät nennt beim Beziehen seiner IP-Adresse eine Herstellerklasse und eine Liste der Optionen, die es vom DHCP-Server wünscht. Diese Liste ist für eine Gerätefamilie recht typisch; daraus entstehen drei Angaben.
- **Gerätetyp:** Computer, Smartphone oder IoT-Gerät.
- **Betriebssystem:** Das vermutete System (Apple, Android, Windows oder Linux), nur wenn die Zuordnung eindeutig ist.
- **DHCP-Merkmale:** Kleine Kästchen (Chips), jeweils mit dem Nummerncode und einer Kurzbezeichnung wie „3 Router“ oder „162 Verschlüsseltes DNS“. Ein Mauszeiger über einem Chip nennt die vollständige Bezeichnung der Option.

Die Zeilen erscheinen nur, wenn zu dem Gerät eine ausgewertete DHCP-Anfrage vorliegt; sonst bleibt es bei Name und Hersteller.
Bei Internet-Servern kann die Herkunftsangabe trügen: Viele große Anbieter und Cloud-Dienste nutzen Anycast, das heißt, dieselbe IP-Adresse wird an vielen Orten der Welt zugleich bedient, und die Geodatenbank nennt dann irgendeinen davon. Solche Server kennzeichnet der Monitor: Das Land erscheint mit einem vorangestellten „≈“ als Näherung, Hinweistext und Detailfenster erklären den Vorbehalt, und bei einer Gruppierung nach Land stehen diese Server in einer eigenen Gruppe, ohne dass ihnen ein Land zugeschrieben wird. Dasselbe „≈“ steht vor einem Servernamen, den die Box nur aus ihrem Katalog erschlossen hat, damit eine Vermutung als solche erkennbar bleibt.

4.6 Wie der Monitor die Daten vorhält

Der Monitor sieht aus wie eine Live-Ansicht, ist aber eine Datenbank-Auswertung. Jede beobachtete Verbindung wird zunächst als einzelnes Ereignis in einer lokalen Datenbank auf der TrutzBox festgehalten (SQLite, eine Datei auf der SSD, kein Datenbank-Server). Das reicht für die Live-Sicht, wird aber schnell unhandlich: Ein einziges gesprächiges Gerät erzeugt in wenigen Stunden Hunderttausende Zeilen.
Deshalb verdichtet die TrutzBox die Aufzeichnung fortlaufend zu Minutenwerten: Alle Ereignisse derselben Verbindung innerhalb einer Minute werden zu einer Zeile mit Zähler und Datenmenge zusammengefasst, die Einzelzeilen entfallen. Der Abruf eines Zeitfensters greift danach auf diese Minutenwerte zu und dauert Sekundenbruchteile statt mehrerer Sekunden. Der frei gewordene Platz wird an das Dateisystem zurückgegeben, die Datenbank schrumpft dadurch auf einen Bruchteil ihrer früheren Größe. Anwesenheit und Datenmengen der Geräte berechnet die Box exakt für den gewählten Zeitraum, nicht als grobe Hochrechnung.
Eine zweite Vorkehrung betrifft den Sitzungsspeicher, in dem die Detaildaten der Proxy-Verbindungen liegen. Jedes Gerät hat dort seinen eigenen Rahmen, damit ein einzelnes Gerät, etwa ein Fernseher, der im Sekundentakt dieselbe gesperrte Adresse erneut versucht, den gespeicherten Verlauf der anderen Geräte nicht verdrängen kann; ständige Wiederholungen desselben Ziels werden zu einem Eintrag mit Zähler zusammengefasst statt einzeln abgelegt.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

> **Technischer Hintergrund:** Die Datenbanken der Box laufen im WAL-Modus von SQLite. Schreiben und Lesen behindern sich dadurch nicht gegenseitig: Der Monitor kann eine laufende Aufzeichnung auswerten, während im selben Moment neue Ereignisse hineinlaufen. Das gilt für die Verkehrsdaten des Monitors, für das Zugriffsprotokoll des Proxys und für den Sitzungsspeicher.

Für die Firewall gilt dasselbe Prinzip an anderer Stelle: Abgewehrte Zugriffe aus dem Internet werden nicht unbegrenzt einzeln protokolliert, sondern je Absender begrenzt mitgeschrieben. Die Abwehr selbst arbeitet davon unberührt vollständig, jedes einzelne Paket wird weiterhin blockiert. Nur das Protokollieren ist gedrosselt, damit eine Angriffsflut nicht die Box selbst ausbremst und den Speicher füllt. Die im Ereignis-Dialog genannte Zahl ist deshalb die Zahl der protokollierten Abweisungen und nicht die Zahl aller abgewehrten Pakete; die Oberfläche weist auch darauf hin.

> **Technischer Hintergrund:** Aufgezeichnet wird in zwei Takten: Die Zähler der Netzwerk-Anschlüsse liest die Box jede Sekunde, die Verbindungsverfolgung des Kernels alle fünf Sekunden. Firewall-Ereignisse folgen keinem Takt, sie werden gemeldet, sobald sie anfallen. Deshalb laufen sie auch dann mit, wenn niemand den Monitor geöffnet hat, während die beiden Takte nur bei geöffneter Ansicht arbeiten.
>
> Die Speicherdauer des Monitors wirkt über den Monitor hinaus: Zugriffsprotokoll und Firewall-Protokoll werden mindestens so lange aufbewahrt wie die Monitor-Daten. Die Box bildet dafür das Maximum aus dem eigenen Wert des jeweiligen Protokolls und der eingestellten Speicherdauer. Ist die Speicherdauer auf „Aus“ gestellt, gelten wieder allein die eigenen Werte der Protokolle.
>
> Der graue Punkt „Interner Datenverkehr“ in der Chip-Zeile steuert nur die Anzeige. Mitgeschrieben wird interner Verkehr immer, solange der Monitor geöffnet ist, genau wie die übrigen Verbindungsarten; nach dem Einblenden stehen deshalb auch die Verbindungen aus der Vergangenheit da, soweit die Speicherdauer sie noch vorhält. Das dreistufige Menü früherer Fassungen („Ohne intern“, „Nur intern“, „Beides“) gibt es seit Oktober 2026 nicht mehr.
>
> Auch ohne geöffneten Monitor läuft ein langsamer Aufräum-Takt von fünf Minuten weiter. Er verdichtet die Zeitreihen und setzt die Aufbewahrung durch. Ohne ihn würde das Firewall-Protokoll unbegrenzt wachsen, weil seine Einträge unabhängig von der Anzeige entstehen.

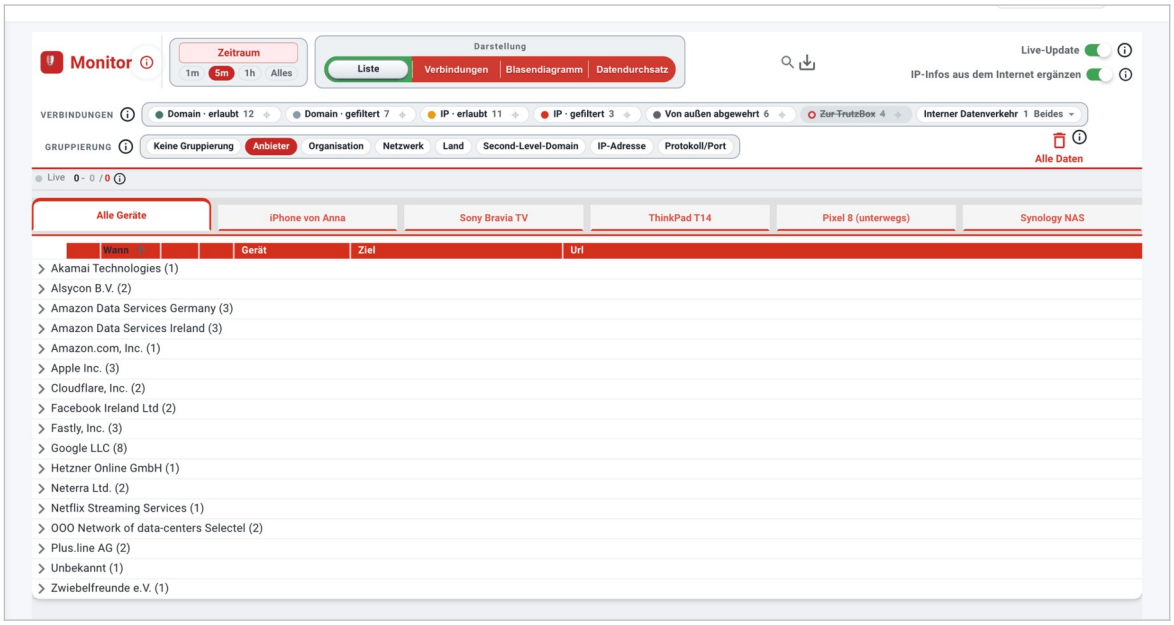
4.7 Server gruppieren: von Anbieter bis Protokoll/Port

Die Internet-Server lassen sich nach mehreren Kriterien gruppieren. Die Auswahl erfolgt über die Chip-Zeile „Gruppierung“ und wirkt in allen Darstellungen: in der Liste als aufklappbare Gruppenzeilen, im Blasendiagramm als zusammengefasste Blasen, in der Darstellung „Verbindungen“ als Gruppen in der Internet-Spalte. Die Zahl neben einer Gruppe nennt, wie viele Einträge sie zusammenfasst; „Alle öffnen“ und „Alle schließen“ klappen alle Gruppen auf einmal. Gezählt wird je IP-Adresse: Ein Anbieter wie apple.com hat viele Adressen und erscheint dann mehrfach. Zur Wahl stehen:

- **Keine Gruppierung:** jeder Server einzeln, sortiert nach Zeit oder Datenmenge.

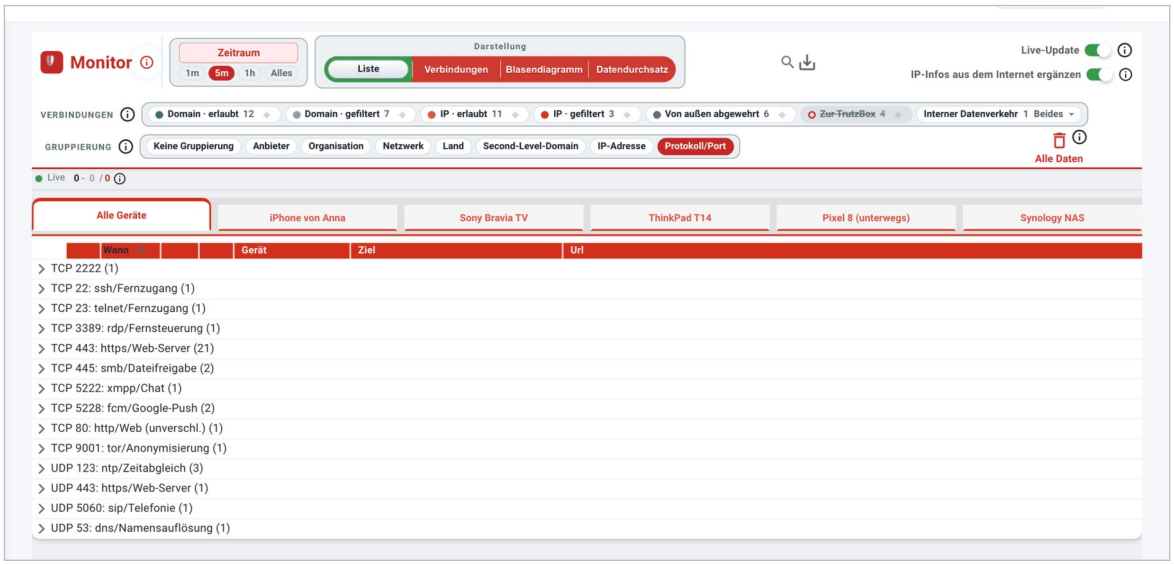
- **Anbieter:** der Netzbetreiber hinter der IP-Adresse (z. B. Google, Amazon, Microsoft, Akamai), meist die hilfreichste Sicht, weil die Namen vertraut sind.
- **Organisation:** die im Registrierungsdienst eingetragene Organisation, die den Adressbereich nutzt; sie kann vom Anbieter abweichen, etwa bei einem Dienst, der in einer fremden Cloud läuft.
- **Netzwerk:** der IP-Netzbereich, gedacht für Administratoren, die Verbindungen einer Adressblock-Klasse bündeln möchten.
- **Land:** die geografische Verteilung, hilfreich, um ungewöhnliche Verbindungsziele zu erkennen. Server großer Cloud-Anbieter mit weltweit gleicher Adresse (Anycast) erscheinen in der Gruppe „Cloud/Anycast (kein Land)“ und tragen ein „≈“ statt einer Landesbehauptung.
- **Second-Level-Domain:** fasst nach der Domain zusammen (z. B. google.com, meta.com) und liefert ohne Registrierungsabfrage sofort erkennbare Gruppen. Lässt sich zu einem Server keine Domain ermitteln (nackte IP-Adresse), gruppiert die TrutzBox ihn ersatzweise nach der Organisation, statt ihn pauschal unter „Unbekannt“ einzuordnen.
- **IP-Adresse:** fasst alle Zeilen derselben Adresse zusammen, auch wenn dahinter verschiedene Domain-Namen stehen.
- **Protokoll/Port:** gruppiert nach Übertragungsweg, etwa TCP 443 (HTTPS), UDP 443 (QUIC), TCP 5228 (Google-Push) oder UDP 123 (Zeitabgleich). So wird auf einen Blick sichtbar, welcher Verkehr am Web-Filter vorbeiläuft.

Menüpfad: Monitor



Gruppierung „Anbieter“: Die Liste fasst die Ziele nach dem Netzbetreiber zusammen, die Zahl in Klammern nennt die Einträge je Gruppe.
(© 2026 Comidio GmbH)

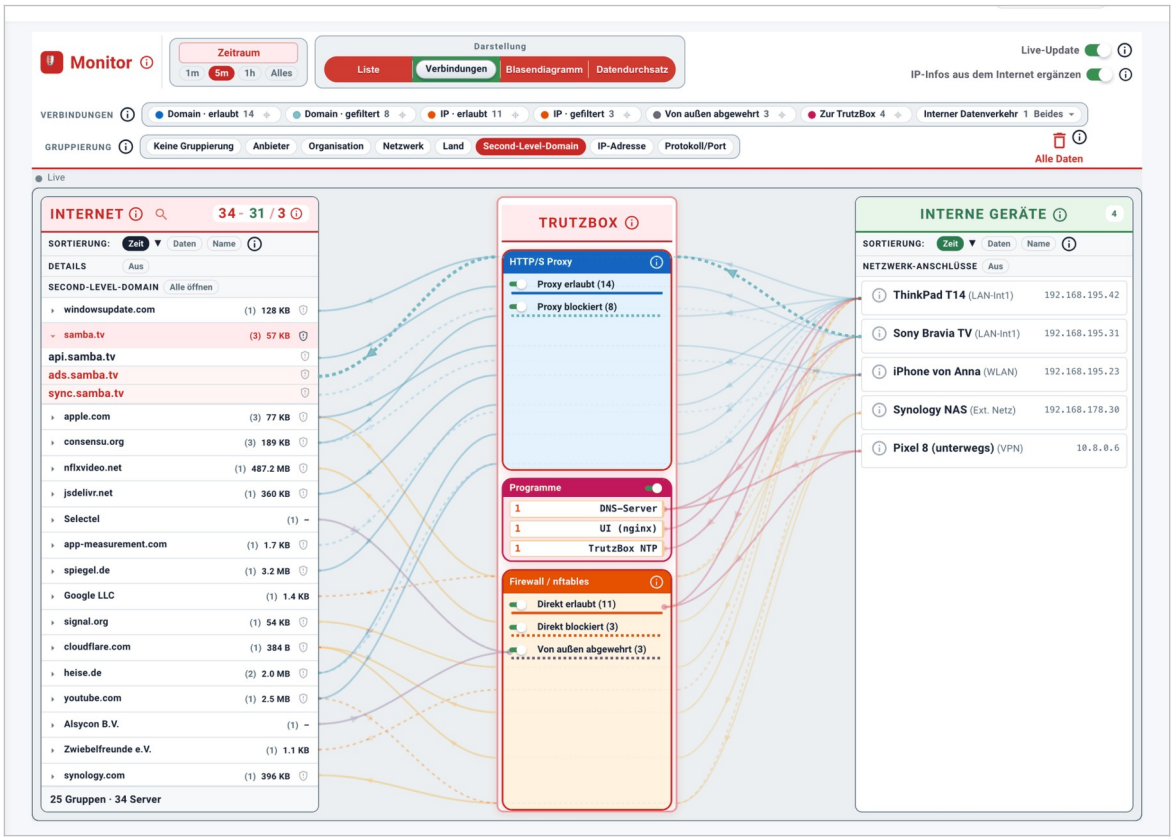
Menüpfad: Monitor



Gruppierung „Protokoll/Port“: UDP 443 (QUIC), TCP 5228 (Google-Push) und UDP 123 (Zeitabgleich) zeigen, welcher Verkehr am Web-Filter vorbeiläuft.
(© 2026 Comidio GmbH)

Die Bildschirmkopie unten zeigt die Gruppierung nach Second-Level-Domain in der Ansicht „Verbindungen“. Im Netz ist nur ein einziges Gerät aktiv, ein Sony-Smart-TV, sodass gut erkennbar ist, mit welchen Servern allein dieser Fernseher Verbindungen aufbaut. Die aufgeklappte Gruppe „samba.tv“ macht die einzelnen Server mit ihren IP-Adressen sichtbar: Dorthin meldet der Fernseher Erkennungsdaten zum laufenden Bildschirminhalt, sofern die ACR-Funktion (automatische Bild-Erkennung) im Gerät aktiviert ist. Die blauen Linien sind Verbindungen über den TrutzContent-Proxy, die orangefarbenen Linien direkte (nur an der Firewall behandelte) Verbindungen; gestrichelte Linien stehen für Blockierungen. Die linke Spalte listet die kontaktierten Domains mit der jeweiligen Anzahl erkannter Server.

Menüpfad: Monitor

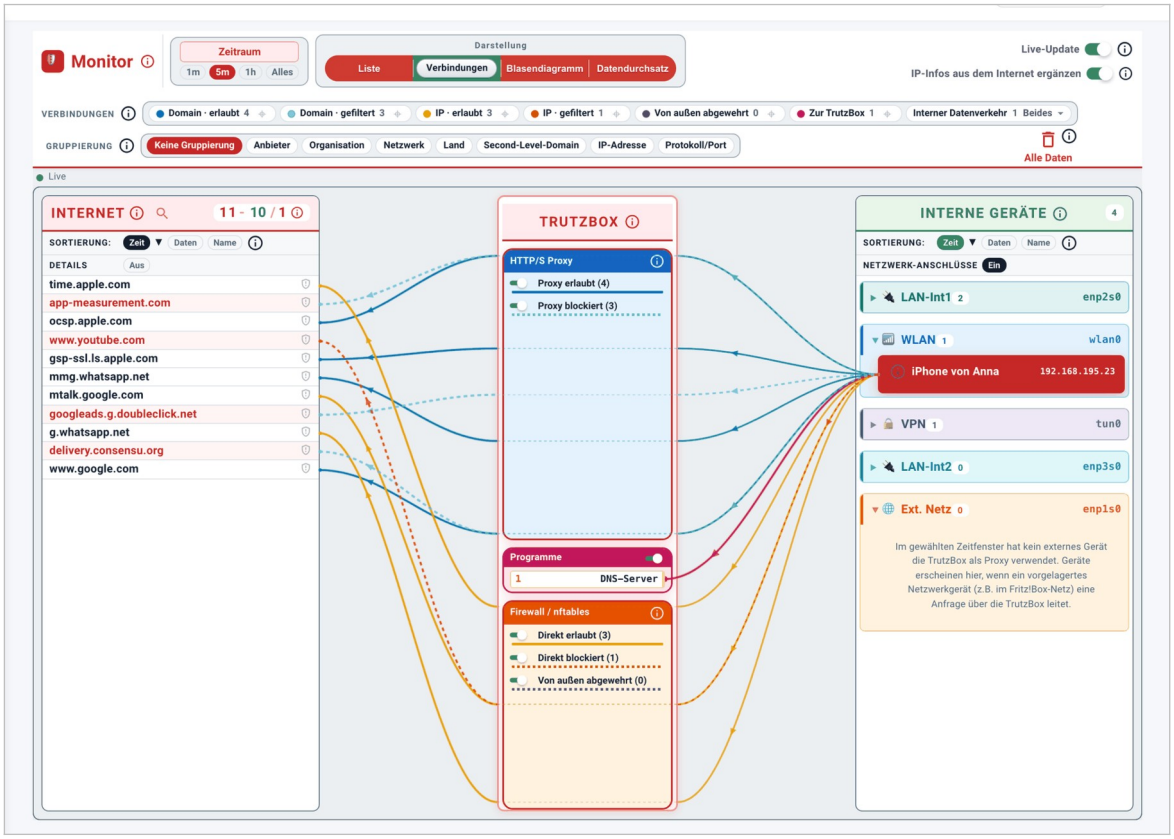


Gruppierung nach Second-Level-Domain: Nur ein Fernseher ist aktiv, seine Ziele sind gut erkennbar. (© 2026 Comidio GmbH)

Anwendungstipp: Um zu erkennen, welche Konzerne hinter den Verbindungen stehen, sind die Gruppierungen nach Second-Level-Domain und nach Anbieter aufschlussreich, da viele Server einer einzelnen Webseite über mehrere Cloud-Provider verteilt sind.

Beispiel: Verkehr am Proxy vorbei, ohne QUIC-Sperre. Diese Bildschirmkopie zeigt ein iPhone im WLAN. Der HTTP/S-Proxy ist hier abgeschaltet, sodass nur der direkt durch die Firewall geführte Verkehr sichtbar ist (orange Linien). Auffällig: Fast alle Verbindungen laufen über UDP 443, also über QUIC, und damit am Web-Filter vorbei direkt ins Internet (u. a. zu Apples „Private Relay“ und zu Google). Der Schalter „QUIC sperren“ schließt diesen Weg, sodass die Geräte auf das filterbare TCP 443 zurückfallen; Einzelheiten im Kapitel „IP-Blocklisten-Verwaltung“.

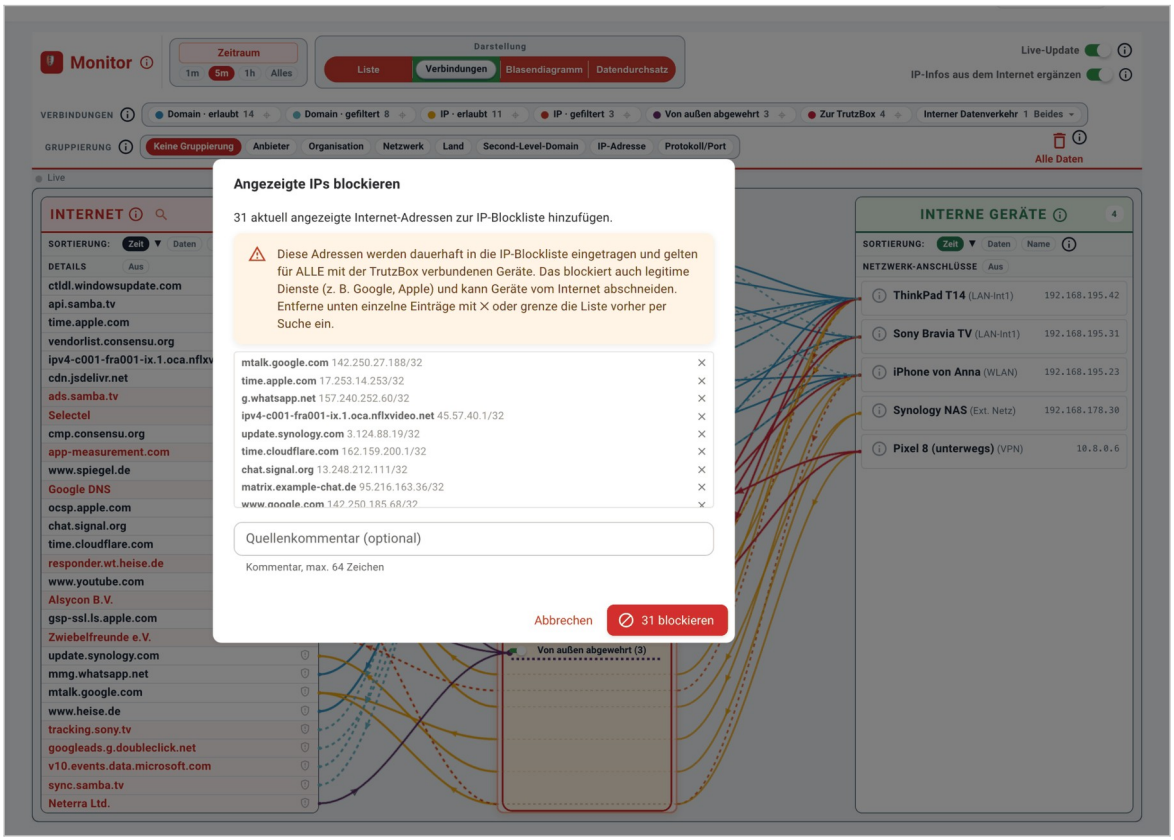
Menüpfad: Monitor



Verkehr am Proxy vorbei: Ohne QUIC-Sperre laufen fast alle Verbindungen über UDP 443. (© 2026 Comidio GmbH)

Beispiel: Angezeigte IPs gesammelt blockieren. Auch ein Sony-Fernseher erreicht Google-Dienste direkt am Proxy vorbei, hier über TCP 5228 (Google-Push) und QUIC (UDP 443). Die Zahlenangabe über der Internet-Liste (im Beispiel „10“ und daneben „10 / 0“) bedeutet: 10 angezeigte Server, davon 10 durchgelassen (grün) und 0 blockiert (rot). Ein Klick auf die grüne Zahl öffnet den Dialog „Angezeigte IPs blockieren“, mit dem sich alle gerade angezeigten Adressen dauerhaft in die IP-Blockliste übernehmen lassen. Achtung: Die Sperre gilt für ALLE Geräte und kann auch legitime Dienste (z. B. Google, Apple) treffen. Einzelne Einträge lassen sich vorher mit × entfernen.

Menüpfad: Monitor



Der Dialog „Angezeigte IPs blockieren“ übernimmt alle gerade sichtbaren Adressen in die Blockliste. (© 2026 Comidio GmbH)

4.8 Sperren und Freischalten direkt aus dem Monitor

Jede Ansicht des Monitors ist zugleich Bedienoberfläche für die Sperrlisten. Über das Schild-Symbol in der Internet-Spalte, in der Blasen-Ansicht, in der Liste, im Detailfenster und im Verbindungs-Hinweis lässt sich ein Ziel unmittelbar sperren oder freischalten, ohne den Umweg über die Filterlisten-Verwaltung.
Angeboten wird dabei nur, was im jeweiligen Zustand sinnvoll ist:

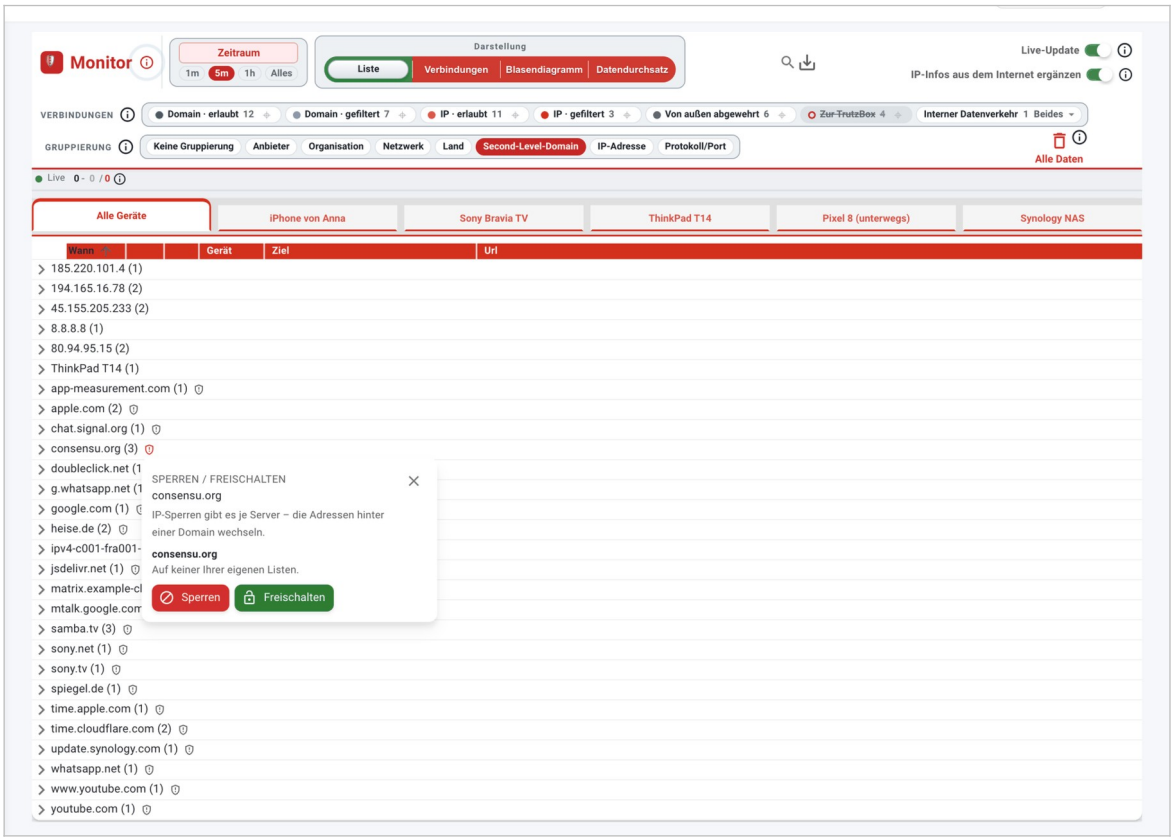
- **Freischalten und Sperren:** Freischalten erscheint ausschließlich bei bereits gesperrten Zielen, Sperren ausschließlich bei erlaubten.
- **Aktueller Zustand:** Das Menü nennt zuerst den Zustand des Ziels, getrennt nach Ebene: ob es auf einer eigenen Sperr- oder Erlaubnisliste des Web-Filters steht, ob es dort nur als Tracker gesperrt ist und ob die Firewall es sperrt oder eine Ausnahme dafür führt.
- **Wirkung des Knopfs:** Darunter steht in einem Satz, was der Knopf bewirken wird, etwa dass die Domain im Web-Filter für alle Geräte über den Proxy gesperrt wird oder dass für eine Adresse eine Firewall-Ausnahme angelegt wird, während die IP-Blockliste unverändert bleibt.

- **Was sperren:** Beim Sperren einer Domain fragt der Dialog unter „Was sperren?“, ob die ganze Domain oder nur diese Adresse gemeint ist.
- **Nur als Tracker:** Ein eigener Knopf sperrt eine Domain nur als Tracker. Sie wird dann nur noch als Folgeaufruf einer anderen Seite abgewiesen, der direkte Aufruf bleibt erlaubt.
- **Firewall-Sperre:** Über „Erweitert: Firewall“ lässt sich die Sperre zusätzlich auf genau die eine IP-Adresse legen, was auch Geräte trifft, die gar nicht über den Proxy laufen.
- **Sperre und Freigabe zurücknehmen:** Steht ein Ziel bereits auf einer eigenen Liste, bietet das Menü den umgekehrten Weg an: „Sperre aufheben“ nimmt den Eintrag aus der eigenen Sperrliste, „Freigabe aufheben“ aus der Erlaubnisliste, wodurch die mitgelieferten Sperrlisten wieder greifen, und „Tracker-Sperre aufheben“ entfernt ihn aus der TrutzBrowse-Sperrliste.
- **Blockliste der Firewall:** Ist zu einem Ziel eine IP-Adresse bekannt, führt das Detailfenster zusätzlich den Bereich „Blockliste“. Dort sperrt „Zur Blockliste hinzufügen“ die Adresse auf Netzwerkebene, „Aus Blockliste entfernen“ gibt sie wieder frei; ein Feld nimmt einen Quellenkommentar auf, damit später nachvollziehbar bleibt, warum der Eintrag entstanden ist.
- **Nur diese Adresse freigeben:** Ist eine Adresse nicht einzeln, sondern über einen importierten Bereich gesperrt, bietet die TrutzBox „Nur diese Adresse freigeben“ an und legt dafür eine Firewall-Ausnahme an. Der Bereich bleibt für alle übrigen Adressen gesperrt. Die Ausnahme hebt allein die IP-Blockliste auf; Inhaltsfilter, QUIC-Sperre und die übrigen Firewall-Regeln gelten weiter.

Ein Eintrag landet je nach Wahl in der Standard-TrutzContent-Blockliste oder in der zugehörigen Ausnahmeliste. Steht eine Domain bereits auf einer eigenen Erlaubnisliste, wäre ein zusätzlicher Sperreintrag wirkungslos; die TrutzBox nennt diese Freigabe deshalb beim Namen und bietet an, sie aufzuheben. Nach dem Freischalten einer Domain bietet sie zudem die passende Firewall-Ausnahme an, falls die IP-Blockliste deren Adressen noch sperrt (Einzelheiten im Kapitel „Eigene Sperren und Ausnahmen“).

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Menüpfad: Monitor



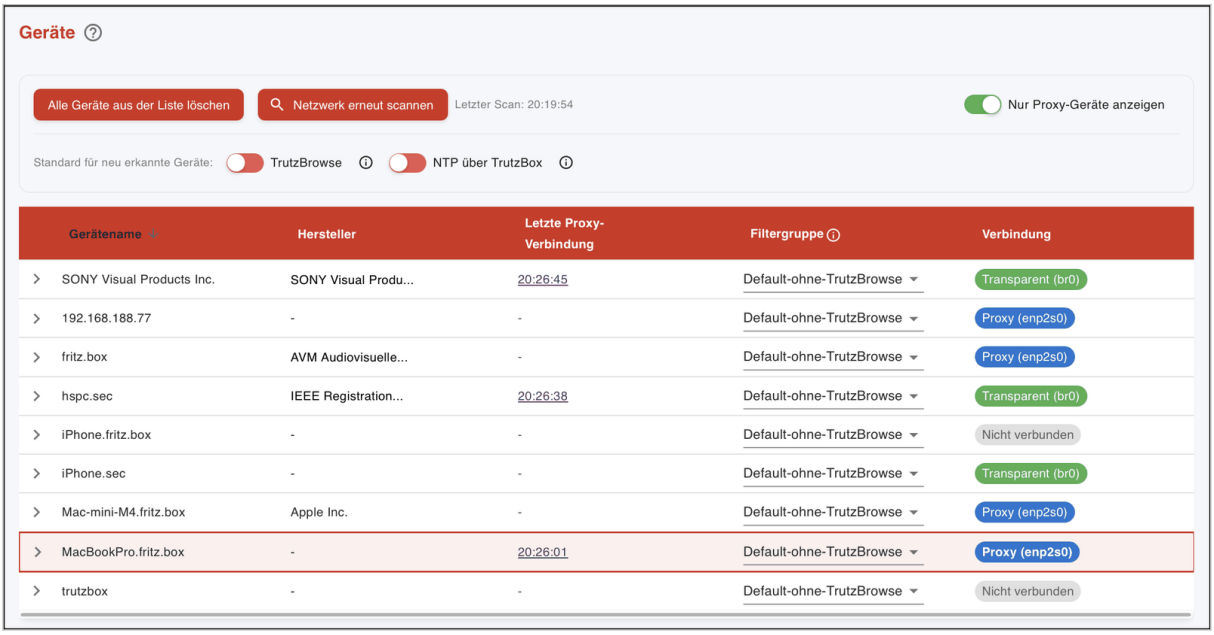
Das Menü „Sperren / Freischalten“ am Schild-Symbol einer Gruppe in der Liste. (© 2026 Comidio GmbH)

5 Geräte

5.1 Geräte-Übersicht

In der Geräte-Verwaltung werden automatisch alle erkannten Geräte aufgelistet. Jedem Gerät ist eine TrutzContent-Filtergruppe zugeordnet. Die TrutzBox identifiziert Geräte anhand ihrer MAC-Adresse; falls diese nicht ermittelt werden kann, wird der Hostname oder die IP-Adresse verwendet. Geräte, die hinter einem weiteren Router liegen und deshalb keine eigene MAC-Adresse zeigen (zum Beispiel VPN-Teilnehmer einer FRITZ!Box), werden über ihre Adresse geführt: Ein hier vergebener Name wird zu dieser Adresse gespeichert und erscheint sofort in der Geräteliste und im Monitor.
Vor allen Einstellungen steht die Frage, welchen Weg der Verkehr eines Geräts überhaupt nimmt. Die Spalte „Verbindung" nennt die beiden Fälle beim Namen. „Transparent" heißt: Das Gerät hängt am internen Netz der TrutzBox, an ihrem WLAN oder am VPN-Zugang. Sein gesamter Verkehr läuft durch die Box und wird gefiltert, ohne dass am Gerät etwas einzustellen wäre. „Proxy" heißt: Das Gerät steht am externen Anschluss, meist am Internet-Router, und spricht die TrutzBox ausdrücklich als Proxy an. Gefiltert wird dann nur, was es über diesen Proxy schickt; alles andere geht am Filter vorbei. In Klammern steht, über welches Netz die Verbindung gerade läuft: intern, extern, WLAN oder VPN.
Für die Praxis heißt das: Filtergruppe, TrutzBrowse, Zeitsteuerung und die übrigen Einstellungen dieser Seite lassen sich jedem Gerät zuordnen, sie wirken aber nur auf den Verkehr, der tatsächlich über die TrutzBox läuft. Bei einem Gerät hinter der Box ist das alles. Bei einem Gerät am externen Anschluss ist es nur der Teil, den das Gerät über den Proxy schickt. Wer eine lückenlose Filterung will, hängt das Gerät hinter die TrutzBox.

Menüpfad: Verwaltung → Geräte



Die Geräte-Übersicht mit Name, Hersteller, Filtergruppe und Verbindungsart je Gerät.
(© 2026 Comidio GmbH)

Die Geräteliste bietet folgende Funktionen und Informationen:

- **Alle Geräte aus der Liste löschen:** Löscht alle gespeicherten Gerätekonfigurationen und liest die Geräteliste neu ein. Achtung: Alle manuell vorgenommenen Einstellungen (Filtergruppe, Name, Proxy-Einstellungen) gehen dabei verloren und müssen neu vorgenommen werden.
- **Netzwerk erneut scannen:** Liest die Geräteliste neu ein, ohne gespeicherte Einstellungen zu löschen. Ein solcher Scan läuft auch automatisch beim Öffnen der Seite; der Zeitpunkt des letzten Scans wird angezeigt.
- **Standardmäßig TrutzBrowse aktivieren:** Legt fest, ob für neu erkannte Geräte TrutzBrowse automatisch aktiviert wird. Im öffentlichen Raum (z.B. Krankenhaus, Seniorenheim oder öffentliches WLAN) sollte die Option aus sein, weil dort kein TrutzBox-Stammzertifikat auf die Endgeräte kommt (Einzelheiten im Kapitel „Verschlüsselte (SSL/TLS)-Verbindungen“).
- **Standardmäßig „NTP über TrutzBox“ aktivieren:** Legt fest, ob neu erkannte Geräte ihre Uhrzeit automatisch von der TrutzBox beziehen (siehe „NTP über TrutzBox leiten“). Beide Standard-Schalter wirken nur auf das jeweils nächste neu erkannte Gerät; bereits konfigurierte Geräte bleiben unverändert.
- **Nur Proxy-Geräte:** Wenn dieser Schalter aktiviert ist, werden nur Geräte angezeigt, die über den Proxy (externes Interface) verbunden sind. Der Schalter ist standardmäßig aktiv.
- **Erweiterte Ansicht:** Blendet zusätzlich die IP-Adresse und die MAC-Adresse jedes Geräts ein. Für den Alltag ist die schmale Ansicht übersichtlicher, für die Fehlersuche sind die Adressen nützlich.
- **Standard für neu erkannte Geräte:** Zwei Schalter über der Liste legen fest, womit ein Gerät startet, das die TrutzBox zum ersten Mal sieht: „TrutzBrowse bei neu erkannten Geräten aktivieren“ und „NTP über TrutzBox bei neu erkannten Geräten leiten“. Bereits bekannte Geräte behalten ihre eigene Einstellung, die Vorgabe wirkt nur auf neu hinzukommende.
- **Spalte „Letzte Proxy-Verbindung“:** Wenn Verbindungsdaten gespeichert sind, erscheint hier ein Link, der direkt zur Monitor-Liste des Geräts führt.
- **Spalte „Hersteller“:** Zeigt den anhand der MAC-Adresse ermittelten Geräte-Hersteller. Bei Geräten mit zufällig vergebener (privater) MAC-Adresse weist die TrutzBox darauf hin, dass keine eindeutige Hersteller-Zuordnung möglich ist.
- **Spalte „TrutzBrowse“:** Zeigt an, ob TrutzBrowse für dieses Gerät aktiv ist. Bei IoT-Geräten (z. B. Smart-TV), auf denen kein TrutzBox-Zertifikat installiert werden kann, sollte TrutzBrowse deaktiviert sein.
- **Spalte „Filtergruppe“:** Zeigt die zugewiesene TrutzContent-Filtergruppe. Über das Dropdown kann die Gruppe direkt in der Liste geändert werden.
- **Spalte „Verbindung“:** Zeigt den Verbindungstyp des Geräts: grüne Markierung „Transparent“ = über das interne Netzwerk-Interface verbunden (LAN-Int, WLAN oder VPN); blaue Markierung

„Proxy“ = über das externe Netzwerk-Interface per Proxy verbunden; „Nicht verbunden“ = Gerät war früher bekannt, ist aktuell nicht verbunden. In Klammern nennt die Markierung zusätzlich den tatsächlichen Schnittstellennamen (z. B. „Proxy (enp2s0)“).

- **Verkehrsdaten eines Geräts löschen:** Über das Mülleimer-Symbol in der Gerätezeile lassen sich die aufgezeichneten Verkehrsdaten genau dieses Geräts entfernen, ohne die Aufzeichnung aller anderen Geräte anzutasten. Gelöscht wird alles, was zum Gerät gehört, einschließlich seiner Firewall-Einträge. Der Vorgang zeigt einen Fortschritt und meldet zum Schluss, wie viel gelöscht wurde oder woran es gescheitert ist.
- **Sortierung:** Das Gerät, an dem der Administrator gerade sitzt, steht in der Liste zuerst, bis er selbst eine andere Sortierung wählt.

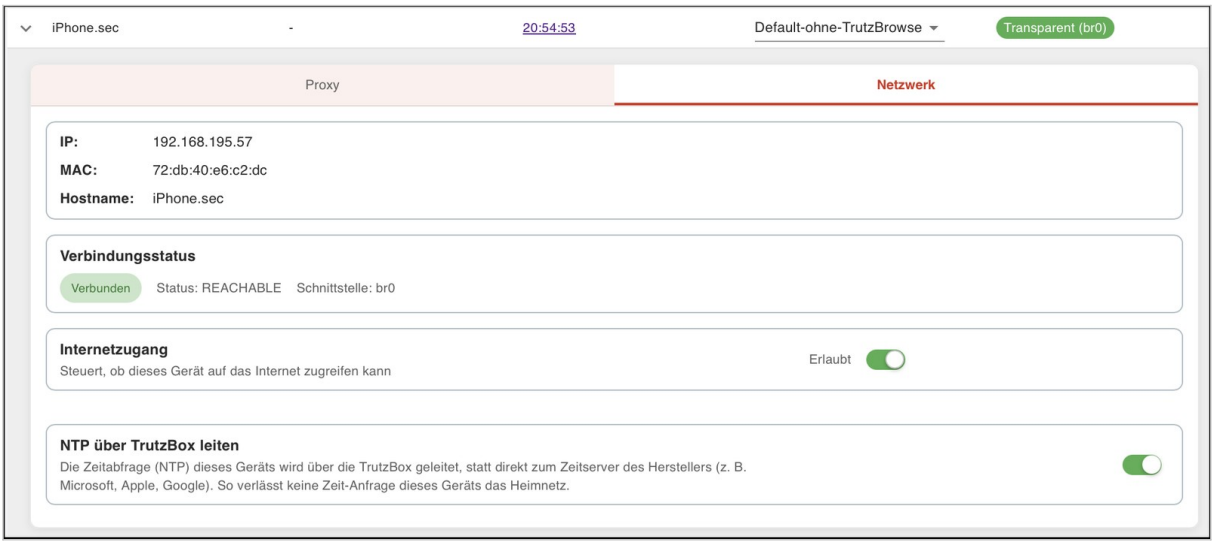
5.2 Geräte-Detaileinstellungen

Per Klick auf den Pfeil „>“ links vor dem Gerätenamen öffnen sich die Detail-Einstellungen des Geräts. Die Ansicht ist in zwei Tabs unterteilt: zuerst „Proxy“, danach „Netzwerk“.
Die beiden Tabs trennen zwei Ebenen. Der Tab „Netzwerk“ zeigt, was die TrutzBox über den Netzwerkanschluss des Geräts weiß, und steuert, was sie dort durchsetzen kann: Adressen, Verbindungsstatus, Internetzugang und Zeitabgleich. Diese Einstellungen wirken für jedes Gerät im Netz, auch für eines, das den Web-Filter gar nicht nutzt, denn die TrutzBox setzt sie in der Firewall und über ihre eigenen Dienste durch. Der Tab „Proxy“ enthält die Einstellungen für den Web-Verkehr, den das Gerät über die TrutzBox schickt: Filterausnahmen, TrutzBrowse, Gerätetyp und SecuritySlider. Sie greifen nur, solange der Verkehr des Geräts tatsächlich über den HTTP/S-Proxy läuft. Bei einem reinen Netzwerkgerät, etwa einem Drucker oder einer Überwachungskamera ohne Proxy-Verbindung, steht an dieser Stelle der Hinweis „Dies ist ein reines Netzwerkgerät. Proxy-Einstellungen sind nicht verfügbar.“

Tab „Netzwerk“:

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Menüpfad: Verwaltung → Geräte

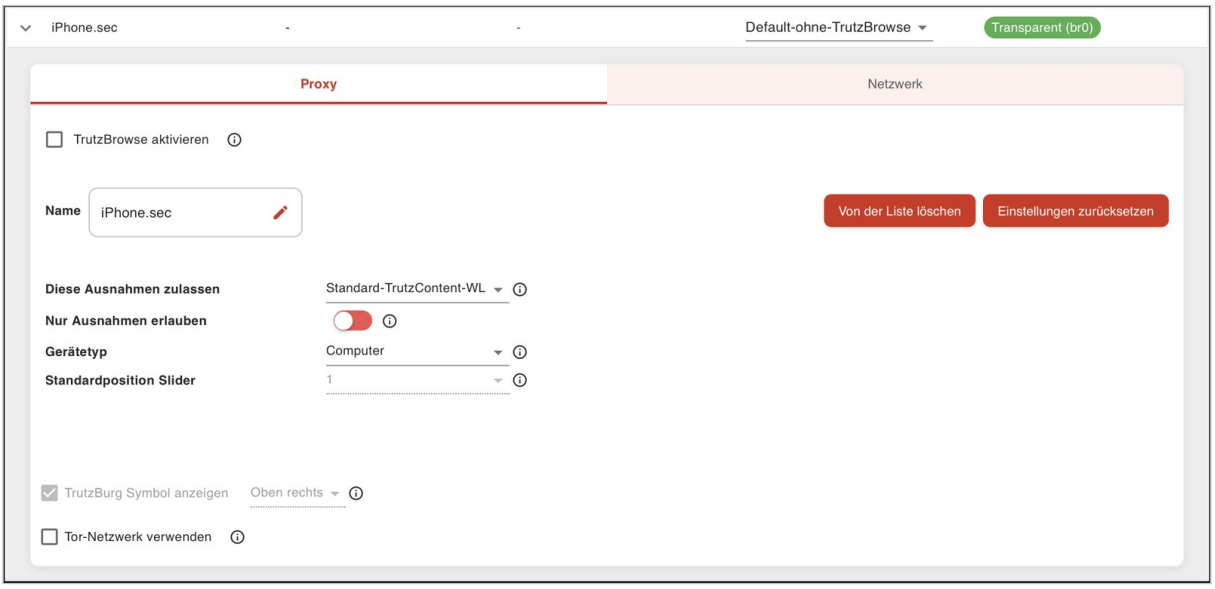


Geräte-Detail, Tab „Netzwerk“: Adressen, Verbindungsstatus, Internetzugang und Zeitabgleich. (© 2026 Comidio GmbH)

- **IP, MAC, Hostname:** Zeigt die aktuellen Netzwerkidentifikatoren des Geräts.
- **Verbindungsstatus:** Zeigt ob das Gerät gerade verbunden ist, den REACHABLE-Status und die Schnittstelle (z. B. enp2s0 für das externe Interface).
- **Internetzugang:** Steuert, ob dieses Gerät überhaupt auf das Internet zugreifen darf. Standard: „Erlaubt“. Wird der Zugang entzogen, sperrt die TrutzBox das Gerät direkt an der Firewall (anhand seiner MAC-Adresse) und kappt zusätzlich bereits laufende Verbindungen sofort; die Sperre wirkt also nicht erst beim nächsten Verbindungsaufbau. Dieser Schalter läuft bewusst über einen eigenen Weg (nicht über die Proxy-Konfiguration), damit ein getrenntes Gerät auch dann blockiert ist, wenn es den Proxy gar nicht nutzt.
- **NTP über TrutzBox leiten:** Mit diesem Schalter bezieht das Gerät seine Uhrzeit (Zeitabgleich, „NTP“) von der TrutzBox statt von externen Zeitservern (z. B. time.windows.com, Apple, Google). Vorteil für die Privatsphäre: Es verlassen keine Zeit-Anfragen mit Geräte-Kennungen mehr das eigene Netz. Technisch leitet die TrutzBox die Zeit-Anfragen des Geräts (Port UDP 123) auf ihren eigenen Zeitdienst um; im Monitor erscheint dieser Verkehr daher als boxinterner Dienst „TrutzBox NTP“ statt als Verbindung zu Apple o. Ä. Die Umleitung wirkt nur für Geräte, die ihren Verkehr über die TrutzBox führen.

Tab „Proxy“:

Menüpfad: Verwaltung → Geräte



Geräte-Detail, Tab „Proxy“: Name, Ausnahmen, Gerätetyp und Slider-Vorgabe.
(© 2026 Comidio GmbH)

Im Tab „Proxy“ werden die gerätespezifischen TrutzBrowse- und TrutzContent-Einstellungen vorgenommen:

- **Name:** Hier kann dem Gerät ein verständlicherer Name vergeben werden. Der tatsächliche Hostname des Geräts im Netzwerk wird dadurch nicht verändert. Dieser Name wird zentral verwendet und erscheint auch im Monitor an allen Stellen. Ist kein eigener Name vergeben, zeigt die TrutzBox in dieser Reihenfolge: Hostname, dann Hersteller, dann IP-Adresse.
- **Von der Liste löschen:** Entfernt dieses Gerät aus der Geräteliste. Es wird beim nächsten Verbinden wieder automatisch erkannt.
- **Einstellungen zurücksetzen:** Setzt alle Proxy-Einstellungen dieses Geräts auf die Standardwerte zurück.

Diese Ausnahmen zulassen

Über das Feld „Diese Ausnahmen zulassen“ ist es möglich, dem Gerät eine „Whitelist“ zuzuweisen, also eine Liste erlaubter Domains. Mit einer solchen Whitelist können z. B. Standard-Blockierungen, die von Comidio vorgegeben werden, aufgehoben werden. Es gibt eine „Standard-TrutzContent-WL“ die immer existiert, anfangs leer ist und allen Geräten zugewiesen ist. Weitere persönliche Whitelists kann man in „Filterlisten“ als zusätzliche Whitelist anlegen und dann hier direkt unter „Diese Ausnahmen zulassen“ einzelnen Geräten individuell zuweisen.

Nur Ausnahmen erlauben

Während „Diese Ausnahmen zulassen“ eine Whitelist zusätzlich freischaltet, dreht der Schalter „Nur Ausnahmen erlauben“ das Prinzip um: Das Gerät darf dann ausschließlich die in seinen Ausnahmen eingetragenen Adressen erreichen; alles andere wird blockiert („Default-Deny“). Ist keine Ausnahme eingetragen, kommt das Gerät bewusst nirgends hin. Blockierte Aufrufe zeigen eine eigene Sperrseite (deutsch, englisch, niederländisch).
Wichtig: QUIC bleibt gesperrt. Die globale QUIC-Sperre (Port UDP 443) ist standardmäßig eingeschaltet; beim Einschalten von „Nur Ausnahmen erlauben“ stellt die TrutzBox sicher, dass sie aktiv ist. QUIC ist ein neueres Übertragungs-Protokoll, das am Filter vorbeiläuft und die Whitelist aushebeln würde; die Sperre zwingt die Geräte auf das prüfbare TCP 443 zurück. Zu beachten: Die QUIC-Sperre gilt für das ganze Netz (nicht nur dieses Gerät) und bleibt aktiv, auch wenn „Nur Ausnahmen erlauben“ später wieder ausgeschaltet wird.

Gerätetyp festlegen

Unter „Gerätetyp“ kann für jedes Gerät eingestellt werden, ob es sich um ein Computer-, Android- oder iOS-Gerät handelt, sodass dem Server mit einem passenden „user-agent“-Wert angezeigt werden kann, für welchen Gerätetyp die Webseite aufbereitet werden soll. Der tatsächlich zum Server gesendete „user-agent“ Wert kann unter „Browseranonymität“ → „Slider-Definition“ → „immer dieser user-agent Wert senden“ angepasst werden.

Standardposition Slider

Die Einstellung "Standardposition Slider" bietet bei eingeschaltetem TrutzBrowse eine Möglichkeit, einen fest definierten SecuritySlider Wert für alle Server-Zugriffe dieses Geräts festzulegen. Diese Funktion ermöglicht es, selbst solche Geräte zu kontrollieren, die auf ständig wechselnde Server eines Dienstleisters zugreifen.

Tor-Netzwerk verwenden

Mit dem Schalter „Tor-Netzwerk verwenden“ kann die Pseudonymisierung der IP-Adresse aktiviert werden, indem dieses Gerät das Tor-Netzwerk[1] für Internet-Zugriffe verwendet. Allerdings ist hierbei zu beachten, dass die Internet-Nutzung langsamer sein kann und manche Web-Server bei der Benutzung von Tor zusätzliche Probleme bereiten können. Hinweis: die IP-Adresse kann unter Umständen trotz aktiviertem Tor-Netzwerk vom Server ermittelt werden. Siehe hierzu das Kapitel über Tor im TrutzBox-Kompendium Teil 1.
Im Browser ist es dann auch möglich, Tor-Hidden-Services, also Web-Adressen die mit „.onion“ enden, aufzurufen. Alle sonstigen TrutzContent und TrutzBrowse Funktionen sind weiterhin zusätzlich aktiv.
Mit dem Schalter „TrutzBrowse aktivieren“ wird für dieses Gerät TrutzBrowse aktiviert oder komplett deaktiviert.

[1] https://de.wikipedia.org/wiki/Tor_(Netzwerk)

Bei ausgeschaltetem TrutzBrowse wird ein von TrutzContent erlaubter Zugriff unverändert durchgelassen und das Zertifikat des Servers bis zum Endgerät (z.B. Browser oder App) durchgereicht; die TrutzContent-Filter der Filtergruppe bleiben aktiv.

Was genau ist der Unterschied, wenn TrutzBrowse ein- oder ausgeschaltet ist?

Bei eingeschaltetem TrutzBrowse anonymisiert die TrutzBox den Datenaustausch mit erlaubten Servern, abgestuft nach der SecuritySlider-Position des jeweiligen Servers; die zugehörigen Einstellungen liegen im Menü „Browseranonymität“. Einzelheiten im Kapitel „TrutzContent und TrutzBrowse: neben der Firewall zwei weitere Schutzebenen“.
TrutzBrowse setzt voraus, dass auf dem Gerät das TrutzBox-Stammzertifikat installiert ist; wo das nicht geht (z. B. TV oder Kamera), sollte TrutzBrowse abgeschaltet werden. Einzelheiten im Kapitel „Verschlüsselte (SSL/TLS)-Verbindungen“.
Wenn TrutzBrowse abgeschaltet ist, sollte man für dieses Gerät eine TrutzContent-Gruppe aktivieren, die strenger filtert. Das Gerät ist also einer Gruppe mit mehr Blacklists zuzuordnen. In dieser Gruppe sollten zumindest auch die Tracker blockiert werden.

TrutzBurg-Symbol anzeigen

Falls TrutzBrowse für dieses Gerät aktiviert ist, wird im Browser des Anwenders i.d.R. oben rechts das TrutzBox-Symbol, die TrutzBurg angezeigt. Dann ist es hier möglich, die Anzeige der TrutzBurg abzuschalten. Das ist dann immer sinnvoll, wenn das TrutzBurg Symbol im Browser stört. Z.B. wenn eine Seite ohne TrutzBurg gedruckt werden soll, oder wenn man Filme auf dem Fernseher über die TrutzBox schauen möchte. Dazu kann hier für das gewünschte Gerät das Flag "TrutzBurg Symbol anzeigen" deaktiviert werden. Die TrutzBrowse-Filterfunktionen der TrutzBox werden dadurch nicht verändert.
Hier kann auch festgelegt werden, an welcher Ecke im Browser das TrutzBurg-Symbol angezeigt werden soll. Wenn nichts anderes festgelegt wurde, ist das Symbol immer oben rechts im Browser-Fenster angeordnet.
Technische Umsetzung: wie Geräte-Einstellungen gespeichert werden und stabil bleiben: Alle Geräte-Richtlinien stehen in einer zentralen Konfiguration der TrutzBox. Zwei Prozesse teilen sich die Arbeit: Der Web-Server (die Bedienoberfläche) ist die allein verwaltende Instanz der Einstellungen, der Proxy liest sie und meldet nur erkannte Geräte-Merkmale (Hostname, IP, MAC) zurück. Der Proxy überträgt ausschließlich reine Geräte-Merkmale; alle Richtlinien (Internetzugang, TrutzBrowse, NTP, „Nur Ausnahmen“, Filtergruppe, Name …) bleiben fest beim Web-Server. So kann auch ein Gerät mit sehr häufigen Netzwerkanfragen (z. B. ein iPhone mit ständigen Zeit- und Verbindungsproben) die Konfiguration nicht überschreiben, und die Schalter halten zuverlässig.
Verwaiste Geräte werden automatisch aufgeräumt: Beim Öffnen der Geräte-Seite entfernt die TrutzBox stillschweigend verwaiste Einträge, also Geräte, die nur über ihre IP-Adresse (ohne Hostname/MAC) bekannt sind, nie konfiguriert wurden und gerade offline sind. Alles mit MAC-Adresse, Namen oder einer manuellen Einstellung bleibt immer erhalten; ein versehentlich entferntes Gerät erscheint beim nächsten Kontakt von selbst wieder.

6 Benutzer

6.1 Arten von Benutzer-Accounts

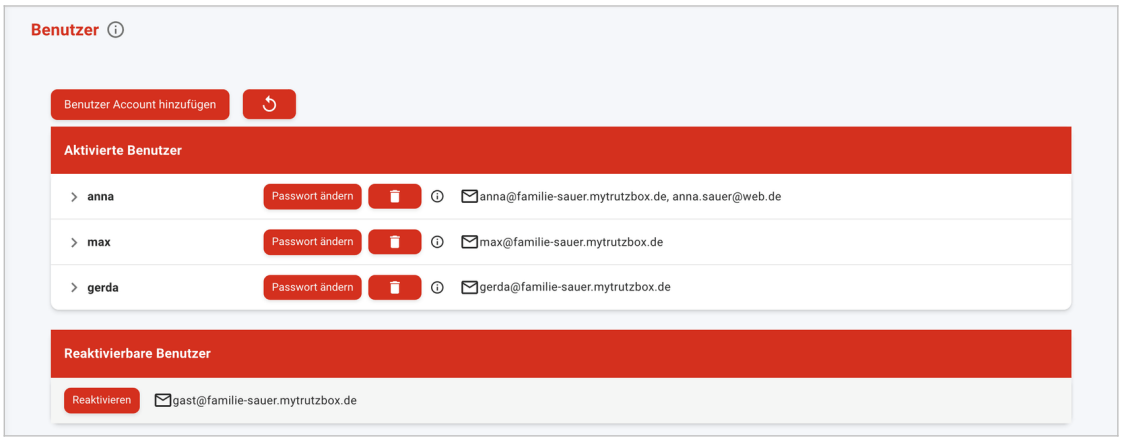
Die TrutzBox hat eine eigene Verwaltung ihrer Benutzer. Es gibt drei Arten von Nutzer-Accounts:

- admin: Gibt es nur einmal; wird beim Setup angelegt. Hat Administrator-Rechte auf Betriebssystemebene, wird zum Einloggen in die Bedienoberfläche und in Webmin benötigt und ermöglicht auch den Terminal-Zugang. Per SSH ist admin das einzige Konto, das sich mit einem Passwort anmelden kann (Abschnitt „Anmeldung an der Kommandozeile (SSH)“ im Kapitel „Webmin“).
- **Benutzer ohne TrutzMail-Adresse:** Kann beliebig oft angelegt werden; primär für TrutzContent-Filtergruppen verwendet.
- **Benutzer mit TrutzMail-Adresse:** Wird benötigt für TrutzMail (zwischen TrutzBoxen), PGP-Mails an externe Empfänger, Chat, das Öffnen eines Videokonferenzraums und für den Fernzugriff per VPN. Die Anzahl ist durch den Service-Vertrag begrenzt; TrutzMail-Adressen müssen global eindeutig sein.

Benutzer mit TrutzMail-Adresse können aktiv oder deaktiviert sein. Nach Ablauf des Service-Vertrags wird das TrutzMail-Zertifikat nicht weiter erneuert; Mails mit abgelaufenem Zertifikat werden von der Empfänger-TrutzBox nicht angenommen. Maßgeblich sind die jeweils gültigen AGB und die Leistungsbeschreibung.

6.2 Benutzer-Übersicht

Menüpfad: Verwaltung → Benutzer



Die Benutzer-Übersicht mit den angelegten TrutzBox-Benutzern und ihren Adressen.
(© 2026 Comidio GmbH)

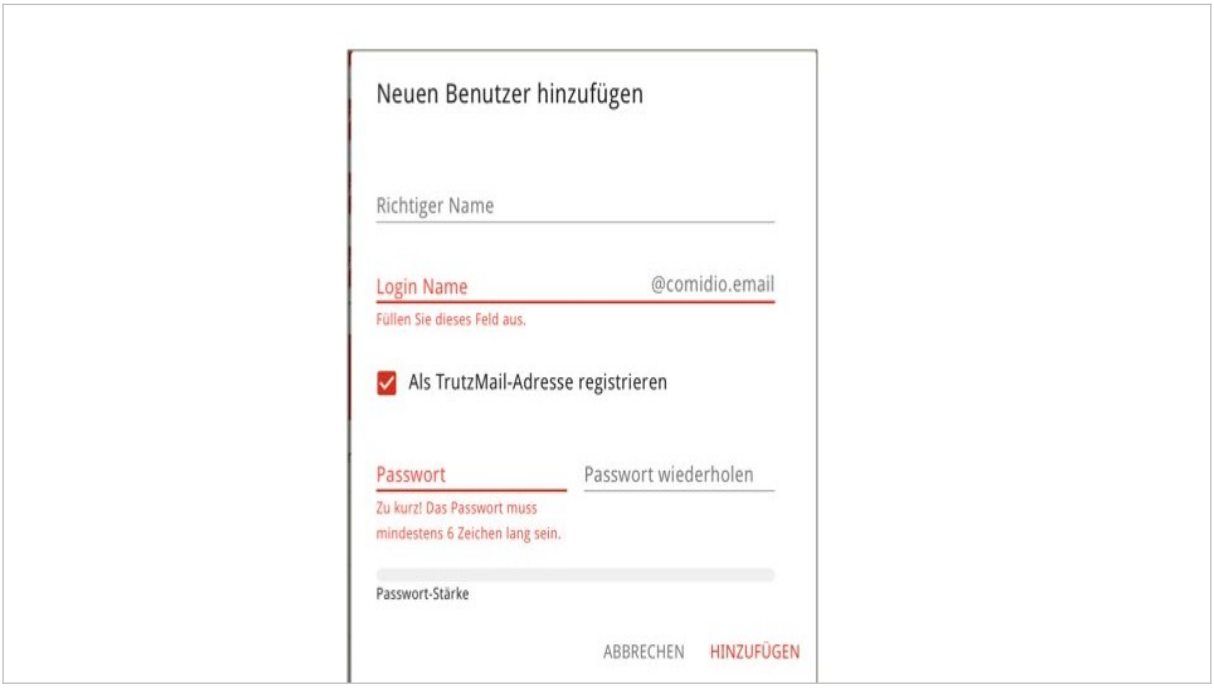
Die Benutzer-Übersicht gliedert sich in zwei Bereiche:

- **Aktivierte Benutzer:** Alle aktuell eingerichteten Benutzer. Passwort ändern, Benutzer löschen oder per Klick auf den Pfeil links in die Detail-Einstellungen wechseln. Benutzer ohne TrutzMail-Adresse sind daran erkennbar, dass keine E-Mail-Adresse angezeigt wird. Beim Löschen eines Benutzers mit TrutzMail-Adresse wird diese automatisch deaktiviert.
- **Reaktivierbare Benutzer:** Benutzer, die mit der gleichen TrutzLegitimation bereits registriert wurden, derzeit aber nicht eingerichtet sind (z. B. nach Reset oder Hardware-Austausch). Per Klick auf „Reaktivieren“ wird der Account wiederhergestellt.

6.3 Benutzer hinzufügen

Über die Schaltfläche „Benutzer Account hinzufügen“ öffnet sich folgendes Formular:

Menüpfad: Verwaltung → Benutzer



Das Formular zum Anlegen eines neuen Benutzer-Kontos.
(© 2026 Comidio GmbH)

Beim Anlegen eines neuen Benutzers werden folgende Felder ausgefüllt:

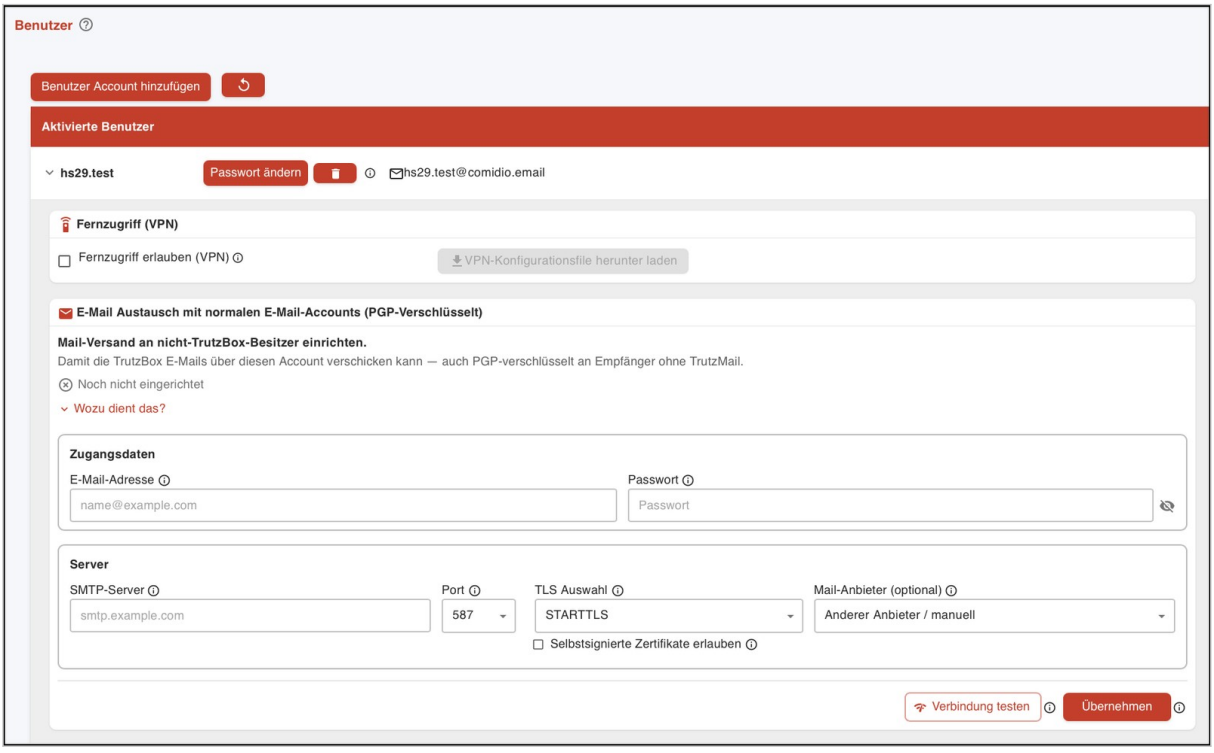
- **Richtiger Name:** Anzeigename des Benutzers.
- **Login Name:** Lokaler Benutzername; wird mit @comidio.email zur TrutzMail-Adresse ergänzt, wenn die Checkbox aktiviert ist.
- **Als TrutzMail-Adresse registrieren:** Wenn aktiviert, wird der Benutzer gleichzeitig als TrutzMail-Adresse bei Comidio registriert.

- **Passwort:** Es gilt die Passwortregel der TrutzBox: 10 bis 128 Zeichen, Leerzeichen und Umlaute erlaubt; mindestens drei der vier Zeichenarten Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen, ab 16 Zeichen genügen zwei. Nicht erlaubt sind die Wörter TrutzBox, Comidio und admin, der eigene Benutzername, einfache Folgen aus vier Zeichen (etwa 1234, abcd, qwertz, aaaa) und bekannte Allerweltspasswörter wie Sommer2024! oder Passwort123. Dieselbe Regel gilt für das Administrator-Passwort und im Setup; bereits vergebene Passwörter bleiben gültig und werden beim Anmelden nicht geprüft. Das „i“ am Passwortfeld fasst die Regel zusammen, der Passwort-Stärke-Indikator dient nur noch der Orientierung. Die Regel ist bewusst streng, weil das TrutzMail-Passwort über die Chat-Anmeldung der Videokonferenz aus dem Internet erreichbar ist (Abschnitt „Externe Verbindungen zum TrutzRTC-Konferenz-Server“).

6.4 Detail-Einstellungen eines Benutzers

Der Pfeil links neben einem aktivierten Benutzer öffnet die Detail-Einstellungen:

Menüpfad: Verwaltung → Benutzer



Die Detail-Einstellungen eines Benutzers, aufgeklappt über den Pfeil links.
(© 2026 Comidio GmbH)

- **Fernzugriff (VPN):** Hier kann der VPN-Fernzugriff für diesen Benutzer freigeschaltet werden. Ist der Fernzugriff aktiv, steht eine Schaltfläche zum direkten Download der VPN-Konfigurationsdatei (.ovpn) für das mobile Gerät zur Verfügung.
- **E-Mail-Austausch mit normalen E-Mail-Accounts (PGP-Verschlüsselung):** Für das Versenden von PGP-verschlüsselten Mails an nicht-TrutzBox-Adressen muss ein externer SMTP-

Postausgangsserver konfiguriert werden. Zum Empfangen von E-Mails ist dieser Eintrag nicht erforderlich.

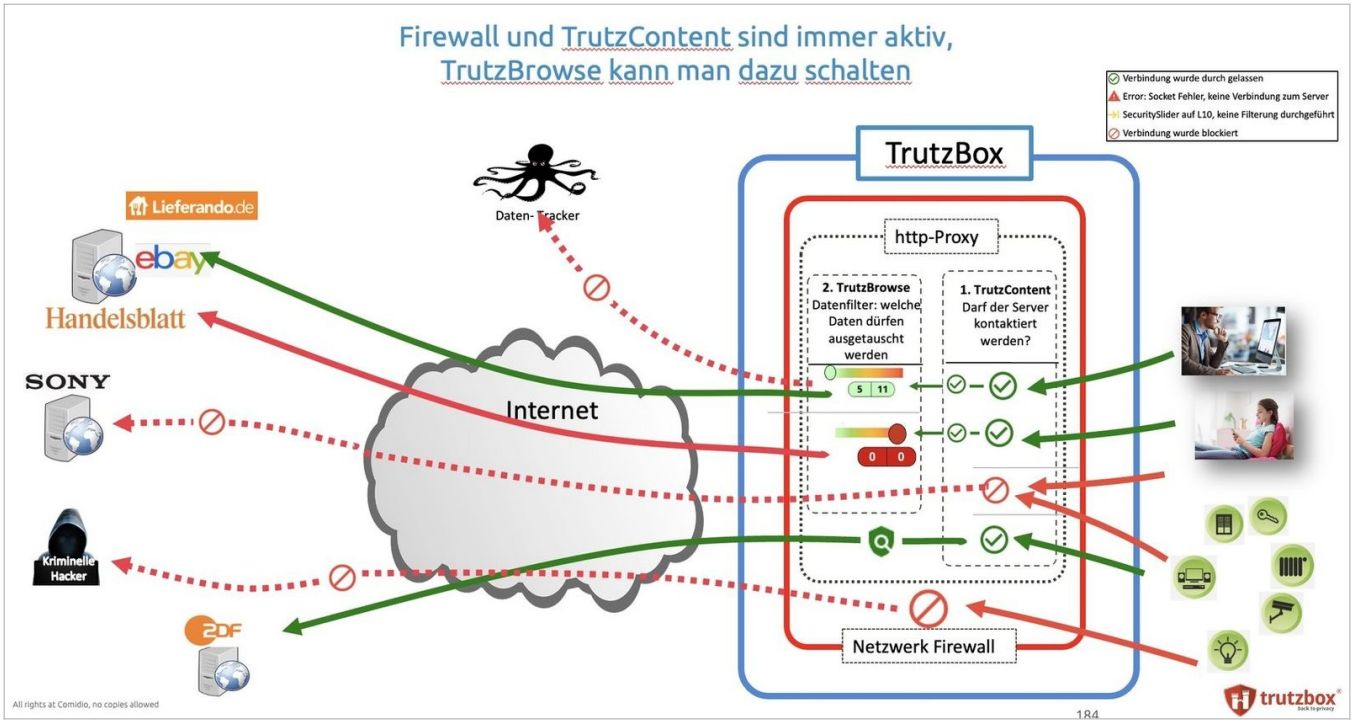
- **Selbstsignierte Zertifikate erlauben:** Erlaubt Verbindungen zu Servern mit selbstsignierten Zertifikaten für diesen Benutzer. Hinweis: Damit entfällt für diesen Benutzer die Echtheitsprüfung solcher Server; die Option sollte nur bei Bedarf und für bekannte Server aktiviert werden. Hinweis: Damit entfällt für diesen Benutzer die Echtheitsprüfung solcher Server; die Option sollte nur bei Bedarf und für bekannte Server aktiviert werden.

Anmeldung bleibt auch nach einem Neustart erhalten: Die Anmelde-Sitzung der Bedienoberfläche überdauert einen Neustart der TrutzBox; man muss sich nach einem Box-Neustart nicht mehr neu anmelden. Das Anmelde-Cookie ist zusätzlich gehärtet.
Live-Ansichten und Anmeldung zusätzlich abgesichert: Die Echtzeit-Ansichten (Monitor, Live-Protokolle) verlangen ebenfalls eine angemeldete Sitzung; ihre Datenverbindung wird mit demselben Sitzungs-Cookie geprüft wie die übrige Oberfläche. Außerdem bricht die Anmelde-Prüfung beim Start nach 15 Sekunden ab und zeigt die Anmeldemaske, statt den Bildschirm bei einem hängenden Hintergrunddienst dauerhaft auf einem Ladezeichen stehen zu lassen.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

7 TrutzBox-Proxy: Funktion und interner Aufbau

Die TrutzBox schützt den Internet-Anwender, indem sie es Angreifern und Daten-Sammlern erheblich erschwert, bei der Nutzung des Internets an dessen Profildaten zu kommen. Die TrutzBox, mit ihrer TrutzContent und TrutzBrowse Funktion, ist kein „Werbeblocker“. Allerdings erschwert die TrutzBox, dass Werbefirmen Nutzungsdaten sammeln können. In den Standard-Einstellungen verhindert die TrutzBox nicht, dass im Browser Werbung angezeigt wird. Das Blockieren von Werbung kann der TrutzBox-Administrator allerdings bei Bedarf einschalten.
Mit TrutzContent und TrutzBrowse bietet die TrutzBox ein „Privatisierungs-Werkzeug“, das die heimliche Analyse des Nutzerverhaltens bei der Internet-Kommunikation erschwert. Informationen über das Verhalten der Internet-Nutzer lassen sich so deutlich schwerer ohne ihr Wissen sammeln und vermarkten. Informationen, die zwischen Ihren Geräten und einem Server im Internet ausgetauscht werden, können kontrolliert, ggf. blockiert oder zumindest „anonymisiert“ werden.
Das folgende Bild fasst zusammen, wie die TrutzBox jeden Internet-Zugriff prüft und wie sich TrutzBrowse als zweite Stufe dazuschalten lässt.



Der Weg eines Internet-Zugriffs durch die TrutzBox, von TrutzContent bis TrutzBrowse.
(© 2026 Comidio GmbH)

Die Legende oben rechts erklärt die Symbole: Ein grüner Haken bedeutet, dass eine Verbindung durchgelassen wurde. Ein rot durchgestrichenes Zeichen steht für eine blockierte Verbindung. Ein Warndreieck zeigt einen Socket-Fehler an, also keine Verbindung zum Server. Ein gelber Pfeil bedeutet, dass der SecuritySlider auf Stufe 10 steht: Die Verbindung wird nicht entschlüsselt und nicht anonymisiert. Geprüft wird nur der erste Aufruf, also der angesteuerte Server, gegen die Sperrlisten; die Folgeaufrufe innerhalb der verschlüsselten Verbindung sieht die TrutzBox nicht.

Die Pfeile zeigen Beispiele aus dem Alltag: Erwünschte Server wie ebay, das Handelsblatt oder das ZDF werden durchgelassen (grün), während Verbindungen zu Daten-Trackern oder kriminellen Servern blockiert werden (rot gestrichelt). Rechts stehen die Geräte des eigenen Netzes (Computer, Smartphone und IoT-Geräte), von denen die Zugriffe ausgehen. Wie stark TrutzBrowse die durchgelassenen Daten anonymisiert, richtet sich nach dem SecuritySlider, dessen Stellung im Bild für einzelne Verbindungen dargestellt ist.
Wie bereits festgestellt, kann man bei der Nutzung von Apps, beim Surfen im Internet oder bei jeder anderen Internet-Kommunikation von Web-Server Betreibern oder Dritten ausgespäht werden. Und das sogar Webseiten übergreifend. Dies geschieht, indem der „Ausspäher“ Sie durch Ihre einmalige Browser- und Betriebssystem-Einstellungen (Browser-Fingerprint) oder einem Cookie (eine Datei, die die Webseite auf Ihrem Gerät erstellt, und die die Webseite beim nächsten Aufruf wieder lesen kann) wiedererkennt.
Die meisten Ansätze für mehr Anonymisierung im Internet versuchen das Problem im Browser zu lösen. Dazu gibt es Plugins für die Verwaltung von Cookies, um JavaScript abzuschalten, ferner Blockerplugins im Browser, die Domains von bekannten Trackern blockieren oder sogar speziell angepasste Browser (z. B. Chromium oder Tor-Browser). Comidio kam nach der Analyse vieler dieser angebotenen Lösungen und nach Erfahrung des Comidio-Teams zu der Einschätzung, dass

- vielen Anwendern die Installation und Bedienung eines neuen Browsers oder Browser-Plugins zu aufwendig ist.
- JavaScript abschalten zur Folge hat, dass die meisten Webseiten nicht mehr funktionieren.
- DNT-Flag (Do-not-Track) von Tracking-Domains nicht beachtet wird.
- viele Browser-Sicherheitseinstellungen den Laien überfordern oder die Bedienung für den Anwender zu umständlich ist (z. B. Flash abschalten, Third Party Cookie-Handling, Chronik-Handling.
- IP-Adress-Verschleierungs-Tools wie Tor den Web-Browser nicht daran hindern, dem aufgerufenen Web-Server und den Daten-Trackern weiterhin Daten zu liefern. Und bei VPNs gibt es keine Garantie, dass der VPN-Betreiber nicht auch noch die Benutzer ausspäht.
- Browser ohne Aufforderung des Anwenders HTTP-Zugriffe auf Web-Server durchführen, sodass ein Browser-Plugin das gar nicht mitbekommt und somit auch nicht analysieren oder blocken kann (z. B. Zugriffe auf Browser- und Plugin-Updates, auf mozilla.org oder Googles 10e100 Domain[2] o.ä.).
- Irgendwelche anderen Geräte im Haushalt oder in der Firma (IoT-Geräte) die Web-Zugriffe durchführen, für die es gar keine Plugins gibt (z. B. für Spielekonsolen und Fernseher).

Die TrutzBox umgeht durch ihre besondere Architektur aus TrutzContent und TrutzBrowse diese Einschränkungen. Mit ihrer Hilfe können auch Anwender ohne technische Vorkenntnisse das ungewollte Ausspähen erschweren.

[2] https://www.webmasterworld.com/google/4050443.htm

Dabei schützt TrutzContent sämtliche Geräte im Netzwerk, nicht nur Browser, sondern auch Apps, Smartphones, Betriebssysteme und IoT-Geräte, indem es kontrolliert, welche Server kontaktiert werden dürfen; TrutzBrowse anonymisiert zusätzlich die ausgetauschten Daten und setzt dafür das TrutzBox-Stammzertifikat auf dem Gerät voraus. Einzelheiten im Kapitel „TrutzContent und TrutzBrowse: neben der Firewall zwei weitere Schutzebenen“.
Die TrutzBox Funktionen TrutzBrowse und TrutzContent wurden durch einen intelligenten Proxy (Stellvertreter) implementiert, der an zentraler Stelle (in der TrutzBox) jeglichen HTTP-Datenaustausch zwischen dem gesamten eigenen Netz und dem Internet überwacht. Dieser Proxy fasst Funktionen der gängigen Browser-Plugins zusammen und bietet darüber hinaus vieles mehr. Er stellt sicher, dass

- alle Anfragen auf verräterische HTTP-Header-Daten hin untersucht und nach Bedarf verschleiert werden, indem der Proxy diese HTTP-Header blockiert oder verfälscht,
- unerwünschte Cookies blockiert werden und
- alle Server-Verbindungen mit auf der TrutzBox gespeicherten Blacklists vergleicht und bei Bedarf unerwünschte oder sogar gefährliche Verbindungen blockiert werden. Oftmals sind dies Verbindungen, die gar nicht bewusst aufgerufen wurden, sondern solche, auf die die aufgerufene Webseite verlinkt ist. Das können einerseits Werbe- oder Statistik-Server sein aber andererseits auch gefährliche Web-Server, die bekanntermaßen Schad-Software verteilen.

Damit ist es Dritten, denen die von Ihnen aufgerufene Webseite Zugang zu Ihren Daten gewähren wollte, nicht mehr so einfach möglich, an diese Informationen zu gelangen. Außerdem erhält auch der Web-Server, den Sie aufgerufen haben, nur noch die Daten, die er für seine Arbeit unbedingt benötigt.

7.1 TrutzContent und TrutzBrowse: neben der Firewall zwei weitere Schutzebenen

Die TrutzBox bietet zwei voneinander unabhängige Schutzfunktionen, die je nach Gerät einzeln oder kombiniert greifen. Beide laufen über denselben Proxy, unterscheiden sich aber grundlegend in dem, was sie kontrollieren, und vor allem darin, wann sie aktiv sind.

TrutzContent: der Grundschutz, immer aktiv

TrutzContent ist immer eingeschaltet, sobald der Netzwerk-Verkehr eines Geräts durch die TrutzBox geleitet wird. Es lässt sich pro Gerät nicht abschalten; wer die TrutzBox nutzt, profitiert automatisch von TrutzContent. Auf Verbindungs-Ebene wird entschieden, welche Server überhaupt kontaktiert werden dürfen: Versucht ein Gerät, egal ob Smartphone-App, Browser, Smart-TV oder IoT-Gerät, eine Verbindung zu einem Server aufzubauen, vergleicht TrutzContent die Zieladresse mit den Filterlisten der für das Gerät eingestellten Filtergruppe. Bekannte Tracker, Werbenetzwerke oder Schadsoftware-Verteiler werden blockiert, bevor überhaupt Daten fließen.
TrutzContent schützt jedes Gerät im Netzwerk, ohne dass dort etwas installiert oder konfiguriert werden muss. Die Stärke des Schutzes ergibt sich allein aus der Filtergruppe, der das jeweilige Gerät zugeordnet ist.

Die zweite Stufe, TrutzBrowse, wird im eigenen Kapitel „TrutzBrowse“ beschrieben, nachdem TrutzContent vollständig dargestellt ist. Dort stehen auch ihre Vorteile und Nachteile sowie ein Vergleich beider Stufen.

7.2 TrutzBox-Proxy: interner Aufbau

Comidio hat verschiedene Open-Source-Proxys geprüft und sich entschieden, für die besonderen Anforderungen der TrutzBox (Anonymisierungsgrad, Ressourcenverbrauch, Bedienung durch Technik-Laien, enge Verzahnung mit der Bedienoberfläche) eine eigene, auf node.js basierende Lösung zu entwickeln.[3]

Die eigene Implementierung ermöglicht Funktionen wie den „Intelligenten Security-Slider“, mit dem Anwender die Sicherheitseinstellung für eine aufgerufene Webseite selbst anpassen können.

Um die Einstellungen des Proxys für den TrutzBox-Administrator (TrutzBox Bedienoberfläche) und die Bedienung dieser Einstellungen durch den Benutzer (SecuritySlider) möglichst benutzerfreundlich zu gestalten, wurde das TrutzBox Bedienoberfläche und der SecuritySlider eng mit dem Proxy integriert. Neben der Generierung der SSL-Zertifikate, der Kontrolle der jeweilig zu blockierenden Seiten und der Anpassung der HTTP-Header übernimmt der Proxy auch:

- die Authentisierung eines Benutzers beim: Admin-Login und TrutzContent auf Benutzerebene
- die Browser-Sessions, um die Browser Zugriffe im SecuritySlider anzuzeigen und in Status zu speichern
- die SecuritySlider Positionen für die jeweiligen Web-Server
- die Unterscheidung, ob ein Server bewusst (TrutzContent) oder indirekt (TrutzBrowse) aufgerufen wurde und nutzt dazu die jeweilig eingestellten Blocking-Listen
- für verschlüsselte (TLS) Zugriffe die Daten entschlüsselt, für den aufgerufenen Server einen neuen Schlüssel generiert und die Seite damit neu verschlüsselt an den Browser liefert
- das Sammeln der Statistikdaten

Gerade bei verschlüsselten Webseiten stellt dieser ganze Vorgang eine erhebliche Ressourcenbelastung für die Proxy-Hardware dar. Deswegen ist es umso wichtiger, dass die Proxy-Hardware über genügend Rechenleistung verfügt. Das ist bei der TrutzBox-Hardware der Fall, zumal diese zusätzlich auch noch über eine AES-NI Unterstützung auf Prozessor-Ebene verfügt[4], die gerade die Ver- und Entschlüsselung beschleunigt und den Prozessor entlastet.
Um eine bessere Ausfallsicherheit und den Zugriffs-Durchsatz zu erhöhen, wurde der eigentliche HTTP-Proxy, der die angeforderten HTTP-Zugriffe durchführt, mehrfach instanziiert.

3 http://nodejs.org

4 https://de.wikipedia.org/wiki/AES_(Befehlssatzerweiterung)

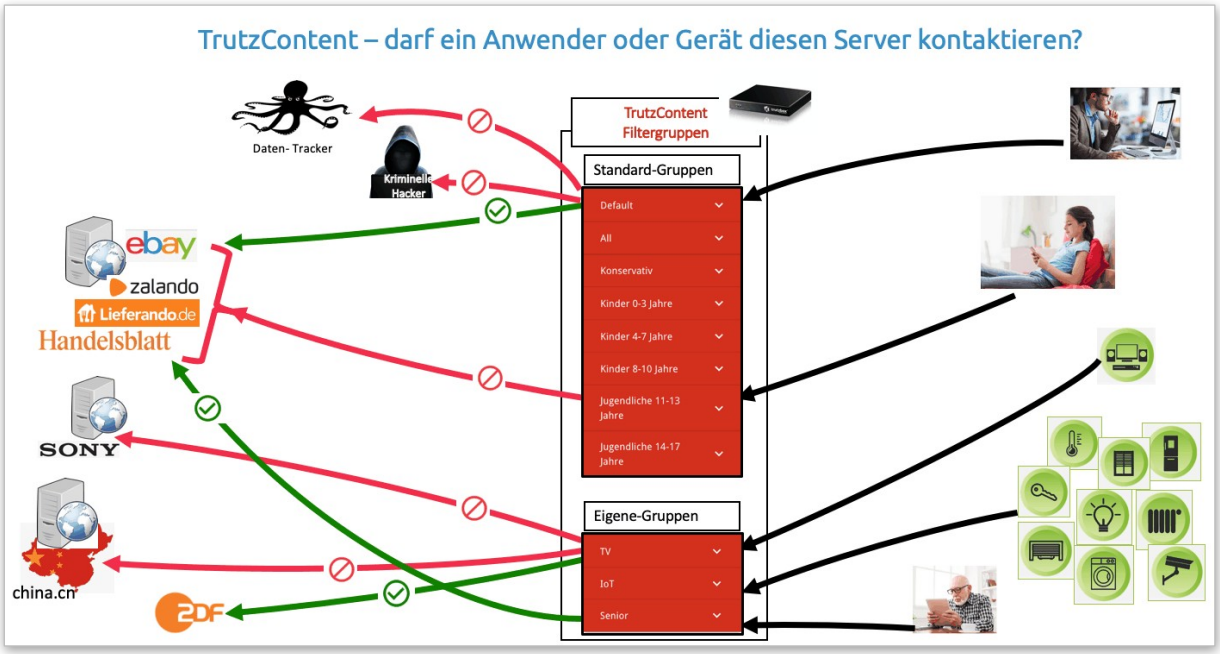
8 TrutzContent

Um die Kontaktaufnahme von Geräten oder TrutzBox-Benutzern zu bestimmten Servern zu blockieren, kann ein Gerät oder einen TrutzBox-Benutzer einer Filtergruppe zugeordnet werden.
Hier ein paar sinnvolle Anwendungsmöglichkeiten des Zugriffsblockers:

- Kinder und Kinder und Jugendliche vor ungeeigneten Internet-Seiten schützen (Inhaltsfilter; die TrutzBox ist kein anerkanntes Jugendschutzprogramm im Sinne des JMStV und ersetzt keine Aufsicht) (Inhaltsfilter; die TrutzBox ist kein anerkanntes Jugendschutzprogramm im Sinne des JMStV und ersetzt keine Aufsicht)
- Schutz vor Kostenfallen und ungewollten Bestellungen in Web-Shops, etwa beim Einsatz in Seniorenheimen (rechtlichen Hinweis am Anfang dieses Dokuments beachten)
- IoT-Geräte (Video-Kamera, Heizung, Fernseher usw.) daran hindern, dass diese Geräte zu unerwünschten Servern Kontakt aufnehmen
- Apps auf Smartphones oder das Smartphone selbst daran hindern, dass es zu unerwünschten Servern Kontakt aufnimmt. Z.B. Kontakt zum Hersteller oder einer Tracking-Firma
- Da viele Betriebssysteme regelmäßig Kontakt zum Hersteller aufnehmen (Telemetrie, Updates), kann man diesen Datenaustausch hiermit kontrollieren und einschränken.

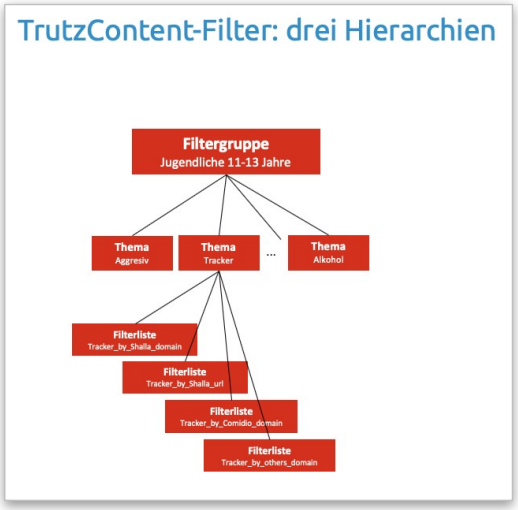
Wenn ein Gerät von der TrutzBox neu erkannt wird, dann gehört dieses Gerät zunächst automatisch zur Filtergruppe „Default“. Danach kann man z. B. den PC und das iPhone der zwölfjährigen Tochter der Gruppe „Kinder von 11 bis 13 Jahren“ zuordnen, oder den Fernseher der selbst definierten Gruppe „TV“.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2



TrutzContent entscheidet je Gerät und Filtergruppe, welcher Server überhaupt kontaktiert werden darf.
(© 2026 Comidio GmbH)

Filterlisten sind nach Themengebieten wie „Tracker“ oder „Werbung“ zusammengefasst; je Themengebiet kann es mehrere Listen geben, von Comidio mitgelieferte und automatisch aktualisierte ebenso wie selbst angelegte. Einzelheiten im Kapitel „TrutzBox Filterlisten“.
Eine Filtergruppe besteht aus selbst angelegten Filterlisten und Themengebieten. Somit gibt es diese drei Hierarchien:

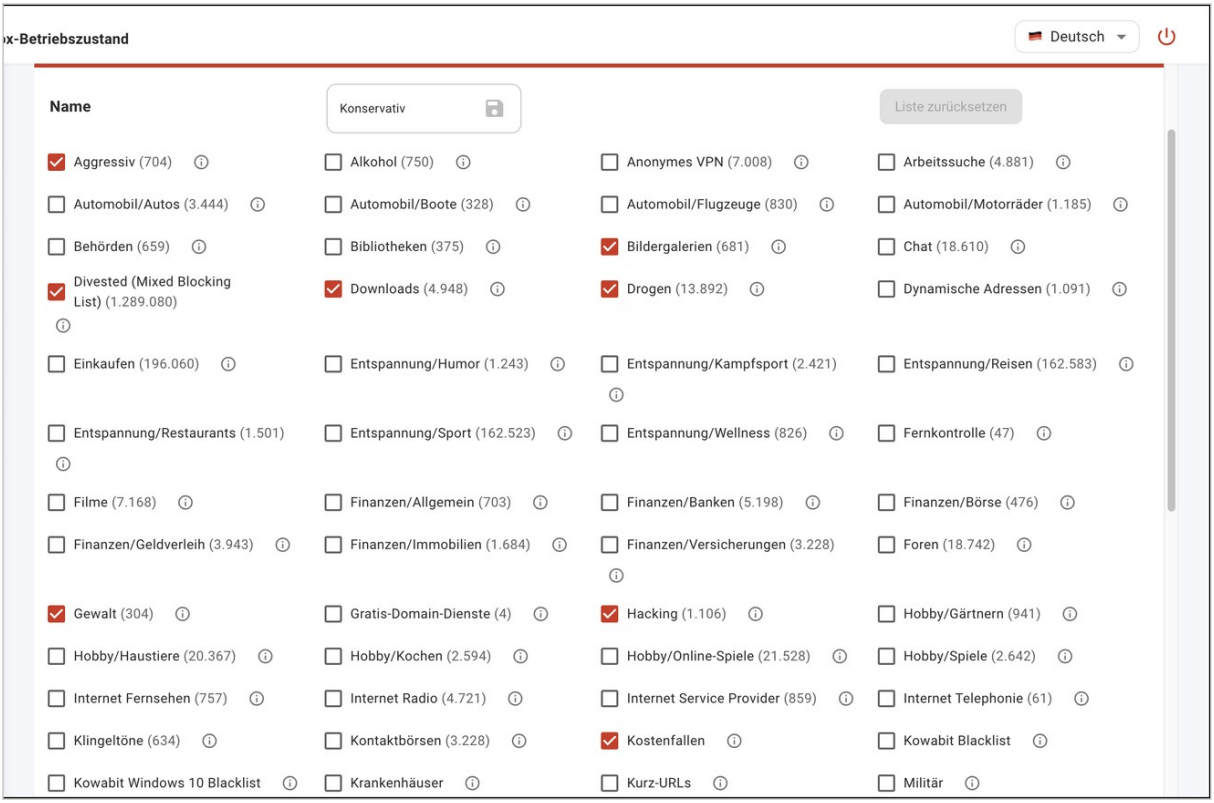


Die drei Ebenen: Filtergruppe, Filterliste und Themengebiet.
(© 2026 Comidio GmbH)

8.1 Filtergruppen

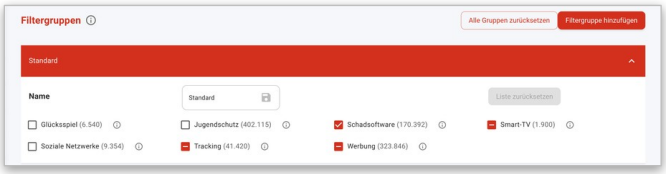
Über das TrutzBox-Menü Filtergruppen können vorhandene Filtergruppen editiert und neue Filtergruppen angelegt werden. Über „Alle Gruppen zurücksetzen“ in der Kopfzeile lassen sich sämtliche Vorgabegruppen auf den Auslieferungszustand zurücksetzen; selbst angelegte Gruppen bleiben dabei erhalten. Je Gruppe steht dafür der Knopf „Liste zurücksetzen“ bereit; bei unveränderten Gruppen ist er ausgegraut. Klappt man eine Gruppe auf, erscheint die Auswahl der Kategorien mit einem Ankreuzfeld je Kategorie. Hinter jedem Namen steht die Summe der Einträge aller Listen dieser Kategorie, etwa „Chat (18.610)“ oder „Drogen (13.892)“ (Beispielwerte). Das ist die Zahl, die zählt: Sie zeigt auf einen Blick, wie schwer eine Kategorie wiegt, bevor man sie einschaltet. Wie sich diese Summe auf die einzelnen Listen verteilt, zeigt das Info-Symbol hinter der Kategorie. Selbst hinzugefügte Listen sind an ihrem roten Namen zu erkennen.

Menüpfad: Verwaltung → Filtergruppen



Das Menü „Filtergruppen“ mit den Themengebieten einer Gruppe.
(© 2026 Comidio GmbH)

Menüpfad: Verwaltung → Filtergruppen



Filtergruppe „Standard“ mit den aktivierten Themengebieten und ihren Eintragszahlen.
(© 2026 Comidio GmbH)

Eine Filtergruppe speichert, welche einzelnen Listen zu ihr gehören. Weil der Katalog der mitgelieferten Listen mit den täglichen Updates wächst und eine Kategorie dabei neue Listen erhalten kann, gleicht die TrutzBox die Gruppen beim Laden mit dem Katalog ab, damit eine Gruppe nicht weniger filtert, als ihr Häkchen verspricht:

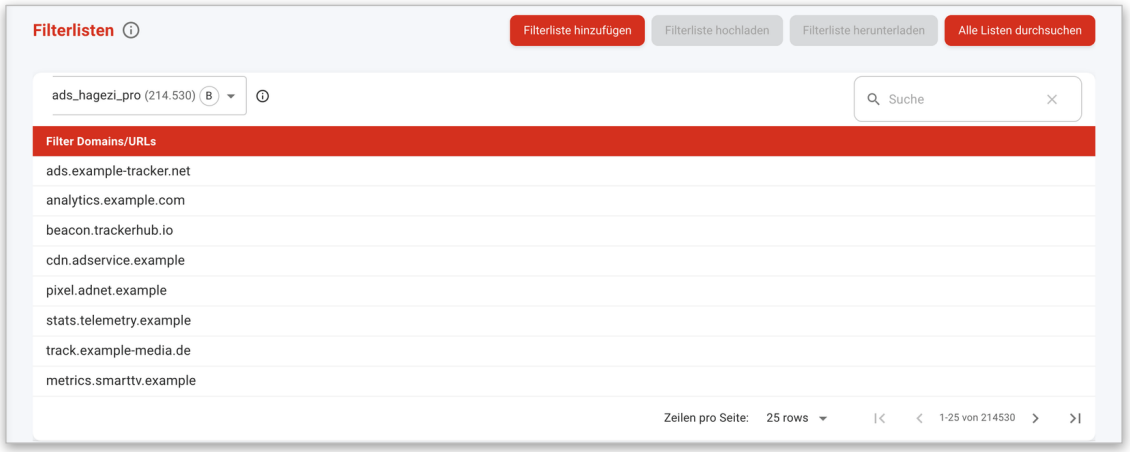
- **Genutzte Kategorien:** Nutzt eine Gruppe eine Kategorie (also mindestens eine ihrer Listen), erhält sie automatisch alle Listen dieser Kategorie.
- **Abgewählte Kategorien:** Vollständig abgewählte Kategorien bleiben abgewählt, alle anderen Einstellungen der Gruppe bleiben unverändert.
- **Verschwundene Listen:** Verweise auf Listen, die es nicht mehr gibt, werden entfernt. Listen, die Comidio aus dem Katalog zurückzieht, verschwinden aus den Gruppen.
- **Eigene Listen:** Selbst importierte Listen bilden keine Kategorie und werden nie automatisch ergänzt. Sie bleiben genau so in der Gruppe, wie sie eingetragen wurden.

In der Kategorie-Auswahl einer Gruppe zeigt ein Strich statt eines Häkchens an, dass nur ein Teil der Listen dieser Kategorie aktiv ist. Ein Klick auf das Feld ergänzt die fehlenden Listen; das Info-Symbol hinter der Kategorie nennt je Liste, ob sie aktiv ist oder fehlt. Die Gruppe „All“ steht für alle Listen einschließlich der selbst importierten und wird bei der Anzeige entsprechend aufgelöst.

8.2 Filterlisten

Beim Anlegen einer eigenen Filterliste wird festgelegt, ob sie als Whitelist (Ausnahmen von den TrutzContent- und TrutzBrowse-Filtern, in der Geräte-Einstellung zuweisbar) oder als Blacklist (zusätzliche Sperren über die vorgegebenen Listen hinaus) wirkt. Einzelheiten im Kapitel „TrutzBox Filterlisten“.

Menüpfad: Verwaltung → Filterlisten

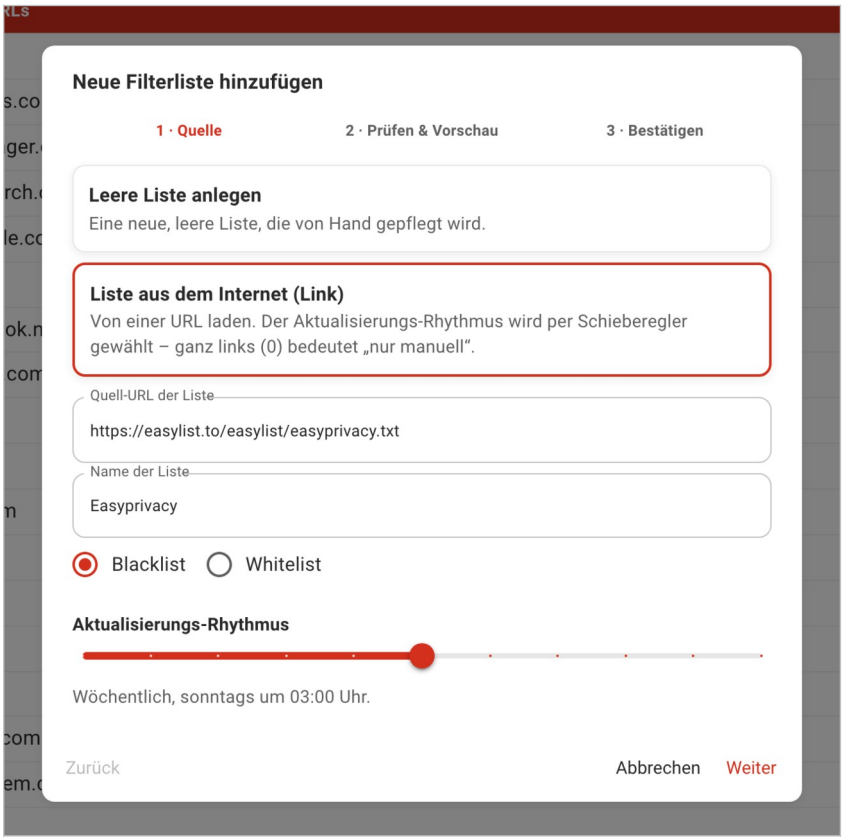


Das Menü „Filterlisten“ mit den mitgelieferten und den selbst angelegten Listen.
(© 2026 Comidio GmbH)

TrutzBox Filterlisten

Unter dem Menüpunkt „Verwaltung“ → „Filterlisten“ kann der TrutzBox Administrator einzelne Filterlisten, die Internet-Domains oder Internet-URLs beinhalten, verwalten. Die von Comidio ausgelieferten Filterlisten sind nach Internet-Themengebieten gegliedert; die aktuelle Zahl der Kategorien und Listen zeigt das Menü „Filtergruppen“. Diese Filterlisten bezieht Comidio von Listen-Anbietern, ergänzt sie um eigene Listen und überspielt sie täglich auf die TrutzBoxen. Der Administrator ist mit diesem Menüpunkt in der Lage, diese von Comidio ausgelieferten Standardlisten einzusehen, sie zu durchsuchen oder eigene, neue Black- und Whitelisten zu erstellen.
Die von der TrutzBox verwalteten Filterlisten finden sowohl bei TrutzBrowse als auch bei TrutzContent Verwendung: Welche Listen eine Filtergruppe verwendet, wird in der Gruppe selbst ausgewählt (siehe „Filtergruppen“). Defekte Einträge im Listenkatalog, etwa nach einem abgebrochenen Import, repariert die Box beim Start selbstständig.

Menüpfad: Verwaltung → Filterlisten



Der Assistent „Neue Filterliste hinzufügen" mit Quelle, Name und Aktualisierungs-Rhythmus. (© 2026 Comidio GmbH)

Filterlisten, die als Whitelist gekennzeichnet sind, können in den Geräteeinstellungen als Whitelist einem Gerät zugeordnet werden.

Bei den täglichen automatischen Systemupdates durch Comidio werden nur Standard-TrutzBox Blacklists angepasst, die selbst verwalteten Listen werden dadurch nicht verändert. Zu den mitgelieferten Listen gehört auch „Freehoster von comidio". Sie erfasst Anbieter kostenloser Domains, die nach Beobachtung des Comidio-Teams häufig für Betrugs- und Werbeseiten genutzt werden.
Bei selbsterstellten Filterlisten können sowohl Einträge manuell editiert als auch Listen komplett gelöscht, oder durch Upload einer Datei mit vielen Einträgen ergänzt werden.
Über „Liste umbenennen" lässt sich der angezeigte Name einer Liste ändern. Quelle, Aktualisierungs-Rhythmus und Einträge bleiben dabei unverändert.
Einträge in den Black- und Whitelists dürfen keine unqualifizierten Angaben beinhalten, da hier lediglich ein Stringvergleich durchgeführt wird. Sollen z. B. alle Domains gesperrt werden, die mit facebook.com enden, dann nur facebook.com eintragen. Bitte auch nicht „http" vor die Domain schreiben, da der Vergleich nur auf die Domain wirkt. Ebenso wenig gehören IP-Adressen in eine Filterliste: Filterlisten prüfen ausschließlich Namen, niemals Adressen. Ein solcher Eintrag wird deshalb mit einem Verweis auf die IP-Blocklisten-Verwaltung abgelehnt. Beim Hochladen oder Importieren einer ganzen Liste nennt die TrutzBox, wie viele Zeilen daraus wirkungslose IP-Adressen enthalten.

Filterlisten aus dem Internet importieren (automatische Aktualisierung)

Über die Schaltfläche „Neue Filterliste hinzufügen“ lässt sich neben einer leeren, von Hand gepflegten Liste auch eine fertige Filterliste direkt aus dem Internet übernehmen, etwa eine der vielen öffentlich gepflegten Tracker- oder Werbeblock-Listen. Ein Assistent führt in drei Schritten durch den Import:

- **Quelle:** Auswahl zwischen „Leere Liste anlegen“ und „Liste aus dem Internet (Link)“. Beim Import per Link werden die Quell-Adresse (URL), der Name der neuen Liste und der Aktualisierungs-Rhythmus festgelegt. Der Rhythmus wird per Schieberegler gewählt, von „nur manuell“ (ganz links) über monatlich, wöchentlich oder täglich bis hin zu „alle 6 Stunden“. So hält die TrutzBox die Liste ohne weiteres Zutun aktuell.

- **Prüfen & Vorschau:** Die TrutzBox lädt die Liste herunter und prüft sie streng. Gängige Formate (reine Domain-Listen, URL-Listen, Hosts-Dateien, dnsmasq-Listen und einfache Adblock-Domain-Regeln) werden erkannt und automatisch in das TrutzBox-Format umgewandelt. Angezeigt werden das Prüfergebnis, die Zahl der verwertbaren Domains, verworfene Kommentare sowie der zu erwartende Platz- und Speicherbedarf; eine Vorschau stellt die Original-Zeilen der umgewandelten Fassung gegenüber. Enthält die Liste auch nur einen nicht umwandelbaren Eintrag, wird sie komplett abgelehnt; so kann keine fehlerhafte Liste den Filter beschädigen.

Überschneidung mit vorhandenen Listen: Zusätzlich gleicht die TrutzBox die neuen Einträge mit den bereits aktiven Filter-Gruppen ab und zeigt, welcher Anteil davon schon abgedeckt ist (z. B. „320 neu · 78 % schon abgedeckt“) sowie die Listen mit den größten Überschneidungen. Das dient nur der Einordnung; importiert wird immer die komplette Liste.

- **Bestätigen:** Vor dem Anlegen weist der Assistent darauf hin, dass die automatische Aktualisierung manuelle Änderungen an der importierten Liste überschreibt. Eigene Ausnahmen gehören deshalb in eine eigene Whitelist, denn diese hat im Filter Vorrang.

Bei einer importierten Liste zeigt eine Quell-Karte das erkannte Format, den Zeitpunkt der letzten Aktualisierung und den Status („aktuell“ bzw. „veraltet, Update überfällig“). Über „Jetzt aktualisieren“ lässt sich die Liste sofort neu laden, über „Rhythmus ändern“ der Aktualisierungs-Rhythmus anpassen. Die automatischen Updates laufen nachts (ab 03:00 Uhr); schlägt ein Update fehl, bleibt die zuletzt funktionierende Fassung der Liste aktiv. Während Download und Speichern zeigt die Box den Fortschritt an. Die Quell-Karte nennt außerdem die nächste geplante Aktualisierung und stellt über einen Download-Link die aktuell gespeicherte Fassung der Liste bereit.
Aus Sicherheitsgründen akzeptiert die TrutzBox nur http/https-Quellen mit Größen- und Zeitbegrenzung (maximal 50 MB) und lehnt Adressen ab, die auf interne Netzwerkbereiche zeigen.
Der Aktualisierungs-Rhythmus hat elf Stufen: nur manuell, alle 6 Monate, alle 3 Monate, monatlich, alle 14 Tage, wöchentlich, alle 3 Tage, alle 2 Tage, täglich, alle 12 Stunden und alle 6 Stunden. Die Läufe finden zu festen Uhrzeiten statt. Alle Stufen bis „täglich“ laufen um 03:00 Uhr, wöchentliche Listen sonntags, monatliche und seltenere am Ersten des Monats. „Alle 12 Stunden“ läuft um 03:00 und 15:00 Uhr, „alle 6 Stunden“ um 00:00, 06:00, 12:00 und 18:00 Uhr. Fällig ist eine Liste, sobald seit dem letzten Laden der nächste planmäßige Termin verstrichen ist. Eine tägliche Liste, die um 14:00 Uhr importiert oder von Hand aktualisiert wurde, läuft deshalb schon in der folgenden Nacht.

War die TrutzBox zum geplanten Termin ausgeschaltet, holt sie den Lauf nach: ab zwei Stunden nach dem verpassten Termin beim nächsten Prüfdurchgang (die Box prüft alle zehn Minuten). Ist der letzte Versuch gescheitert, wartet die Liste auf das nächste reguläre Zeitfenster, damit eine nicht erreichbare Quelle nicht dauernd angefragt wird; zwischen zwei Versuchen derselben Liste liegen mindestens 50 Minuten. Ein fehlgeschlagener Lauf behält die vorhandene Fassung der Liste und zählt den Fehler; nach zwei Fehlschlägen in Folge warnt die Kachel „Filterlisten“ auf der Seite „TrutzBox-Betriebszustand“. Ein Erfolg setzt den Zähler zurück. Eine defekte Liste hält die anderen nicht auf.
Die Vorprüfung im Assistenten nennt neben dem Prüfergebnis auch den Bedarf: die Größe des Downloads, den Platz auf der Festplatte, den Bedarf im Hauptspeicher (der Proxy hält aktive Listen im Arbeitsspeicher, dort wiegt eine Liste rund das Vierfache ihrer Dateigröße), den Spitzenbedarf auf der Festplatte während des Imports und den freien Platz auf der Datenpartition. Übersteigt der Spitzenbedarf den freien Platz, lehnt die Box den Import ab.

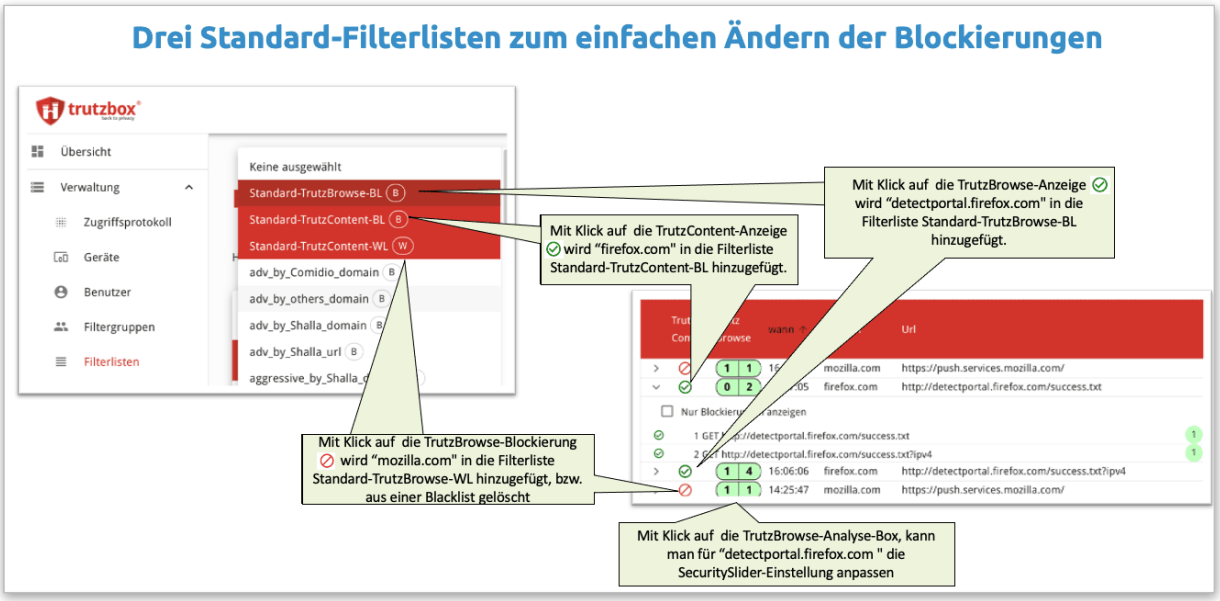
Drei Standard TrutzBox Filterlisten

Es gibt drei Filterlisten mit besonderen Eigenschaften, die vom TrutzBox-Administrator angepasst werden können. Alle drei Filterlisten beginnen mit dem Namen „Standard“: Diese Standardlisten sind geschützt: Sie lassen sich weder umbenennen noch löschen; eigene Einträge können ihnen aber jederzeit hinzugefügt oder daraus entfernt werden. Diese drei Listen gelten immer und auf jedem Gerät, unabhängig davon, welche Filtergruppe dem Gerät zugeordnet ist. Die mitgelieferten Schutzlisten arbeiten ebenso fest im Hintergrund für alle Geräte und lassen sich nicht versehentlich abwählen.

- Standard-TrutzBrowse-BL: diese Liste ist als „TrutzBrowse-Blacklist“ aktiviert. Wenn die TrutzBox einen impliziten Zugriff auf einen Server anzeigt, kann man diesen Server direkt mit einem Klick sperren, indem die URL/Domain in diese Liste übernommen wird.
- Standard-TrutzContent-BL: diese Liste gilt für alle Geräte. Wenn die TrutzBox einen Zugriff auf einen Server anzeigt, kann man diesen Server direkt mit einem Klick sperren, indem die URL/Domain in diese Liste übernommen wird.
- Standard-TrutzContent-WL: diese Liste ist bei allen Geräten und Benutzern als Ausnahme aktiviert (Whitelist). Wenn die TrutzBox einen impliziten oder direkten Zugriff auf einen Server blockiert, kann man diesen Server direkt mit einem Klick freigeben (entsperren), indem die URL/Domain in diese Liste übernommen wird.

Der TrutzBox-Administrator kann diese Listen im Menü „Filterlisten“ verwalten oder in der Monitor-Liste ist es einfacher möglich, in die richtige Liste einen Eintrag vorzunehmen. Dazu können einzelne TrutzBrowse/TrutzContent-Symbole direkt angeklickt werden. Die mitgelieferte Filtergruppe heißt auf allen TrutzBoxen einheitlich „Standard“. Die internen Systemlisten erscheinen nicht in der Gruppenauswahl, weil sie ohnehin immer wirken.

Menüpfad: Verwaltung → Filterlisten



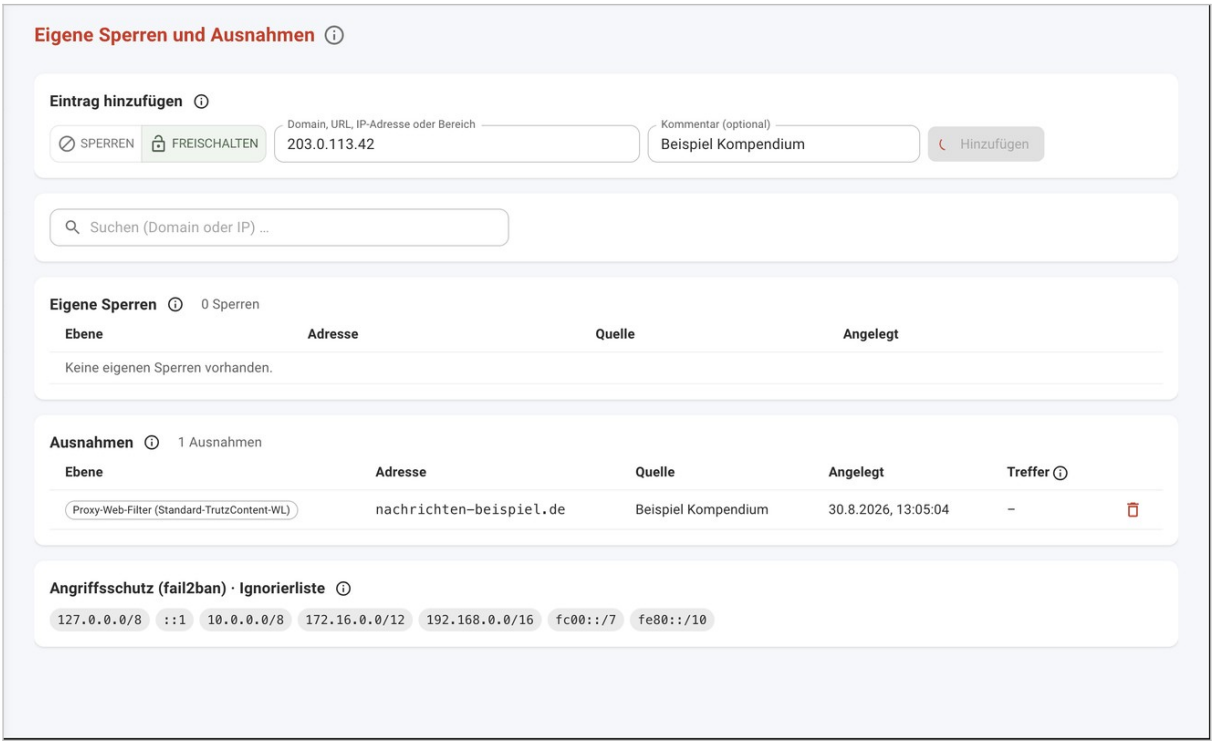
Die drei geschützten Standardlisten der TrutzBox.
(© 2026 Comidio GmbH)

8.3 Eigene Sperren und Ausnahmen

Ob eine Adresse auf Ebene des Web-Filters oder der Firewall gesperrt wird, hängt von ihrer Art ab: Ein Name gehört in eine Filterliste des Web-Filters, eine IP-Adresse in die Firewall. Die Seite „Eigene Sperren und Ausnahmen“ unter „Verwalten“ nimmt dem Administrator diese Entscheidung ab.
Ein einziges Eingabefeld genügt. Die TrutzBox erkennt selbst, was eingegeben wurde: Eine Domain landet in der Ausnahmeliste des Web-Filters, eine IP-Adresse oder ein Adressbereich in den Firewall-Ausnahmen. Die Rückmeldung nennt ausdrücklich, wo der Eintrag gelandet ist, damit die Wirkung nachvollziehbar bleibt.
Ein Umschalter über dem Eingabefeld legt fest, ob der Eintrag eine Sperre oder eine Freigabe werden soll; ein Kommentarfeld nimmt die Begründung auf. Darunter stehen zwei Tabellen, „Eigene Sperren“ und „Ausnahmen“, jeweils mit der Ebene, auf der ein Eintrag wirkt (etwa „Proxy-Web-Filter (Standard-TrutzContent-WL)“), der Adresse, der Herkunft und dem Anlegedatum; bei den Ausnahmen kommt eine Spalte mit der Trefferzahl hinzu. Ein Suchfeld findet einen Eintrag über Domain oder IP-Adresse. Am Fuß der Seite steht zusätzlich die Ignorierliste des Angriffsschutzes mit den Adressbereichen, die nie gesperrt werden. Damit gibt es eine einzige Stelle, an der sich beantworten lässt, warum eine bestimmte Adresse erreichbar ist oder eben nicht.
Ein Sonderfall verdient Beachtung, weil er in der Praxis oft für Verwirrung sorgt: Eine Domain freizuschalten genügt nicht immer. Manche Dienste werden zusätzlich auf Netzwerkebene über die IP-Blockliste gesperrt, weil ihre Server-Adressen in einer eingebundenen IP-Blockliste stehen. Die Freigabe des Namens läuft dann ins Leere, weil die Verbindung schon vorher an der Firewall endet. Nach dem

Freischalten einer Domain zeigt die Seite deshalb, welche ihrer Adressen die IP-Blockliste noch sperrt, und bietet mit einem Knopf die passende Firewall-Ausnahme an.
Am Fuß der Seite steht außerdem die Übersicht „Geräte mit eigenen Ausnahmen“. Sie führt die Geräte auf, denen unter „Verwalten“ → „Geräte“ eine eigene Ausnahmeliste zugewiesen wurde, und kennzeichnet die Geräte, bei denen „Nur Ausnahmen erlauben“ eingeschaltet ist. Die Übersicht ist nur lesend; geändert wird die Zuordnung beim Gerät selbst.

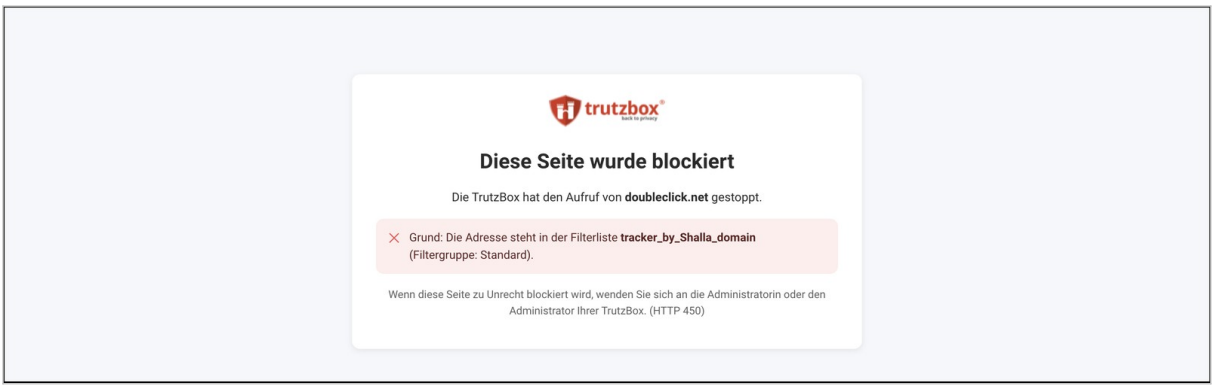
Menüpfad: Verwaltung → Eigene Sperren und Ausnahmen



Die Seite „Eigene Sperren und Ausnahmen“ mit Eingabefeld, eigenen Sperren und Freigaben. (© 2026 Comidio GmbH)

8.4 Was der Anwender bei einer gesperrten Seite sieht

Blockiert die TrutzBox einen Aufruf, beantwortet der Proxy die Anfrage selbst mit dem Statuscode 450 und einer eigenen Hinweisseite im Layout des TrutzBox-Handbuchs. Die Seite nennt die gestoppte Adresse und den Grund: den Namen der Filterliste, die Filtergruppe und die konkrete Regel, die gegriffen hat. Ist die Adresse als Tracker eingestuft, steht das ausdrücklich dabei. Am Fuß der Seite steht der Hinweis, sich an die Administratorin oder den Administrator der TrutzBox zu wenden, falls die Sperre unberechtigt erscheint. Bei einem Gerät im Betrieb „Nur Ausnahmen erlauben“ erscheint stattdessen die Meldung, dass nur freigegebene Ausnahmen erreichbar sind.



Die Sperrseite, die der Anwender bei einem blockierten Aufruf im Browser sieht.
(© 2026 Comidio GmbH)

Diese Hinweisseite kann die TrutzBox nur dort ausliefern, wo sie den Inhalt der Verbindung überhaupt erzeugen darf:

- **Möglich:** bei unverschlüsselten Aufrufen und bei HTTPS-Verbindungen, die mit aktivem TrutzBrowse entschlüsselt werden.
- **Nicht möglich:** Wird schon der Verbindungsaufbau einer verschlüsselten Verbindung abgewiesen (etwa auf Stufe 10 oder bei abgeschaltetem TrutzBrowse), gibt es keinen Kanal für eine HTML-Seite.
- **Antwort der Box:** Die TrutzBox antwortet dann mit der reinen Statuszeile 450 und stellt den Sperrgrund zusätzlich in eine Kopfzeile, die sich im Zweifelsfall vom betroffenen Gerät aus auslesen lässt.
- **Anzeige am Gerät:** Der Browser meldet in diesem Fall nur einen allgemeinen Verbindungsfehler, Apps oft gar nichts.

Das ist keine Fehlfunktion, sondern die Folge davon, dass eine verschlüsselte Verbindung ohne Entschlüsselung nicht beschrieben werden kann.
Die Hinweisseite erscheint in der Sprache, die der Browser des Geräts anfordert (Deutsch, Englisch oder Niederländisch). Sie wird mit der Anweisung ausgeliefert, sie nicht zwischenzuspeichern. Sonst zeigte ein Browser die gespeicherte Sperrseite auch dann noch an, wenn die Adresse längst freigegeben ist.
Auch auf Stufe 10 des SecuritySliders, auf der die TrutzBox verschlüsselte Verbindungen nicht öffnet, prüft der Proxy den ersten Aufruf: Der angesteuerte Server wird beim Verbindungsaufbau gegen die Sperrlisten der Filtergruppe geprüft und bei einem Treffer abgewiesen. Alles, was danach innerhalb der verschlüsselten Verbindung geladen wird, bleibt auf Stufe 10 unsichtbar und wird nicht geprüft. Wird eine solche Verbindung abgewiesen, antwortet der Proxy mit dem Statuscode 450 und der Kopfzeile „X-TRUTZBOX-BLOCKED“, die Filtergruppe, Filterliste und Regel als Text enthält. Browser zeigen diese Kopfzeile nicht an; der Support kann sie vom betroffenen Gerät aus mit einem Kommandozeilen-Werkzeug (etwa „curl -v“) auslesen, um den Sperrgrund zu ermitteln.

9 TrutzBrowse

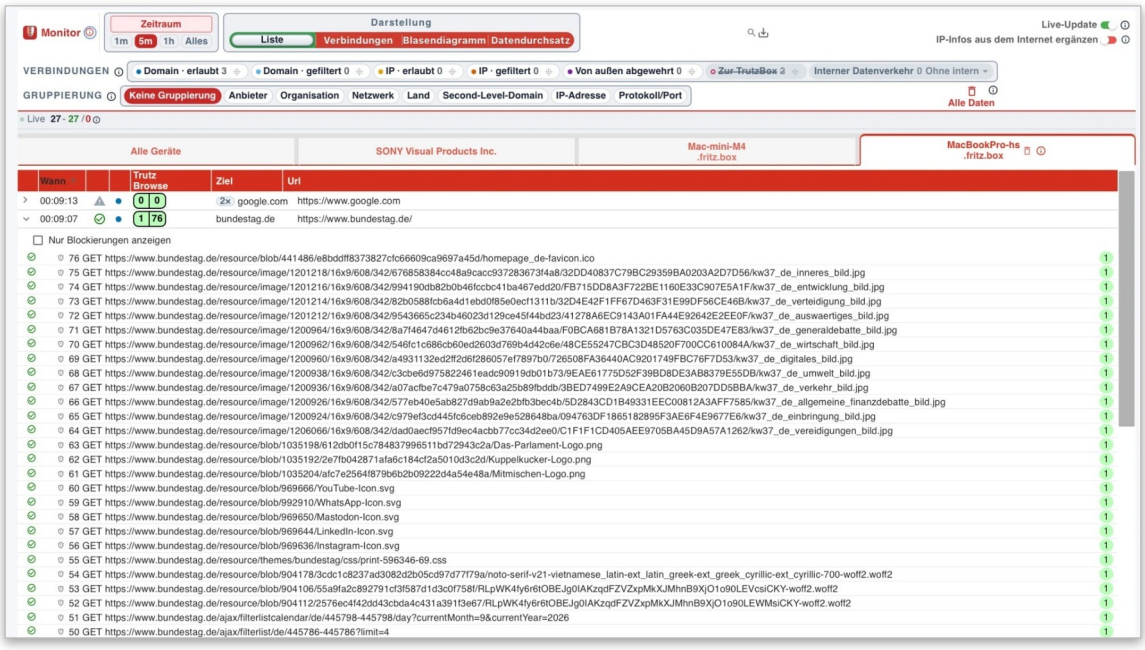
9.1 TrutzBrowse: verräterische Daten aus der Internet-Kommunikation herausfiltern

TrutzBrowse setzt an, sobald TrutzContent einen Zugriff erlaubt hat: Der TrutzBox-Proxy „neutralisiert“ die gesendeten Daten soweit möglich, damit der Server kein Profil des Aufrufers erstellen kann („Browseranonymität“), und zwar bei allen Zugriffen auf Web-Server, auch von Apps und IoT-Geräten. Die Abgrenzung zu TrutzContent beschreibt das Kapitel „TrutzContent und TrutzBrowse: neben der Firewall zwei weitere Schutzebenen“.

Woran man TrutzBrowse im Monitor erkennt

Am schnellsten wird der Unterschied in der Liste des Monitors sichtbar. Sobald für ein Gerät TrutzBrowse eingeschaltet ist, führt die Liste eine eigene Spalte „TrutzBrowse“, und jede Zeile lässt sich aufklappen. Darunter stehen dann alle Einzelabrufe, die der Browser für diese eine Seite nachgeladen hat, jeder mit seiner eigenen Adresse. Ohne TrutzBrowse sieht die Box bei verschlüsselten Verbindungen nur den angefragten Server, nicht die einzelnen Dateien dahinter.

Menüpfad: Monitor



Ein aufgeklappter Seitenaufruf in der Liste: Unter www.bundestag.de stehen die 76 Einzelabrufe, die der Browser für diese Seite nachgeladen hat.
(© 2026 Comidio GmbH, TrutzBox-Bildschirmkopie)

Das farbige Oval in der Spalte „TrutzBrowse“ fasst jeden Seitenaufruf in zwei Zahlen zusammen.



Das Oval eines Seitenaufrufs: links die gesperrten, rechts alle Server-Kontakte.
(© 2026 Comidio GmbH, TrutzBox-Bildschirmkopie)

- Die linke Zahl nennt die Server-Kontakte, die TrutzBrowse bei diesem Aufruf gesperrt hat.
- Die rechte Zahl nennt alle Server-Kontakte, die der Aufruf ausgelöst hat. Im Beispiel oben hat die eine Seite 76 weitere Abrufe nach sich gezogen, von denen einer gesperrt wurde.
- Die Farbe zeigt die Stufe des SecuritySliders für genau diese Seite, von hellgrün bei Stufe 1 über Gelb- und Orangetöne bis Rot bei Stufe 9.
- Ein Klick auf das Oval öffnet den SecuritySlider für diese Domain, die Stufe lässt sich also direkt aus der Liste heraus ändern.

Ist TrutzBrowse für das Gerät ausgeschaltet, steht an dieser Stelle statt des Ovals ein grünes Schild-Symbol. Die Spalte selbst erscheint nur, wenn im gewählten Zeitraum überhaupt ein Aufruf mit eingeschaltetem TrutzBrowse aufgezeichnet wurde.

Im Folgenden werden die Bestandteile von TrutzBrowse näher beschrieben.

HTTP-Header korrigieren

Beim Aufruf einer Webseite sendet der Browser im HTTP-Header Daten an den Server. In der weiteren Kommunikation zwischen Web-Server und Browser, liefert der Server auch Daten an den Browser zurück und kann im HTTP-Header weitere Daten vom Browser abfragen[5]. Über diese Kommunikation kann ein Web-Server die einzigartigen Daten des Clients und des Umfelds des Clients einsammeln (z. B. Betriebssystem-Version des Rechners).
Damit kann der Server einen Client-basierten Fingerprint erstellen. Beim späteren Aufruf weiterer Webseiten kann ein Server den Internet-Nutzer nun wiedererkennen. Im Laufe der Zeit kann ein Tracking-Server auf diese Weise ein umfangreiches Nutzerprofil erstellen.
Einem Web-Server gar keine Header-Daten zu liefern ist manchmal keine gute Alternative, da diese Daten gelegentlich dazu verwendet werden, die einzelnen Elemente auf der angeforderten Webseite so aufzubereiten, dass sie optimal auf dem Endgerät angezeigt werden können. Außerdem könnte der Tracking-Server merken, dass ihm keine brauchbaren Fingerprints mehr geliefert werden und der Tracker-Betreiber könnte sein Fingerprinting daraufhin optimieren.
Manchmal ist es besser, dem Web-Server möglichst solche Informationen zu liefern, deren individuelle Zusammenstellung bei möglichst vielen anderen Internet-Benutzern ebenso auftritt. Somit ist der einzelne Nutzer nicht mehr von der Menge anderer Nutzer mit gleichem Nutzerprofil zu unterscheiden.

5 http://www.iana.org/assignments/message-headers/message-headers.xhtml

http://de.wikipedia.org/wiki/Liste_der_HTTP-Headerfelder

Manche Webseiten sind wiederum so programmiert, dass sie diese HTTP-Header Informationen für die richtige Funktionsweise der Webseite benötigen. Dann kann es vorkommen, dass solche Webseiten nicht mehr richtig funktionieren, wenn man diesen Webseiten nicht alle Informationen zurückgibt. Es kann also passieren, dass plötzlich einzelne Bereiche auf einer Webseite fehlen oder ein Login nicht funktioniert.

9.2 TrutzBrowse: die zusätzliche Tiefenfilterung

TrutzBrowse ist eine optionale Erweiterung, die zusätzlich zu TrutzContent eingeschaltet werden kann. Sie setzt eine Stufe tiefer an: Während TrutzContent nur den Verbindungsaufbau prüft, kontrolliert TrutzBrowse die Inhalte der erlaubten Verbindungen. Dazu werden verräterische HTTP-Header verschleiert, unerwünschte Cookies blockiert, Browser-Fingerprints reduziert und implizite Folgeaufrufe (Tracker auf eingebetteten Drittseiten) gegen separate, schärfere Listen abgeglichen.

TrutzBrowse: Vorteile

Selbst Verbindungen, die TrutzContent passieren lässt, werden inhaltlich entschärft. Damit erreicht TrutzBrowse einen Anonymisierungsgrad, der unabhängig vom verwendeten Browser greift. Ein Schwerpunkt ist die Erkennung impliziter Drittaufrufe, etwa eingebetteter Werbe- oder Statistik-Server, die eine Webseite im Hintergrund nachlädt; rein domain-basierte Filter setzen an dieser Stelle nicht an.

TrutzBrowse: Nachteile

TrutzBrowse muss verschlüsselte Verbindungen aufbrechen, um deren Inhalte analysieren und anonymisieren zu können. Daraus ergeben sich mehrere praktische Einschränkungen:

- **Stammzertifikat erforderlich:** Auf jedem Gerät mit TrutzBrowse muss das TrutzBox-Stammzertifikat installiert sein; manche Apps und Smart-Home-Geräte lassen sich gar nicht oder nur eingeschränkt mit fremden Zertifikaten versorgen (Einzelheiten im Kapitel „Verschlüsselte (SSL/TLS)-Verbindungen“).
- **Höheres Risiko von Funktionsstörungen:** Durch das Verändern von Headern, Cookies und Inhalten steigt die Wahrscheinlichkeit, dass Webseiten nicht mehr fehlerfrei funktionieren. Login-Vorgänge, Online-Banking, interaktive Web-Anwendungen oder bestimmte Streaming-Dienste reagieren empfindlich auf solche Eingriffe. Wenn solche Probleme im Browser auftreten, kann der Anwender durch den SecuritySlider das Problem meist selbst beheben. Ansonsten muss der TrutzBox-Administrator Einstellungen anpassen.
- **Konfigurations- und Pflegeaufwand:** Wenn eine Seite Probleme macht, muss der Anwender den SecuritySlider für diese Seite anpassen oder TrutzBrowse für das betroffene Gerät zeitweise deaktivieren. Dieser laufende Anpassungsaufwand entfällt bei reiner TrutzContent-Nutzung.

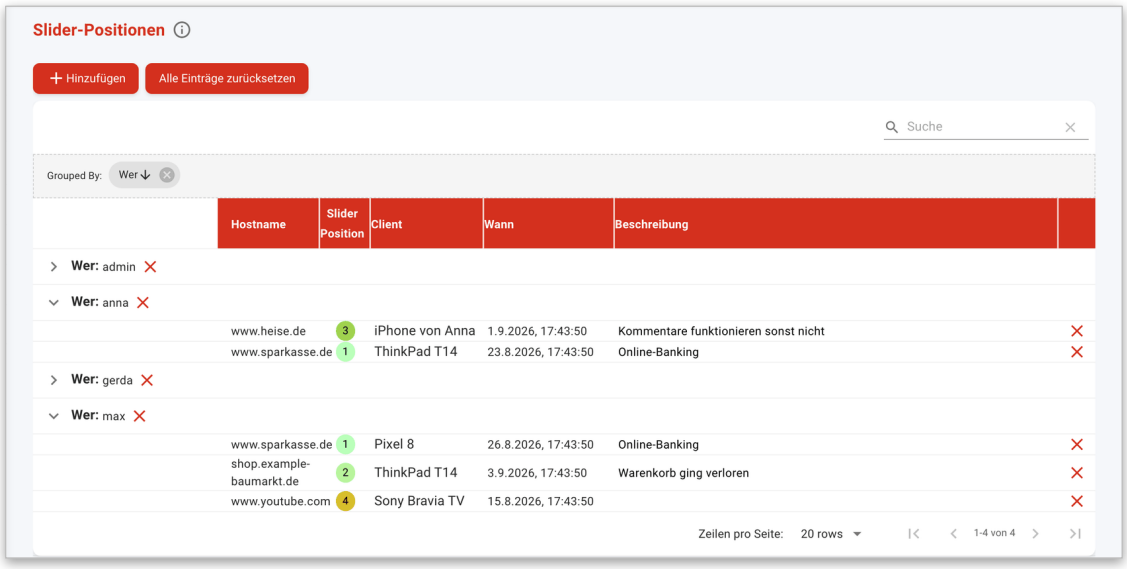
Aus diesen Gründen empfiehlt Comidio, **TrutzBrowse nur von erfahrenen TrutzBox-Nutzern aktivieren zu lassen**, die mit dem SecuritySlider umgehen können und bereit sind, gelegentliche Funktionsstörungen einzelner Webseiten manuell zu beheben. Für Einsteiger und für Geräte, auf denen

Stabilität wichtiger ist als maximaler Anonymisierungsgrad, ist TrutzContent allein bereits ein wirksamer Grundschutz.

9.3 Slider-Positionen

Für welche Server der Slider schon einmal von seiner Standard-Einstellung 1 verschoben wurde, kann der TrutzBox-Administrator im Menü „Slider-Positionen“ sehen und anpassen.

Menüpfad: Browseranonymität → Slider-Positionen

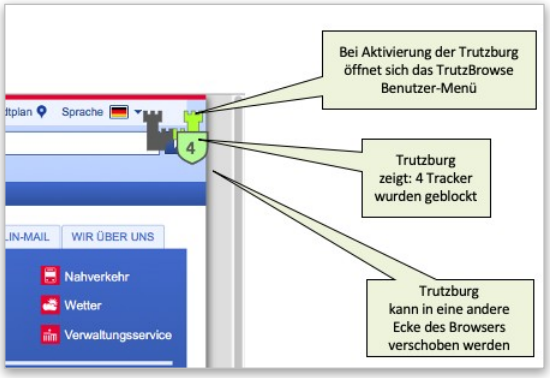


Das Menü „Slider-Positionen“: Server, für die der Slider verschoben wurde.
(© 2026 Comidio GmbH)

Durch Ziehen der Überschrift dieser Auflistung in den grauen Balken „Grouped by“ zeigt die Tabelle die Slider-Positionen gruppiert nach dieser Tabellen-Spalte an. So kann man mit der Gruppierung nach „wer“ mit einem Klick alle Einstellungen von einem „Verursacher“ löschen.
Comidio liefert in den Standardeinstellungen für ein paar wenige Web-Server ein paar oft benötigte Slider-Einstellungen aus. Des Weiteren kann der TrutzBox-Administrator Slider-Einstellungen vornehmen und der Benutzer der TrutzBox ist evtl. auch in der Lage über das eingeblendete TrutzBurg-Symbol im Browser des Anwenders die Position des Sliders zu verändern.
Die Slider-Positionen je Webseite gelten für alle Geräte und Benutzer der TrutzBox: Verstellt ein Anwender für eine Webseite den Security-Slider, wird diese Einstellung gespeichert und wirkt für alle TrutzBox-Anwender. Je Gerät lässt sich zusätzlich unter „Standardposition Slider“ in den Geräte-Detaileinstellungen eine feste Slider-Position für alle Server-Zugriffe dieses Geräts festlegen (siehe Kapitel „Geräte“).
Eine SecuritySlider-Einstellung für eine Domain kann auch unqualifiziert erfolgen, indem linksbündig vor dem „.“ ein „*“ angehängt wird. So kann man nicht nur die Domain „apple.com“, sondern mit „*.apple.com“ auch alle Subdomains wie z. B. „cdn.apple.com“ auf eine SecuritySlider-Position stellen.

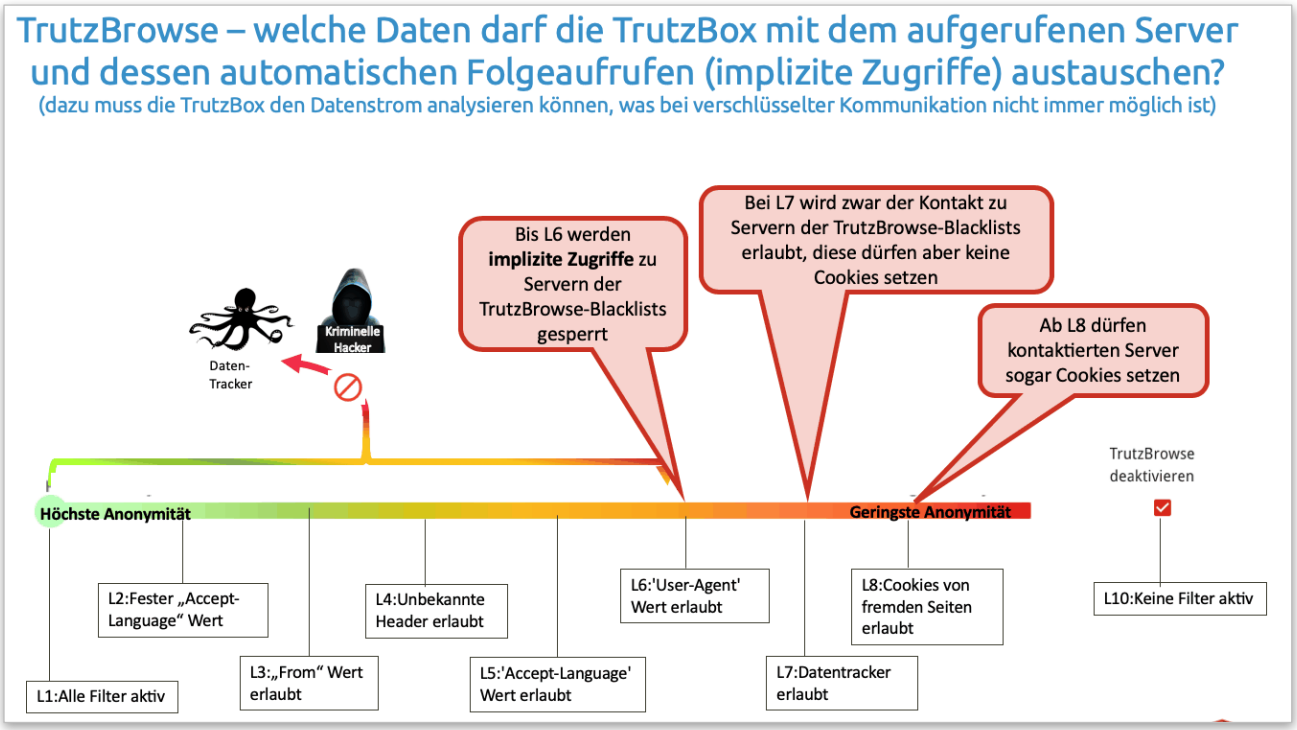
Intelligenter SecuritySlider

Dank der TrutzBrowse-Technologie kann der Sicherheitsgrad einer jeden Webseite mit Hilfe des intelligenten Sicherheits-Schiebereglers (Security-Sliders) jederzeit individuell für einen Server angepasst werden. Falls der Server-Kontakt über einen Browser stattfindet, schleust der TrutzBox-Proxy extra Code in die HTML-Seite ein, sodass die TrutzBurg im Browser angezeigt wird.



Die TrutzBurg im Browser nennt die Zahl geblockter Tracker und lässt sich in eine andere Ecke verschieben.
(© 2026 Comidio GmbH)

Wenn der Benutzer die TrutzBurg anklickt, wird ein Auswahl-Menü angezeigt, das es unter anderem auch erlaubt, den Sicherheits-Schieberegler (SecuritySlider) zu verschieben.
Mit diesem Sicherheits-Schieberegler kann der Nutzer die Sicherheitsstufe der gerade angesteuerten Webseite kontinuierlich reduzieren bzw. erhöhen. Je weniger Sicherheit er für diese Seite einstellt, umso weniger Daten werden von TrutzBrowse gefiltert, und im Gegenzug eventuelle Funktionsstörungen der Seite vermieden.

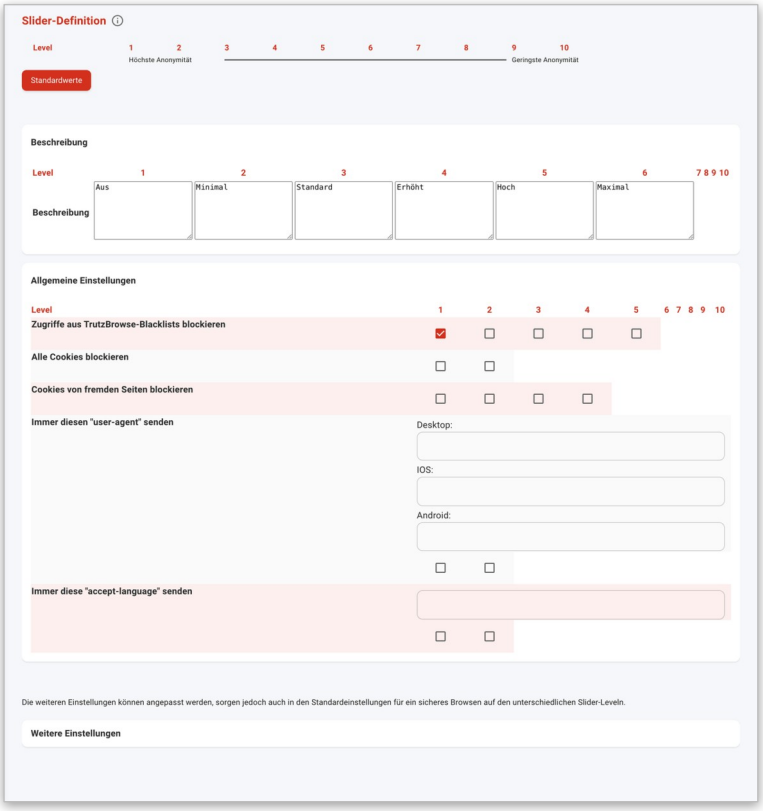


Die zehn Stufen des SecuritySliders und was auf jeder Stufe erlaubt oder blockiert wird.
(© 2026 Comidio GmbH)

Der SecuritySlider kann in neun Positionen (L1 bis L9) verschoben werden; hinzu kommt die Sonderstellung L10, die nicht durch Verschieben erreicht werden kann (siehe unten). Je weiter der SecuritySlider nach rechts verschoben wird, umso mehr „echte Daten“ werden mit dem Server ausgetauscht. Somit bietet die linke Position 1 höchste Anonymität und die rechte Position 9 die niedrigste durch Verschieben erreichbare Anonymität für eine Webseite (Position 10 schaltet alle Filter aus). Wichtig zum Verständnis: L10 schaltet nur die Entschlüsselung der HTTPS-Verbindung ab, nicht den Schutz insgesamt. Die TrutzBox prüft auch auf dieser Stufe den aufgerufenen Server gegen die Sperrlisten der Filtergruppe. Steht er darauf, wird die Verbindung abgewiesen, obwohl gar nicht in sie hineingesehen wird. Unsichtbar bleiben auf L10 nur die Folgeaufrufe innerhalb der verschlüsselten Verbindung, denn genau dafür wäre die Entschlüsselung nötig.
Die Position 10 lässt sich nicht durch Verschieben erreichen, denn auf ihr greift der Proxy nicht mehr in den Inhalt ein: Verschlüsselte Verbindungen werden nicht entschlüsselt, unverschlüsselte ohne TrutzBrowse-Filter durchgereicht, und das TrutzBurg-Symbol lässt sich nicht mehr in die Seite einsetzen. Gesetzt wird Position 10 nur über die entsprechende Option oder automatisch bei Verbindungen, die die TrutzBox nicht aufbrechen kann (Einzelheiten im Kapitel „Verschlüsselte (SSL/TLS)-Verbindungen“).
Was TrutzBrowse in jeder einzelnen Sliderstellung genau filtert, kann der TrutzBox-Administrator im Menü „Slider-Definition“ genau sehen und einstellen.
Die Slider-Definition ist als Matrix aufgebaut: In den Spalten stehen die zehn Stufen (1 bis 10), in den Zeilen die einzelnen Filter; je Zelle legt ein Häkchen fest, ob der Filter auf dieser Stufe aktiv ist. Im Bereich „Allgemeine Einstellungen“ lassen sich u. a. die Optionen „Zugriffe aus TrutzBrowse-Blacklists

blockieren“, „Alle Cookies blockieren“ und „Cookies von fremden Seiten blockieren“ je Stufe schalten sowie feste Werte für „user-agent“ (getrennt für Desktop, iOS und Android) und „accept-language“ hinterlegen. Unter „Weitere Einstellungen“ können zusätzlich einzelne Request- und Response-Header pro Stufe freigegeben oder gefiltert werden. Über „Standardwerte“ lässt sich die gesamte Definition auf die Comidio-Voreinstellung zurücksetzen.
Unterhalb der Matrix liegt der Bereich „Weitere Einstellungen“ mit den beiden Abschnitten „Request Header“ und „Response Header“, also den Kopfzeilen der Anfrage an den Server und seiner Antwort. Dort ist je Kopfzeile hinterlegt, wie TrutzBrowse mit ihr verfährt; die Sammeleinträge „Restliche Header erlauben“ regeln alles, was nicht einzeln aufgeführt ist. Die Voreinstellungen ergeben bereits ein sicheres Surfen, Änderungen sind für Fachleute gedacht.

Menüpfad: Browseranonymität → Slider-Definition



Die Slider-Definition als Matrix: Stufen in den Spalten, Filter in den Zeilen.
(© 2026 Comidio GmbH)

Comidio hat aus der Praxiserfahrung des Comidio-Teams eine Standard-Konfiguration festgelegt, die der Administrator der TrutzBox für seine Sicherheitsbedürfnisse verändern kann.
In diesem Standard wurden folgende 10 Sicherheitsstufen festgelegt:

- **L1:** Alle Filter aktiv
- **L2:** Fester „Accept-Language“ Wert

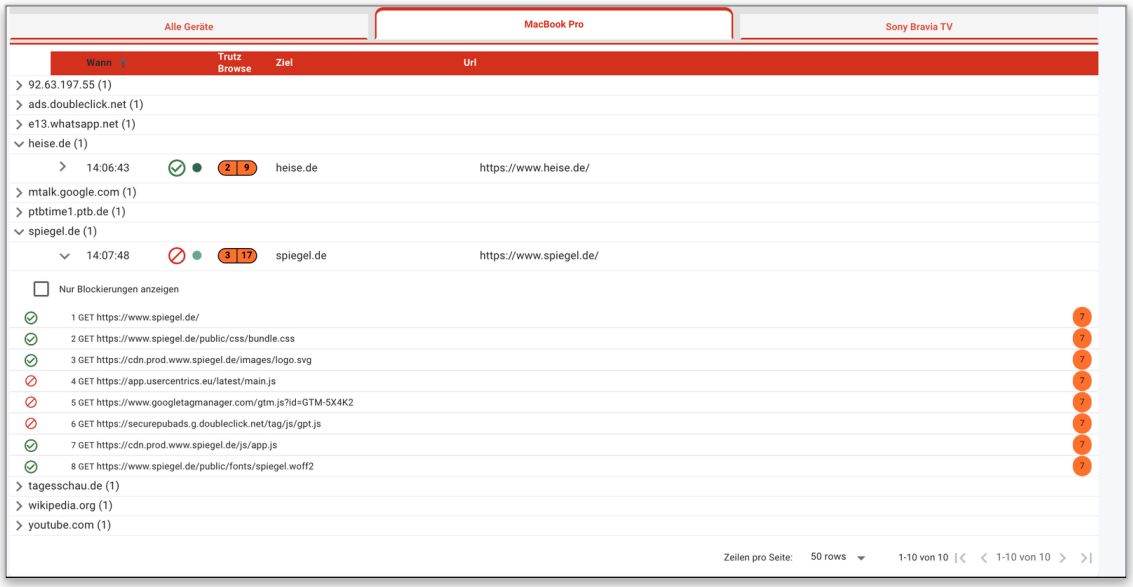
- **L3:** „From“ Wert erlaubt
- **L4:** Unbekannte Header erlaubt
- **L5:** 'Accept-Language' Wert erlaubt
- **L6:** 'User-Agent' Wert erlaubt
- **L7:** Datentracker erlaubt
- **L8:** Cookies von fremden Seiten erlaubt
- **L9:** Derzeit ohne eigene Belegung (wirkt wie L8)
- **L10:** keine TrutzBrowse-Filter aktiv (die TrutzContent-Sperrlisten greifen weiterhin)

In der Standard-Einstellung sind folgende Einstellungen eingestellt:

- Daten-Tracker sind bis Slider-Position L6 geblockt
- Cookies sind zunächst auf allen Stufen erlaubt, aber
- Cookies von fremden Seiten (Third-Party-Cookies) bis einschließlich L7 geblockt. Dadurch können Webseiten, die ohne Tracker nicht funktionieren, auf L7 angezeigt werden. Die dann aktiven Tracker können allerdings keine Cookies setzen und sind somit meist recht unwirksam.
- Der „user-agent“ Wert des HTTP-Protokolls, mit dem ein Server den Hardware- und Betriebssystem-Typ des Clients ermittelt, ist auf ein „Allerwelts-Profil“ der drei verschiedenen Geräte-Typen Desktop, iOS und Android voreingestellt.
- Der „accept-language“ Wert des HTTP-Protokolls ist auf ein „Allerwelts-Profil“ eingestellt.

Der SecuritySlider gilt auch für alle TrutzBrowse Folgeaufrufe

TrutzBrowse kontrolliert und anonymisiert Server-Zugriffe in Abhängigkeit des SecuritySliders. Jedoch nicht nur die Daten des gerade abgerufenen Servers. Die Einstellungen des SecuritySliders gelten sowohl für den gerade abgerufenen Server, als auch immer für alle „Folgeaufrufe einer Webseite“ des ursprünglich aufgerufenen Servers. Die Bildschirmkopie zeigt die aufgeklappten Folgeaufrufe eines Server-Kontakts in der Monitor-Liste: Alle Folgeaufrufe tragen dasselbe Level wie der ursprüngliche Aufruf; als Tracker erkannte Folgeaufrufe darunter sind blockiert (rotes Symbol).



Der SecuritySlider wirkt auch auf alle Folgeaufrufe einer Seite.
(© 2026 Comidio GmbH)

Verschiedene Blockinglisten für TrutzBrowse und TrutzContent

Die Unterscheidung, ob ein Server-Kontakt zu TrutzBrowse oder TrutzContent gehört, ist ein zentrales Merkmal der TrutzBox-Architektur.

Somit ist es möglich, verschiedene Blockinglisten zu nutzen. So kann, wie beim facebook.com-Beispiel im Abschnitt „TrutzContent und TrutzBrowse: neben der Firewall zwei weitere Schutzebenen“, für bewusste Aufrufe (TrutzContent) eine andere Blockingliste gelten als für implizite Folgeaufrufe (TrutzBrowse). Die Blockinglisten für solche „impliziten Folgeaufrufe“ werden durch die TrutzBrowse-Blacklists bestimmt. Wie diese Folgeaufrufe dargestellt werden, zeigt die Bildschirmkopie im vorigen Abschnitt.

Da die TrutzBox jedoch in beiden Fällen lediglich den Aufruf des facebook.com Servers „sieht“, und nicht „wissen“ kann, ob dieser Aufruf durch einen Benutzer bewusst abgerufen wurde oder ein impliziter Aufruf ist, wurden für diese Unterscheidung im TrutzBox-Proxy einige komplexe Algorithmen implementiert.

Die TrutzBox nutzt mehrere Informationen, um zu erkennen, ob ein aufgerufener Server vom Anwender bewusst eingegeben oder angeklickt wurde (TrutzContent), oder ob es ein impliziter Aufruf einer Webseite ist (TrutzBrowse). Das wichtigste Kriterium für diese TrutzBrowse/ TrutzContent Unterscheidung ist der HTTP-Parameter „Referer“, aber auch das Timing zwischen zwei Server-Aufrufen spielt eine Rolle.

So kann es vorkommen, dass bei fehlendem Referer-Hinweis eine zu schnell angeklickte zweite Webseite irrtümlich als TrutzBrowse erkannt wird. In diesem Fall übernimmt die TrutzBox dann irrtümlicherweise den SecLevel der vorherigen Seite.

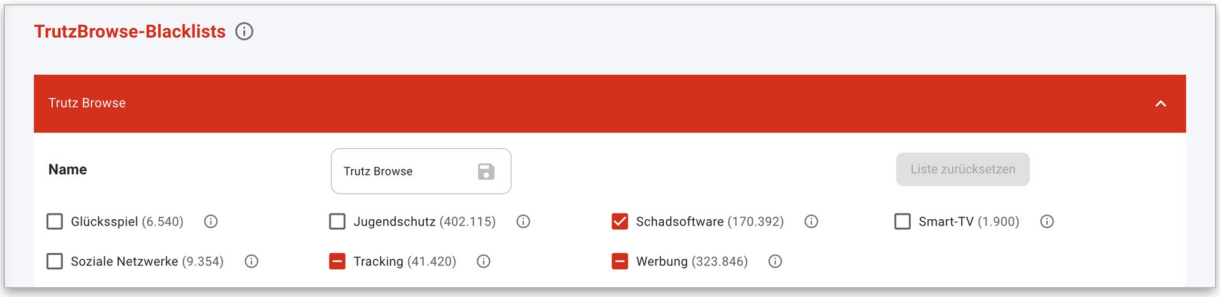
Die TrutzBox kann somit nicht immer mit 100 % Sicherheit feststellen, ob der Anwender die Seite bewusst aufgerufen hat oder ob sie implizit nachgeladen wurde. Wenn man z. B. zu schnell nach dem

Laden einer Seite einen Link dieser Seite in einer Mail anklickt, dann kann es vorkommen, dass die TrutzBox diesen Server-Abruf als TrutzBrowse erkennt, obwohl es ein bewusster Aufruf des Anwenders war und somit unter TrutzContent fallen sollte. Da die TrutzBox dann „denkt“, dass dies jetzt ein impliziter Aufruf sei, kann es vorkommen, dass sie den SecuritySlider-Level der vorherigen Seite übernimmt.
Auch wenn ein bewusst aufgerufener Link auf eine weitere Webseite verweist, kann die TrutzBox evtl. nicht erkennen, dass der zweite Aufruf ein impliziter Aufruf des ersten Links ist. Das kommt z. B. dann vor, wenn man im Google-Suchergebnis einen Link anklickt. Suchmaschinen verlinken Suchergebnisse häufig über eine Weiterleitungsseite, sodass nicht der Ziel-Server direkt angeklickt wird, sondern zunächst eine Seite der Suchmaschine, die dann weiterleitet. So kann der Suchmaschinen-Betreiber nachvollziehen, welcher Eintrag in der Ergebnisliste angeklickt wurde.
Ist diese angeklickte Seite im TrutzBrowse-Filter aktiviert, kann es auch vorkommen, dass dadurch auf dem Bildschirm die TrutzContent Blockierungsmeldung erscheint, obwohl sie gar nicht im TrutzContent-Filter aktiviert ist. Dieser „Nebeneffekt“ kann manchmal durch ein Browser-Refresh umgangen werden.

9.4 TrutzBrowse-Blacklists

In den allgemeinen Einstellungen der Slider-Definition gibt es die Funktion „Zugriffe aus TrutzBrowse-Blacklists blockieren“. Standardmäßig werden bis Slider-Position 6 Datentracker blockiert. Welche Server hier blockiert werden sollen, kann im Menü TrutzBrowse-Blacklists eingestellt werden. Ähnlich wie auch bei den TrutzContent Filtergruppen Einstellung, werden dazu die zu blockierenden Filterlisten aus einer Liste von Content-Gruppen ausgewählt.

Menüpfad: Browseranonymität → TrutzBrowse-Blacklists

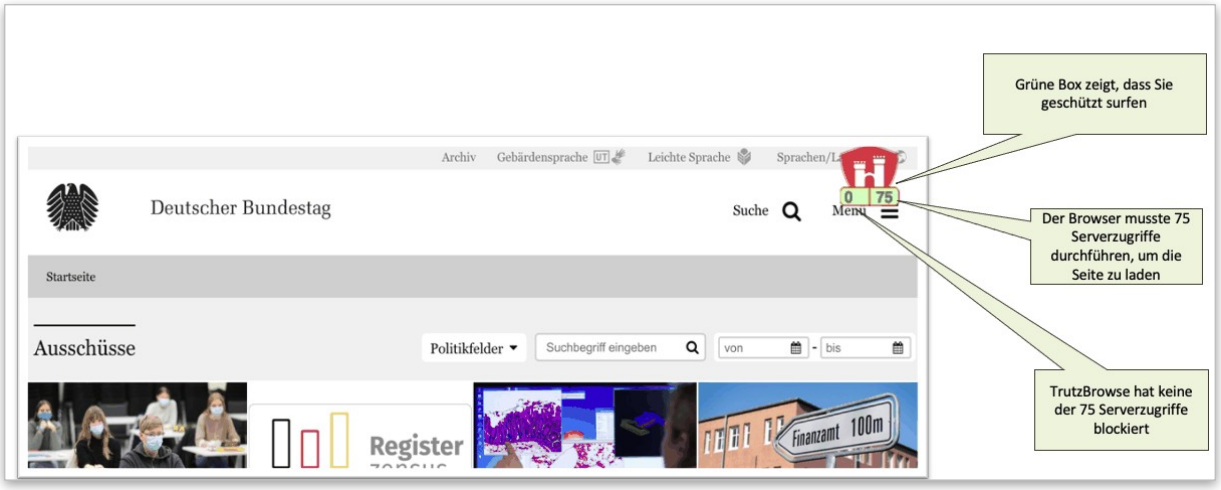


Das Menü „TrutzBrowse-Blacklists“ mit den Servern, die als Tracker blockiert werden.
(© 2026 Comidio GmbH)

9.5 TrutzBurg-Symbol im Browser

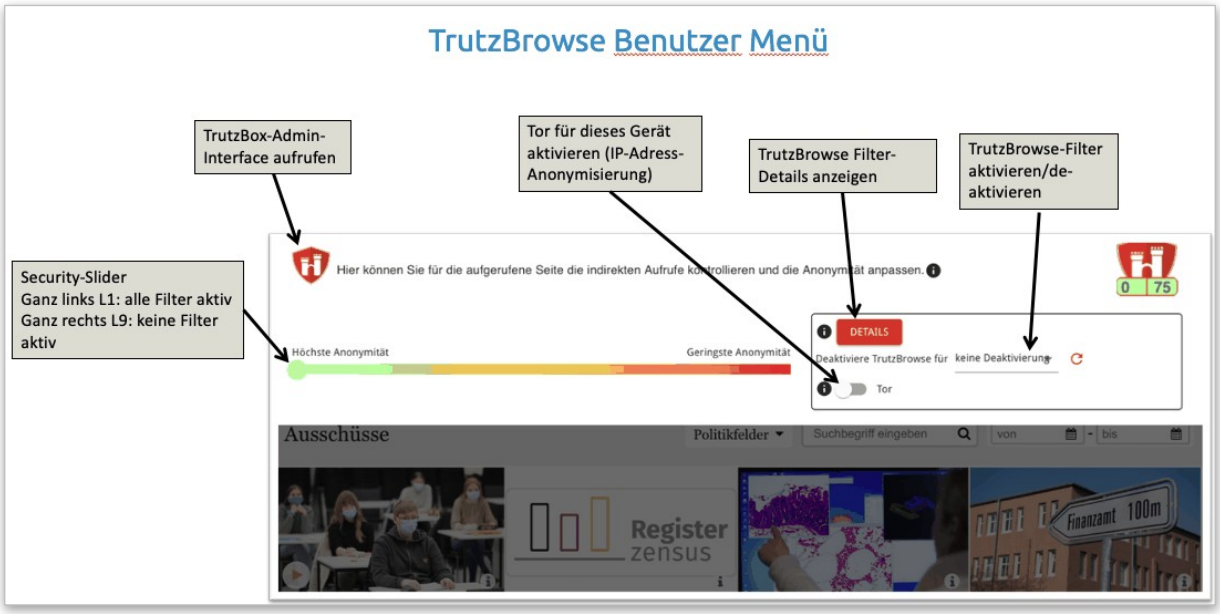
Immer wenn bei der Internet-Nutzung TrutzBrowse aktiviert ist und somit die TrutzBox Anonymitätsfunktionen genutzt wurden, zeigt der Browser oben rechts das TrutzBurg Symbol an. Des Weiteren wird auf dem TrutzBurg Symbol angezeigt, ob Tor aktiv ist (also auch die IP-Adresse anonymisiert wurde), wie viele indirekten weitere Server-Zugriffe der Browser benötigte um die Seite zu

laden und wie viele Zugriffe dabei auf Tracker-Server komplett blockiert wurden. Die Farbe der SecuritySlider-Box entspricht dem aktuellen Security Level für diese Seite.



Das TrutzBurg-Symbol im Browser zeigt an, dass TrutzBrowse für diese Seite aktiv ist.
(© 2026 Comidio GmbH)

Falls sich Bedienelemente auf der Webseite befinden, die durch die TrutzBurg verdeckt werden und somit nicht mehr bedienbar sind, kann die TrutzBurg auf eine andere Ecke des Browser-Fensters verschoben werden. Bei Touch-Screens dazu einfach das Symbol länger als eine Sekunde berühren. Eine veränderte TrutzBurg-Position wird pro Seite gespeichert, sodass die TrutzBurg-Position nur einmal angepasst werden muss.
Nach Anklicken der TrutzBurg stehen der SecuritySlider und weitere Funktionen zur Verfügung:



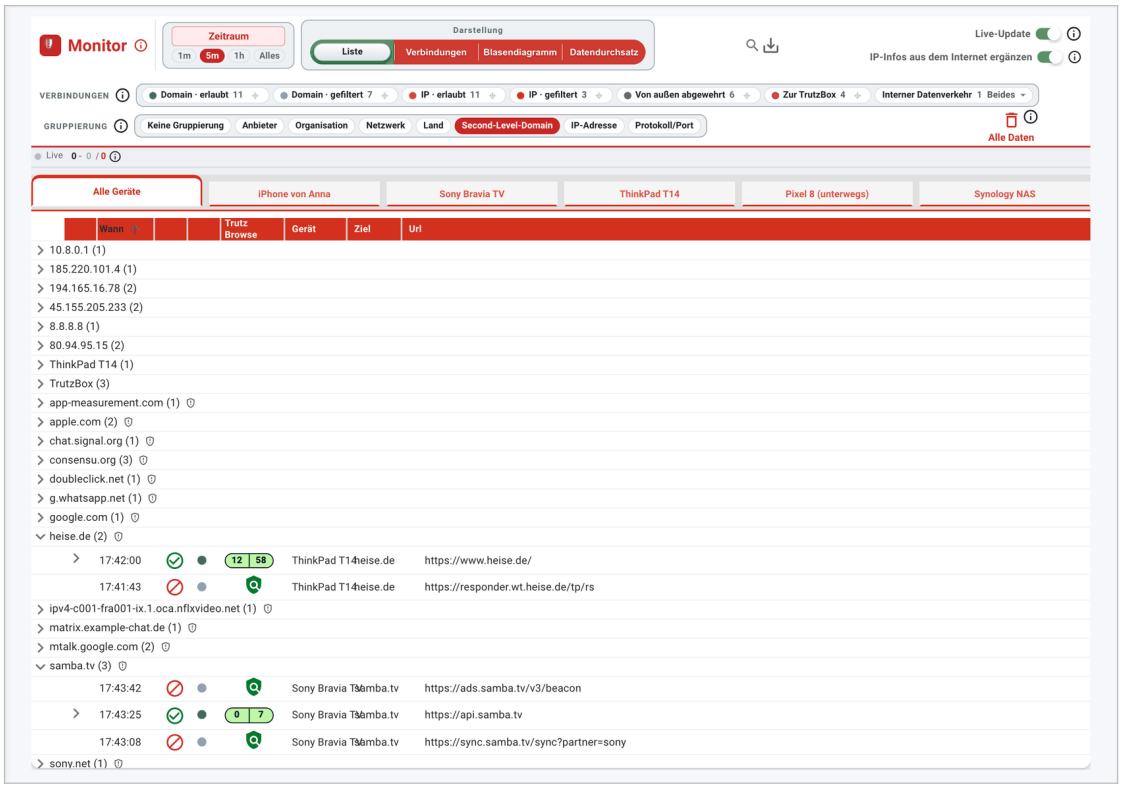
Nach dem Anklicken der TrutzBurg erscheinen SecuritySlider und weitere Funktionen.
(© 2026 Comidio GmbH)

Standardmäßig steht der SecuritySlider ganz links auf Stufe 1 (grün); auf dieser Stufe ist die größtmögliche Sicherheit eingestellt. D.h. alle Sicherheits- und Anonymisierungs-Möglichkeiten der TrutzBox sind aktiv. Falls die Webseite Funktionsstörungen zeigt, weil sie z. B. einen Cookie speichern möchte den TrutzBrowse verhindert, kann der Anwender durch Ziehen des SecuritySliders nach rechts (in Richtung rot) stufenweise einzelne Sicherheits- und Anonymisierungs-Vorkehrungen deaktivieren, um somit die Funktionsfähigkeit der Webseite wiederherzustellen.

9.6 Die Spalte „TrutzBrowse“ in der Liste des Monitors

Was das Zahlenpaar und die Farbe im Oval bedeuten, steht am Anfang dieses Kapitels im Abschnitt „Woran man TrutzBrowse im Monitor erkennt“. Für die Liste gilt darüber hinaus: Der Pfeil am Zeilenanfang öffnet die einzelnen Folgeaufrufe mit ihrer jeweiligen Bewertung. Neue Unterzugriffe einer bereits geöffneten Zeile erscheinen dort laufend, ohne dass die Ansicht neu geladen werden muss. Hat ein Gerät eine Verbindung zwar aufgebaut, aber nie benutzt, steht in der Zeile das Urteil der Sperrlisten, also ob das Ziel gesperrt gewesen wäre, wenn tatsächlich eine Anfrage gekommen wäre.

Menüpfad: Monitor

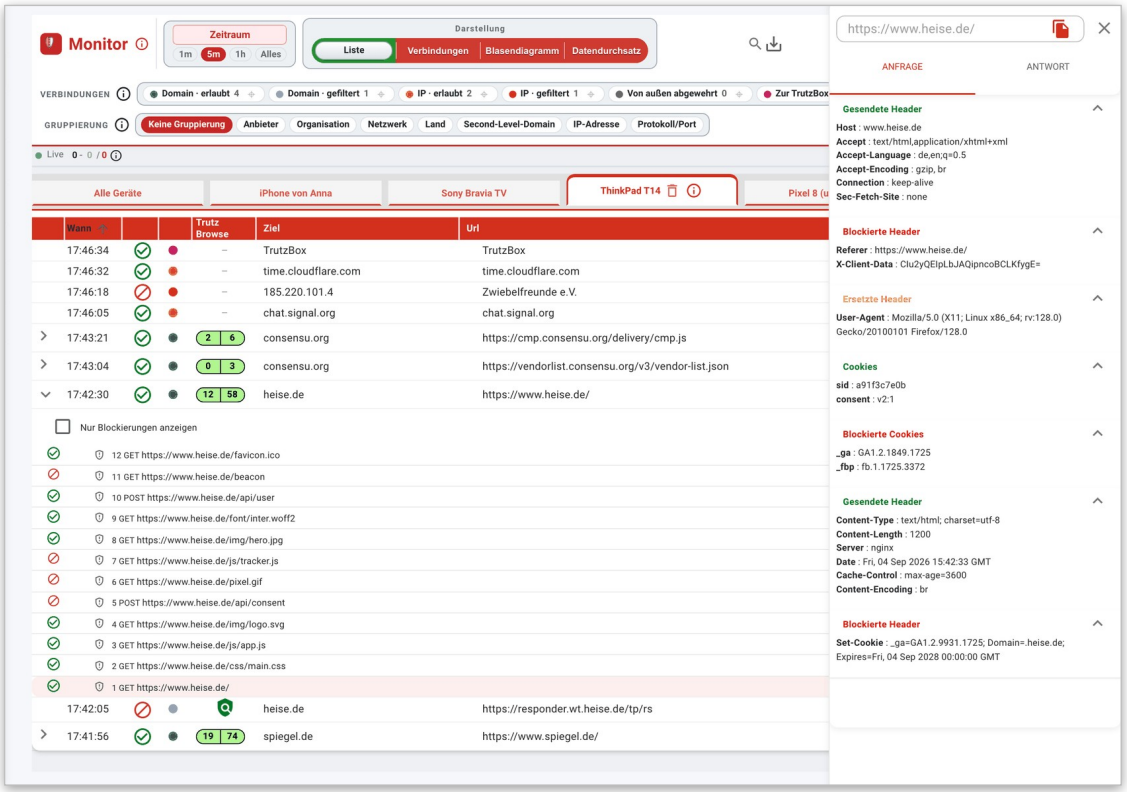


Die Spalte „TrutzBrowse“ mit Slider-Level als Farbe und dem Zahlenpaar der Folgeaufrufe.
(© 2026 Comidio GmbH)

9.7 TrutzBrowse HTTP-Header-Filter

Bei Aktivierung des Detail-Knopfes zeigt TrutzBrowse eine Liste aller von dieser Seite aufgerufenen Web-Zugriffe; hier am Beispiel eines Artikels der Webseite krone.de:

Menüpfad: Monitor

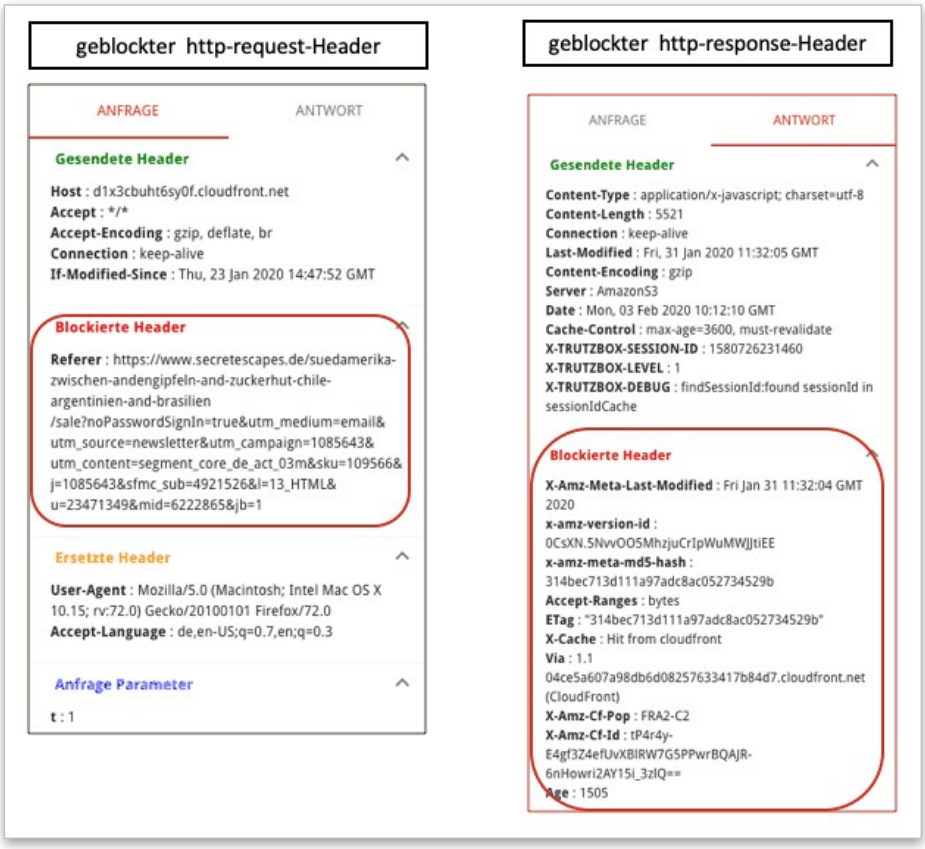


Die Liste aller Folgeaufrufe einer Webseite, aufgeklappt über den Detail-Knopf.
(© 2026 Comidio GmbH)

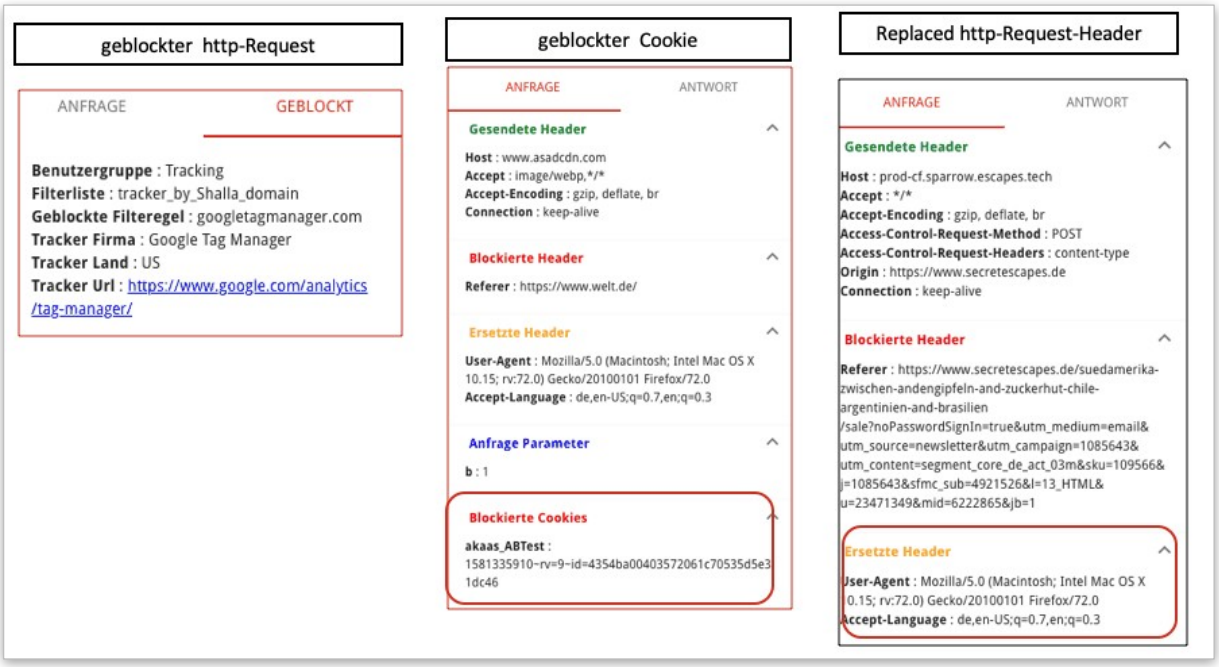
Geblockte HTTP-Aufrufe sind durch gekennzeichnet.

Die Übersicht zeigt auch die HTTP-Aufrufe an, die nicht komplett geblockt wurden (durch gekennzeichnet). Dadurch ist offensichtlich, welche Daten vom Browser an einen Web-Server übermittelt wurden (Tab Request) und welche Daten von einem Web-Server zum Browser gingen (Tab Response).

Für jeden http-Zugriff, werden auf der rechten Seite unter „Details“ die bei jedem Aufruf übertragenen „http-Query Parameter“ und „http-header“ angezeigt. Je nachdem, welche Position des Security-Sliders für diesen Zugriff gilt, werden bestimmte HTTP-Header-Daten gar nicht (Blocked Headers) oder verändert (Replaced Headers) an den Web-Server übermittelt:



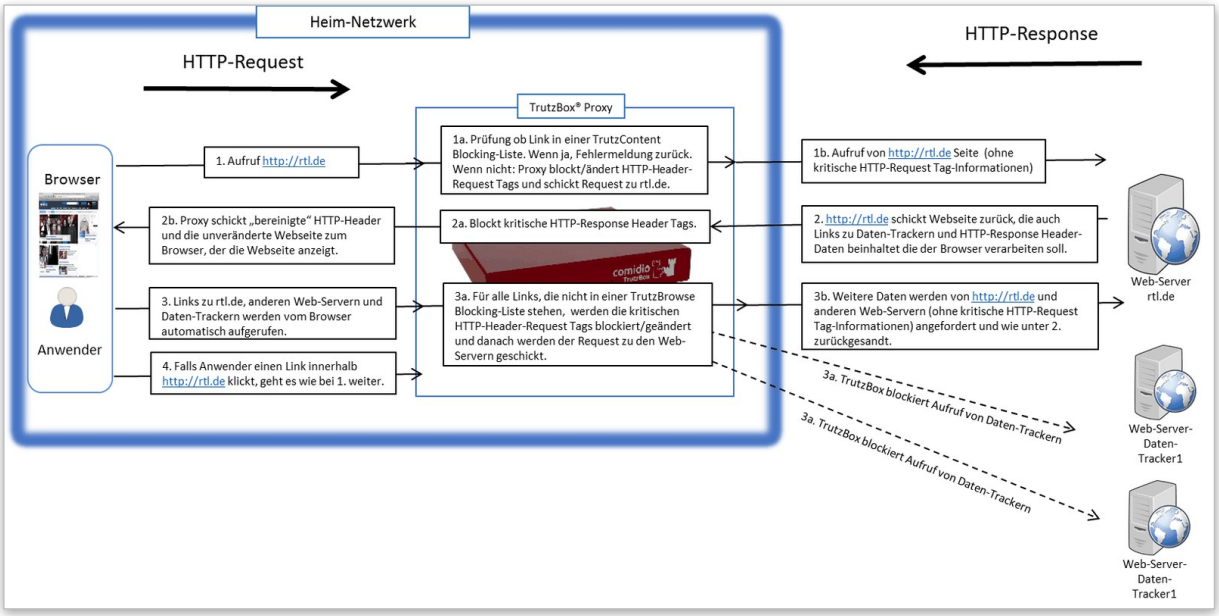
Details eines einzelnen Zugriffs mit Query-Parametern und HTTP-Kopfzeilen.
(© 2026 Comidio GmbH)



Blockierte und ersetzte Kopfzeilen sind eigens gekennzeichnet.
(© 2026 Comidio GmbH)

- Rote Überschriften wie „Blocked request Headers“ oder „Cookies“ bedeuten, dass diese Daten komplett blockiert wurden, also nicht übertragen wurden.
- Grüne Überschriften wie „Sent Headers“ bedeuten, dass diese Daten unverändert übertragen wurden.
- Orange Überschriften wie „Replaced request Headers“ bedeuten, dass der Proxy diese Daten angepasst hat.
- Blaue Überschriften wie „Query parameters“ stehen für die Query-Parameter; sie werden vom Proxy angezeigt, aber nicht verändert.

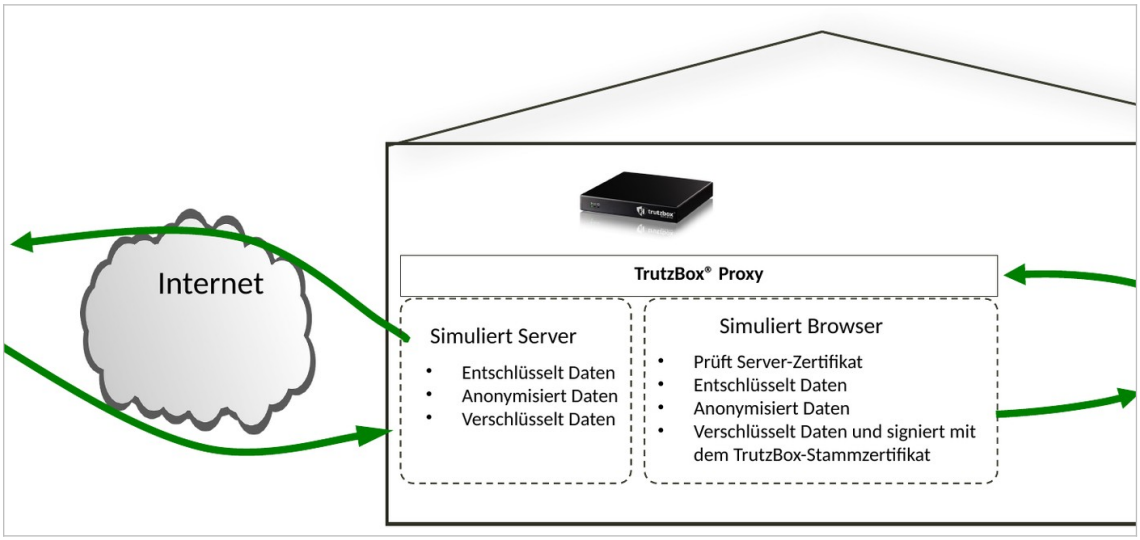
Bei jedem (erlaubten) Zugriff auf einen Web-Server werden vom Web-Browser über den HTTP-Header Informationen an den Web-Server gesandt (http-request-header). Ohne die TrutzBox würde der Browser diese angeforderten Daten dann unverändert an den Web-Server liefern. Das können sehr persönliche Daten sein, wie z. B. welche weiteren Seiten riefen Sie in der letzten Zeit auf, sind Sie gerade bei Facebook eingeloggt oder wie sieht Ihre PC/Browser Konfiguration genau aus, um Sie bei weiteren Aufrufen wiederzuerkennen. Mit dem HTTP-Header-Filter wird auch das Setzen und Abrufen von Cookies kontrolliert.
Die TrutzBox ist mit ihrer TrutzContent/TrutzBrowse-Funktion somit in der Lage, den über den Proxy laufenden HTTP-Datenaustausch zu kontrollieren und HTTP-Header-Daten zu blockieren bzw. zu ersetzen, soweit sie nicht unbedingt benötigt werden.



Der Weg einer Anfrage durch TrutzContent und TrutzBrowse, mit Prüfung von Anfrage und Antwort.
(© 2026 Comidio GmbH)

9.8 Verschlüsselte (SSL/TLS)-Verbindungen

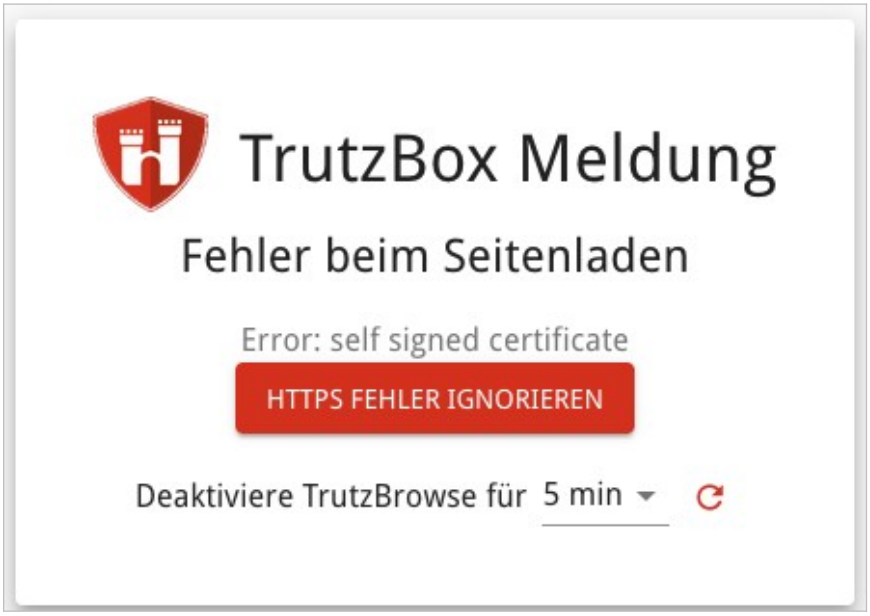
Immer mehr Web-Server unterstützen eine verschlüsselte Verbindung mit dem Endgerät (SSL/TLS). Das ist gut so, damit niemand, der Daten zwischen Endgerät und Web-Server abfangen kann in der Lage ist, Daten mitzulesen oder sogar zu manipulieren. Dadurch wird das Surfen im Internet sicherer.



Warum das Stammzertifikat auf das Gerät muss: Der Proxy beendet die TLS-Verbindung zum Server und stellt dem Gerät ein von der TrutzBox signiertes Zertifikat aus.
(© 2026 Comidio GmbH)

Da die TrutzContent-Funktion lediglich prüft ob ein Link aufgerufen werden darf und dazu nicht in die übertragenden Daten hineinschauen muss, hat TrutzContent auch kein Problem mit verschlüsselten Daten.
Die TrutzBrowse-Funktion kann jedoch den Datenstrom zwischen Browser, App oder IoT-Gerät und einem Server im Internet analysieren und anonymisieren. Eigentlich wäre die TrutzBox nicht in der Lage, diese verschlüsselten Daten zu analysieren, da die Verschlüsselung Ende-zu-Ende stattfindet, also zwischen Web-Browser und Web-Server. Um eine Datenanalyse dennoch zu ermöglichen, verhält sich die TrutzBox zu dem Browser des Teilnehmers wie ein Server und baut in diesem Fall auf der einen Seite eine verschlüsselte Verbindung zum Browser (Proxy-Funktion) und auf der anderen Seite zum Web-Server auf.
Dies ist eigentlich typisch für einen „Man-in-the-Middle“ Angriff. Allerdings stellt ein der TrutzBox zugeordnetes Stammzertifikat sicher, dass die Verbindung vom Endgerät als sicher anerkannt wird. Nur für Geräte bzw. Browser, bei denen es möglich ist das TrutzBox-Stammzertifikat zu importieren, kann die TrutzBrowse Analyse der ausgetauschten Daten durchgeführt werden. Für Geräte, bei denen kein Stammzertifikat importiert werden kann, sollte man TrutzBrowse in der Geräte-Verwaltung abschalten.
Wenn die TrutzBrowse Funktion aktiv ist, verhält sich die TrutzBox gegenüber dem Server wie ein Browser und akzeptiert alle ihr bekannten Zertifikate (genauer gesagt, sie akzeptiert alle Zertifikate, die mit einem ihr bekannten Root-Zertifikat signiert wurden). Die Liste der Root-Zertifikate, die die TrutzBox im Namen des Nutzers akzeptiert, ist in der TrutzBox fest hinterlegt und nicht durch den Benutzer veränderbar.
In der Grundeinstellung sind alle St-Zertifikate, die durch das Debian-Update automatisch verteilt werden geladen. Dadurch werden sie auch von der TrutzBox akzeptiert. Die Liste dieser Stamm-Zertifikate wird von der TrutzBox regelmäßig aus dem Debian „ca-certificates Paket“[6] übernommen.
Falls die TrutzBox ein Server-Zertifikat nicht als vertrauenswürdig erkennt, wird der Anwender gefragt, ob er trotzdem diese Seite laden möchte. Solche Zertifikats-Fehler können mit badssl.com sehr gut simuliert werden.

[6] https://packages.debian.org/de/jessie/ca-certificates



Fragt die TrutzBox bei einem nicht vertrauenswürdigen Server-Zertifikat nach.
(© 2026 Comidio GmbH)

Wenn ein solcher Fehler von einem Browser erkannt wird, kann man den Fehler ignorieren oder TrutzBrowse für eine ausgewählte Zeit ausschalten. Warnung: Wer einen Zertifikatsfehler ignoriert, verzichtet für diese Verbindung auf die Prüfung, ob der Server echt ist; das sollte nur bei bekannten und vertrauenswürdigen Servern geschehen. Warnung: Wer einen Zertifikatsfehler ignoriert, verzichtet für diese Verbindung auf die Prüfung, ob der Server echt ist; das sollte nur bei bekannten und vertrauenswürdigen Servern geschehen.

Was muss auf Client- bzw. auf Geräte-Seite sichergestellt werden, damit die TrutzBox verschlüsselten Datenverkehr analysieren kann (TrutzBrowse)?

Die TrutzBox generiert beim Setup der TrutzBox ein Root-Zertifikat (Stamm-Zertifikat), das über die TrutzBox Bedienoberfläche heruntergeladen werden kann. Jede von einem Gerät angesteuerte Webseite, wird von der TrutzBox (genau genommen vom Proxy der TrutzBox) mit diesem Root-Zertifikat signiert, bevor die Daten an den Client weitergeleitet werden. Dieses Root-Zertifikat sollte bei Nutzung von TrutzBrowse dem Client-Programm bekannt sein.

Wenn der Client dieses Stammzertifikat kennt wird verhindert, dass der Browser oder andere Programme wie z. B. ein E-Mail-Client bei jeder Verbindung zur TrutzBox nachfragen muss, ob diese Verbindung vertrauenswürdig ist.

Leider verwaltet jedes Betriebssystem und jedes Programm auf Client-Seite diese Stammzertifikate unterschiedlich. Somit ist es in manchen Fällen nicht nur notwendig, das TrutzBox-Stammzertifikat auf jedes Gerät zu laden, sondern abhängig davon, welcher Browser und welches Mail-Programm benutzt wird, muss das Zertifikat evtl. auch noch zusätzlich, einmalig in ein Programm importiert und bestätigt werden.

Glücklicherweise nutzen die meisten Programme den Zertifikatsspeicher des Betriebssystems. Dann muss es nur einmalig in den Zertifikatsspeicher des Betriebssystems geladen werden. Die Programme

von Mozilla (Firefox, Thunderbird) führen einen eigenen Zertifikatsspeicher; je nach Version und Einstellung können sie zusätzlich den Speicher des Betriebssystems berücksichtigen.
Diese Übersicht zeigt, welche Programme die Zertifikate selbst verwalten und welche den zentralen Schlüsselbund des Betriebssystems nutzen:

	Mac OS						Windows							Android				IOS		
	Browser			Mail			App	Browser				Mail		Apps	Browser		Mail	Apps	Browser	Mail	Apps
	Safari	Firefox	Chrome	Apple Mail	Thund erbird	Outlook	z.B. App Store	Internet Explorer (IE)	Firefox	Edge	Chrome	Thund erbird	Outlook		Chrome	Firefox		Play-store			App-Store
Zertifikat wird vom System-Schlüsselbund genommen	x		x	x				x		x	x		x		x		x		x		
Zertifikat muss extra in die Applikation geladen werden		x							x							x mit extra Plugin					
Zertifikat muss nur beim ersten Mal bestätigt werden				x	x	x						x									
Zertifikat ist in der App fest eingestellt und akzeptiert kein anderes Zertifikat							x							x				x			x
Bemerkungen	Mit dem Konsolen-Befehl: open -a "Google Chrome" --args --proxy-pac-url="https://trutzbox/api/proxy/pac" kann man Chrome auch mit Nutzung des Proxies öffnen, ohne dass Chrome die System-Einstellungen für den Proxy nutzt. Wenn man in Chrome den Befehl: chrome://net-internals/#proxy absetzt, dann kann man sehen, ob der Proxy aktiv ist. Wenn der Proxy aus irgendeinem Grund nicht funktioniert, schaltet chrome auf direct-mode um (anders als in firefox).																				

Übersicht, welche Programme eigene Zertifikatsspeicher führen und welche den des Betriebssystems nutzen.
(© 2026 Comidio GmbH)

Apps auf Smartphones (nicht Browser), die eine Verbindung immer zu ihrem gleichen Server aufbauen, haben das Zertifikat des Servers, mit dem sie kommunizieren, oft fest im Programm einprogrammiert. Das Zertifikat kann die TrutzBox nicht ändern und auch nicht mit dem TrutzBox-Stammzertifikat signieren und somit ist es für die TrutzBox technisch nicht möglich, die Daten zu entschlüsseln.
Die TrutzBox hat in diesem Fall zwei Möglichkeiten:

- die Verbindung standardmäßig nicht erlauben, also sperren und es dem TrutzBox-Administrator freistellen, den angesteuerten Server freizuschalten
- oder die Verbindung erst mal zu erlauben und es dem TrutzBox-Administrator freistellen, den angesteuerten Server zu sperren

Die TrutzBox geht hier standardmäßig den zweiten Weg: Kann sie eine verschlüsselte Verbindung nicht aufbrechen, setzt sie den aufgerufenen Server automatisch auf L10, sodass der Zugriff beim nächsten Versuch funktioniert; einen Schalter zur Umkehr dieses Verhaltens gibt es in der aktuellen TrutzBox-Version nicht mehr. So bleibt die Administration der TrutzBox einfach.

Das Stammzertifikat der TrutzBox bleibt über Neustarts und Software-Updates hinweg unverändert:

- **Neuerzeugung:** Sie geschieht nur, wenn das Zertifikat auf der Box fehlt, also nach einer Neuinstallation des Images, nach einem Werksreset oder nach einer Wiederherstellung aus einer Sicherung, die das Zertifikat nicht enthält. Eine Wiederherstellung mit vollständiger Sicherung bringt das vorhandene Stammzertifikat zurück.
- **Neuer Schlüssel:** Jedes neu erzeugte Stammzertifikat ist ein anderes Zertifikat mit neuem Schlüssel; sein Name trägt den Erzeugungszeitpunkt. Die Geräte müssen es dann erneut importieren.
- **Server-Zertifikat:** Das Server-Zertifikat der Box (für https://trutzbox/, Mail und Chat) kann dagegen häufiger neu ausgestellt werden, etwa nach einer Umbenennung der Box. Es wird immer vom selben Stammzertifikat unterschrieben.
- **Ausnahme statt Import:** Wer auf einem Gerät nur das Server-Zertifikat als Ausnahme bestätigt hat, verliert dieses Vertrauen bei jeder Neuausstellung.

Deshalb gehört auf die Geräte immer das Stammzertifikat, nie eine Ausnahme für das Server-Zertifikat. Das Stammzertifikat trägt als Beginn der Gültigkeit bewusst das Jahr 1970 und läuft rund 30 Jahre. Eine frisch aufgesetzte Box hat oft noch keine gestellte Uhr; ein Zertifikat, das „ab jetzt“ gilt, könnte dann in der Zukunft beginnen und wäre ungültig. Der frühe Beginn hat einen Nebeneffekt: Die Grenze von Apple für die Laufzeit von Zertifikaten gilt nur für Zertifikate, die nach dem 1. Juli 2019 ausgestellt wurden; Safari und iOS akzeptieren die lange Laufzeit deshalb.
Nach einem Wechsel des Stammzertifikats sind auf den Geräten die alten TrutzBox-Stammzertifikate und alle einzeln bestätigten Ausnahmen zu entfernen, nicht nur das neue hinzuzufügen. Sammeln sich über Jahre alte Zertifikate und Ausnahmen im Schlüsselbund an, zeigt Safari die Bedienoberfläche der Box unter Umständen nur noch als leere Seite, ohne Fehlermeldung. Abhilfe schafft das Aufräumen im Schlüsselbund und der Import des aktuellen Stammzertifikats.

9.9 Die optimale TrutzBrowse- und TrutzContent-Einstellung

TrutzContent ist immer für alle Geräte aktiv, TrutzBrowse standardmäßig für alle Geräte aus; in den meisten Fällen genügt TrutzContent in den Standard-Einstellungen, TrutzBrowse ist die zusätzliche Anonymisierungsstufe mit gelegentlichem Nachjustier-Aufwand (Einzelheiten im Kapitel „TrutzContent und TrutzBrowse: neben der Firewall zwei weitere Schutzebenen“).

Die in der TrutzBrowse-Funktion per Default eingestellten Header-Filter basieren auf der Erfahrung des Comidio-Teams. Diese Filterwerte sind je nach SecuritySlider-Stellung ein guter Kompromiss zwischen möglichst wenig Funktionalitätseinschränkung bei typischen Webseiten einerseits und Schutz der Privatsphäre andererseits.

Um einen Browser wiedererkennen zu können, ist für einen Tracker besonders der Wert im Feld „user-agent“ wichtig. In diesem HTTP-Header teilt der Browser dem Tracker mit, welcher Browser und welches Betriebssystem gerade genutzt wird. Hier sollte möglichst ein Wert eingesetzt werden, der im Internet am häufigsten Verwendung findet. Im Blog „most-common-user-agents“[7] findet man dazu gute Anregungen.

Weitere Hinweise auf HTTP-Header Anonymisierung sind bei der Beschreibung von Squid[8], JonDo[9] und bei Lutz Donnerhacke[10] zu finden.
Auch die standardmäßig eingestellten TrutzBrowse- und TrutzContent-Filterlisten sind Erfahrungswerte, die einen Kompromiss zwischen möglichst hoher Bedienerfreundlichkeit (möglichst wenig den SecuritySlider verschieben müssen) und hoher Anonymität im Internet darstellen.
Wer noch mehr Anonymität und Schutz im Internet möchte, der kann folgende weitere Punkte „strenger“ einstellen:

- Cookies auch für aufgerufene Seiten auf L1 sperren



- in der Filtergruppe „Standard“ (TrutzContent) weitere Kategorien aktivieren, etwa zur Telemetrie von Betriebssystemen.
- in der TrutzBrowse-Blacklist (TrutzBrowse) zusätzlich die Kategorie „Werbung“ und weitere Tracker-Kategorien aktivieren.
- In der Monitor-Liste regelmäßig überprüfen, ob irgendwelche Geräte immer wieder auf Server des Herstellers zugreifen und diese Zugriffe sperren. Siehe auch Kapitel „TrutzBrowse: verräterische Daten aus der Internet-Kommunikation herausfiltern“.

9.10 Kann die TrutzBox auch zu viel filtern?

Es kann vorkommen, dass die TrutzBox mehr filtert, als der Anwender das wünscht oder so viel, dass eine Anwendung (App) oder der Seitenaufbau im Browser nicht mehr richtig funktioniert.
In diesem Fall kann der Anwender meist über den SecuritySlider im Browser, die an den Server gelieferten Daten so weit anpassen, dass das Problem gelöst wird. Wenn man den SecuritySlider allerdings auf Level 7 oder höher zieht, werden alle Tracker zugelassen. Es kann allerdings manchmal sinnvoll sein, dass man lediglich einen Tracker zulassen möchte.

[7] https://techblog.willshouse.com/2012/01/03/most-common-user-agents/

[8] http://www.squid-cache.org/Versions/v2/HEAD/cfgman/header_access.html

http://wiki.squid-cache.org/SquidFaq/ConfiguringSquid#Can_Squid_anonymize_HTTP_requests.3F

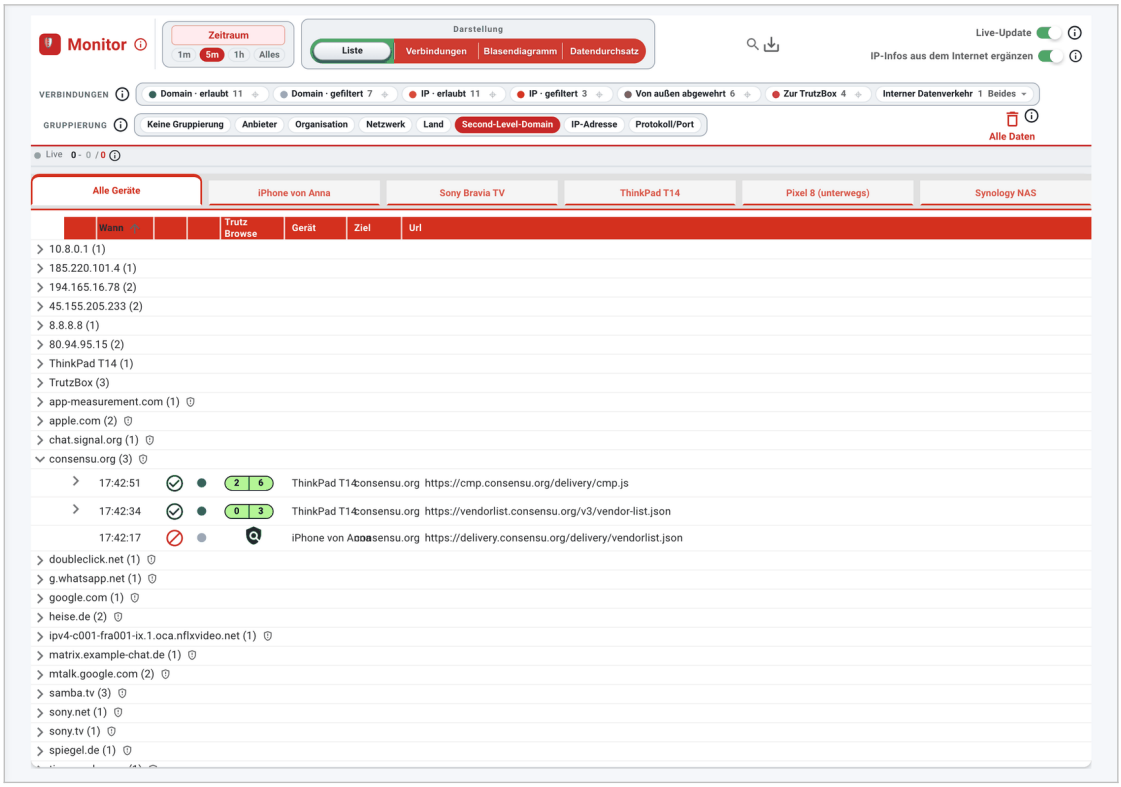
[9] http://ip-check.info/description.php?lang=de

[10] http://altlasten.lutz.donnerhacke.de/mitarb/lutz/anon/web.en.html

Es kann aber auch vorkommen, dass weitere Anpassungen der TrutzBox-Filter notwendig sind, die ein Anwender nicht durchführen kann. Manche Filter-Anpassungen kann nur der TrutzBox-Administrator vornehmen.
Dazu hier ein Beispiel: in den Standard-Einstellungen werden evtl. auch Consent-Management-Links geblockt. Unter Consent-Management versteht man das Einverständnis des Benutzers, z. B. die Benutzung von Cookies einzuholen (also einen Konsens finden). Wenn der Entwickler der Webseite, diese Funktion an eine Firma ausgelagert hat, die evtl. den Benutzer tracken könnte, dann kann es vorkommen, dass der Link zu diesem Dienstleister von der TrutzBox blockiert wird.
Dann wird dem Benutzer evtl. nicht mehr die Frage nach der Benutzung von Cookies angezeigt. Das kann der TrutzBox-Administrator in der Monitor-Liste sehen. Wenn er möchte, kann er diese Blockierung aufheben und der Nutzer der Webseite würde die Consent-Anfrage wieder bekommen.

In diesem Beispiel nutzt berliner-zeitung.de den Dienstleister consensu.org für das Consent-Management; die TrutzBox blockiert den Aufruf von sourcepoint.mgr.consensu.org; im Monitor ist er als blockierte Verbindung markiert:

Menüpfad: Monitor



Ein blockierter Consent-Dienst im Monitor: Hier filtert die TrutzBox mehr, als die Seite verträgt. (© 2026 Comidio GmbH)

Ein Klick auf die blockierte Verbindung öffnet den Detail-Dialog des Monitors; dort kann der TrutzBox-Administrator die Domain sourcepoint.mgr.consensu.org über „Domain erlauben“ direkt freigeben.

9.11 Vergleich auf einen Blick

	TrutzContent	TrutzBrowse
Status	immer aktiv, sobald Verkehr durch die TrutzBox läuft	optional, zusätzlich zu TrutzContent zuschaltbar
Greift auf Ebene	Verbindungsaufbau (Server-Adresse)	Inhalt der Kommunikation (HTTP/HTTPS)
Schützt	alle Geräte im Netz	nur Geräte mit installiertem TrutzBox-Stammzertifikat
Blockiert / verändert	Tracker-Server, Werbe-Domains, Malware-Verteiler	HTTP-Header, Cookies, Browser-Fingerprints, implizite Folgeaufrufe
Voraussetzung am Gerät	keine	TrutzBox-Stammzertifikat installiert
Aktivierung	Filtergruppen-Zuordnung in der TrutzBox	Schalter pro Gerät, Feinjustierung über SecuritySlider
Empfohlen für	alle Anwender	erfahrene Anwender
Risiko		Webseiten können fehlerhaft werden, laufender Anpassungsaufwand

Die Trennung in zwei Ebenen ist ein Grundprinzip der TrutzBox: Sie kombiniert Domain-Sperren und Inhaltsfilterung und kann dadurch z. B. erlauben, dass facebook.com im Browser aufgerufen wird, gleichzeitig aber blockieren, dass eine Shop-Seite implizit Tracking-Daten an Facebook nachlädt.

Internet-Zugriffe gehen immer von einem Gerät im internen Netzwerk aus. Das kann irgendeine Anwendung, also eine App auf einem Smartphone oder IoT-Gerät, oder ein Browser sein. Wenn der Internet-Zugriff, der über Port 80 (http) oder verschlüsselt über Port 443 (https) über die TrutzBox geleitet wird, wird dieser vom TrutzBox-Proxy verarbeitet.
Proxy ist der englische Begriff für „Stellvertreter“. Dieser Proxy verhält sich gegenüber dem aufrufenden Programm wie ein Web-Server und führt dann den eigentlichen Zugriff auf den angeforderten Web-Server durch. Die Antwort vom Web-Server geht in umgekehrter Richtung auch wieder durch den TrutzBox-Proxy, der auch die Antwort des Servers kontrolliert.

Der TrutzBox-Proxy verarbeitet den angeforderten Zugriff in der TrutzBox in zwei Schritten:

- 1. **TrutzContent** prüft zunächst auf Basis der für dieses Gerät eingestellten Filtergruppe, ob der adressierte Server kontaktiert werden darf. Wenn nicht, wird der Zugriff von der TrutzBox blockiert. Welche Filterlisten für ein Gerät genutzt werden sollen, hängt davon ab, welcher Filtergruppe ein Gerät zugeordnet wurde.
- 2. Wenn ein Server im Internet kontaktiert werden darf, wird eine evtl. verschlüsselte Kommunikation entschlüsselt und **TrutzBrowse** filtert die ausgetauschten Daten mehr oder weniger, je nach Einstellung des SecuritySliders. Dieser zweite Schritt wird nur dann durchgeführt, wenn TrutzBrowse für das entsprechende Gerät aktiviert wurde.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

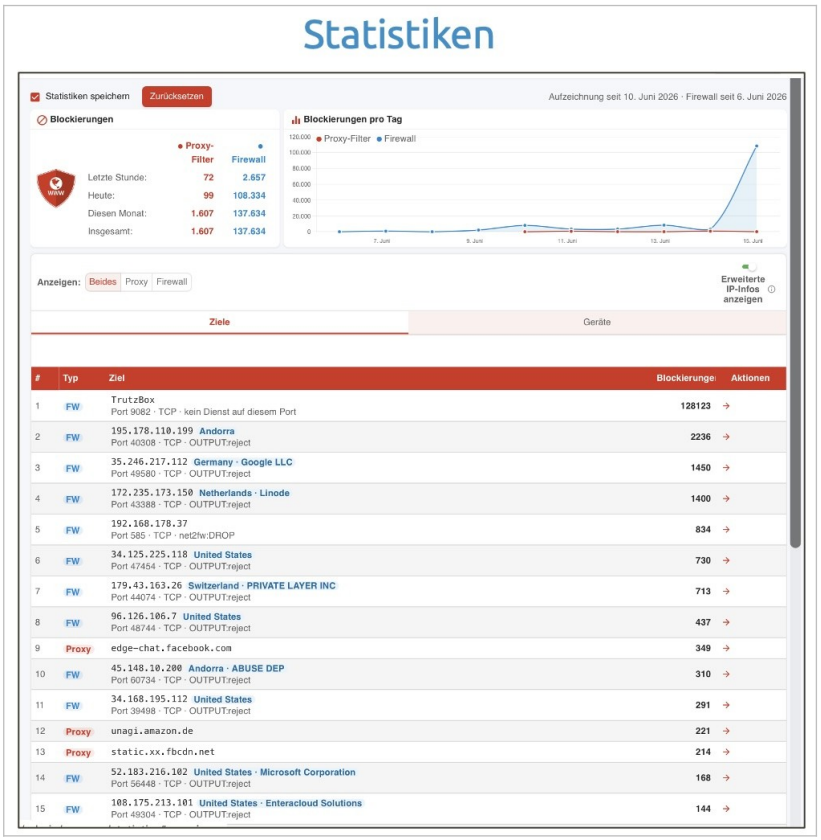
10 Statistiken

Die Statistiken-Ansicht zeigt eine Übersicht der geblockten Verbindungen. Dabei wird zwischen zwei Arten von Blockierungen unterschieden: Proxy-Blockierungen (vom HTTP/S-Proxy auf Anwendungsebene, also durch TrutzContent oder TrutzBrowse) und Firewall-Blockierungen (von der nftables-Firewall auf Netzwerkebene, protokollunabhängig). Über den Umschalter „Anzeigen“ lässt sich zwischen „Beides“, „Proxy“ und „Firewall“ wechseln. Innerhalb der Proxy-Blockierungen wird nicht weiter zwischen TrutzContent und TrutzBrowse unterschieden.
Standardmäßig ist die Statistik deaktiviert. Sie muss vom Administrator zunächst über „Statistiken speichern“ aktiviert werden, bevor Daten erfasst werden.
Der Kopfbereich der Seite fasst die Blockierungen zusammen:

- **Karte „Blockierungen“:** zeigt die Anzahl geblockter Verbindungen für „Letzte Stunde“, „Heute“, „Diesen Monat“ und „Insgesamt“, jeweils getrennt nach Proxy-Filter und Firewall.
- **Diagramm „Blockierungen pro Tag“:** stellt den Tagesverlauf der Blockierungen dar, ebenfalls getrennt nach Proxy-Filter und Firewall. Daneben wird angezeigt, seit wann die jeweilige Aufzeichnung läuft („Aufzeichnung seit … · Firewall seit …“).
- **IP-Infos aus dem Internet ergänzen:** ergänzt bei Firewall-Zielen Land und Anbieter/Organisation (per WHOIS).

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Menüpfad: Verwaltung → Statistiken



Die Statistik der geblockten Verbindungen nach Zielen und Geräten.
(© 2026 Comidio GmbH)

Die Statistik-Ansicht ist in zwei Tabs unterteilt:

- **Tab „Ziele“:** Listet alle geblockten Ziele (Domains bzw. Server) sortiert nach Anzahl der Blockierungen. Die Spalte „Typ“ kennzeichnet je Eintrag, ob es sich um eine Proxy- oder eine Firewall-Blockierung handelt; bei Firewall-Zielen werden zusätzlich Land, Anbieter, Port/Protokoll und die auslösende Firewall-Regel angezeigt. Per Klick auf den Pfeil rechts (→) in der Spalte „Aktionen“ öffnet sich die Drill-Down-Ansicht für dieses Ziel.
- **Tab „Geräte“:** Zeigt die gerätebezogene Gesamtübersicht: welches Gerät im Netzwerk insgesamt wie viele blockierte Verbindungen verursacht hat. Die Geräte erscheinen mit dem Namen, den sie zum Zeitpunkt der Blockierung trugen (fest vermerkt statt der MAC-Adresse); auch nach Umbenennen oder Entfernen eines Geräts bleibt die historische Zuordnung erhalten.

Drill-Down: Welche Geräte haben eine Domain aufgerufen?

Per Klick auf den Pfeil (→) neben einer Domain öffnet sich die Drill-Down-Ansicht. Sie zeigt, welche Geräte im Netzwerk diese Domain wie oft aufgerufen haben. So lässt sich nachvollziehen, welches Gerät besonders viele Verbindungen zu einer bestimmten Tracking-Domain aufbaut. Bei Firewall-Blockierungen nennt die Überschrift das benannte Ziel („Geräte mit Blockierungen zu …“). Gehört zu

einer Blockierung kein internes Gerät, erklärt ein Hinweis, dass die TrutzBox selbst betroffen war, etwa durch einen Zugriff aus dem Internet auf einen ihrer Ports oder eine Verbindung, die die Box selbst aufgebaut hat.

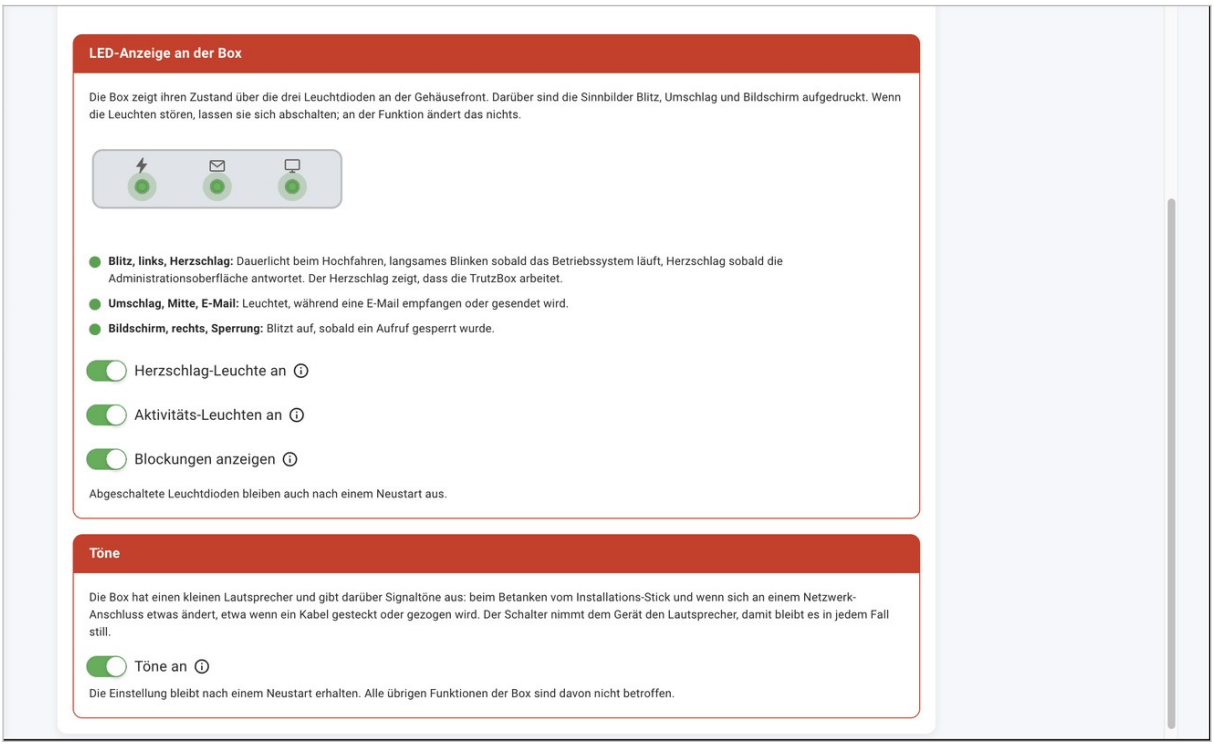
Der Schalter „Statistiken speichern“ steuert, ob Blockierungen überhaupt aufgezeichnet werden (siehe oben); es ist kein Export. Mit „Zurücksetzen“ werden alle gesammelten Statistikdaten gelöscht.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

11 Allgemeine Einstellungen

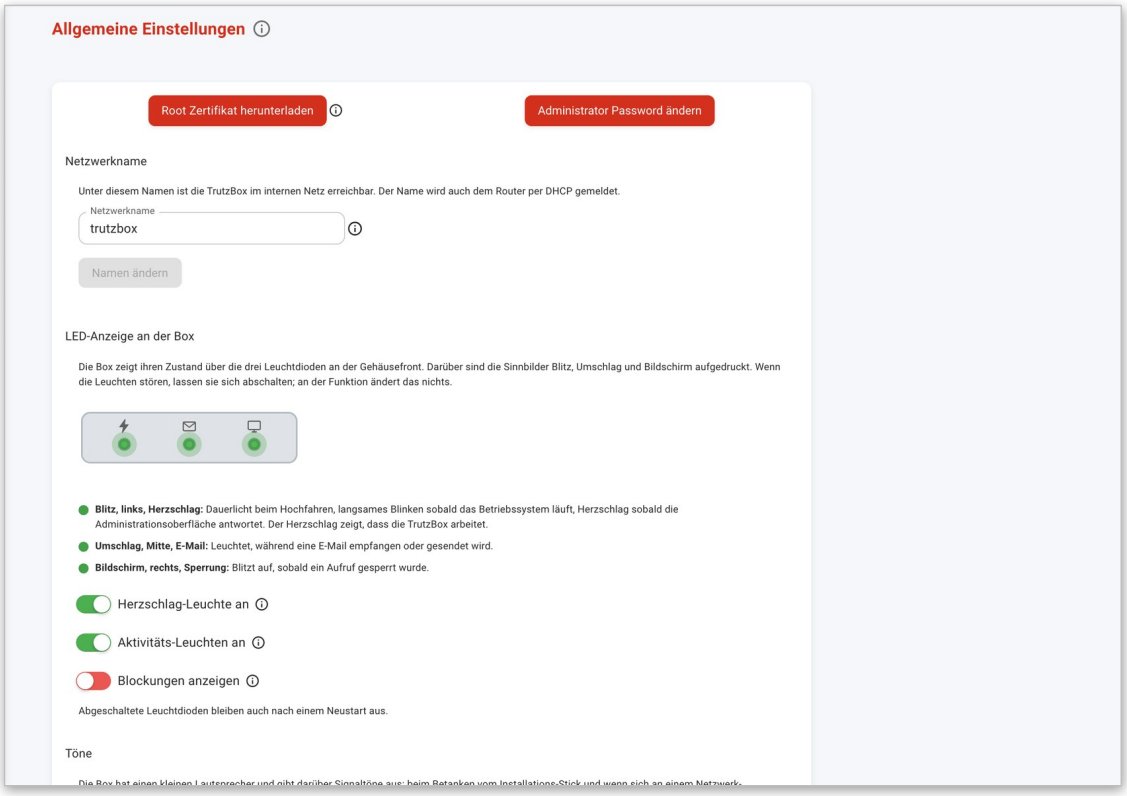
Über den Menüpunkt „Allgemeine Einstellungen“ sind allgemeingültige Einstellungen und das Herunterladen des TrutzBox-Stammzertifikats möglich. Das Stammzertifikat muss auf jedem Endgerät installiert sein, für das TrutzBrowse aktiviert ist oder das mit einem Mail-Programm verschlüsselt auf den Mail-Server der TrutzBox zugreift (Einzelheiten im Kapitel „Verschlüsselte (SSL/TLS)-Verbindungen“).
Neben dem Download des Root-Zertifikats („Root Zertifikat herunterladen“) bietet die Seite die Schaltfläche „Administrator Password ändern“, mit der sich das Passwort des Administrator-Kontos der TrutzBox neu setzen lässt.
Wichtig nach einem Neuaufsetzen oder Werksreset ohne eingespieltes Backup: Die TrutzBox erzeugt dann ein neues Stammzertifikat. Auf allen Geräten muss das neue Zertifikat installiert und das alte entfernt werden, ebenso früher angeklickte Browser-Ausnahmen; sonst verweigern manche Browser irgendwann kommentarlos die Verbindung.
Der Abschnitt „Netzwerkname“ legt fest, unter welchem Namen die TrutzBox im internen Netz erreichbar ist. Der Name wird zugleich dem Internet-Router per DHCP gemeldet, sodass die Box auch dort unter diesem Namen auftaucht. Über „Namen ändern“ wird er übernommen, ohne dass die Box neu starten muss. Der Name gilt für alle internen Zugänge zugleich, also für die Bedienoberfläche, den Web-Chat und die Zertifikate der Box.
Zusätzlich kündigt sich die TrutzBox im internen Netz und im Netz des Routers per mDNS unter dem Netzwerknamen mit der Endung .local an, ab Werk also als trutzbox.local. Diese Adresse ist der Rückfall, wenn ein Gerät den kurzen Namen nicht auflösen kann (Abschnitt „Die TrutzBox im Netz finden: trutzbox.local (mDNS)“).
Der Abschnitt „LED-Anzeige an der Box“ zeigt eine Grafik der Gehäusefront mit den drei aufgedruckten Sinnbildern Blitz, Umschlag und Bildschirm und erklärt sie in derselben Reihenfolge: Blitz links für den Herzschlag, Umschlag in der Mitte für TrutzMail, Bildschirm rechts für eine Sperrung. Vier Schalter steuern die Anzeige getrennt: „Herzschlag-Leuchte an“, „Netzwerk-Leuchten an“, „Aktivitäts-Leuchten an“ und „Blockungen anzeigen“. Abgeschaltete Leuchtdioden bleiben auch nach einem Neustart aus. Der eigene Abschnitt „Töne“ schaltet den kleinen Lautsprecher der Box ab, der sich beim Betanken vom Installations-Stick meldet und immer dann, wenn sich an einem Netzwerk-Anschluss etwas ändert, etwa beim Stecken oder Ziehen eines Kabels. An der Funktion der Box ändert keiner dieser Schalter etwas.

Menüpfad: Verwaltung → Allgemeine Einstellungen



Der Abschnitt „LED-Anzeige an der Box“ mit den Schaltern für die Leuchtdioden und die Töne. (© 2026 Comidio GmbH)

Menüpfad: Verwaltung → Allgemeine Einstellungen



Die Seite „Allgemeine Einstellungen“ mit Stammzertifikat, Administrator-Passwort und Netzwerkname. (© 2026 Comidio GmbH)

12 E-Mail (TrutzMail)

Wie bereits dargestellt worden ist, sollte vor allem der E-Mail-Verkehr sehr sicher verschlüsselt und die Identität des Absenders eindeutig erkennbar sein. Die derzeit in fast allen Mail-Programmen angebotene E-Mail-Verschlüsselungslösungen basieren alle auf PGP[11] oder S/MIME[12]. Sowohl PGP als auch S/MIME Lösungen, sind zwar bei sachgemäßer Verwendung recht sicher, aber kompliziert und umständlich anzuwenden. Vor allem die Verwaltung der Schlüsselpaare stellt im täglichen Gebrauch, nicht nur für den Technik-Laien, oft eine zu große Komplexität dar.

PGP und S/MIME E-Mail-Verschlüsselung ist deswegen in der Bedienung zu kompliziert, da der Benutzer zunächst einmal eine funktionale Erweiterung (Plugin) in seinen E-Mail-Programmen installieren muss. Und das auf allen seinen Geräten. Er muss deren zusätzliche Funktionalität verstehen und ein eigenes Schlüsselpaar generieren und verwalten.

Schließlich muss er auch noch die öffentlichen Schlüssel seiner Kommunikationspartner erfragen und verwalten. Und gerade diese Verwaltung der Schlüssel seiner Kommunikationspartner, das der Nutzer ja auf allen seinen Geräten aktuell halten muss, gestaltet sich in der Praxis als kaum durchführbar.
Er sollte außerdem gewährleisten, dass er weder die eigenen Schlüssel noch die seiner Kommunikationspartner verliert. Ein zusätzliches Problem ist, dass sich jeder für eine beliebige E-Mail-Adresse ein PGP-Schlüsselpaar auf irgendeinem PGP Schlüsselserver generieren kann und zwar auch dann, wenn ihm diese E-Mail-Adresse gar nicht gehört. Somit kann irgendjemand mit meiner E-Mail-Adresse ein Schlüsselpaar generieren und dieses auf einem globalen Schlüsselserver als meinen Schlüssel für alle Internet-Nutzer bekannt geben.

Darüber hinaus werden bei der E-Mail-Verschlüsselung mit PGP die Metadaten selbst nicht verschlüsselt. In den vorangegangenen Kapiteln wurde schon dargestellt: gerade bei direkter Kommunikation mit anderen Internet-Nutzern sind die Metadaten für Datenspione oftmals interessanter als der eigentliche Inhalt der E-Mail.
Aus diesem Grunde nutzen sogar IT-Fachleute, die das geschilderte Verfahren verstehen, installieren und bedienen können, diese Art der Verschlüsselung nur als Notbehelf. In Verbindung mit der PGP Verschlüsselung gibt es weitere Probleme, die auf der Webseite „15 reasons not to start using PGP“[13] und in den folgenden Abschnitten, beschrieben worden sind[14]. Dazu kommt, dass die PGP-ID mit ihren 32 Bit zu klein ist, um wirklich immer eindeutig zu sein. Somit ist es auch möglich, gefälschte Schlüssel zu generieren[15].
E-Mails werden im Internet nicht direkt zwischen Sender und Empfänger ausgetauscht. Der E-Mail-Sender übergibt zunächst die E-Mail dem E-Mail-Server seines E-Mail-Providers (z. B. gmx oder

11 http://de.wikipedia.org/wiki/Pretty_Good_Privacy

12 https://de.wikipedia.org/wiki/S/MIME

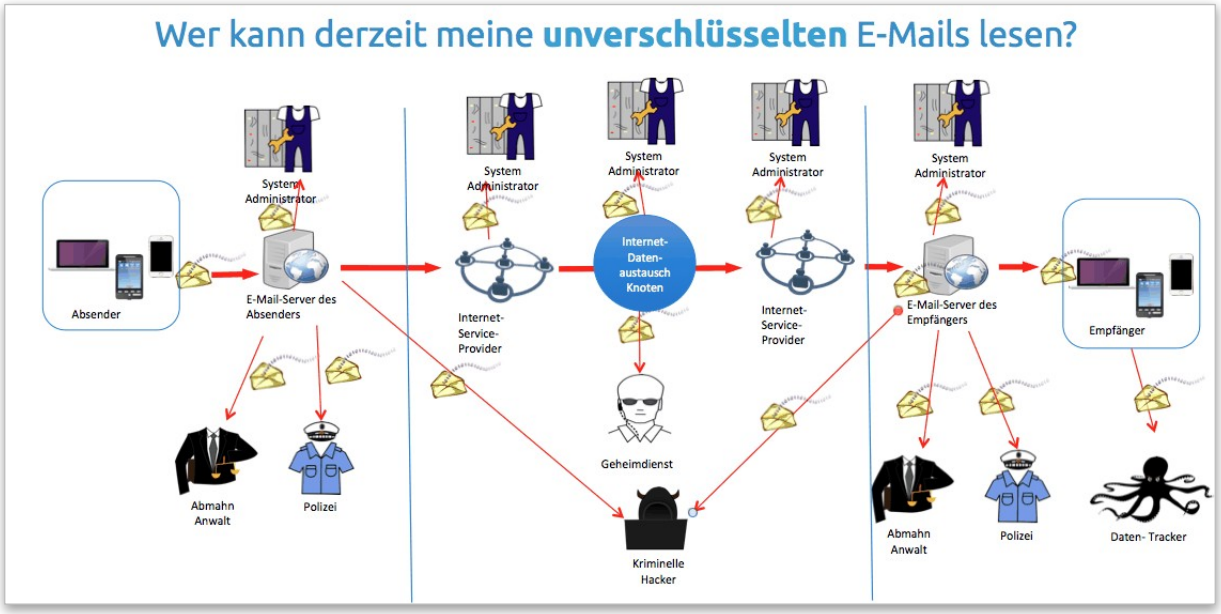
13 http://secushare.org/PGP

14 http://www.heise.de/security/meldung/Massentaugliche-E-Mail-Verschluesselung-gesucht-2557237.html?wt_mc=nl.heisec-summary.2015-02-23

15 http://www.heise.de/security/meldung/Haufenweise-Fake-PGP-Schluessel-im-Umlauf-3297175.html?wt_mc=nl.heisec-summary.2016-08-18

Google-Mail), der dann diese E-Mail (direkt oder manchmal auch indirekt) über mehrere Netzwerkknoten dem E-Mail-Provider des Empfängers zustellt. Dieser speichert die E-Mail so lange, bis der Empfänger die E-Mail mit seinem E-Mail-Programm abholt.

Die E-Mail-Provider müssen, um die E-Mail ausliefern zu können, natürlich wissen, für wen die E-Mail bestimmt ist. Die diesbezüglichen E-Mail Metadaten können deswegen nicht verschlüsselt werden.



Wer unverschlüsselte E-Mails auf ihrem Weg mitlesen kann: Administratoren, Provider, Ermittler und Datensammler.
(© 2026 Comidio GmbH)

Ein weiteres Sicherheitsproblem des heutigen E-Mail-Systems ist, dass man nicht darauf vertrauen kann, dass die E-Mail tatsächlich von dem genannten Absender oder dem versendenden Mail-Server stammt. Wer heute eine Nachricht verschicken möchte, kann in die E-Mail eine x-beliebige Absender-Adresse eintragen. Oft kommen Spam-E-Mails von gekaperten Servern, die zum Versenden von Massen-E-Mails genutzt werden.

Das kann sogar der eigene PC oder ein IoT-Gerät im Haushalt sein, wenn dieser gehackt wurde (und Teil eines Bot-Netzes wurde). So kann der eigentliche Versender von Spam-E-Mails weder mit Hilfe der Schadcode enthaltenden E-Mail noch über die IP-Adresse des Servers ausfindig gemacht werden. Eine gute Übersicht über die Gefahren bei E-Mails und deren Lösungen gibt das „Privacy-Handbuch“[16].
Die allgemeinen Security-Anforderungen bei Kommunikation über öffentliche Netze und deren TrutzBox-Lösung sind:

- **Authentizität**: die Gesprächspartner wissen zuverlässig, mit wem sie kommunizieren
- **Vertraulichkeit**: kein Dritter kann mithören oder Daten ändern

16 http://de.wikibooks.org/wiki/Privacy-Handbuch:_E-Mail_Kommunikation

- **Perfect Forward Secrecy** (*Folgenlosigkeit):* bei abgefangenen Nachrichten kann niemand nach Beendigung der Sitzung den geheimen Langzeitschlüsseln rekonstruieren.
- **Abstreitbarkeit**: der Absender kann Dritte nicht für den Inhalt der Nachricht verantwortlich machen.
-

Mit diesen Security-Anforderungen und weiteren Anforderungen bzgl. einfachster Bedienbarkeit und Verfügbarkeit auf allen Clients, wurden von Comidio folgende Anforderungen an die TrutzMail Architektur gestellt und implementiert:

- **Einfachste Bedienung** in der Art, dass der Nutzer nicht mit wie auch immer gearteten Schlüsseln in Berührung kommt und (nach der Installation) sich nichts an seiner gewohnten E-Mail Bedienung ändert.
- Verschlüsselung der gesamten E-Mail einschließlich der Metadaten auf dem Übertragungsweg zwischen TrutzBoxen.
- Verschlüsselung mit etablierten, standardisierten kryptografischen Verfahren (OpenPGP, TLS).
- **die Authentizität der E-Mail-Absenderadresse und des E-Mail-Servers sind überprüfbar** und werden verifiziert. Beim ersten Mail-Kontakt lädt der Adressat das Zertifikat des Absenders vom zentralen Comidio Server. Dadurch wird verhindert, dass sich ein Absender als jemand anderes ausgibt als er in Wirklichkeit ist. Des Weiteren kann ein E-Mail-Absender nur von seiner TrutzBox E-Mails versenden. Innerhalb des TrutzMail-Verbunds ist Absenderfälschung damit praktisch ausgeschlossen; über das Gateway empfangene Standard-E-Mails können dagegen weiterhin Spam und gefälschte Absender enthalten.

Beim Austausch zwischen TrutzBoxen liegt keine zentrale Instanz im Nachrichtenweg: Die geheimen Schlüssel verwaltet jede Box selbst, und die Boxen prüfen Absender und Server unmittelbar gegeneinander. Comidio betreibt daneben zentrale Registrierungs-, Verzeichnis- und Zertifikatsdienste, und beim Austausch mit Standard-Mail-Servern ist zusätzlich das Comidio-Gateway beteiligt. Welche Angaben dabei jeweils sichtbar werden, beschreiben die Abschnitte zu den einzelnen Betriebsfällen.

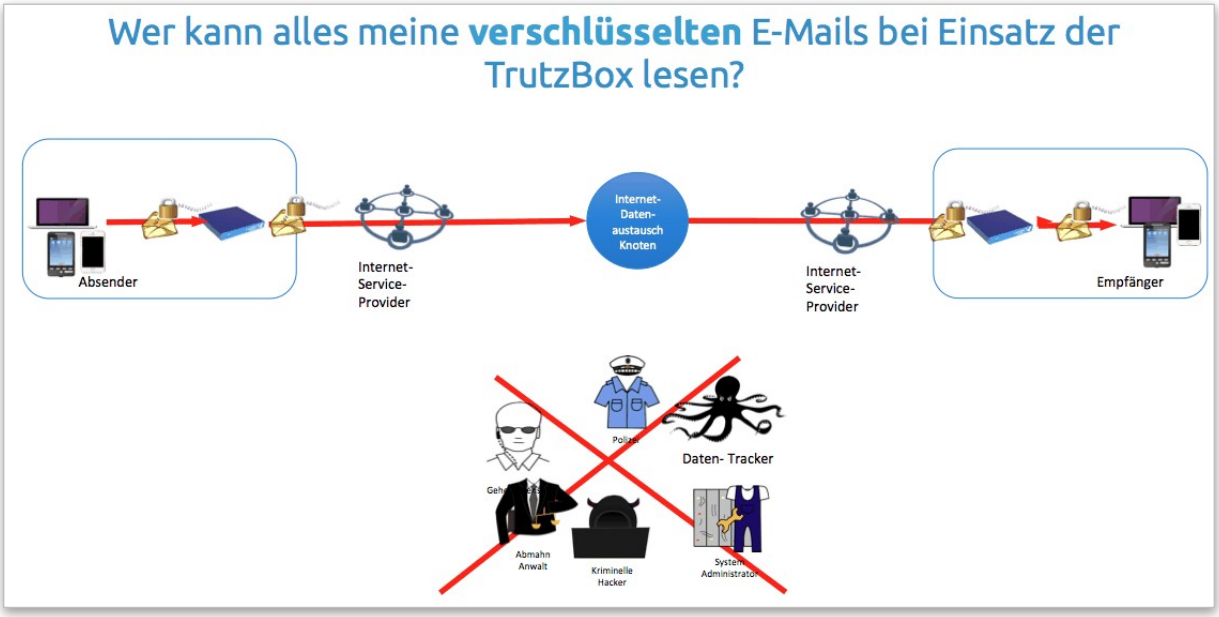
- **E-Mail-Adressen sind nur Absender und Empfänger bekannt**. Selbst wer Daten im Internet „mithören“ kann, ist praktisch nicht in der Lage, die E-Mail-Adressen zu sammeln und zu missbrauchen.
- **Das E-Mail-System darf kein geschlossenes System sein**. Da nicht davon auszugehen ist, dass alle Kommunikationspartner durch diese sichere E-Mail erreichbar sind, muss es weiterhin möglich sein, auch unsichere E-Mails mit anderen Kommunikationspartnern auszutauschen.
- Es muss einem Benutzer möglich sein, sein **E-Mail-Konto zu löschen** und die E-Mail-Adresse danach erneut anzulegen. Da sich dadurch das Zertifikat der E-Mail ändert, die alten Zertifikate aber noch in Umlauf sind, ist die Umsetzung dieser Anforderung nicht trivial.

- Es muss möglich sein, **kompromittierte E-Mail-Adressen** (Accounts) im gesamten System zu **sperren.**

12.1 Austausch von sicheren E-Mails über die TrutzBox

Die Verschlüsselung der Metadaten kann nur gewährleistet werden, wenn die gesamte E-Mail verschlüsselt ist und wenn zwischen Absender und Empfänger keine weitere Instanz die E-Mail Adresse benötigt um die E-Mail ausliefern zu können, somit bei einem „Vermittler“ auch keine Metadaten anfallen. Eine Lösung wäre, die E-Mails direkt zwischen Absender und Empfänger auszutauschen (p2p, peer-to-peer).

Dass E-Mail-Programme Nachrichten direkt untereinander austauschen ist allerdings keine gute Lösung, da dann sowohl der Absender als auch der Empfänger das Mail-Endgerät zur selben Zeit eingeschaltet haben und online sein müssten. Da man einerseits davon ausgehen kann, dass dies sehr selten der Fall ist, und man andererseits sicherstellen will, dass TrutzMail auf allen Endgeräten nutzbar ist, wurde TrutzMail auf einer dedizierten Server-Hardware implementiert (Eigenhosting).



Mit der TrutzBox bleibt der Inhalt auf dem gesamten Weg verschlossen; die Mitleser entfallen.
(© 2026 Comidio GmbH)

Dieser Server (die TrutzBox) sollte immer eingeschaltet sein, sodass TrutzMails jederzeit empfangen werden können. Auf der TrutzBox läuft ein ganz normaler Standard-Mail-Server, mit dem sich das gewohnte E-Mail-Programm des Benutzers verbinden kann. Der Anwender ist damit beim Austausch über sichere E-Mails nicht mehr auf einen fremden E-Mail-Provider angewiesen.

Der Benutzer wird sozusagen zu seinem eigenen E-Mail-Anbieter (Stichwort „Eigenhosting“ oder „Edge-Computing“). Und wird ein großer E-Mail-Anbieter gehackt und dabei viele Millionen E-Mail-

Adressen einschließlich Passwörtern entwendet, dann sind die E-Mail oder Login-Daten von TrutzBox Nutzern nicht mehr dabei.

Wenn mit der TrutzBox eine E-Mail an einen anderen TrutzBox Besitzer verschickt wird, muss nichts zusätzlich konfiguriert werden. Die Verwaltung der Schlüssel, sowie die Ver- und Entschlüsselung selbst, wird von der TrutzBox automatisch durchgeführt.
In manchen Ländern zwingen Behörden E-Mail-Provider zur Herausgabe von E-Mail-Passwörtern (Lavabit). Comidio besitzt weder die geheimen Schlüssel noch die E-Mail-Inhalte seiner Kunden und kann sie daher auch nicht herausgeben (Einzelheiten im Kapitel „Neue TrutzMail-Adresse registrieren“).[17]
Mit dem Link https://trutzbox/mail kann der Nutzer von jedem Gerät den eingebauten Web-Mailer aufrufen und seine TrutzMails bearbeiten. Der Anwender nutzt dann den auf der TrutzBox installierten Web-Mailer (RoundCube), der es dem Nutzer erlaubt, mit Hilfe eines Web-Browsers seine E-Mails zu verwalten.

Falls er seinen gewohnten E-Mail-Client weiterverwenden möchte, kann der Benutzer den TrutzMail Server als weiteren Mail-Server in seinem E-Mail-Client eintragen und wie gewohnt alle E-Mail Funktionen seines E-Mail-Clients weiter verwenden (Server-Parameter siehe TrutzBox Handbuch). Dabei nutzt der Anwender den auf der TrutzBox installierten Mail-Server „Dovecot“, um seine Mails über das IMAP Protokoll von seinem E-Mail-Client abzuholen. Für das Versenden von E-Mails mit Hilfe des SMTP Protokolls kommt ein Mail-Submission-Agent Server (MSA-Server) auf der TrutzBox zum Einsatz. Dovecot ist der weit verbreitete quelloffene IMAP/POP3-Server, der die Postfächer bereitstellt; der Mail-Submission-Agent nimmt umgekehrt die ausgehenden Nachrichten des E-Mail-Clients entgegen und ist damit vom Abhol-Server getrennt.

Folgende beiden alternativen Ports und Protokolle sollten im Mail-Client konfiguriert werden:

Posteingang IMAP Server: trutzbox

Port	Protokoll	Bezeichnung
143	STARTTLS	TLS oder SSL
993	TLS	TLS oder SSL

Postausgang SMTP Server: trutzbox

Port	Protokoll	Bezeichnung
587	STARTTLS	TLS
465	TLS	TLS

12.2 Maximalgröße einer TrutzMail

Bevor eine E-Mail versendet werden kann, müssen die Anhänge der E-Mail in lesbare Zeichen umcodiert werden. Dadurch wird eine E-Mail immer erheblich größer, als die ursprüngliche Summe der Anhänge. Da die Größe einer E-Mail nur durch die aktuelle Größe des derzeit verfügbaren Hauptspeichers begrenzt ist, lässt sich kaum voraussagen, ob eine große E-Mail noch gesendet (oder auch durch die TrutzBox des Empfängers) empfangen werden kann. Falls es zu Problemen aufgrund der

17 http://bits.blogs.nytimes.com/2013/08/08/two-providers-of-encrypted-e-mail-shut-down/?_r=1

Mailgröße kommen sollte, hilft oft ein Neustart der TrutzBox. Dadurch wird der Hauptspeicher „geleert“.

12.3 Technische TrutzMail Implementierung

TrutzMail nutzt für das Auffinden der Empfänger-TrutzBox und für die Übertragung der E-Mails Tor-Hidden-Services (siehe unten). Verfahren mit verteilten Hash-Tabellen (DHT, distributed hash tables), wie sie andere Peer-to-Peer-Netze nutzen, kommen dabei nicht zum Einsatz, weil sie eine Portfreigabe am Internet-Router erfordern, die IP-Adressen der Beteiligten erkennbar lassen und unterschiedlich lange brauchen, um den Empfänger zu finden.[18]
Die Architektur des E-Mail-Austauschs basiert auf Tor-hidden-services (ths).
Das Tor-Netzwerk bietet nicht nur die Möglichkeit seine eigene IP-Adresse im Internet zu verschleiern, sondern auch eigene Services im Tor Netzwerk anzubieten: die sogenannten Tor-hidden-services (versteckte Dienste).[19][20] Domain-Namen im Tor Netzwerk haben keine gewöhnlichen Domain-Namen wie google.de sondern enden mit .onion. Die .onion Adressen werden im Tor-Netzwerk, unabhängig vom „normalen Internet“ vergeben und verwaltet.

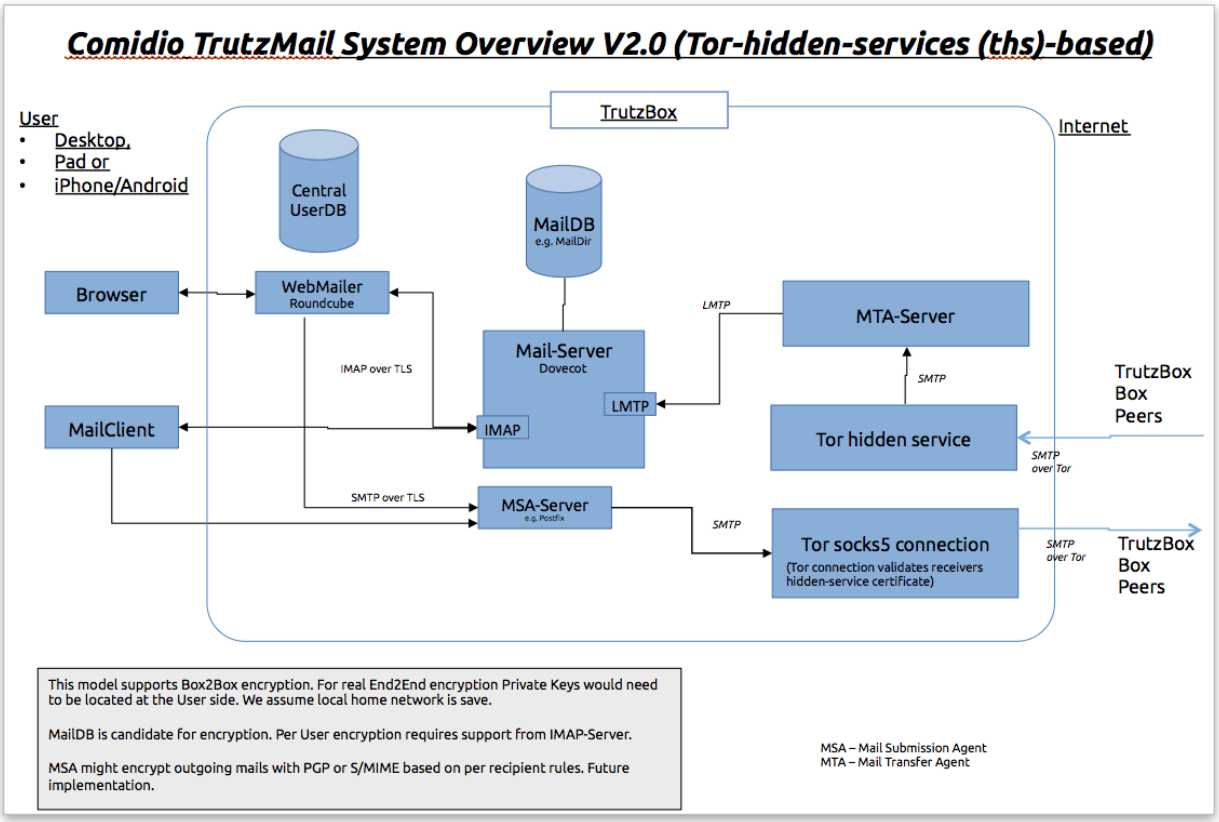
Beim Anlegen einer neuen TrutzMail-Adresse wird auf der TrutzBox ein neuer Tor-Hidden-Service konfiguriert und im Tor-Netzwerk bekanntgegeben. Dabei bekommt jede TrutzMail-Adresse auch eine .onion-Adresse zugeordnet. Falls dann eine andere TrutzBox Kontakt aufnehmen möchte, um eine TrutzMail zu übermitteln, muss diese sendende TrutzBox zunächst die .onion Adresse der Ziel TrutzBox ermitteln. Diese Ziel-Adresse ist im Public-Key Zertifikat des zentralen Comidio-Adressbuchs gespeichert und kann dort von der Absender-TrutzBox bezogen werden.

Mit dieser .onion Adresse kann dann die sendende TrutzBox Kontakt mit der Empfänger TrutzBox aufnehmen. Dabei authentisiert das Tor-Netzwerk automatisch diese Empfänger TrutzBox und baut eine TrutzBox-zu-TrutzBox verschlüsselte Verbindung auf, über die dann die Mail-Server der beiden TrutzBoxen über Standard-SMTP die Mail austauschen.
Nachstehend ist eine Übersicht der Comidio TrutzMail Architektur abgebildet:

[18] https://de.wikipedia.org/wiki/Verteilte_Hashtabelle

[19] https://www.torproject.org/docs/hidden-services.html.en

[20] https://de.wikipedia.org/wiki/Tor_(Netzwerk)#Versteckte_Dienste



Die Architektur von TrutzMail mit den beteiligten Diensten auf der Box.
(© 2026 Comidio GmbH)

Die meisten TrutzMail Funktionen wurden mit Hilfe standardisierter Open-Source E-Mail-Programme umgesetzt. Damit kann gewährleistet werden, dass sich an der Schnittstelle zum Nutzer nichts bzgl. seines gewohnten E-Mail-Programms ändert. Durch Einsatz dieses Standard Mail-Servers kann der E-Mail-Nutzer sich mit jedem Standard E-Mail-Programm verbinden und ohne Anpassungen im E-Mail-Client sichere, verschlüsselte E-Mail-Nachrichten senden und empfangen.
Alle dazu notwendigen Erweiterungen und die Verwaltung der Schlüssel übernimmt die TrutzBox. Der Nutzer kann sowohl seine gewohnten E-Mail-Clients, als auch seine Adressverwaltung weiterverwenden. Er muss lediglich einen neuen E-Mail-Account in seinem E-Mail-Programm konfigurieren. Für unsichere E-Mails kann er weiterhin seine alten E-Mail-Accounts des öffentlichen Mail-Providers nutzen.
Die TrutzBox erzeugt und verwaltet die persönlichen Schlüssel selbst; Comidio verwaltet lediglich das globale Adressbuch mit den öffentlichen Schlüsseln (Zertifikaten) und ist weder an der Ver- und Entschlüsselung noch an der Übertragung der E-Mails beteiligt (Einzelheiten im Kapitel „Neue TrutzMail-Adresse registrieren“).
Um sichere von unsicheren E-Mails besser unterscheiden zu können, haben sichere E-Mail-Adressen die Endung (Domain) @comidio.email. Comidio nennt diese Art der E-Mail-Adresse die „TrutzMail Adresse“.

E-Mails senden

Alle E-Mails, die über die TrutzBox gesendet werden, werden automatisch von der TrutzBox verschlüsselt, falls der Empfänger eine TrutzBox ist (und somit die Mail-Adresse mit @comidio.email endet). Dann besorgt sich die TrutzBox automatisch den benötigten öffentlichen Schlüssel des Empfängers. Damit dieser Weg nicht umgangen werden kann, nimmt die TrutzBox Mails von Programmen im eigenen Netz nur über die dafür vorgesehenen Zugänge mit Anmeldung und Verschlüsselung an: Port 587 (STARTTLS) und Port 465 (TLS). Geräte, die Mails selbst versenden, etwa ein Drucker, ein Scanner oder ein Netzwerkspeicher, werden deshalb auf Port 587 eingestellt. Port 25 bleibt ausschließlich das, wofür er im Internet gedacht ist: die Annahme von Mails anderer Mailserver.

Falls der Empfänger keine TrutzBox ist (und somit eine normale E-Mail-Adresse adressiert wurde), dann muss der TrutzBox-Administrator zuvor der TrutzBox den öffentlichen PGP-Schlüssel des Empfängers mitteilen. Aus Sicherheitsgründen ist es nicht möglich, eine E-Mail an einen Empfänger zu versenden, wenn der öffentliche Schlüssel des Empfängers unbekannt ist.

E-Mails empfangen

Alle verschlüsselten E-Mails, die von der TrutzBox empfangen werden, werden von der TrutzBox automatisch entschlüsselt und zur Abholung eines E-Mail-Programms bereitgestellt.
Die TrutzBox kann auch von normalen E-Mail-Servern E-Mails empfangen. Diese können sowohl verschlüsselt als auch unverschlüsselt sein. Um dem Empfänger der E-Mail anzuzeigen, ob die E-Mail verschlüsselt oder unverschlüsselt war, und ob die TrutzBox die Signatur des Absenders prüfen konnte, passt die TrutzBox das Mail-Betreff-Feld in der E-Mail an. Die TrutzBox setzt dazu vor dem Mail-Betreff-Text in eckigen Klammern eingerahmt
als ersten Buchstaben die Absender-Bestätigung

- U: für unsigniert (die TrutzBox konnte den Absender nicht bestätigen), oder
- S: für signiert (die TrutzBox konnte den Absender bestätigen)

und als zweiten Buchstaben die E-Mail Verschlüsselung

- U: für unverschlüsselt (der Mailinhalt war unterwegs lesbar), oder
- E: für encrypted (der Mailinhalt war unterwegs nicht lesbar)

ein.
Beispiele:

- Eine unverschlüsselte E-Mail, die von einem normalen Mail-Account an die TrutzBox gesendet wurde, hat im Betreff-Feld [UU], also unsigniert, unverschlüsselt.
- Eine verschlüsselte TrutzMail, die von einer TrutzBox an eine TrutzBox gesendet wurde, hat im Betreff-Feld [SE], signiert, encrypted.

- Eine verschlüsselte E-Mail, die von einem normalen Mail-Account an die TrutzBox gesendet wurde, hat im Betreff-Feld [UE], unsigniert, encrypted.

Hinweis: Bei [SE] ist im Mail-Programm kein Signatur-Anhang sichtbar, denn nach erfolgreicher Prüfung entfernt die TrutzBox die Signatur und bestätigt sie über das „S“ im Betreff. Ein sichtbarer Signatur-Anhang bleibt nur erhalten, wenn die Prüfung nicht möglich war.
Kommt eine Mail eines TrutzBox-Partners unerwartet als [UU] oder [UE] an, wurde sie meist an einen veralteten Schlüssel verschlüsselt bzw. mit einem veralteten Schlüssel signiert; das korrigiert sich automatisch (siehe „Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen“).

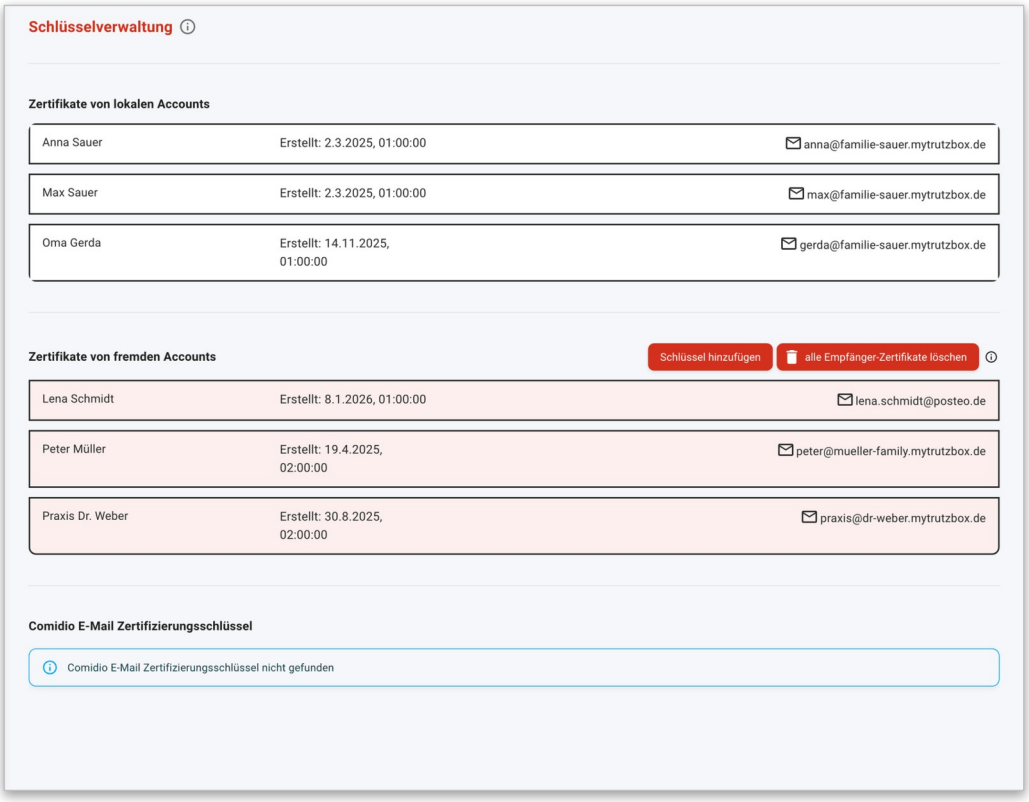
12.4 Austausch von E-Mails mit (Standard) Mail-Servern (mit jemandem, der keine TrutzBox besitzt)

Mit der TrutzBox ist es auch möglich, verschlüsselte E-Mails mit jemanden auszutauschen, der keine TrutzBox besitzt. Dabei ist jedoch jeweils ein Gateway zu „normalen“ E-Mail-Servern notwendig. Da die TrutzBox ihre sicheren E-Mails mit Standard-PGP-Verschlüsselung verschlüsselt, ist es somit sogar möglich, mit jemanden verschlüsselte E-Mails auszutauschen, der keine TrutzBox hat. Falls die TrutzBox den Public-Key des Empfängers kennt, wird die Mail automatisch PGP-verschlüsselt.

Öffentlichen Schlüssel eines Empfängers hinterlegen

Um auch PGP-verschlüsselte E-Mails mit jemandem auszutauschen, der keine TrutzBox besitzt, muss die TrutzBox den öffentlichen Schlüssel des Empfängers kennen. Dazu muss zuvor auf der TrutzBox dieser öffentliche Schlüssel der TrutzBox unter „E-Mail“ → „Schlüsselverwaltung“ bekannt gemacht werden: Die Seite selbst ist weiter unten im Abschnitt „Schlüsselverwaltung“ beschrieben.

Menüpfad: E-Mail → Schlüsselverwaltung



Die Schlüsselverwaltung unter „E-Mail“ mit den öffentlichen Schlüsseln der Empfänger.
(© 2026 Comidio GmbH)

Mit dem Menüpunkt „Schlüssel hinzufügen“ kann dieser neue Schlüssel importiert werden, indem er aus einer Datei geladen oder indem er aus der Zwischenablage eingefügt wird:

Menüpfad: E-Mail → Schlüsselverwaltung



Der Dialog „Schlüssel hinzufügen“ übernimmt einen Schlüssel aus Datei oder Zwischenablage.
(© 2026 Comidio GmbH)

Sobald die TrutzBox einen öffentlichen Schlüssel für einen Mail-Empfänger kennt, dessen Mail-Adresse nicht mit @comidio.email endet, wird diese E-Mail mit diesem öffentlichen Schlüssel des Empfängers verschlüsselt.
Ein „TrutzBox Besitzer“ kann von einem „Nicht TrutzBox Besitzer“, eine PGP-verschlüsselte E-Mail empfangen, wenn der Absender den öffentlichen Schlüssel des „TrutzBox Accounts“ kennt. Damit kann dann der Absender („Nicht TrutzBox Besitzer“) die E-Mail verschlüsseln. Der öffentliche Schlüssel jeder TrutzMail-Adresse kann mit Klick auf den lokalen Account unter „E-Mail“ → „Schlüsselverwaltung“ heruntergeladen und an einen anderen Mail-Versender geschickt werden:

Menüpfad: E-Mail → Schlüsselverwaltung



Der öffentliche Schlüssel eines TrutzMail-Kontos mit Vertrauensstufe, Länge und Fingerabdruck, zum Weitergeben an den Kommunikationspartner.
(© 2026 Comidio GmbH)

Die TrutzBox entschlüsselt automatisch alle E-Mails, auch E-Mails, die Sie von einem normalen E-Mail Server bekommen (siehe nächstes Kapitel).

Empfangen von Standard-E-Mails

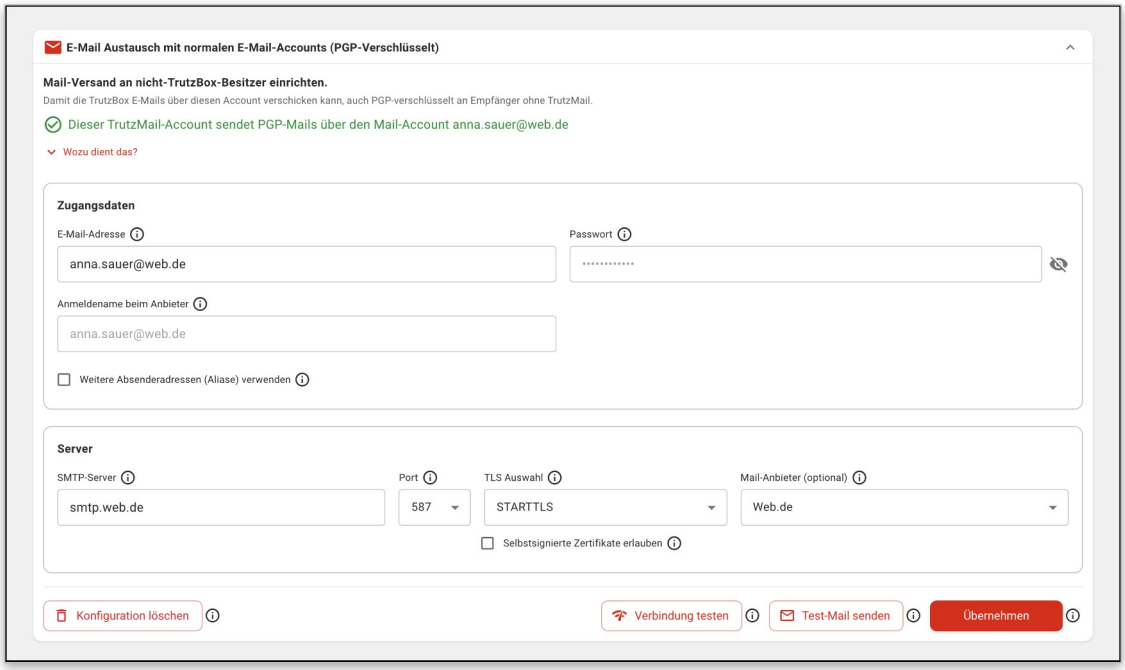
Um unverschlüsselte oder PGP-verschlüsselte E-Mails auch von normalen Mail-Servern (Nicht-TrutzMail-Adressen) empfangen zu können, hat Comidio ein Gateway zu Standard E-Mail-Servern eingerichtet. Dieses Gateway leitet alle an eine @comidio.email gerichteten E-Mails aus dem Internet an die zuständige TrutzBox weiter, auch unverschlüsselte E-Mails. Nach außen fungiert dieser Server wie ein ganz normaler Standard E-Mail-Server und nach innen wie eine TrutzBox, die E-Mails verschlüsselt und über das Tor-Netzwerk an den richtigen TrutzMail Account (die richtige TrutzBox) weiterleitet.

Senden von PGP-verschlüsselten E-Mails an Standard-E-Mail-Accounts

Das von Comidio betriebene E-Mail-Gateway kann jedoch aus Sicherheitsgründen keine E-Mails von einer TrutzBox an einen „normalen“ E-Mail-Account weiterleiten. Eine TrutzBox kann über dieses Gateway somit keine Mail an einen normalen Mail-Account senden. Um von der TrutzBox aus auch normale Standard-Mail-Accounts adressieren zu können, muss zuvor für den TrutzBox-Benutzer auf der

TrutzBox ein anderes, externes Mail-Gateway eingerichtet werden. Dieses Mail-Gateway kann ein ganz normaler SMTP-Server eines Standard-Mail Accounts bei einem öffentlichen Mail-Anbieter sein. Unter dem Menüpunkt „Benutzer verwalten“ kann dazu für jeden TrutzBox Nutzer ein eigenes, externes Mail-Gateway eingetragen werden (z. B. seines t-online Mail-Accounts):

Menüpfad: Verwaltung → Benutzer



Eintrag eines externen Mail-Gateways für einen Benutzer, mit getrennten Feldern für Absenderadresse und Anmeldename.(© 2026 Comidio GmbH)

Nachdem die SMTP-Daten des externen E-Mail Accounts eingetragen wurden, bitte „übernehmen“ drücken. Dabei versucht die TrutzBox testweise eine Verbindung zu diesem SMTP-Server aufzubauen. **Die Eingabe wird durch mehrere Hilfsfunktionen erleichtert:** Anhand der E-Mail-Adresse erkennt die TrutzBox bei vielen Anbietern automatisch die passenden Server-Einstellungen (Server, Port und Verschlüsselung) und füllt die Felder vor; Port und Verschlüsselung (z. B. STARTTLS oder SSL/TLS) lassen sich zusätzlich über Auswahllisten festlegen. Über „Verbindung testen“ prüft die TrutzBox die Zugangsdaten Schritt für Schritt (Namensauflösung, Verbindungsaufbau, Anmeldung) und zeigt das Ergebnis an; mit „Test-Mail senden“ kann eine Probe-E-Mail verschickt werden. Eine eingerichtete Konfiguration lässt sich auch wieder löschen. Hinweis: Viele Anbieter verlangen für den Zugriff über Fremdprogramme ein eigenes App-Passwort.
Absenderadresse und Anmeldename: Das Feld „E-Mail-Adresse“ nimmt die vollständige Absenderadresse des externen Postfachs auf. Unter ihr geht die Mail hinaus: Die TrutzBox verwendet sie im SMTP-Umschlag (MAIL FROM) und im Absenderfeld der Mail. Das Feld „Anmeldename beim Anbieter“ wird nur gebraucht, wenn der Anbieter für die Anmeldung einen eigenen Namen vergibt, der keine E-Mail-Adresse ist; bei Webhosting-Paketen ist das häufig eine technische Kennung aus Buchstaben und Ziffern. Bleibt das Feld leer, meldet sich die TrutzBox mit der E-Mail-Adresse an, was

bei den meisten Anbietern richtig ist. Eine Absenderadresse ohne @ und Domain nimmt die TrutzBox nicht an, denn jeder regelkonforme Mail-Server würde sie mit dem Fehler 501 ablehnen. Leerzeichen, die beim Kopieren vor oder hinter Server, Adresse oder Anmeldename geraten, entfernt die TrutzBox selbst; beim Passwort bleiben sie unangetastet.

Antwortadresse: Weil die Mail unter der Adresse des externen Postfachs hinausgeht, trägt die TrutzBox die TrutzMail-Adresse des Absenders als Antwortadresse (Reply-To) ein. Antworten des Empfängers kommen so wieder auf der TrutzBox an.

Weitere Absenderadressen (Aliase): Viele Anbieter erlauben unter einem Zugang mehrere Absenderadressen, etwa info@ und kontakt@ derselben Domain. Diese Adressen lassen sich nach einem Häkchen bei „Weitere Absenderadressen (Aliase) verwenden“ eintragen, eine pro Zeile. Wählt der Benutzer im Mail-Programm eine davon als Absender, geht die Mail unverändert unter ihr hinaus. Jede andere Absenderadresse ersetzt die TrutzBox durch die E-Mail-Adresse des Postfachs, damit niemand unter fremden Adressen versenden kann. Die Aliase müssen beim Anbieter für das Postfach freigeschaltet sein. Mails unter einem Alias sind verschlüsselt, tragen aber keine PGP-Signatur, weil die TrutzBox für einen Alias keinen eigenen Schlüssel hat, und sie erhalten keine Antwortadresse der TrutzBox.

Prüfen: „Verbindung testen“ prüft Namensauflösung, Verbindungsaufbau und Anmeldung. Ob der Anbieter den Versand unter der eingetragenen Absenderadresse erlaubt, zeigt erst „Test-Mail senden“: Dabei geht eine echte Mail an die TrutzMail-Adresse des Benutzers. Lehnt der Anbieter beim Versand die Absenderadresse ab, meldet die TrutzBox das dem Mail-Programm ausdrücklich als abgelehnte Absenderadresse, zusammen mit der Antwort des Servers.

Falls zuvor für eine Standard-E-Mail-Adresse ein Public-Key eingetragen wurde, verschlüsselt die TrutzBox dann automatisch die Mail mit dem PGP-Verschlüsselungsverfahren. Somit kann auch eine Nicht-TrutzMail-Adresse über die TrutzBox adressiert werden.

Fehlt der öffentliche Schlüssel des Empfängers, weist die TrutzBox die Mail mit einer Fehlermeldung an den Absender ab; unverschlüsselt sendet sie nie (Einzelheiten im Kapitel „E-Mails senden“). Einen fehlenden Schlüssel sucht die TrutzBox dabei nicht selbst im Internet (etwa über ein Web Key Directory), sondern verwendet ausschließlich die in der Schlüsselverwaltung hinterlegten Schlüssel; die Meldung kommt deshalb sofort.

12.5 Austausch von sicheren TrutzMails zwischen TrutzBoxen

Beim Senden einer TrutzMail sucht die TrutzBox zunächst das TrutzMail Zertifikat des Empfängers im lokalen Keyring. Fehlt es dort, erfragt sie es einmalig beim Comidio-Server und hält es danach lokal vor; aktuell bleibt es über den normalen Mailverkehr, Einzelheiten im Kapitel „Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen“. Aus dem Empfänger-Zertifikat liest sie die .onion-Adresse (die Tor-Hidden-Service-Adresse) des TrutzMail Server-Zertifikats und baut zur gefundenen Empfänger-TrutzBox eine verschlüsselte Verbindung auf.

Danach wird die Mail auf der Sender-TrutzBox PGP-verschlüsselt und mit Hilfe von SMTP über das Tor-Netzwerk zur Empfänger-TrutzBox übertragen. Auf der Empfänger-TrutzBox wird die PGP-verschlüsselte Mail entschlüsselt und im lokalen Mail-Store abgelegt.

Damit wird nicht nur sichergestellt, dass die Datenübertragung zwischen den TrutzBoxen verschlüsselt ist, sondern dass auch der Empfänger und Absender authentifiziert werden.
Natürlich können TrutzMails, die zwischen TrutzBoxen ausgetauscht werden, vom Anwender selbst auch zusätzlich mit PGP verschlüsselt werden.

12.6 Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen

Wird ein TrutzMail-Konto neu eingerichtet (z. B. nach dem Zurücksetzen der TrutzBox oder einer Wiedereinrichtung), erhält es einen neuen Schlüssel. Kommunikationspartner, die schon einmal eine Mail an diese Adresse geschickt haben, besitzen noch den alten öffentlichen Schlüssel und würden weiter an diesen verschlüsseln; solche Mails könnten nicht mehr gelesen werden (Betreff [UU] bzw. [UE]).
Die TrutzBoxen bemerken das selbst, ohne dass Comidio den laufenden Mailverkehr mitbekommt: Jede TrutzMail trägt einen unsichtbaren Hinweis auf den aktuellen Schlüssel des Absenders, und eine an einen veralteten Schlüssel verschlüsselte Mail löst eine signierte, verschlüsselte Schlüssel-Korrektur-Notiz an den Absender aus; verbindlich ist dabei stets der Schlüssel aus dem Comidio-Adressbuch, nie der in der Mail mitgereiste. Kennt die TrutzBox des Absenders diesen Mechanismus noch nicht, genügt es, den gespeicherten Schlüssel einmal in der Schlüsselverwaltung zu löschen und die Nachricht erneut zu senden. Der folgende Abschnitt beschreibt den Ablauf im Einzelnen.

Was passiert, wenn der Empfänger seinen Schlüssel gewechselt hat?

Der vorige Abschnitt beschreibt den Regelfall, in dem die Aktualisierung von selbst greift. Der umgekehrte Fall ist lehrreicher, weil er zeigt, wo die Grenze liegt: Ein Kommunikationspartner, mit dem schon Mails ausgetauscht wurden, setzt seine TrutzBox neu auf. Sein Konto bekommt dabei einen neuen Schlüssel, der alte ist verloren. Im Schlüsselbund des Absenders liegt aber weiterhin der alte.
Beim Versand fragt die TrutzBox das Verzeichnis von Comidio nicht bei jeder Mail. Das ist Absicht: Eine Abfrage pro Mail würde Comidio verraten, wer wem gerade schreibt. Sie prüft stattdessen zuerst, ob sie mit dem vorhandenen Schlüssel überhaupt verschlüsseln kann und ob dieser Schlüssel eine Onion-Adresse für den Transportweg trägt. Passt beides, wird er ohne Rückfrage verwendet. Nur wenn kein brauchbarer Schlüssel vorliegt, etwa beim allerersten Kontakt, holt sie ihn beim Verzeichnis.
Die Mail wird also mit dem alten Schlüssel verschlüsselt und ganz normal zugestellt. Die Empfänger-TrutzBox kann sie nicht öffnen, weil der zugehörige geheime Schlüssel nicht mehr existiert. Sie landet dort mit der Kennzeichnung [UU] im Betreff und einem Hinweistext, der den Grund benennt, statt kommentarlos leer zu bleiben.
An dieser Stelle greift die Selbstheilung. Beim Wechsel eines Schlüssels merkt sich jede TrutzBox die Kennungen ihrer eigenen früheren Schlüssel. Trifft eine Mail ein, die an einen dieser früheren Schlüssel verschlüsselt wurde, erkennt die Box die Lage eindeutig und schickt dem Absender eine Schlüssel-Korrektur-Notiz zurück: eine signierte und verschlüsselte Nachricht, die den aktuellen Schlüssel als Hinweis mitführt. Sie geht niemals im Klartext hinaus und niemals an einen Absender, dessen Schlüssel die Box nicht kennt, damit sich daraus kein Weg zum Versand unverschlüsselter Nachrichten ergibt. Höchstens eine solche Notiz je Absender und Tag verlässt die Box, damit zwei Boxen sich nicht gegenseitig Notizen zuwerfen.

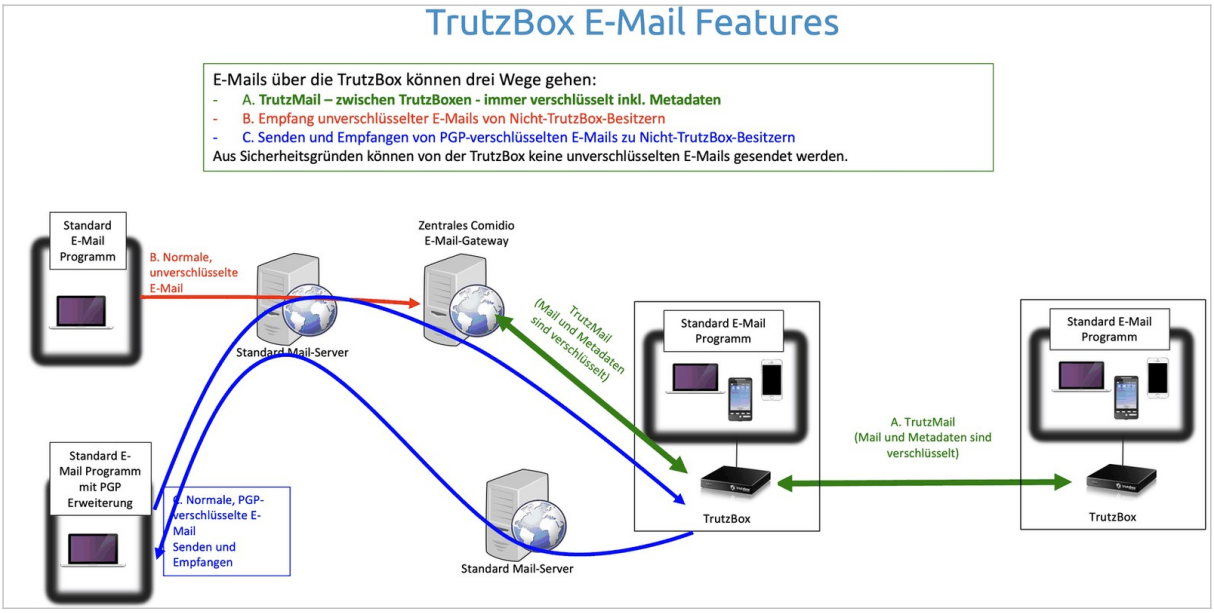
Die Absender-TrutzBox liest an dieser Notiz, dass der Fingerabdruck des Partners nicht mehr zu dem passt, was sie gespeichert hat. Sie übernimmt den Schlüssel jedoch nicht aus der Mail. Das ist bewusst so gebaut: Wer eine Mail fälschen kann, könnte sonst einen eigenen Schlüssel unterschieben. Stattdessen holt sie den maßgeblichen Schlüssel beim Verzeichnis von Comidio, ersetzt den alten und löscht ihn. Eine Sperre verhindert, dass dieselbe Adresse öfter als alle zehn Minuten dort nachgefragt wird. Die nächste Mail an diesen Partner geht damit an den richtigen Schlüssel und kommt als [SE] an.
Wer nicht warten will, hat einen kurzen Weg: Wird der Schlüssel des Empfängers unter E-Mail, Schlüsselverwaltung gelöscht, findet die TrutzBox beim nächsten Versand keinen brauchbaren Schlüssel mehr und holt ihn frisch aus dem Verzeichnis.
Ein per Sperrliste widerrufener Schlüssel wird dabei nie wieder angenommen. Widerruf hat immer Vorrang vor Aktualisierung, sonst könnte ein einmal kompromittierter Schlüssel über den Aktualisierungsweg zurückkehren.

12.7 Mail-Austausch über die TrutzBox: Zusammenfassung

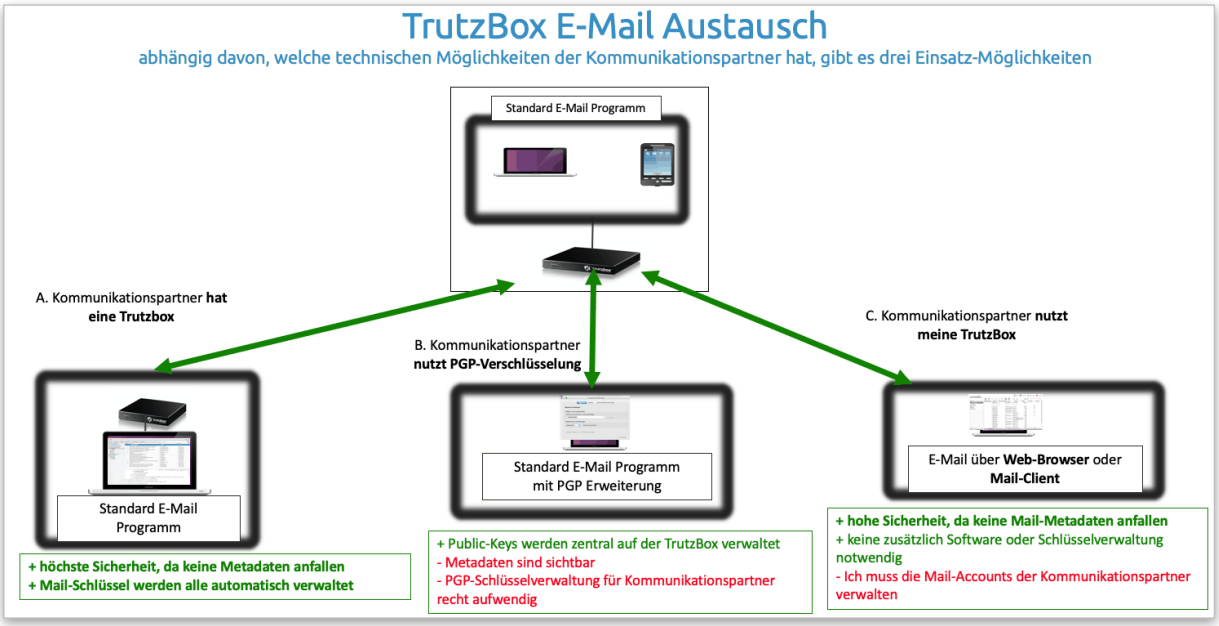
Obige Beschreibungen lassen erkennen, dass es aus technischer Sicht somit drei Möglichkeiten gibt, E-Mails mit der TrutzBox auszutauschen:

- A. TrutzMail (zwischen TrutzBoxen): immer verschlüsselt inkl. Metadaten
- B. Empfang unverschlüsselter E-Mail von Nicht-TrutzBox-Besitzern
- C. Senden und Empfangen von PGP-verschlüsselten E-Mails zu Nicht-TrutzBox-Besitzern

Aus Sicherheitsgründen können von der TrutzBox keine **un**verschlüsselten E-Mails gesendet werden.



Die drei Wege einer E-Mail über die TrutzBox: TrutzMail zwischen TrutzBoxen, Empfang unverschlüsselter Post und PGP mit Nicht-TrutzBox-Besitzern.
(© 2026 Comidio GmbH)



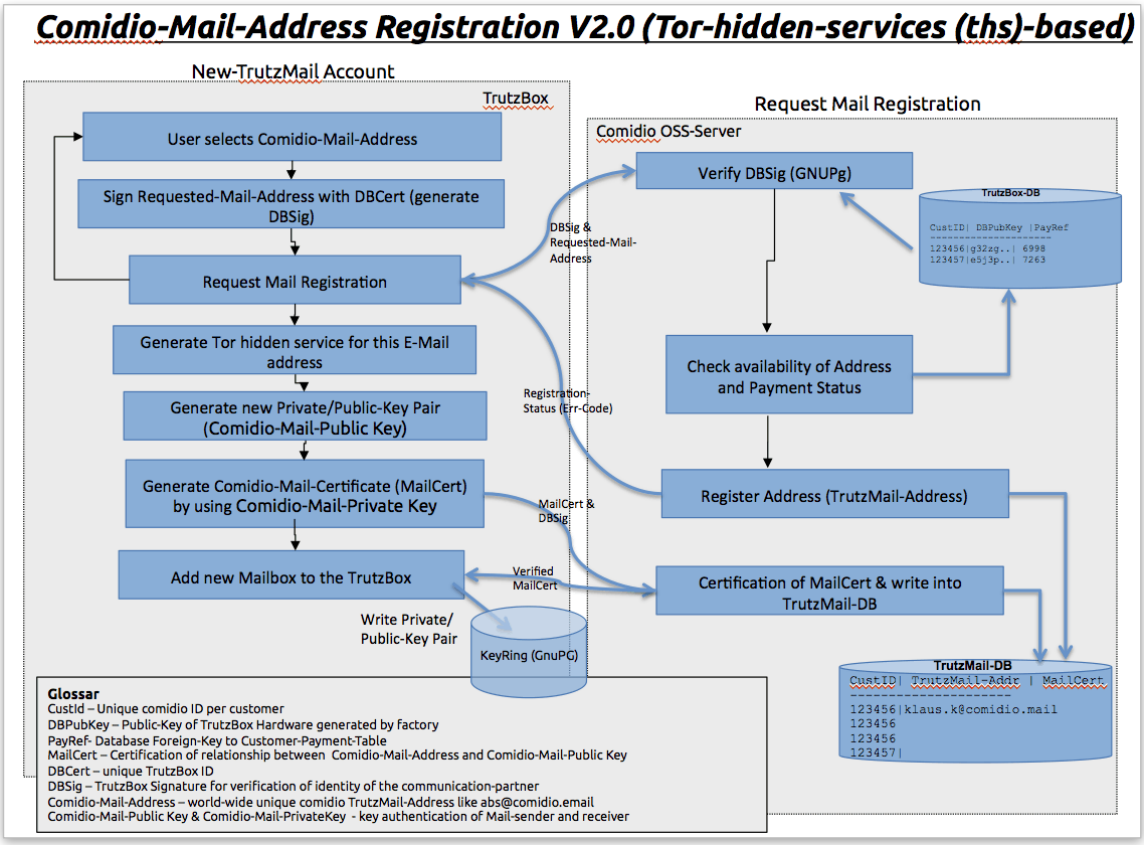
Welcher der drei Wege zum Einsatz kommt, hängt davon ab, was der Kommunikationspartner technisch kann.
(© 2026 Comidio GmbH)

12.8 Neue TrutzMail-Adresse registrieren

Wenn auf der TrutzBox ein neuer Benutzer angelegt wird, kann man diesem Benutzer auch eine TrutzMail-Adresse und somit einen TrutzMail-Account auf der TrutzBox zuweisen (siehe Kapitel „Benutzer“).
Die zentrale Comidio Kundendatenbank (OSS), die von der Comidio GmbH betrieben wird, verwaltet ein zentrales Adressbuch. Dieses Adressbuch kann nur von einer TrutzBox abgefragt werden. Wenn eine neue TrutzMail auf der TrutzBox registriert werden soll, wird zunächst automatisch auf der Comidio Kundendatenbank (OSS) geprüft, ob die gewünschte TrutzMail-Adresse noch frei ist.

Somit müssen TrutzMail-Adressen über alle TrutzBoxen hinweg eindeutig sein und dürfen nur einmalig vergeben werden. Zusätzliche TrutzMail-Adressen sind Teil des Vermarktungsmodells der Comidio GmbH. Deswegen wird beim Anlegen einer neuen TrutzMail-Adresse auch geprüft, ob der Kunde einen laufenden Service-Vertrag hat und noch freie TrutzMail-Adressen im Kontingent vorhanden sind.
Sind diese Kriterien erfüllt, wird auf der TrutzBox ein Schlüsselpaar (Private- und Public-Key) und ein Zertifikat (MailCert) generiert. Dieser private Schlüssel wird auf der TrutzBox erzeugt und im laufenden Betrieb nicht übertragen; Comidio ist er nicht bekannt. Die einzige Ausnahme ist eine vom Administrator angelegte Sicherung: Sie enthält die privaten Schlüssel in verschlüsselter Form und gehört entsprechend geschützt (Kapitel „Sichern und Wiederherstellen“). Ohne den privaten Schlüssel kann Comidio bereits vorhandene TrutzMails weder bei einem Einbruch noch auf behördliche Anordnung entschlüsseln. Comidio kennt die TrutzMail-Adressen und deren Zertifikate (Public-Keys).

Die folgende Übersicht zeigt den Ablauf und die Kommunikation zwischen TrutzBox und dem OSS beim Anlegen einer neuen TrutzMail-Adresse.



Ablauf beim Anlegen einer neuen TrutzMail-Adresse zwischen TrutzBox und Comidio-Server.
(© 2026 Comidio GmbH)

12.9 TrutzMail-Zertifikat Updates

Siehe auch das Kapitel „Aktualität und Pflege der TrutzBox“, in dem die verschiedenen Update-Mechanismen der TrutzBox zusammenfassend beschrieben sind.
Es kann vorkommen, dass eine TrutzMail Adresse kompromittiert wird; z. B. weil eine TrutzBox inkl. der Passwörter gestohlen wurde. Oder es kann vorkommen, dass der Inhalt des TrutzBox-internen Speichermediums gelöscht wird, z. B. wenn eine TrutzBox neu aufgesetzt wurde (durch Hardware-Austausch oder Zurücksetzen der TrutzBox auf Werksauslieferung). In beiden Fällen wird das Zertifikat auf dem zentralen Comidio CA-Server als ungültig gekennzeichnet.

Dazu gibt es auf dem zentralen Comidio Server eine „TrutzMail-Adress-Blacklist“. Aber es muss auch möglich sein, einzelne oder mehrere TrutzMail Zertifikate, die auf einer TrutzBox gespeichert sind und zuvor eine Mail an eine solche Mailadresse geschickt haben, als ungültig zu kennzeichnen.
Aber keine zentrale Stelle weiß, wer solche als ungültig zu kennzeichnenden Zertifikate im Laufe der Zeit auf irgendeiner TrutzBox gespeichert hat (auch Comidio nicht). Es ist in dem Konzept auch durchaus beabsichtigt, dass keine zentrale Stelle weiß, wer an wen E-Mails geschrieben hat.

Aus diesem Grund gibt es einen automatischen Prozess, der jede TrutzBox einmal täglich die lokal gespeicherten Empfänger-Zertifikate mit denen der zentralen Comidio TrutzMail-Zertifikat-Datenbank abgleicht. Falls eines der gespeicherten TrutzMail-Zertifikate ungültig geworden ist, wird diese dann auf der TrutzBox gelöscht. Benötigt die TrutzBox danach das Zertifikat wieder, wird es erneut vom zentralen Comidio CA-Server angefragt.

Bei all diesen Abfragen wird immer nur der Hash einer TrutzMail Adresse abgefragt, so dass es nicht möglich ist, über den zentralen Comidio-Server an TrutzMail Adressen zu gelangen. Der tägliche Abgleich dient ausschließlich dem Widerruf von Zertifikaten (kompromittierte Schlüssel, gelöschte Konten); den Wechsel auf einen neuen Schlüssel nach einer Neueinrichtung regeln die TrutzBoxen untereinander, Einzelheiten im Kapitel „Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen“. Zusätzlich kann der TrutzBox Administrator alle lokal gespeicherten Empfänger-Zertifikate von Hand löschen („Alle Empfänger-Zertifikate löschen“, Einzelheiten im Kapitel „Schlüsselverwaltung“); benötigte Zertifikate holt die TrutzBox danach erneut vom zentralen Comidio CA-Server.

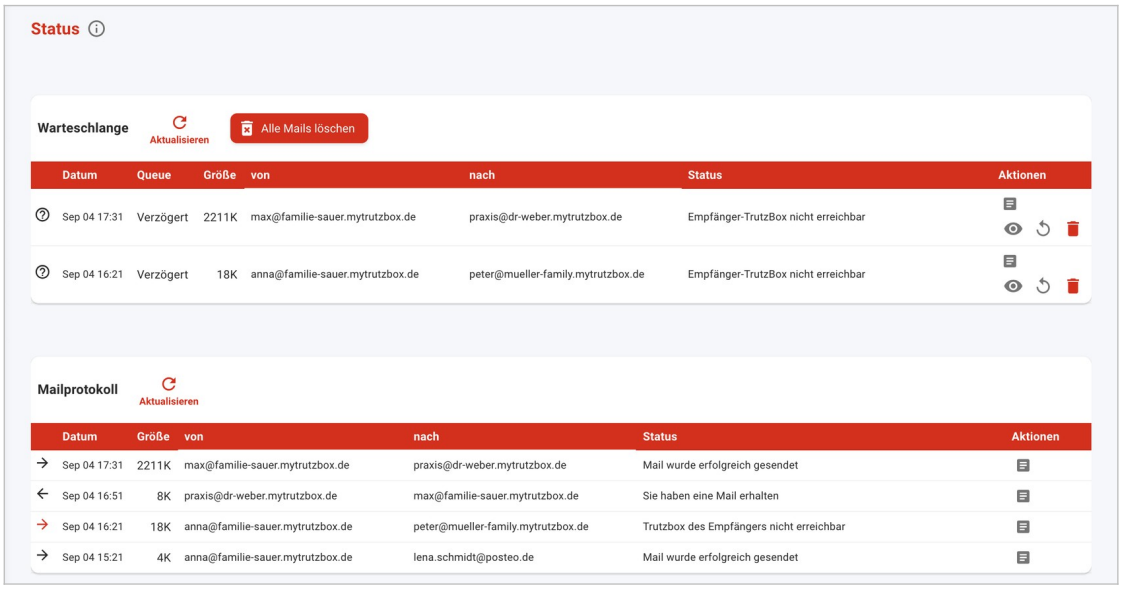
12.10 TrutzMail-Adressen löschen und wiederverwenden

Wird eine TrutzMail Adresse auf der TrutzBox gelöscht, sind zuvor ausgetauschte Zertifikate dieser Adresse evtl. noch auf anderen TrutzBoxen gespeichert. Solche veralteten Zertifikate ersetzt die nächste Korrespondenz automatisch, Einzelheiten im Kapitel „Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen“.
Der Comidio Server wird über die Löschung informiert und markiert das Zertifikat in seiner CA-Datenbank, stößt aber keine sofortige Aktualisierung auf anderen TrutzBoxen an, weil das Konto oft erneut eingerichtet wird. Eine gelöschte Adresse lässt der Comidio Server nur dann erneut anlegen, wenn die Anforderung von derselben TrutzLegitimation stammt wie bei der Erst-Registrierung; das gilt ebenso nach dem Zurücksetzen der TrutzBox auf Werkseinstellung, denn die Adresse ist an die TrutzLegitimation gebunden und nicht an die Hardware. Einzelheiten im Kapitel „Die TrutzLegitimation aus Anwendungssicht“.

12.11 TrutzMail Ein- und Ausgang kontrollieren

Das Menü „E-Mail → Status“ zeigt dem Administrator den aktuellen Zustand der TrutzMail-Infrastruktur: noch nicht ausgelieferte Mails in der Warteschlange sowie alle vergangenen ein- und ausgehenden E-Mails im Mailprotokoll.

Menüpfad: E-Mail → Status



Das Menü „E-Mail → Status“ mit Warteschlange und Mailprotokoll.
(© 2026 Comidio GmbH)

Die Status-Ansicht besteht aus zwei Bereichen:

- **Warteschlange:** Zeigt alle Mails, die noch nicht ausgeliefert werden konnten, mit Datum, Queue-Typ, Größe, Absender, Empfänger, Status und Fehlermeldung (z. B. Connection timed out zur .onion-Adresse der Ziel-TrutzBox). In der Spalte „nach“ wird die Empfänger-Mailadresse angezeigt.
- Warteschlange aktualisieren (↻): Lädt die Liste neu.
- Alle Mails löschen: Löscht alle Mails aus der Sende-Warteschlange.
- E-Mail anzeigen: Zeigt den Inhalt der noch nicht versendeten Mail an.
- E-Mail erneut senden: Versucht die Zustellung sofort erneut.
- E-Mail löschen: Entfernt die Mail aus der Warteschlange.

- **Mailprotokoll:** Listet alle abgeschlossenen Ein- und Ausgänge mit Datum, Größe, Absender, Empfänger und Status (z. B. „Mail wurde erfolgreich gesendet“, „Sie haben eine Mail erhalten“). Ausgehende Mails sind mit → markiert, eingehende mit ←.
- Mailprotokoll aktualisieren (↻): Lädt das Protokoll neu.

- Rohes Postfix-Log (pro Eintrag): Über das Log-Symbol in einer Tabellenzeile lässt sich das detaillierte Postfix-Rohprotokoll dieser Mail für die Fehleranalyse einsehen. Einen globalen „System Postfix-Log“-Knopf gibt es nicht.

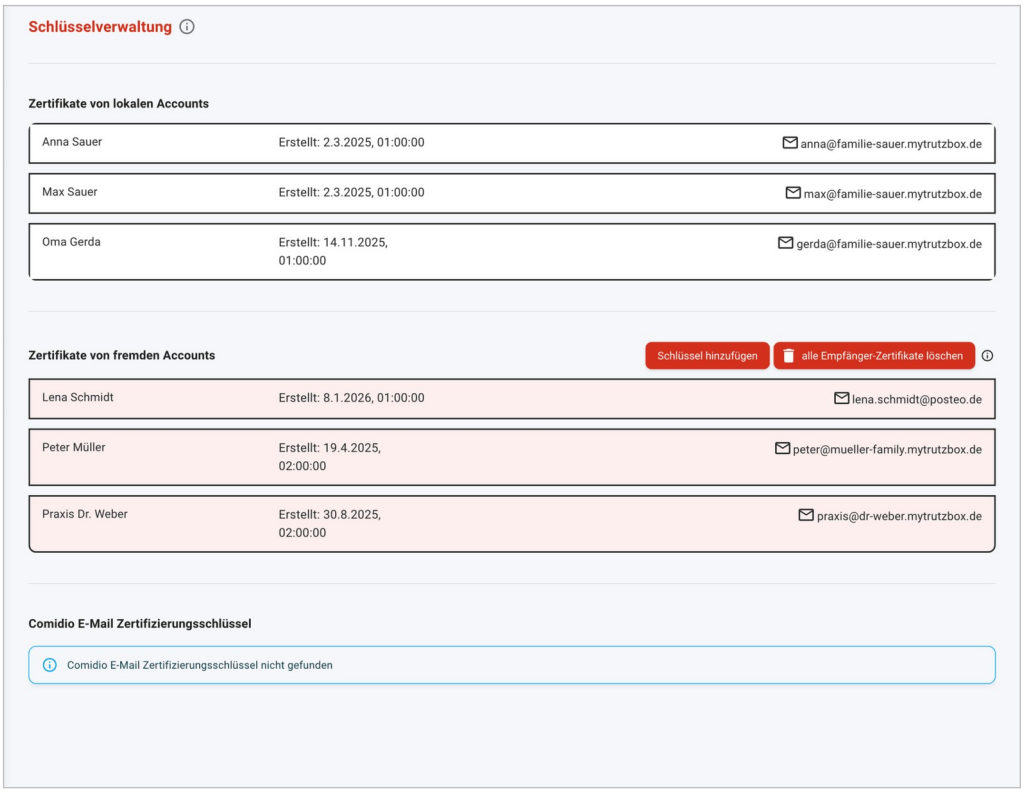
Eine TrutzMail kann nicht zugestellt werden, wenn eine der folgenden Voraussetzungen nicht erfüllt ist:

- Empfänger-Adresse muss existieren und als aktive TrutzMail-Adresse registriert sein.
- TrutzMail-Zertifikat des Empfängers muss gültig sein.
- Empfänger-TrutzBox muss eingeschaltet und online sein. Bei vorübergehender Nichterreichbarkeit versucht die TrutzBox die Zustellung in regelmäßigen Abständen erneut.
- Eigenes TrutzMail-Zertifikat muss gültig sein. Ohne gültigen Service-Vertrag wird das Zertifikat nicht erneuert, und die Empfänger-TrutzBox nimmt die Mail nicht an (maßgeblich sind die jeweils gültigen AGB und die Leistungsbeschreibung).
- Die Mail darf nicht an einen veralteten Schlüssel des Empfängers verschlüsselt sein; das korrigiert sich automatisch, Einzelheiten im Kapitel „Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen“.

12.12 Schlüsselverwaltung

Die Schlüsselverwaltung zeigt alle auf der TrutzBox gespeicherten Mail-Schlüssel. Mail-Schlüssel werden für jede TrutzMail-Adresse automatisch generiert und auf der TrutzBox gespeichert. Die jeweils passenden öffentlichen Schlüssel werden im zentralen Comidio-Adressbuch gespeichert.

Menüpfad: E-Mail → Schlüsselverwaltung



Die Schlüsselverwaltung mit den lokalen Mail-Schlüsseln jeder TrutzMail-Adresse.
(© 2026 Comidio GmbH)

Die Schlüsselverwaltung ist in drei Bereiche unterteilt:

- **Zertifikate von lokalen Accounts:** Zeigt die Mail-Schlüssel aller auf dieser TrutzBox eingerichteten TrutzMail-Adressen. Durch Klick auf einen Eintrag öffnet sich die Detail-Ansicht des Schlüssels.
- **Zertifikate von fremden Accounts:** Der Mail-Schlüssel-Cache für externe Mail-Accounts. Enthält automatisch heruntergeladene Schlüssel anderer TrutzBoxen sowie manuell importierte Schlüssel. Schlüssel, die nicht auf @comidio.email enden, stammen von öffentlichen Mail-Servern und wurden manuell importiert. Per „Schlüssel hinzufügen“ kann der öffentliche Schlüssel eines PGP-Kommunikationspartners manuell eingefügt werden. Per „Alle Empfänger-Zertifikate löschen“ wird der Cache geleert. Das Löschen eines einzelnen Empfänger-Schlüssels erzwingt beim nächsten Senden das Nachladen seines aktuellen Schlüssels (Einzelheiten im Kapitel „Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen“).
- **Comidio E-Mail Zertifizierungsschlüssel:** Der öffentliche Schlüssel von Comidio, mit dem die Signaturen eingehender TrutzMails geprüft werden.

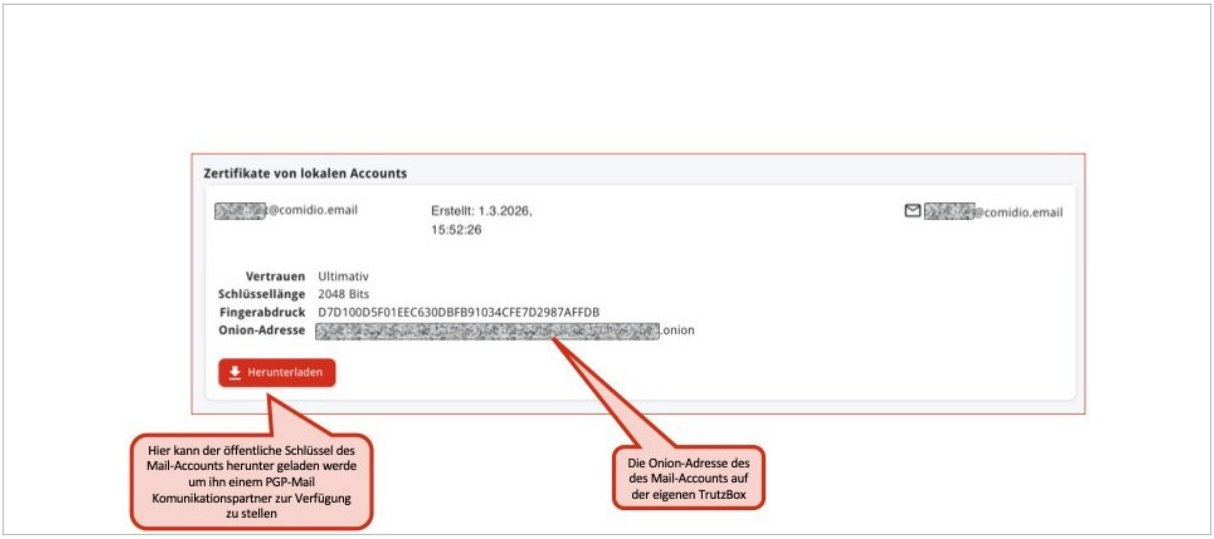
Beim Hinzufügen nimmt die TrutzBox nur Schlüssel an, mit denen ihre Mail-Dienste unbeaufsichtigt arbeiten können. Enthält die Datei einen privaten Schlüssel, der durch eine Passphrase geschützt ist, entfernt sie ihn nach einer Probesignatur wieder und meldet das: Im Hintergrund könnte niemand die Passphrase eingeben, und jede Mail des Kontos würde scheitern. Für einen PGP-

Kommunikationspartner genügt ohnehin dessen öffentlicher Schlüssel. Enthält ein Eintrag einen privaten Schlüssel, fragt die TrutzBox vor dem Löschen nach, denn damit verschlüsselte Nachrichten lassen sich danach nicht mehr öffnen. Scheitert das Löschen, zeigt die Oberfläche das an, statt den Eintrag scheinbar zu entfernen.

TrutzMail-Schlüssel Detail-Ansicht

Durch Klick auf einen lokalen Schlüssel-Eintrag öffnet sich die Detail-Ansicht:

Menüpfad: E-Mail → Schlüsselverwaltung



Die Detail-Ansicht eines lokalen Schlüssels mit Fingerabdruck und der .onion-Adresse des Kontos. (© 2026 Comidio GmbH)

Die Detail-Ansicht zeigt:

- Erstellungsdatum, Vertrauensstufe (Ultimativ für eigene Schlüssel).
- **Schlüssellänge:** 2048 Bits (RSA).
- **Fingerabdruck:** Eindeutiger kryptographischer Hashwert des Schlüssels zur Verifikation.
- **Onion-Adresse:** Die .onion-Adresse dieser TrutzMail-Adresse, über die eingehende TrutzMails über das Tor-Netzwerk zugestellt werden.
- **Herunterladen:** Lädt den öffentlichen Schlüssel herunter, um ihn einem PGP-Kommunikationspartner zur Verfügung zu stellen, der keine TrutzBox besitzt.

12.13 Mail-Programme einrichten

TrutzMail arbeitet mit jedem Mail-Programm, das IMAP und SMTP beherrscht. Die Schritte je Programm beschreibt das TrutzBox-Handbuch im Anhang im Kapitel „Mail-Programme für TrutzMail einrichten“. Hier steht, welche Angaben gelten, woher ein Programm sie bekommt und warum.

Angabe	Wert
Benutzername	die TrutzMail-Adresse, für Eingang und Ausgang
Passwort	das Passwort des TrutzMail-Accounts, nicht das Admin-Passwort
Server für Eingang und Ausgang	der Netzwerkname der TrutzBox, ab Werk trutzbox
Eingang	IMAP (Dovecot), Port 993, SSL/TLS
Ausgang	SMTP (Postfix), Port 587 mit STARTTLS oder Port 465 mit TLS

Anzeige in der Oberfläche: Unter „Verwaltung → Benutzer“ steht hinter der TrutzMail-Adresse eines Benutzers ein „i“. Es zeigt diese Angaben mit dem tatsächlichen Netzwerknamen der TrutzBox. Die Oberfläche fragt den Namen einmal je Seitenaufruf über die Schnittstelle /api/system/hostname ab und zeigt ihn in Kleinbuchstaben; antwortet die Schnittstelle nicht, bleibt „trutzbox“ stehen.
Welcher Name wo gilt: Im internen Netz und über TrutzVPN beantwortet die TrutzBox Namensanfragen selbst; dort ist sie immer unter trutzbox erreichbar, auch nach einer Umbenennung. Im lokalen Netz am Internet-Router kennt der Router sie unter dem Namen, den sie bei der Adressvergabe meldet. Dort gilt trutzbox nur, solange die TrutzBox ihren Werksnamen trägt; nach einer Umbenennung gilt der eigene Name, auch mit der Endung .local (Abschnitt „Die TrutzBox im Netz finden: trutzbox.local (mDNS)“). Aus dem Internet sind die Mail-Ports nicht erreichbar, solange sie am Router nicht freigegeben sind; unterwegs führt der Weg über TrutzVPN (Abschnitt „Portübersicht: was der Internet-Router durchlassen muss“).
Zertifikat: IMAP und SMTP weisen sich mit demselben TLS-Zertifikat aus wie die Weboberfläche (Anhang „Zertifikate und Schlüssel“, Nr. 3). Es stammt von der Zertifizierungsstelle der TrutzBox; das Gerät muss deshalb dem Root-Zertifikat der TrutzBox vertrauen, Thunderbird zusätzlich in seinem eigenen Zertifikatsspeicher (Abschnitt „Verschlüsselte (SSL/TLS)-Verbindungen“). Das Zertifikat nennt trutzbox, den Netzwerknamen und den Namen mit der Domäne des Routers. Neu ausgestellte Zertifikate tragen zusätzlich den Namen mit .local. Ein vorhandenes Zertifikat stellt die TrutzBox dafür nicht neu aus; der Name kommt erst hinzu, wenn ohnehin ein neues entsteht, etwa nach einer Umbenennung oder auf einer neuen TrutzBox.
Automatische Einrichtung mit Thunderbird: Thunderbird, auf Android auch Thunderbird für Android, sucht beim Anlegen eines Kontos die Einstellungen zur Domäne der Adresse selbst. Für Adressen auf @comidio.email fragt es zuerst https://autoconfig.comidio.email/mail/config-v1.1.xml ab und hängt dabei die Mail-Adresse als Parameter an. Comidio liefert dort eine Datei im Format, das Thunderbird dafür vorsieht (Autoconfig): IMAP an trutzbox, Port 993, SSL/TLS; SMTP an trutzbox, Port 587, STARTTLS; Benutzername ist die Mail-Adresse. Die Datei ist für alle Adressen gleich und enthält weder Kontodaten noch ein Passwort; die Adresse setzt das Mail-Programm selbst ein.
Die Datei liegt auf einem Server von Comidio und nicht auf der TrutzBox, weil das Mail-Programm beim Abruf ein öffentlich anerkanntes Zertifikat für autoconfig.comidio.email erwartet. Ein solches

Zertifikat kann nur Comidio als Inhaber der Domäne erhalten, nicht die einzelne TrutzBox. Weil die Datei für alle gleich ist, nennt sie den Werksnamen trutzbox. Im internen Netz und über TrutzVPN passt das immer. Wird eine umbenannte TrutzBox aus dem Netz des Internet-Routers eingerichtet, ersetzt der Anwender den Namen von Hand.

Andere Programme: Apple Mail, Outlook und die Mail-Apps der Android-Hersteller lesen diese Datei nicht; dort werden die Angaben von Hand eingetragen. Ein Verfahren für Outlook (Autodiscover) stellt Comidio nicht bereit.

Das neue Outlook: Das neue Outlook für Windows und die Outlook-App für Telefon und Tablet holen Mail nicht selbst ab, sondern über Server von Microsoft, bei denen auch das Passwort hinterlegt wird. Diese Server erreichen die TrutzBox nicht, und das Passwort läge außerhalb der TrutzBox. Für TrutzMail eignet sich deshalb nur das klassische Outlook.

13 TrutzDynDNS: Erreichbarkeit aus dem Internet

Dieses Kapitel fasst zusammen, wie TrutzDynDNS arbeitet: wie der Name entsteht, wie die TrutzBox ihre Adressen meldet, was der Server von Comidio damit tut, an welchen Anschlüssen die TrutzBox überhaupt von außen erreichbar ist, wie sie das selbst prüft und was Comidio dabei speichert. Die Bedienung beschreibt das TrutzBox-Handbuch im Kapitel „TrutzDynDNS: Ihre TrutzBox aus dem Internet erreichbar machen“.

13.1 Wozu TrutzDynDNS dient

Die Internet-Adresse eines privaten Anschlusses vergibt der Internet-Anbieter, und sie wechselt, bei vielen Anschlüssen täglich oder bei jeder neuen Einwahl. TrutzDynDNS gibt der TrutzBox einen festen Namen der Form [name].mytrutzbox.de, der immer auf die aktuelle Adresse des Anschlusses zeigt. Diesen Namen nutzen:

- **Fernzugriff:** Die Zugangsdateien von TrutzVPN (OpenVPN und WireGuard) enthalten den Namen als Gegenstelle für unterwegs (Kapitel „Fernzugriff: VPN (Virtual Private Network)“).
- **Videokonferenz und Chat:** Gäste kommen über einen Link mit diesem Namen in eine Konferenz; für den Namen holt die TrutzBox ein öffentlich anerkanntes Zertifikat (Abschnitt „Zertifikat für den TrutzDynDNS-Namen“).

Wer keinen dieser Dienste von außen nutzt, braucht TrutzDynDNS nicht. Eingeschaltet wird es unter „Netzwerk → Fernzugriff“ oder auf der Seite „Videokonferenz und Chat“ im Schritt „1. Domain-Namen festlegen“.

> **Die Kehrseite: Angriffsversuche von außen.** Der Name allein öffnet keinen Zugang. Erreichbar wird die TrutzBox erst durch die Freigaben am Internet-Router für Fernzugriff oder Videokonferenz, und jede Freigabe ist von außen sichtbar: Suchprogramme tasten das Internet ununterbrochen nach offenen Ports ab, ob es zu einer Adresse einen Namen gibt oder nicht. Hinzu kommt, dass jeder Name, für den ein öffentlich anerkanntes Zertifikat ausgestellt wird, in den öffentlichen Zertifikatsprotokollen (Certificate Transparency) erscheint und damit auffindbar ist. Die TrutzBox begegnet dem mit Freigaben nur für einzelne Dienste, einer von außen verschlossenen Bedienoberfläche und dem Angriffsschutz, der wiederholte Versuche sperrt (Abschnitt „Angriffsschutz“). Ein Restrisiko bleibt bei jeder Freigabe; deshalb sollten nur die Dienste freigegeben sein, die tatsächlich gebraucht werden.

13.2 Der Name und seine Vergabe

Den Namen vergibt der Kontoserver von Comidio bei der Registrierung der TrutzBox. Er besteht aus zehn Zeichen, die ein kryptografischer Zufallsgenerator aus Kleinbuchstaben und Ziffern wählt; leicht verwechselbare Zeichen wie 0 und o, 1, l und i kommen nicht vor. Frei wählen lässt sich der Name nicht. Er gehört zur TrutzKennung und nicht zum Gerät, ist eindeutig und bleibt der TrutzKennung reserviert,

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

auch wenn TrutzDynDNS ausgeschaltet wird. Wer einen Namen nach eigener Wahl verwenden möchte, nutzt dafür einen eigenen Namen (Abschnitt „Eigener Name neben TrutzDynDNS“).

13.3 Wie die TrutzBox ihre Adressen meldet

Ein Zeitgeber des Systems (systemd-Timer trutz-dyndns-update.timer) startet alle zehn Minuten den Lauf trutzDynDnsUpdate.sh. Sofort läuft er außerdem, wenn TrutzDynDNS eingeschaltet, der Schalter „TrutzDynDNS nur mit IPv6“ umgelegt oder die Veröffentlichung nach einer Prüfung der Erreichbarkeit umgestellt wird. Der Lauf arbeitet nur, wenn die Markierungsdatei /etc/comidio/trutzDNSEnabled vorhanden ist; sie enthält den Namen.

- **Öffentliche IPv4-Adresse:** An der eigenen Schnittstelle kann die TrutzBox sie nicht ablesen, weil der Internet-Router davor die Adressen umsetzt. Sie fragt deshalb den Namen myip.opendns.com direkt bei den Namensservern von OpenDNS (208.67.222.222 und 208.67.220.220) ab, die als Antwort die Absenderadresse der Anfrage liefern. Die Anfrage geht verschlüsselt über DNS-over-TLS (Port 853, mit Prüfung des Serverzertifikats); nur wenn das scheitert, fragt die TrutzBox unverschlüsselt über Port 53.
- **IPv6-Adresse:** Unter IPv6 setzt der Router keine Adressen um. Die TrutzBox meldet ihre eigene globale Adresse an der Schnittstelle, über die ihre IPv6-Standardroute läuft; private Adressen (fc00::/7) zählen nicht. Die hintere Hälfte dieser Adresse bildet sie fest aus ihrer MAC-Adresse (EUI-64), sodass sie gleich bleibt, wenn der Anbieter ein neues Präfix zuteilt. Diese hinteren vier Gruppen sind die Interface-ID, die man an einer FRITZ!Box für IPv6-Freigaben einträgt.

Gemeldet wird nur, wenn sich etwas geändert hat: Der Lauf löst den eigenen Namen auf und vergleicht A- und AAAA-Eintrag mit den ermittelten Adressen. Fehlt nur der AAAA-Eintrag, meldet er höchstens einmal in der Stunde. Eine eigene Wiederholung bei Fehlern gibt es nicht; der nächste Lauf versucht es zehn Minuten später erneut. Den letzten Fehler hält die TrutzBox in /var/lib/trutzbox/dyndns-status fest. Zeigt der Name länger als 25 Minuten nicht auf den Anschluss, wird die Karte „TrutzDynDNS“ im Betriebszustand orange.
Ändert sich die Adresse, passt der Lauf auch die Adresse an, die die Videobrücke der Videokonferenz nach außen nennt, und startet die Videobrücke neu, damit Gäste den Medienstrom weiter erreichen.

13.4 Der Weg zum Server von Comidio

Die TrutzBox meldet ihre Adressen dem Kontoserver von Comidio (account.comidio.com) über HTTPS mit dem Aufruf POST /api/box/dns/; im Inhalt stehen die IPv4- und die IPv6-Adresse. Sie weist sich dabei mit ihrem Box-Zertifikat aus (gegenseitige TLS-Anmeldung, mTLS; Anhang „Zertifikate und Schlüssel“, Nr. 2 und 19); einen Benutzernamen oder ein Kennwort gibt es dafür nicht. Der Server erkennt die TrutzBox am Fingerabdruck dieses Zertifikats und ändert nur den Eintrag der zugehörigen TrutzKennung. Er nimmt nur öffentlich gültige Adressen an und lehnt private ab. Beim Ausschalten meldet sich die TrutzBox mit DELETE /api/box/dns/ ab.
Die Zone mytrutzbox.de betreibt Comidio selbst, mit BIND9 auf den eigenen Namensservern ns1.comidio.com und ns2.comidio.com. Der Kontoserver trägt jede Meldung als dynamische

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Aktualisierung ein (nsupdate, abgesichert mit einem TSIG-Schlüssel): Er löscht die bisherigen Einträge des Namens und legt A- und AAAA-Eintrag neu an, beide mit einer Gültigkeitsdauer (TTL) von 600 Sekunden. Ein Namensdienst im Internet fragt also spätestens nach zehn Minuten neu nach. Zusammen mit dem Zehn-Minuten-Takt der TrutzBox zeigt der Name nach einem Adresswechsel in der Regel nach höchstens rund 20 Minuten wieder auf den Anschluss.

13.5 Welche Anschlüsse von außen erreichbar sind

Ein Name und eine Freigabe am Internet-Router genügen nur, wenn der Internet-Anbieter Verbindungen aus dem Internet überhaupt bis zum Anschluss durchlässt. Für IPv4 und IPv6 gilt dabei Verschiedenes:

Anschluss	Von außen über IPv4	Von außen über IPv6
Eigene öffentliche IPv4 und IPv6 (Dual-Stack)	Ja, über eine Portweiterleitung am Internet-Router.	Ja, über eine Freigabe in der IPv6-Firewall des Routers auf die Adresse der TrutzBox.
DS-Lite	Nein. IPv4 läuft durch einen Tunnel zum Anbieter und wird dort mit anderen Kunden geteilt (Carrier-Grade-NAT). Verbreitet bei Kabel- und Glasfaser-Anschlüssen. Eine eigene öffentliche IPv4-Adresse richten viele Anbieter auf Wunsch ein, oft gegen eine zusätzliche Gebühr.	Ja, wie bei Dual-Stack. Dazu der Schalter „TrutzDynDNS nur mit IPv6“.
Geteilte IPv4 ohne DS-Lite (CGNAT)	Nein. Der Router erhält eine Adresse aus 100.64.0.0/10, die der Anbieter mit anderen Kunden teilt.	Ja, sofern der Anschluss IPv6 hat.
Router hinter Router	Nur mit einer Portweiterleitung an jedem der beiden Router.	Nur, wenn der vordere Router dem hinteren ein eigenes Präfix weitergibt (Präfix-Delegation, DHCPv6-PD). Sonst bekommt die TrutzBox keine globale Adresse.
Mobilfunk-Router (LTE oder 5G)	Praktisch nie: Im Mobilfunk teilen sich viele Kunden eine IPv4-Adresse.	Selten. Viele Mobilfunk-Router nutzen ihr IPv6-Präfix nur für das eigene Netz und geben keines an einen angeschlossenen Router weiter; manche Netze lassen eingehende IPv6-Verbindungen zudem nicht zu.

Woran man den Anschluss erkennt: An einer FRITZ!Box zeigt „Internet → Online-Monitor“ die IPv4-Adresse, die IPv6-Adresse und das IPv6-Präfix. Eine private IPv4-Adresse (192.168., 10. oder 172.16. bis 172.31.) heißt, dass ein weiterer Router davor sitzt; ein Hinweis auf einen DS-Lite-Tunnel oder eine Adresse aus 192.0.0.0/29 bedeutet DS-Lite; eine Adresse aus 100.64.0.0/10 ein geteiltes IPv4. Ein leeres Feld „IPv6-Präfix“ heißt, dass der Router kein Präfix erhalten hat; dann bekommt auch die TrutzBox keine öffentliche IPv6-Adresse. Ob tatsächlich etwas ankommt, zeigt am Ende nur die Prüfung von außen (nächster Abschnitt).

13.6 Prüfung der Erreichbarkeit von außen

Von innen lässt sich das nicht sicher feststellen, denn viele Router reichen ein Paket an die eigene Anschlussadresse nicht zurück. Die TrutzBox bittet deshalb einen Server von Comidio um Testpakete an ihre eigene Internet-Adresse und zählt selbst, was auf den Anschlüssen von Fernzugriff und

Videokonferenz ankommt. Das Urteil fällt die TrutzBox, nicht der Server. Die Prüfung läuft von selbst nach Änderungen und einmal am Tag; die Schaltfläche „Jetzt prüfen“ startet sie sofort.

> **Was der Server von Comidio dabei tut und was nicht:** Der Server schickt Testpakete nur, wenn die TrutzBox ihn gerade darum gebeten hat, und nur an die Adressen, die sie selbst nennt. Er meldet sich nirgends an, liest nichts und schreibt nichts; ein Verbindungsversuch wird sofort wieder geschlossen. Von sich aus nimmt kein Server von Comidio Kontakt zu einer TrutzBox auf.

Ablauf im Einzelnen: Die TrutzBox bittet mit POST /api/box/dns/probe um eine Messung, angemeldet wie bei der Meldung der Adressen, und nennt dabei die Zieladressen, die Ports und eine für jede Messung neu gewürfelte Kennung aus 16 Zufallsbytes. Ein Sendeprogramm im Netz des Comidio-Servers schickt je UDP-Port drei Pakete im Abstand von einer Sekunde, die mit „TRUTZPRB“ beginnen und die Kennung tragen, und versucht je TCP-Port nach zwei und nach vier Sekunden einen Verbindungsaufbau; dabei geht nur das erste Paket des Verbindungsaufbaus hinaus, Daten werden nicht gesendet. Geprüft werden höchstens vier UDP- und zwei TCP-Ports: für den Fernzugriff der VPN-Port am Router, für die Videokonferenz TCP 443 (über IPv4 an der TrutzBox als 9082 ankommend) und UDP 9083. Das Ergebnis legt die TrutzBox in /var/lib/trutzbox/reachability.json ab.
Zeitplan: Die erste Messung folgt zwischen zwei und 30 Minuten nach dem Start. Danach prüft die TrutzBox alle zehn Minuten, ob eine Messung fällig ist: nach einer Änderung von Ports oder Adressen sofort, sonst einmal am Tag. Bietet der Server keine Messung an, wartet sie sechs Stunden; ein Ergebnis gilt drei Tage.
Technisch: Die TrutzBox legt für die Dauer einer Messung eine eigene Zähltabelle in der Firewall an. UDP-Testpakete erkennt sie an einer Kennung, die sie für jede Messung neu würfelt und nur dem Server nennt; Verbindungsversuche über TCP zählt sie nur, wenn sie von der Adresse des Servers kommen. Der Server antwortet auf die Bitte sofort und sendet danach; je TrutzKennung nimmt er eine Bitte in der Minute und höchstens 30 am Tag an.

13.7 Nur IPv6 oder nur IPv4 veröffentlichen

Anschluss ohne eigene IPv4-Adresse (DS-Lite): Bei DS-Lite gehört die von außen sichtbare IPv4-Adresse dem Anbieter und führt nie zur TrutzBox. Veröffentlicht TrutzDynDNS trotzdem A- und AAAA-Eintrag, nehmen die WireGuard-Apps für Android, iOS und Windows bei einem Namen mit beiden Adressarten immer die IPv4-Adresse und kommen nie an. Dafür gibt es im Domain-Bereich der Seite „Fernzugriff“ den Schalter „TrutzDynDNS nur mit IPv6 (Anschluss ohne eigene IPv4-Adresse, DS-Lite)“. Eingeschaltet legt die TrutzBox die Markierungsdatei /etc/comidio/trutzDNSIPv6Only an und meldet dem Kontoserver von Comidio nur noch die IPv6-Adresse; weil der Kontoserver bei jeder Meldung den ganzen Eintragssatz ersetzt, verschwindet der A-Eintrag. Der Zehn-Minuten-Lauf urteilt dann nach dem AAAA-Eintrag: In Ordnung ist der Name erst, wenn das AAAA auf die eigene Adresse zeigt und kein A mehr vorhanden ist; der Betriebszustand zeigt in der Karte TrutzDynDNS den Modus „nur IPv6“. Umlegen lässt sich der Schalter nur bei eingeschaltetem TrutzDynDNS und vorhandener globaler IPv6-Adresse; bis der Name überall nur noch mit IPv6 aufgelöst wird, können einige Minuten vergehen. Die TrutzBox setzt diesen Schalter auch von selbst, wenn ihre Prüfung der Erreichbarkeit von außen ergibt, dass über IPv4 nichts ankommt und über IPv6 schon. Von Hand muss er dann nicht gestellt

werden (Abschnitt „Erreichbarkeit von außen“ im Kapitel „Status (Netzwerk)“). Der Schalter gilt für alles, was am TrutzDynDNS-Namen hängt, also auch für Videokonferenz, Chat und Mail; für OpenVPN kommt der Schalter „VPN auch über IPv6 anbieten“ hinzu, damit die Zugangsdateien die IPv6-Zeile enthalten.
Aus dem Ergebnis stellt die TrutzBox selbst ein, welche Adressen ihr TrutzDynDNS-Name trägt. Kommt über IPv4 nichts an, über IPv6 aber schon, veröffentlicht sie nur noch die IPv6-Adresse. Das ist der Schalter „TrutzDynDNS nur mit IPv6“, den sie dann von selbst setzt. Kommt umgekehrt über IPv6 bei keinem Dienst etwas an, veröffentlicht sie nur die IPv4-Adresse, damit im Namen kein Eintrag steht, über den niemand hereinkommt. Die Anzeige sagt dann, was die TrutzBox eingestellt hat. Dasselbe zeigt der Betriebszustand in der Karte TrutzDynDNS in der Zeile „Veröffentlicht“: „nur IPv6 (über IPv4 kommt nichts an)“ oder „nur IPv4 (über IPv6 kommt nichts an)“; bei von Hand gesetztem Schalter „nur IPv6 (Anschluss ohne eigene IPv4-Adresse)“. Trägt der Name nur die IPv6-Adresse, beantwortet der Namensdienst an br0 ihn für Geräte im eigenen Netz und im Tunnel mit der internen Adresse der TrutzBox, weil dort nur IPv4 gilt (Datei unter /var/lib/trutz-network/hosts-innen.d); die TrutzBox selbst sieht weiter den öffentlichen Stand.
Dabei geht sie vorsichtig vor: Umgestellt wird erst, wenn zwei Messungen im Abstand von rund zehn Minuten dasselbe ergeben, und nur bei einem eindeutigen Ergebnis. Kommt ein Dienst nur über IPv4 an und ein anderer nur über IPv6, bleibt der Name, wie er ist. Einen von Hand gesetzten Schalter lässt die TrutzBox in Ruhe und weist nur darauf hin, wenn er nicht zum Ergebnis passt. Wer für den Fernzugriff einen eigenen Namen verwendet, bekommt die Anzeige ebenfalls; umgestellt wird dann nichts.
Markierungsdateien: Die Datei /etc/comidio/trutzDNSIPv6Only ist leer, wenn der Schalter von Hand gesetzt wurde, und enthält „auto“, wenn die TrutzBox ihn nach einer Messung gesetzt hat; nur im zweiten Fall nimmt sie ihn auch selbst wieder zurück. Das Gegenstück /etc/comidio/trutzDNSIPv4Only setzt nur die TrutzBox selbst. Den Eintrag für Geräte im eigenen Netz und im Tunnel schreibt sie in die Datei eigener-name im genannten Ordner und gleicht ihn alle 30 Sekunden ab.

13.8 Zertifikat für den TrutzDynDNS-Namen

Für den TrutzDynDNS-Namen holt die TrutzBox ein Zertifikat von Let’s Encrypt (Anhang „Zertifikate und Schlüssel“, Nr. 8). Den Nachweis, dass ihr der Name gehört, führt sie über einen DNS-Eintrag (Verfahren DNS-01): Das Programm acme.sh setzt über den Kontoserver von Comidio, wieder mit dem Box-Zertifikat angemeldet, einen TXT-Eintrag _acme-challenge zum Namen (Gültigkeitsdauer 60 Sekunden) und löscht ihn nach der Prüfung. Dafür muss kein Port am Router geöffnet sein. Ob das Zertifikat erneuert werden muss, prüft die TrutzBox täglich; erneuert wird 30 Tage vor dem Ablauf.

13.9 Eigener Name neben TrutzDynDNS

Neben dem TrutzDynDNS-Namen unter mytrutzbox.de kann die TrutzBox seit September 2026 auch unter einem eigenen Namen erreichbar sein, etwa über die DynDNS-Funktion des Internet-Routers oder eine eigene Domain. Den DNS-Eintrag für diesen Namen pflegt der Betreiber selbst; er muss auf die Internet-Adresse des Anschlusses zeigen. Die TrutzBox prüft das alle zehn Minuten im selben Lauf wie TrutzDynDNS. Ein eigener Name funktioniert auch dann, wenn TrutzDynDNS ausgeschaltet ist.

Die Karte: Die Einstellungen stehen auf der Seite „Fernzugriff“ im Abschnitt „1. Domain-Namen festlegen“ unterhalb von TrutzDynDNS; dieselbe Karte erscheint auf der Seite „Videokonferenz“, dort ohne das Port-Feld. Die Karte heißt „Eigener Domain-Name“ und ist zugeklappt, solange kein eigener Name gespeichert ist; darin gibt der Schalter „Eigenen Domain-Namen verwenden“ die Felder frei. Das Feld „Eigener Name“ nimmt den Namen ohne https:// und ohne Port auf; er braucht mindestens einen Punkt, darf keine IP-Adresse sein, und Namen unter mytrutzbox.de weist die TrutzBox ab, weil TrutzDynDNS sie verwaltet. Unter „Verwenden für“ stehen zwei Haken: „VPN-Zugangsdateien (WireGuard und OpenVPN)“ und „Videokonferenz und Chat von unterwegs“.
VPN: Mit dem ersten Haken schreibt die TrutzBox den eigenen Namen in alle WireGuard-Zugänge und OpenVPN-Zugangsdateien. In den OpenVPN-Profilen bleibt der Netzwerkname im lokalen Netz die erste Zeile; danach folgt der eigene Name, dann der TrutzDynDNS-Name als Rückfall, falls der eigene Name einmal nicht erreichbar ist. Eine Zeile über IPv6 (udp6) erhält nur der TrutzDynDNS-Name, denn die DynDNS eines Routers meldet oft nur eine IPv4-Adresse, und OpenVPN Connect auf dem iPhone bricht bei einer IPv6-Zeile ohne Ziel ab. WireGuard kennt nur eine Gegenstelle und nimmt den eigenen Namen. Unter dem Port-Feld steht die Reihenfolge („Die VPN-Zugangsdateien wählen in dieser Reihenfolge: …“). Nach dem Speichern laden die Nutzer ihre Zugangsdatei unter „Benutzer“ neu herunter und importieren sie erneut.
Port von außen für VPN: Ab Werk erwartet die TrutzBox, dass der Internet-Router UDP-Port 1194 unverändert weiterleitet. Leitet er stattdessen einen anderen Port von außen auf die TrutzBox, trägt man diesen Port hier ein (Standard 1194; Ports anderer Dienste der TrutzBox wie 443, 53 oder 9082 sind gesperrt). Das Feld steht in einem eigenen Block darunter, mit eigenem Knopf „Port speichern“, und gilt auch ohne eigenen Namen. Die Zugangsdateien nennen dann diesen Port, und die Firewall der TrutzBox leitet ihn an ihrem Internet-Anschluss auf den Tunnel-Port um, unter IPv4 wie unter IPv6 (nftables-Kette dienst_umleitung in der Tabelle inet fw, gefüllt von dienst-ports.sh aus /etc/wireguard/endpoint-port). Der Port gilt für beide Tunnel. Unter IPv6, wo der Router keine Ports umsetzt, ist das der Weg, einen anderen Port als 1194 anzubieten.
Zertifikat: Für die VPN-Zugangsdateien braucht der eigene Name kein Zertifikat. Für Videokonferenz und Chat braucht er eines, das zum Namen passt und dem Browser vertrauen. Für den eigenen Namen holt die TrutzBox kein Let’s-Encrypt-Zertifikat; es gibt nur den Upload: Zertifikat, privater Schlüssel und auf Wunsch die Zwischenzertifikate im PEM-Format, so wie Let’s Encrypt oder der Domain-Anbieter sie liefern. Der Schlüssel darf nicht mit einem Kennwort geschützt sein. Beim Hochladen prüft die TrutzBox, ob die Dateien lesbar sind, ob Schlüssel und Zertifikat zusammengehören, ob das Zertifikat gültig ist und den eingetragenen Namen abdeckt (auch als Wildcard), und sie prüft die Kette gegen die Stammzertifikate des Systems. Abgelegt wird es getrennt vom Let’s-Encrypt-Zertifikat unter /etc/comidio/extern.custom/ (fullchain.pem und privkey.pem). Die TrutzBox erneuert hochgeladene Zertifikate nicht; vor dem Ablauf muss ein neues hochgeladen werden.
Nicht öffentlich anerkannte Zertifikate: Ein Zertifikat, dessen Aussteller nicht öffentlich anerkannt ist, nimmt die TrutzBox für die Videokonferenz nur nach einer Warnung und ausdrücklicher Bestätigung an („Trotzdem verwenden“). Sie merkt sich die Freigabe als SHA-256-Fingerabdruck genau dieses Zertifikats; ein neues Zertifikat braucht eine neue Freigabe. Jeder Teilnehmer sieht dann eine Browser-Warnung, auch Gäste mit Einladungslink.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Testen: Der Knopf „Testen“ prüft den Namen in vier Schritten, ohne etwas zu speichern: „1. Schreibweise“ (gültiger Name, keine IP-Adresse, nicht unter mytrutzbox.de), „2. Namensauflösung“ (der Name muss auf die öffentliche IPv4-Adresse des Anschlusses zeigen; eine IPv6-Adresse wird zusätzlich angezeigt), „3. Zertifikat“ (passt das hochgeladene Zertifikat zum Namen, wie lange gilt es, ist der Aussteller anerkannt; unter 30 Tagen Restlaufzeit gibt es eine Warnung) und „4. Erreichbarkeit über den Namen“ (die TrutzBox baut über die öffentliche Adresse eine TLS-Verbindung zu Port 443 auf, nennt dabei den eigenen Namen und prüft, welches Zertifikat antwortet). Der vierte Schritt läuft nur bei eingeschalteter Videokonferenz. Schlägt er fehl, liegt es oft am Router, der Verbindungen aus dem eigenen Netz an die eigene Adresse nicht zurückleitet (Hairpin); ein Aufruf über das Mobilfunknetz schafft Gewissheit.
Technik: Die Einstellung liegt in /var/lib/trutzbox/config.json unter customDomain mit den Feldern name, vpn, rtc, app und vpnPort (null steht für 1194), dazu untrustedApproved mit dem Fingerabdruck eines freigegebenen Zertifikats. Für die Videokonferenz schreibt die TrutzBox einen eigenen nginx-Block (server.d/custom-domain.conf), der auf den Ports 9082 und 443 lauscht; nginx wählt den Block über den vom Browser genannten Namen (SNI), sodass TrutzDynDNS-Name und eigener Name nebeneinander funktionieren. Die Videobrücke erhält den eigenen Namen für ihre Websocket-Adresse, Prosody als http_external_url. Der Webfilter bricht Verbindungen zu den eigenen Namen der TrutzBox nie auf, sonst bliebe die Konferenzseite leer. Nach dem Speichern antwortet nginx sofort unter dem neuen Namen. Die Videobrücke startet dabei nicht neu, eine laufende Konferenz läuft weiter.
Betriebszustand: Die Karte „Eigener Name“ meldet, ob der Name auf den Anschluss zeigt (nach einem Adresswechsel mit 25 Minuten Karenz), und wie lange das Zertifikat gilt: gelb ab weniger als 30 Tagen Restlaufzeit, rot nach dem Ablauf, beides nur, wenn die Videokonferenz den Namen nutzt, denn für VPN allein schadet ein abgelaufenes Zertifikat niemandem.

13.10 Was Comidio speichert und protokolliert

Zu jedem Namen speichert der Kontoserver nur die aktuelle IPv4- und IPv6-Adresse und den Zeitpunkt der letzten Änderung. Jede neue Adresse ersetzt die alte; einen Verlauf führt die Datenbank nicht. Schaltet der Anwender TrutzDynDNS aus, löscht der Server die Adressen, der Name bleibt der TrutzKennung reserviert.
Damit bei einem Ausfall nichts verloren geht, sichert Comidio Datenbank und Zone alle vier Stunden. Die Sicherungen liegen etwa zwei Tage auf den Servern und 90 Tage in einer Sicherung außer Haus; in diesen Sicherungskopien bleiben ältere Adressen also bis zu 90 Tage erhalten und werden danach gelöscht.
Der Webserver des Kontoservers führt kein Zugriffsprotokoll, und die Protokolle der Schnittstelle enthalten keine Adressen. Das Sendeprogramm der Erreichbarkeitsprüfung schreibt nur das Ergebnis ins Protokoll, ohne TrutzKennung und ohne Adresse; nur für eine vom Support befristet eingerichtete Diagnose steht dort mehr.
Bei einem Besitzerwechsel registriert der neue Besitzer die TrutzBox mit seiner eigenen TrutzKennung und erhält einen neuen Namen; der bisherige Name gehört weiter zur alten TrutzKennung (Abschnitt „Was vor einem Besitzerwechsel zu tun ist“).

14 Videokonferenz und Chat (TrutzRTC)

Bitte beachten Sie, dass diese TrutzRTC-Funktion nur in der Business-Version der TrutzBox zur Verfügung steht.

Die TrutzBox wurde entwickelt, um dem Anwender einen zusätzlichen Schutz vor Angriffen und mehr Anonymität im Internet zu bieten. Aber was nutzt es, wenn man anonym surft und E-Mails verschlüsselt, aber dann Skype, WhatsApp oder ähnliche Services für Audio- und Video-Konferenzen und Messaging (Chat) nutzt? Selbst kostenpflichtige, als sicher beworbene Video-Konferenz-Systeme, die vor allem von Firmen genutzt werden, benötigen einen zentralen Kommunikations-Server, der vom Anbieter betrieben wird und somit zumindest die Möglichkeit einer Überwachung bietet.

Firmen oder auch Privat-Anwender nutzen gerne kostenlose Dienste wie WhatsApp, bei denen sie laut Datenschutzerklärung des Anbieters der Verarbeitung von Verbindungs- und Metadaten zustimmen. Somit war von Anfang an klar, dass die TrutzBox auch für Echtzeit Kommunikation eine sichere und anonyme Alternative anbieten muss.

Es gibt eine Vielzahl von Messenger-Programmen auf dem Markt. Für Comidio waren bei der Auswahl einer Lösung drei Eigenschaften entscheidend:[21]

- wie einfach ist das Tool zu installieren und zu bedienen,
- ob es auf allen gängigen Betriebssystemen/User-HW verfügbar ist und
- ob es auch Metadaten verschlüsselt.

Die TrutzMail-Technologie bildet die Grundlage für einen Messenger, der diese drei Eigenschaften berücksichtigt.
Comidio hat dazu auf der TrutzBox zwei Funktionen implementiert:

- XMPP-Server: für Messaging und je nach verwendetem Client auch weitere Funktionen wie Audio-, Videokonferenzen, File-Transfer, Screen-Sharing...
- Und einen Audio- und Video-Konferenz-Server, auf dem man sich mit einem Browser, der den WebRTC-Standard unterstützt, verbinden kann und der in der Lage ist, sehr effizient mehrere Audio- bzw. Video-Konferenz-Teilnehmer zu verbinden.

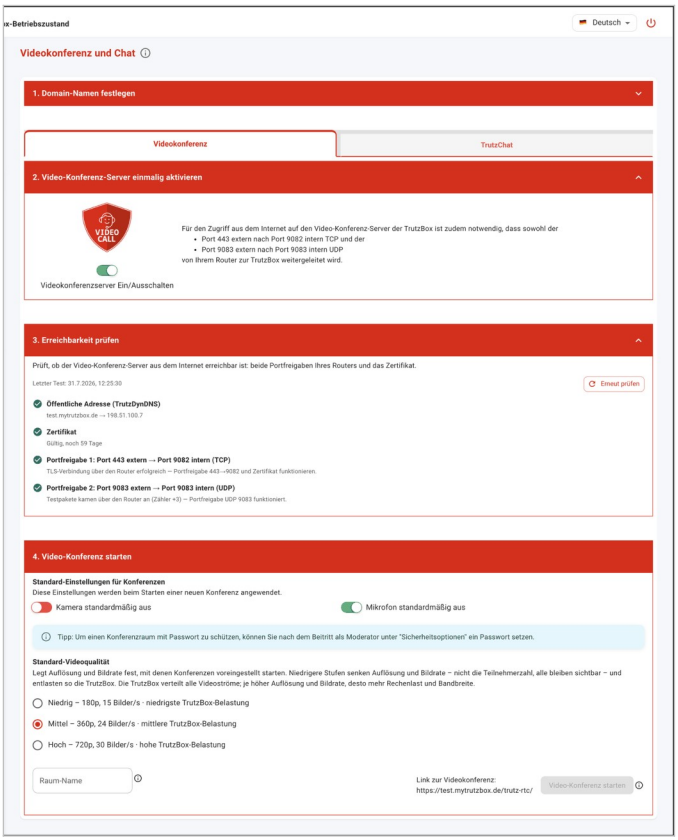
Weiterführende Informationen zu XMPP sind https://de.wikibooks.org/wiki/XMPP-Kompendium und http://xmpp.org/ zu entnehmen.

[21] https://www.eff.org/secure-messaging-scorecard

14.1 Videokonferenz einrichten und starten

Die Seite „Videokonferenz und Chat“ beginnt mit dem gemeinsamen Schritt „1. Domain-Namen festlegen“ (TrutzDynDNS und Zertifikat, Voraussetzung für die Videokonferenz) und teilt sich darunter in zwei Karteikarten: „Videokonferenz“ und „TrutzChat“. Die Karteikarte „Videokonferenz“ führt durch drei weitere Schritte (die technischen Hintergründe beschreibt der Abschnitt „TrutzRTC Videokonferenz Server“ im Detail):

Menüpfad: Videokonferenz und Chat



Die Seite „Videokonferenz und Chat“ mit den Karteikarten Videokonferenz und TrutzChat. (© 2026 Comidio GmbH)

- 1. Domain-Namen festlegen: Damit externe Teilnehmer aus dem Internet einem Videokonferenz-Raum beitreten können, muss die TrutzBox über einen öffentlichen Domain-Namen erreichbar sein. Hierzu wird TrutzDynDNS aktiviert, das der TrutzBox einen festen Domainnamen unter *.mytrutzbox.de zuweist. Zusätzlich sollte ein allgemein anerkanntes Let’s Encrypt-Zertifikat für diesen öffentlichen Namen aktiviert werden, damit Browser der Teilnehmer keine Zertifikatswarnung anzeigen. Schlägt die Zertifikats-Erstellung fehl, nennt die Fehlermeldung die konkrete Ursache (etwa den Prüf-Fehler von Let’s Encrypt). Statt des TrutzDynDNS-Namens kann auch ein eigener Name mit hochgeladenem Zertifikat dienen (Abschnitt „Eigener Name neben TrutzDynDNS“ im Kapitel „TrutzDynDNS: Erreichbarkeit aus dem Internet“).

- 2. Videokonferenz-Server einmalig aktivieren: Der Videokonferenz-Server muss einmalig eingeschaltet werden. Für den Zugriff aus dem Internet müssen am Router folgende Ports weitergeleitet werden: Port 443 extern → Port 9082 intern (TCP) und Port 9083 extern → Port 9083 intern (UDP). Das Einschalten läuft im Hintergrund weiter, auch wenn es länger dauert. Besonders der allererste Start nach der Einrichtung braucht Zeit; die Oberfläche zeigt währenddessen den Fortschritt und wartet bis zu vier Minuten, statt vorschnell einen Fehler zu melden, obwohl der Dienst sauber hochkommt. Solange TrutzDynDNS und Zertifikat noch nicht eingerichtet sind, bleibt der Schalter auf der Übersichtsseite gesperrt, mit einem Hinweis auf den Menüpunkt, an dem das nachzuholen ist.
- 3. Erreichbarkeit prüfen: Auf Knopfdruck prüft die TrutzBox selbst, ob der Konferenz-Server aus dem Internet erreichbar ist, in vier Stationen: „Öffentliche Adresse (TrutzDynDNS)“, „Zertifikat“ sowie die beiden Portfreigaben (443 extern → 9082 intern TCP und 9083 UDP). Jede Station meldet ihr Ergebnis in Klartext, etwa „TLS-Verbindung über den Router erfolgreich, Portfreigabe 443→9082 und Zertifikat funktionieren.“ oder „Keine Verbindung, Portfreigabe fehlt oder der Router unterstützt kein Hairpin-NAT.“
- 4. Videokonferenz starten: Hier werden Standard-Einstellungen für neue Konferenzen festgelegt (Kamera und Mikrofon standardmäßig an/aus). Durch Eingabe eines Raumnamens und Klick auf „Videokonferenz starten“ wird direkt eine neue Konferenz geöffnet. Der generierte Link (https://[name].mytrutzbox.de/trutz-rtc/[raum]) kann an Teilnehmer weitergegeben werden, diese benötigen keinen eigenen TrutzBox-Account. Tipp: Ein Konferenzraum kann per Passwort geschützt werden; das Passwort wird nach dem Beitritt als Moderator unter „Sicherheitsoptionen“ gesetzt. Neben dem Einladungslink steht ein Kopier-Symbol, das den Link mit einem Klick in die Zwischenablage legt. Ob Teilnehmer stumm beitreten, entscheidet ausschließlich diese Vorgabe aus der Verwaltung; der Browser-Speicher eines Teilnehmers überdeckt sie nicht. Der Schalter ist eindeutig beschriftet: grün bedeutet eingeschaltet.

Darüber hinaus lässt sich hier die Standard-Videoqualität für neue Konferenzen festlegen. Zur Wahl stehen drei Stufen: Niedrig (180p, 15 Bilder/s), Mittel (360p, 24 Bilder/s) und Hoch (720p, 30 Bilder/s). Sie sind jeweils mit ihrer Auswirkung auf die TrutzBox-Belastung beschriftet. Niedrigere Stufen verringern Auflösung und Bildrate (nicht die Zahl der gezeigten Teilnehmer, alle bleiben sichtbar) und entlasten so die TrutzBox bei Konferenzen mit mehreren Kameras. Voreingestellt ist die Stufe Niedrig.

14.2 TrutzRTC: Messaging/Chat-Verbindungen (XMPP-Server)

Die Karteikarte „TrutzChat“

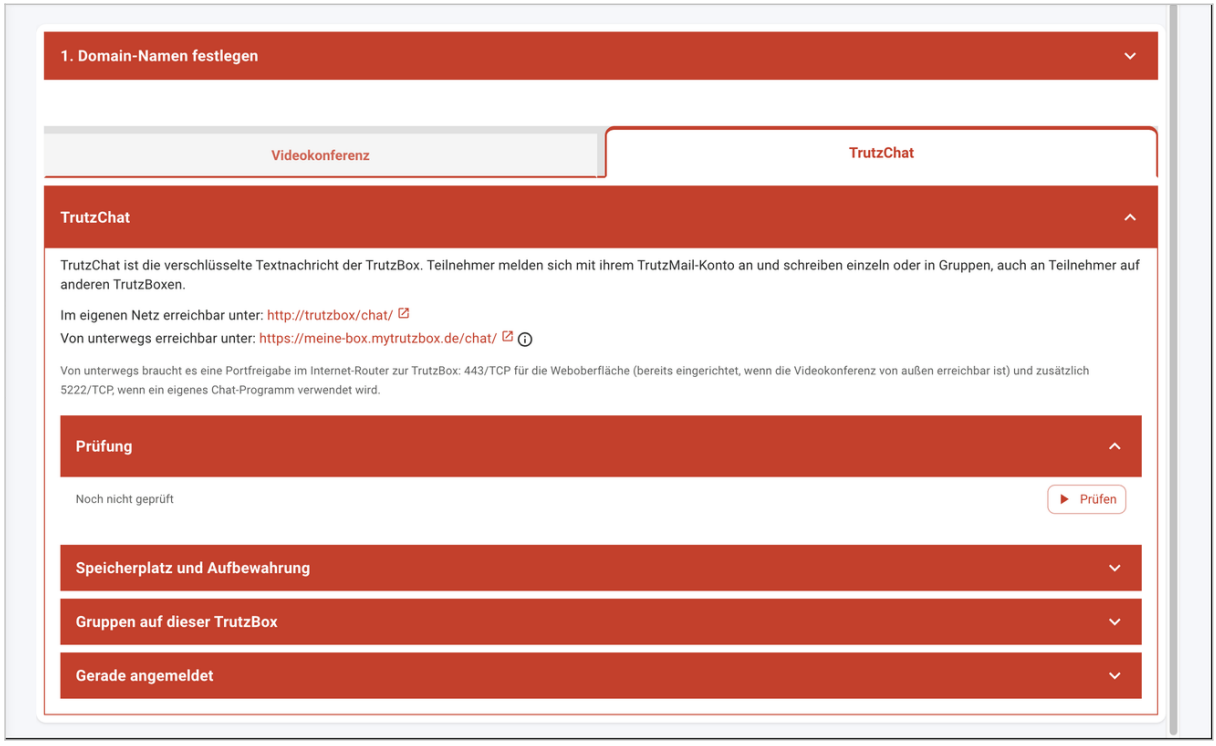
Die zweite Karteikarte verwaltet TrutzChat, die verschlüsselte Textnachricht der TrutzBox. Sie zeigt die Adresse des Chat-Zugangs im Browser im eigenen Netz (https://trutzbox/chat/) und verweist für den Zugriff von unterwegs auf TrutzVPN. Wichtig: Im eigenen Netz und zwischen TrutzBoxen kommt TrutzChat ohne TrutzDynDNS aus; von unterwegs führt der Weg über den Fernzugriff (TrutzVPN), eine eigene Chat-Adresse im Internet gibt es nicht mehr.

Die Karte gliedert sich in vier aufklappbare Bereiche:

- **„Prüfung“:** Der Chat-Selbsttest prüft auf Knopfdruck den Nachrichtenweg auf der Box. Zwei Testteilnehmer verbinden sich und tauschen eine Nachricht aus (Dauer etwa zehn Sekunden); das Ergebnis erscheint in Klartext.
- **„Speicherplatz und Aufbewahrung“:** Unter „Verwaltung“ legt der Administrator fest, wie viele Tage Chat-Verläufe aufbewahrt werden (wirksam ab dem nächsten Start des Servers; Älteres löscht die Box selbsttätig), sieht den Platzbedarf der Verläufe und der Anhänge und kann die Verläufe gesammelt löschen („Alle Verläufe löschen“).
- **„Gruppen auf dieser TrutzBox“:** Die Karte listet die auf dieser TrutzBox angelegten Gruppen mit Teilnehmerzahl. Gruppen lassen sich hier zentral anlegen und löschen und ihre Mitglieder verwalten.
- **„Gerade angemeldet“:** Hier stehen die gerade angemeldeten Chat-Sitzungen.

Die Übersichtskarte nennt zu jedem Gespräch und jeder Gruppe, wann es angelegt wurde und wann zuletzt etwas geschah, dazu die angemeldeten Sitzungen sowie den Speicherplatz, den die Anhänge belegen, samt einer Funktion zum Aufräumen.

Menüpfad: Videokonferenz und Chat



Die Karteikarte „TrutzChat“ mit ihren vier aufklappbaren Bereichen.
(© 2026 Comidio GmbH)

Der Bereich „Gruppen auf dieser TrutzBox“ macht die Chat-Gruppen der Box sichtbar und verwaltbar. Zu jeder Gruppe stehen die Zahl der gerade verbundenen Teilnehmer, die Zahl der Mitglieder und der Zeitpunkt der Gruppengründung in einer Zeile. Aufgeklappt zeigt die Karte jedes Mitglied mit dem

Zeitpunkt seiner Aufnahme und der letzten Anmeldung. Das ist besonders bei ausstehenden Einladungen hilfreich: Man sieht sofort, seit wann eine Einladung unbeantwortet ist.
Über das Papierkorb-Symbol lassen sich Gruppen und einzelne Mitglieder entfernen. Unter „Teilnehmer aufnehmen“ wird ein weiteres TrutzMail-Konto Mitglied und erhält sofort eine Einladung in seinem Chat-Programm. Mit „Neue Gruppe anlegen“ entsteht eine Gruppe samt Ersteller, ganz ohne Chat-Programm. Der Eigentümer einer Gruppe legt außerdem fest, ob auch die Mitglieder weitere Teilnehmer einladen dürfen; ohne diese Berechtigung erscheint das Einladen-Feld bei ihnen gar nicht erst. Eine Einladung an eine Chat-Adresse, die nicht erreichbar ist, wird mit einer klaren Fehlermeldung abgewiesen statt still verworfen: Schon beim Anlegen eines Kontakts und beim Aufnehmen in eine Gruppe prüft die TrutzBox, ob die Gegenstelle überhaupt antwortet.

Menüpfad: Videokonferenz und Chat



Verwaltung einer Chat-Gruppe: Mitglieder aufnehmen, entfernen oder Gruppe neu anlegen. (© 2026 Comidio GmbH)

Die Aufbewahrungsfrist unter „Speicherplatz und Aufbewahrung“ gilt für Einzelgespräche und Gruppen gleichermaßen. Nach Ablauf löscht die TrutzBox die Verläufe selbsttätig; Anhänge räumt sie bereits nach 30 Tagen ab.
Auch bei Ende-zu-Ende verschlüsselten Messenger-Diensten fallen beim Betreiber Metadaten an (wer wann mit wem kommuniziert), soweit die Architektur des Dienstes sie nicht vermeidet. Eine Untersuchung von drei beliebten mobilen Messengern (WhatsApp, Signal und Telegram; Hagen et al., TU Darmstadt/Universität Würzburg, NDSS 2021) hat außerdem gezeigt, dass entgegen den Erwartungen groß angelegte Crawling-Angriffe auch auf vermeintlich sicheren Messenger-Diensten möglich sind.[22]

Es liegt also nahe, selbst einen Messenger-Dienst zu betreiben. Damit ist kein dritter Dienstleister eingebunden, der die Metadaten sehen könnte. Dieser sollte natürlich auf einem Standard basieren, also auf dem XMPP-Standard.

[22] https://encrypto.de/papers/HWSDS21.pdf

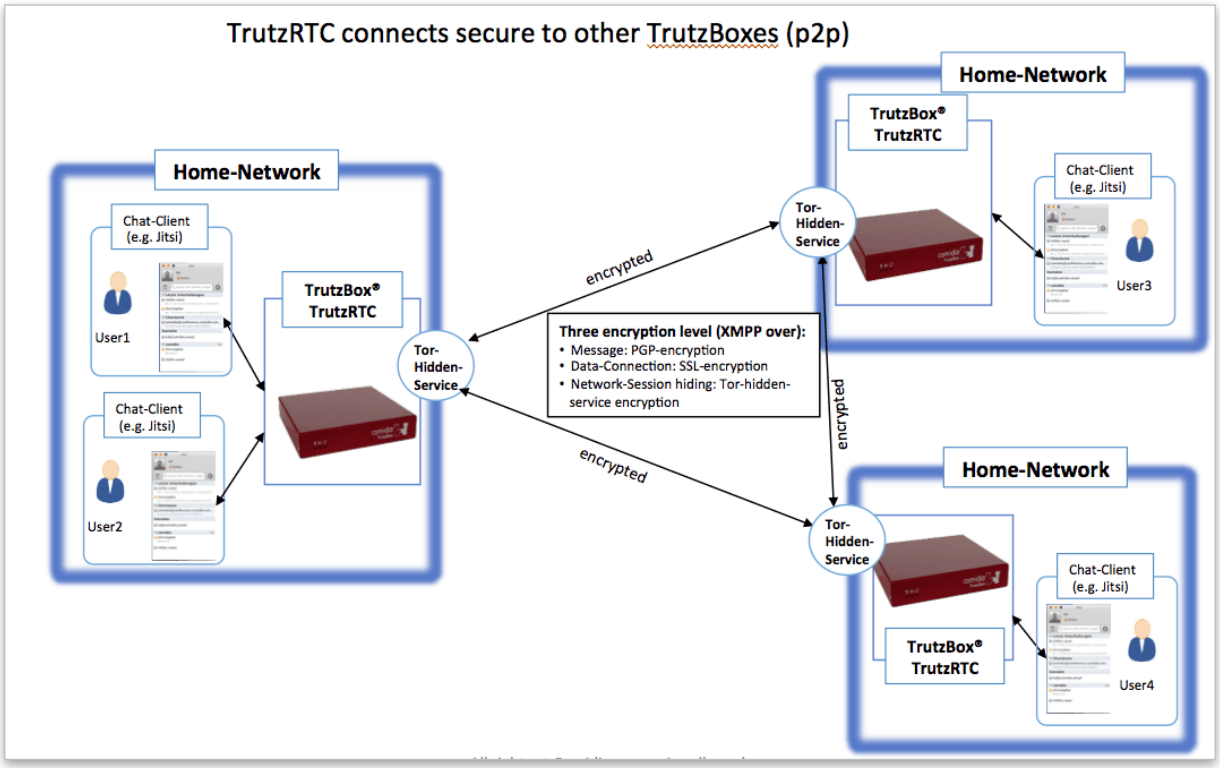
Das XMPP (Extensible Messaging and Presence Protocol), auf Deutsch „erweiterbares Nachrichten- und Anwesenheits-Protokoll“, ist ein Internet-Standard zum Austausch von Nachrichten (Chat). Es basiert auf der vor vielen Jahren entwickelten Jabber-Software und funktioniert ähnlich wie E-Mail. Ein XMPP-Server verwaltet Benutzer, den Online-Status der Benutzer und Nachrichten:
http://www.einfachjabber.de/

Falls eine Nachricht an einen Teilnehmer verschickt werden soll, der sich nicht auf dem gleichen Server wie der Absender befindet, wird der Ziel-Server (TrutzBox des Kommunikationspartners) ermittelt, Kontakt aufgenommen und die Nachricht zu diesem XMPP-Server ausgeliefert. Das gleiche gilt nicht nur für Nachrichten sondern auch für andere Funktionen, wie z. B. Anwesenheitsstatus. Eine gute deutsche Einführung in die Welt der XMPP-Kommunikation bietet die Webseite einfachjabber.de (http://www.einfachjabber.de).

Es gibt viele öffentlich verfügbare XMPP(Jabber)-Server, die aber alle den Nachteil haben, dass bei jeder Chat-Kommunikation, die durch diese Server vermittelt wird, zumindest die Metadaten sichtbar sind. Deshalb läuft der eigene XMPP-Server direkt auf der TrutzBox.
Comidio hat den XMPP-Server auf der TrutzBox so erweitert, dass er in der Lage ist, die gleichen Sicherheitsfunktionen zu nutzen, die auch bei TrutzMail verwendet werden. Das bedeutet:

- Kommunikationspartner werden mit der TrutzMail-Adresse adressiert.
- Der Verbindungsaufbau und die Nachrichtenübermittlung mit Nutzern auf einer anderen TrutzBox finden über Tor-Hidden-Services statt.
- Für die Verschlüsselung der Messages und Authentisierung der TrutzBox des Kommunikationspartners, werden die gleichen Zertifikate und Schlüssel wie bei TrutzMail verwendet.

Somit werden einfache Bedienbarkeit und ein hohes Sicherheitsniveau auch bei TrutzBox-übergreifender Kommunikation erreicht. Einmal angelegte TrutzMail-Adressen können direkt auch für Chat/Messaging verwendet werden. Dazu ist keinerlei Konfiguration auf der TrutzBox notwendig.



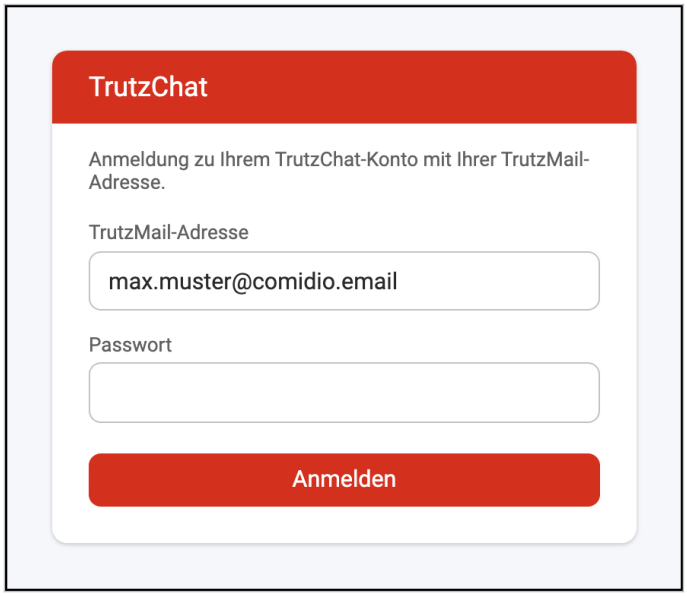
TrutzRTC verbindet TrutzBoxen unmittelbar über Tor-Hidden-Services, mit drei Verschlüsselungsebenen.
(© 2026 Comidio GmbH)

TrutzChat im Browser

Am einfachsten geht der Einstieg ohne jede Installation, denn TrutzChat läuft im Browser unter der Adresse der TrutzBox mit dem Zusatz /chat/:

- **Anmeldung:** Angemeldet wird mit der TrutzMail-Adresse und dem zugehörigen Passwort.
- **Erreichbarkeit:** Im eigenen Netz unter https://trutzbox/chat/, außerdem aus dem Netz vor der TrutzBox über deren Adresse in diesem Netz. Von unterwegs ist der Web-Chat nur über den Fernzugriff (TrutzVPN) erreichbar. Über den TrutzDynDNS-Namen und die Portfreigabe der Videokonferenz ist er seit September 2026 nicht mehr aufrufbar, damit an seiner Anmeldeseite niemand aus dem Internet TrutzMail-Passwörter durchprobieren kann.
- **Kontakte:** Sie werden über ihre TrutzMail-Adresse aufgenommen. Die Gegenseite bestätigt die Aufnahme, danach sehen beide Seiten gegenseitig die Anwesenheit (farbiger Punkt: erreichbar/nicht erreichbar).
- **Verlauf:** Der Gesprächsverlauf kommt aus dem Archiv der Box und steht damit auch nach einem Browserwechsel bereit. Beim Entfernen eines Kontakts oder einer Gruppe kann auf Wunsch der gespeicherte Verlauf gleich mitgelöscht werden.

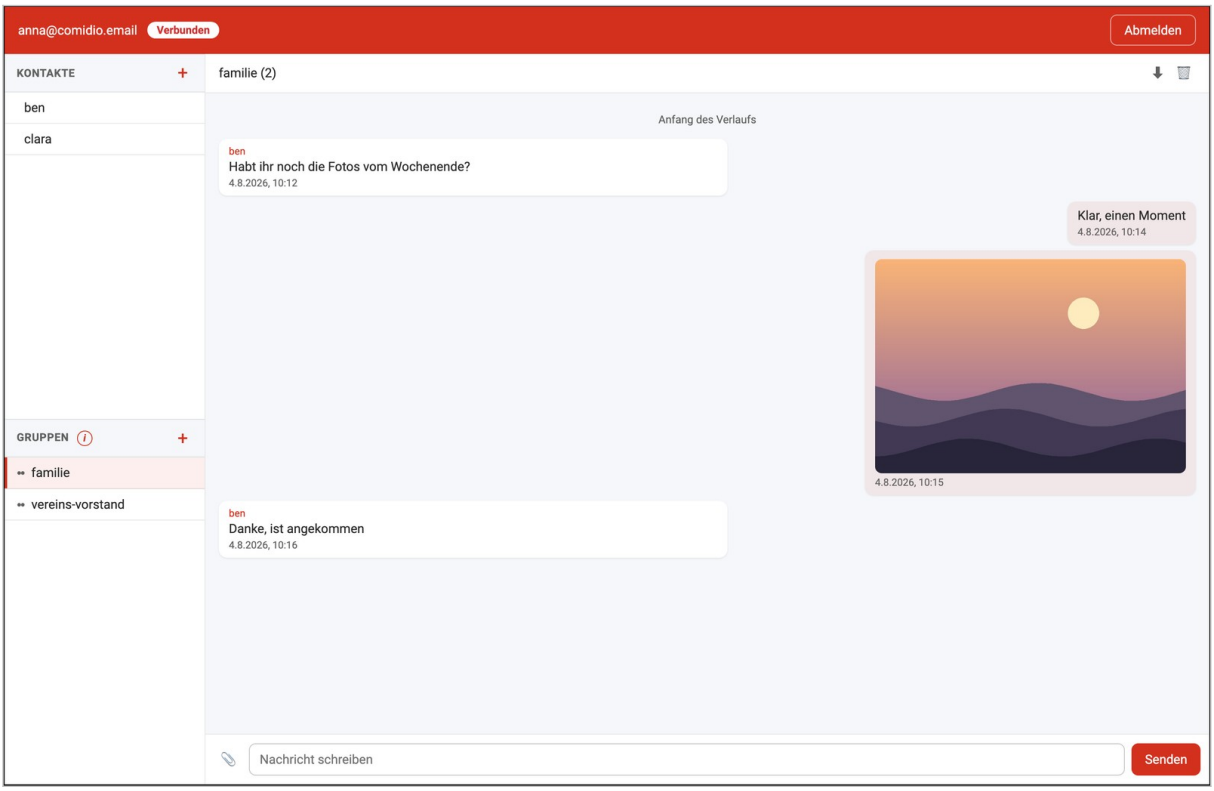
- **Fenster:** Der Chat öffnet sich in einem eigenen Fenster, und es lassen sich mehrere Chat-Fenster nebeneinander offen halten.
- **Verbindungsabbruch:** Bricht die Verbindung ab, etwa durch Standby des Rechners oder einen Netzwechsel, bleibt die Oberfläche nicht stumm. Sie prüft die Verbindung laufend, baut sie selbsttätig neu auf und betritt die Gruppenräume erneut, auch nach einem Rauswurf aus einem Raum.



Die Anmeldung zu TrutzChat im Browser mit der TrutzMail-Adresse.
(© 2026 Comidio GmbH)

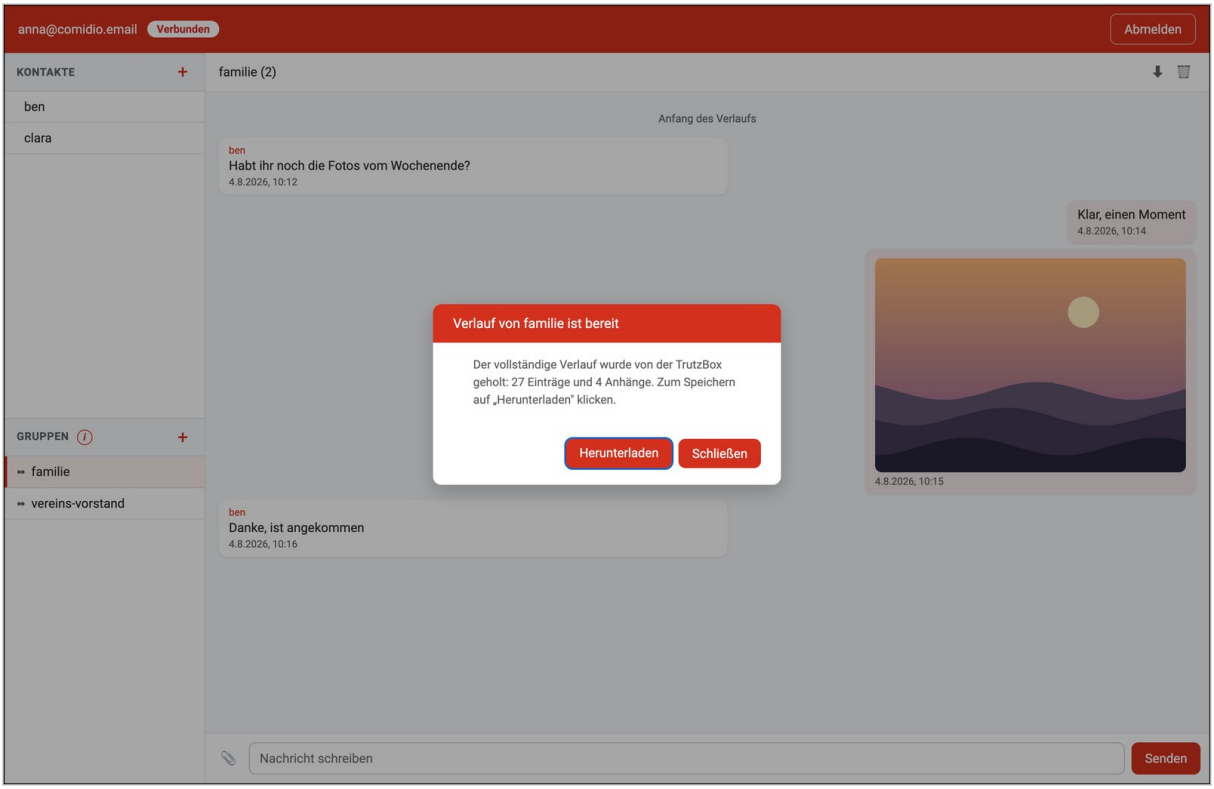
Gruppen lassen sich direkt im Browser anlegen (Name plus Mitglieder als TrutzMail-Adressen); die Mitglieder werden automatisch eingeladen. Das Stift-Symbol am Gruppeneintrag zeigt, wer gerade in der Gruppe ist (Ersteller und Abwesende sind gekennzeichnet); dort lassen sich weitere Teilnehmer einladen, und der Ersteller kann Mitglieder entfernen oder die Gruppe „Für alle löschen“ (wahlweise auch nur bei sich selbst entfernen). Das alles funktioniert auch TrutzBox-übergreifend: Adressiert wird immer die TrutzMail-Adresse, die verschlüsselte Tor-Route zwischen den Boxen setzt die TrutzBox im Hintergrund selbst ein.

Menüpfad: TrutzChat im Browser: https://trutzbox/chat/



TrutzChat im Browser: links Kontakte und Gruppen, rechts das Gespräch samt Anhängen. (© 2026 Comidio GmbH)

Dateien und Bilder verschickt man über das Büroklammer-Symbol oder zieht sie einfach mit der Maus in das Chat-Fenster. Bilder erscheinen als Vorschau direkt im Gespräch, andere Dateien als anklickbarer Verweis. Die Gegenseite lädt den Anhang von der TrutzBox, sobald sie ihn öffnet; nach 30 Tagen löscht die Box Anhänge selbsttätig.
Die Gruppenliste führt die TrutzBox selbst. Wer in eine Gruppe aufgenommen wird, sieht sie automatisch in jedem seiner Chat-Programme, auch in Apps wie Monal oder Siskin; eine gelöschte Gruppe verschwindet überall von selbst. Nachrichten, die während einer Abwesenheit eintreffen, liefert die Box beim nächsten Öffnen nach. Es spielt also keine Rolle, an welchem Gerät man gerade sitzt.
Mit den beiden Symbolen rechts oben im Gespräch lässt sich der Verlauf sichern oder löschen. Beim Sichern holt TrutzChat den vollständigen Verlauf von der TrutzBox und stellt ihn als Datei bereit. Enthält das Gespräch Anhänge, entsteht ein ZIP-Archiv mit dem Text des Verlaufs und allen Dateien, jeweils in der Reihenfolge des Gesprächs nummeriert. Das Löschen entfernt den Verlauf nach einer Rückfrage endgültig aus dem Archiv der Box. Bei einer Gruppe lässt sich der Verlauf vollständig vom Server löschen; einzelne Beiträge lassen sich gezielt entfernen.



Verlauf eines Gesprächs sichern oder löschen, Anhänge kommen als ZIP-Archiv.
(© 2026 Comidio GmbH)

Technische Umsetzung: Der Chat-Server trägt jede Gruppe in die Kontodaten ihrer Mitglieder ein (XMPP-Lesezeichen, in beiden gebräuchlichen Formaten) und führt für Gruppen ein eigenes Nachrichtenarchiv auf der Box. Liste und Verlauf entstehen dadurch auf jedem Gerät identisch aus den Daten der TrutzBox, ohne dass ein Chat-Programm selbst etwas speichern muss.

Wer statt des Browsers lieber eine eigene App nutzt, benötigt auf dem Endgerät ein XMPP-fähiges Programm. Chat-Programme, die das XMPP-Protokoll unterstützen, sind für alle gängigen Betriebssysteme mit unterschiedlichem Funktionsumfang verfügbar. Diese Links geben einen guten Überblick über verfügbare XMPP-Clients:

- https://de.wikipedia.org/wiki/Liste_von_XMPP-Clients
- https://de.wikibooks.org/wiki/XMPP-Kompendium:_Einrichtung
- http://xmpp.org/software/clients.html

Comidio empfiehlt folgende Chat-Programme für das jeweilige Betriebssystem:

Betriebssystem	XMPP-Software	Link
Apple Macintosh	Adium oder Swift	adium.im, swift.im
Microsoft Windows	PSI oder Swift	psi-im.org, swift.im
iOS (iPhone, iPad..)	ChatSecure	chatsecure.org
Android	Xabber	www.xabber.com

Nach der Installation einer solchen App genügt die Anmeldung mit der TrutzMail-Adresse und dem zugehörigen Passwort. Den Server findet die App selbst: Die TrutzBox veröffentlicht im eigenen Netz einen DNS-Eintrag (SRV-Eintrag), der für die Domäne comidio.email auf die Box und den XMPP-Standard-Port 5222 zeigt. Ein Servername muss nicht von Hand eingetragen werden. Das Zertifikat der Box ist auf comidio.email ausgestellt, sodass die Prüfung in der App ohne Warnung durchläuft. Bewährt haben sich BeagleIM (macOS), Monal (iOS und macOS), Conversations (Android) und Gajim (Windows und Linux). Der Port 5222 ist nur im eigenen Netz erreichbar (LAN, WLAN und TrutzVPN); am Internet-Router wird er nicht freigegeben. Von unterwegs verbinden sich App und Web-Chat gleichermaßen über den Fernzugriff (TrutzVPN); eine Chat-Adresse über den TrutzDynDNS-Namen gibt es nicht mehr.

Es können in einem Client auch mehrere TrutzMail-Adressen konfiguriert werden.
Hier ein Beispiel mit dem Chat-Programm Adium (macOS); andere XMPP-Programme sind ähnlich aufgebaut, die Bezeichnungen der Felder können abweichen:

Danach können durch Eingabe der TrutzMail-Adressen beliebig viele Kontakte zugefügt werden.
Je nach Funktionsumfang des Messaging-Clients unterstützt der XMPP-Server auf der TrutzBox diese XMPP-Standard Funktionen:

- **Instant-Messaging:** Text-Nachrichten inkl. Formatierung und Emoticons,
- Kommunikations-Gruppen anlegen und verwalten, Gruppen-Chats (Multi-User-Chat, MUC[23]), auch TrutzBox übergreifend.
- **Audio-/Video-Kommunikation:** Telefongespräche (Jingle RTP Sessions, optional mit ZRTP Verschlüsselung[24]),
- **Datei-Transfer:** Dateien an den/die Kommunikationspartner schicken
- **Screen-Sharing:** seinen eigenen Bildschirm für andere sichtbar machen
- **Remote-Desktop:** der Kommunikations-Partner kann meinen PC bedienen

[23] http://xmpp.org/extensions/xep-0045.html

[24] http://xmpp.org/extensions/xep-0167.html

- OTR (Off-the-Record Messaging)[25]: inoffizielle; vertrauliche, nicht für die Öffentlichkeit bestimmte Nachrichtenübermittlung. Im Gegensatz zur normalen PGP-Verschlüsselung, ist mit OTR später nicht mehr feststellbar, ob ein bestimmter Schlüssel von einer bestimmten Person genutzt wurde. Dadurch lässt sich nach Beenden der Unterhaltung von niemandem (auch keinem der beiden Kommunikationspartner) beweisen, dass einer der Kommunikationspartner eine bestimmte Aussage gemacht hat (glaubhafte Abstreitbarkeit).
- Online-Status, Last-Seen: ist der Kommunikationspartner online, gesprächsbereit... oder wann war er das letzte Mal online

Da die meisten dieser Sonderfunktionen nur dann unterstützt werden, wenn beide Kommunikationspartner den gleichen XMPP-Client benutzen, raten wir dazu, für erweiterte Funktionen besser den Videokonferenz-Service der TrutzBox zu nutzen.

Externe Verbindungen zu TrutzRTC

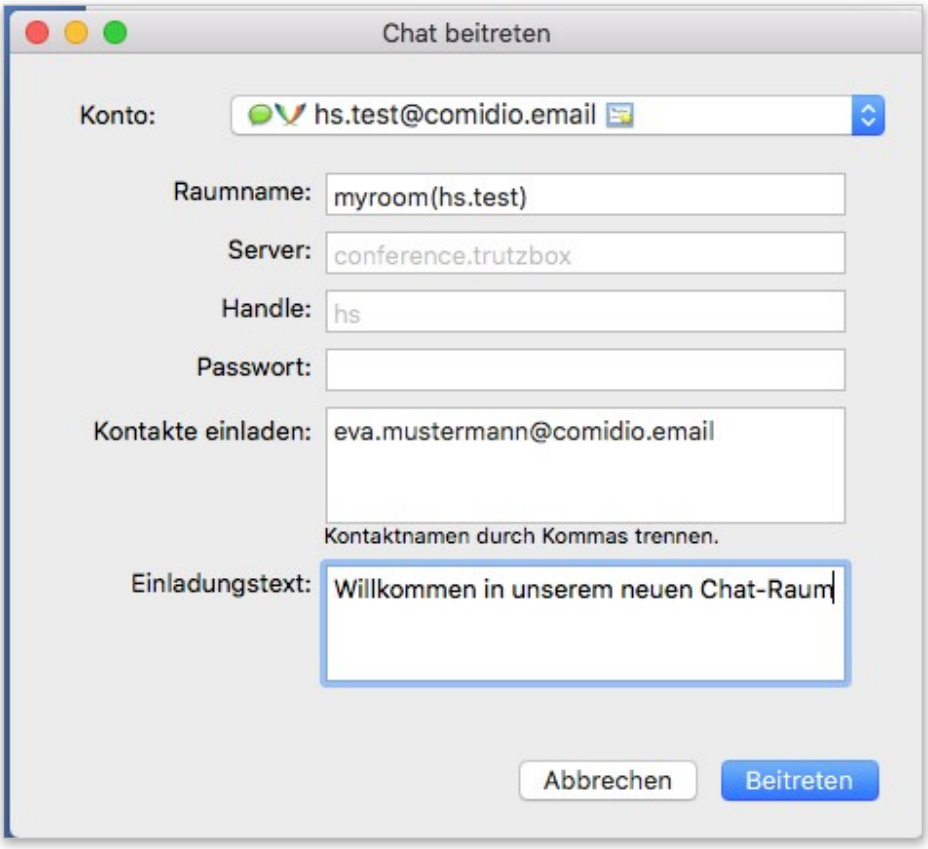
Solange die TrutzBox mit dem Host-Namen „trutzbox“ erreichbar ist, kann sich der Messaging-Client direkt mit dem XMPP-Server auf der TrutzBox verbinden. Das funktioniert allerdings nur aus dem lokalen Netz, wenn der Client mit dem Internet-Router (Proxy-Modus) oder dem sicheren Netzwerk der TrutzBox (Transparent-Modus) verbunden ist.
Um sich auch von unterwegs mit dem XMPP-Server auf der TrutzBox zu verbinden, empfiehlt Comidio ausschließlich den Fernzugriff (VPN): Der Chat-Zugang bleibt hinter der Verschlüsselung des VPN, am Router muss kein zusätzlicher Port geöffnet werden, und das Messaging-Programm arbeitet dann wie im lokalen Netz. Die Einrichtung beschreibt das Kapitel „Fernzugriff: VPN (Virtual Private Network)“.

Vom direkten Weiterleiten des XMPP-Ports 5222 TCP am Internet-Router rät Comidio ab, weil der Anmeldedienst damit dauerhaft offen im Internet stünde.

Einrichtung und Nutzung von Chat-Räumen

Geschlossene Nutzergruppen wie Vereine, Freundeskreise, Schulen oder Projektteams kommunizieren über Chat-Räume (Multi User Chat, MUC). Ein Raum liegt auf der TrutzBox des Mitglieds, das ihn anlegt, und nimmt per Einladung beliebig viele Teilnehmer auf, auch von anderen TrutzBoxen; angelegt und verwaltet wird er im Web-Client, Einzelheiten im Kapitel „TrutzChat im Browser“.

[25] https://de.wikipedia.org/wiki/Off-the-Record_Messaging



Sicherheit und Anonymität bei der Nutzung des XMPP-Servers

Um Sicherheit und Anonymität zu erhöhen, verbinden sich die TrutzRTC-Server bei TrutzBox-übergreifender Kommunikation über das Tor-Netzwerk.
Dadurch wird die Kommunikation zwischen den TrutzBoxen dreifach geschützt und es werden sogar die Metadaten verschlüsselt:

- Die XMPP-Message ist PGP-verschlüsselt.
- Die Datenverbindung zwischen den TrutzBoxen ist SSL-verschlüsselt.
- Die Netzwerk-Verbindung wird durch Tor-Hidden-Service verschlüsselt und „versteckt“.

Bei der XMPP-Kommunikation wird kein zentraler Server außerhalb der TrutzBox verwendet. Wer den Internet-Verkehr abhört, kann die Daten nach heutigem Stand der Technik praktisch nicht entschlüsseln und auch kaum erkennen, dass es sich überhaupt um eine XMPP-Kommunikation handelt oder welche IP-Adressen Absender und Empfänger haben. Restrisiken bleiben, etwa kompromittierte Endgeräte oder aufwendige Verkehrsanalysen.
Die Sicherheit der Verbindung zwischen einem XMPP-Client und dem Server oder auch zwischen den XMPP-Clients bei Jingle-Verbindungen, hängt von den Sicherheits-Funktionalitäten des Clients ab und welche davon aktiviert sind. Somit können zusätzliche Client-Verschlüsselungen wie PGP (nur die

eigentliche Message wird verschlüsselt), OTR (Off-the-Record Messaging) oder ZRTP[26] (Voice-over-IP-Verschlüsselung) aktiviert werden, falls die genutzten Messaging-Clients diese Funktionen unterstützen.

14.3 TrutzRTC Videokonferenz Server

Um effektiv mit einem Gesprächspartner oder einer ganzen Gruppe von Meeting-Teilnehmern kommunizieren zu können, bieten sich Telefon- oder Videokonferenzen an. Konferenz-Lösungen werden häufig als Dienst eines Anbieters gemietet.
Bei kostenlosen wie bei bezahlten Angeboten läuft die Kommunikation über einen zentralen Server des Anbieters, der den Verbindungsaufbau regelt und die Streaming-Daten bündelt; welche Meta- und Nutzungsdaten dort verarbeitet werden, ergibt sich aus der jeweiligen Datenschutzerklärung. Aufsichtsbehörden für den Datenschutz, etwa die Berliner Beauftragte für Datenschutz und Informationsfreiheit, veröffentlichen Hinweise zu den datenschutzrechtlichen Anforderungen an Video-Konferenz-Systeme.[27][28]

Mit Hilfe des XMPP-Servers und dem richtigen Messaging-Client ist es zwar möglich, eine Audio-/Video-Verbindung aufzubauen, allerdings nur mit einem weiteren Teilnehmer, und es ist notwendig, dass alle Teilnehmer den gleichen XMPP-Client im Einsatz haben, der den gleichen Audio-/Video-Codec unterstützt. Somit sind Standard-XMPP Clients keine optimale Lösung für Telefon- oder Videokonferenzen.

Um dem TrutzBox Anwender auch eine sichere Lösung für Telefon- oder Video-Konferenzen mit mehreren Teilnehmern zu ermöglichen, bietet die TrutzBox einen WebRTC-fähigen Konferenz-Server an. WebRTC ist ein recht neuer Internet-Standard, der ursprünglich von Google entwickelt wurde und Audio-/Video-Konferenzen direkt mit einem Standard-Internet-Browser, also ohne zusätzliche Software, ermöglicht. Der Standard wurde zwar von Google entwickelt, allerdings ist bei der TrutzBox-Lösung weder Google, noch irgend eine anderes Unternehmen bei einer Video-Konferenz eingebunden.[29]

Die Einrichtung (TrutzDynDNS-Domain, Portweiterleitung am Internet-Router und Let's Encrypt-Zertifikat) ist im Abschnitt „Videokonferenz einrichten und starten“ beschrieben.

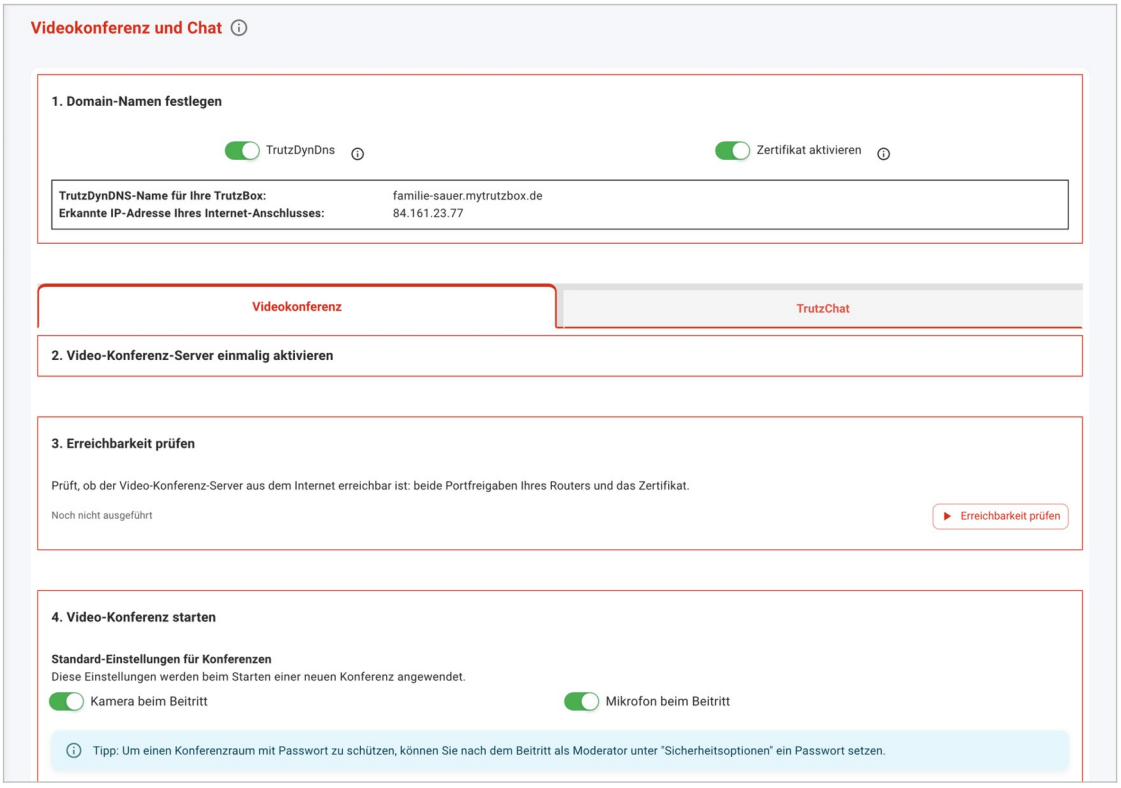
[26] https://de.wikipedia.org/wiki/ZRTP

[27] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf

[28] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

[29] http://webrtc.org/

Menüpfad: Videokonferenz und Chat



Die Karteikarte „Videokonferenz“ mit Domain-Namen, Server-Schalter und Erreichbarkeitstest. (© 2026 Comidio GmbH)

Das LetsEncrypt-Zertifikat für den TrutzDynDNS-Namen erzeugt die TrutzBox automatisch über letsencrypt.org (Einzelheiten im Kapitel „Videokonferenz einrichten und starten“). Da LetsEncrypt nur fünf Zertifikate pro Woche erlaubt, sollte der Schalter nicht öfter als fünfmal pro Woche eingeschaltet werden (https://letsencrypt.org/docs/rate-limits/).https://letsencrypt.org/docs/rate-limits/

Falls die TrutzBox schon mit einer anderen öffentlich nutzbaren Domain erreichbar ist (z. B. mit einer vorhandenen Firmendomain), kann auch diese für die Verbindung zu einem Videokonferenz-Server genutzt werden. In diesem Fall würde der Videokonferenz-Teilnehmer aber eine Zertifikats-Sicherheits-Warnung bekommen, da der Videokonferenz-Server lediglich das Let’s Encrypt-Zertifikat der TrutzDynDNS-Adresse an den Browser übermittelt. Ein evtl. vorhandenes Zertifikat einer anderen vorhandenen Domain kennt der Videokonferenz-Server auf der TrutzBox nicht.

Um eine Videokonferenz zu starten, muss lediglich aus dem internen Netzwerk oder aus dem Internet mit einem WebRTC-fähigen Browser die TrutzBox mit

https://xxxxxx.mytrutzbox.de/trutz-rtc/raumname

aufgerufen werden, wobei

- xxxxxx.mytrutzbox.de der TrutzDynDNS-Name ist und

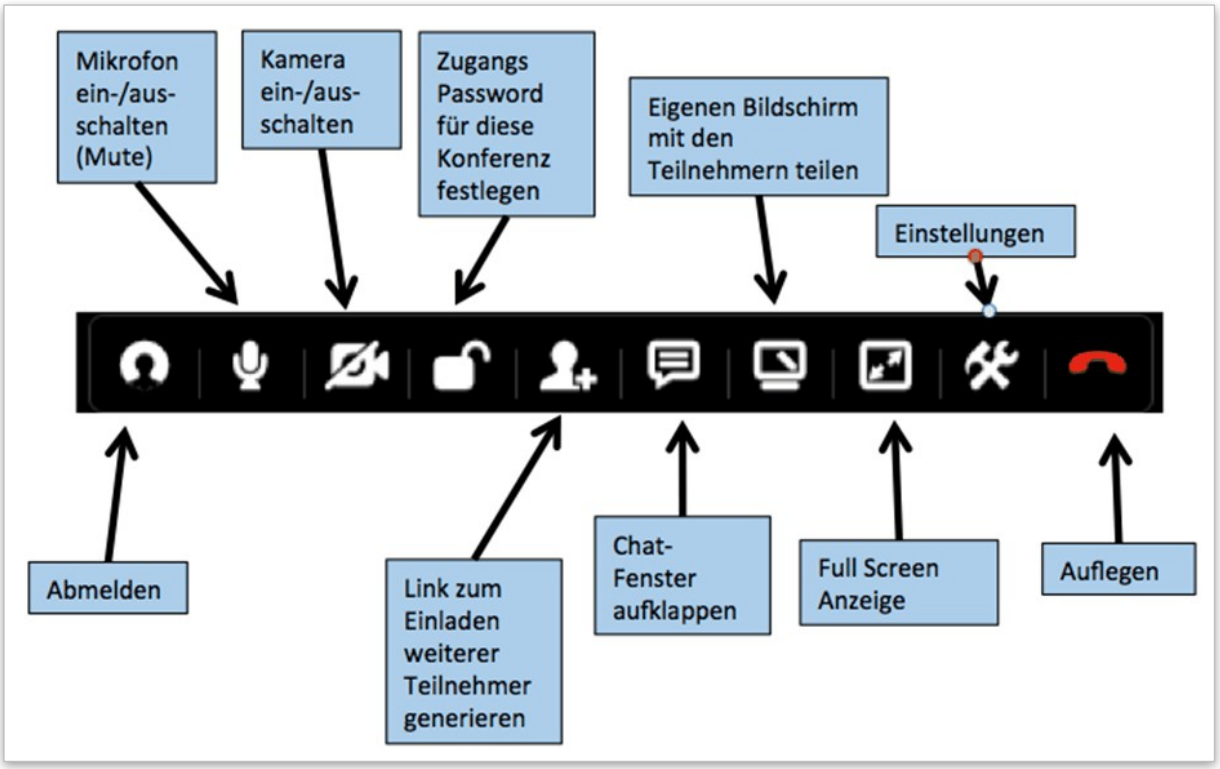
- raumname einfach ein selbst vergebener Raum-Name ist. Beim gewählten Raumnamen dürfen keine Sonderzeichen verwendet werden!

Dabei sind zwei Fälle zu unterscheiden:

- **Der Raum existiert noch nicht:** Somit ist man jetzt der Erste, der diesen Raum anlegen möchte, und man ist der „Raum-Administrator“ für diesen Raum:
- **Anmeldung:** Zunächst ist es notwendig, sich mit seiner TrutzMail-Adresse und dem TrutzMail-Passwort an dem Konferenz-Server anzumelden.
- **Wer eröffnen darf:** Somit können nur TrutzBox-Benutzer, die ein TrutzMail-Konto auf dieser TrutzBox haben, einen neuen Raum eröffnen.
- **Raum-Optionen:** Nach Anlegen und Verbinden mit dem Raum kann der Raum-Administrator wahlweise noch ein Passwort für diesen Raum festlegen und weitere Raum-Optionen festlegen.
- **Der Raum existiert schon:** Dann verbindet sich der Browser mit dem Raum:
- **Passwort:** Falls der Raum-Administrator ein Passwort auf den Raum gelegt hat, muss dieses jetzt eingegeben werden.
- **Teilnahme:** Falls der Raum schon angelegt ist, kann sich jeder zu dem Raum verbinden.
- **Voraussetzungen:** Dazu muss er weder eine eigene TrutzBox besitzen, noch als Benutzer auf der TrutzBox eingetragen sein, noch eine TrutzMail-Adresse besitzen.

Sobald der Browser mit dem Raum verbunden ist, sollte man durch Anklicken des eigenen Verbindungs-Fensters unten seinen „Anzeigenamen“ angeben.
Durch Positionierung der Maus am oberen Bildschirmrand wird ein Bedien-Menü geöffnet. In diesem Menü werden folgende Funktionen angeboten:

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2



Die Bedienleiste einer laufenden Videokonferenz mit ihren Funktionen.
(© 2026 Comidio GmbH)

Ein SIP-Gateway von und zum Videokonferenz-Server wird von Comidio offiziell nicht unterstützt. Wer entsprechendes Know-how besitzt, kann jedoch unter https://github.com/jitsi/jigasi nähere Informationen zur Konfiguration eines SIP-Gateways nachlesen.

Sicherheit und Anonymität bei der Nutzung des Videokonferenz-Servers

Der Videokonferenz-Server befindet sich auf der TrutzBox und nimmt keinerlei Verbindung zu einem anderen Server im Internet auf. Per Browser verbindet man sich mit dem Konferenz-Server und benötigt auch keine andere Verbindung außer zur TrutzBox. Da die Browser-Verbindung zur TrutzBox DTLS-verschlüsselt ist (TLS für UDP), bietet die Lösung Vertraulichkeit und Abhörschutz nach Stand der Technik.

Leistungsgrenzen des Konferenz-Servers

Der TrutzRTC Konferenz-Server basiert auf der Open-Source Software Jitsi-Video-Bridge. [30][31] Die Zahl der möglichen Teilnehmer ist begrenzt. Die Anzahl der Teilnehmer ist in erster Linie abhängig von der Geschwindigkeit der Internet-Anbindung jedes einzelnen Teilnehmers und des TrutzBox Besitzers.

[30] https://de.wikipedia.org/wiki/Jitsi

[31] https://jitsi.org/Projects/JitsiVideobridge

Für die Sprachübertragung genügt ca. 40 kBit/s Upload- und Download-Geschwindigkeit pro Teilnehmer. Für Kamera oder Screen-Sharing sollten ca. 800 kBit/s jeweils zur Verfügung stehen (abhängig von der Bildschirmauflösung und wie oft sich das Bild ändert). Somit werden wahrscheinlich bei normalen DSL/VDSL Internet-Anbindungen zunächst Engpässe bei der Internet-Anbindung entstehen, bevor die TrutzBox Hardware zum Engpass wird. Solche Internet-Engpässe lassen sich am besten auf dem Internet-Router analysieren.

Nach Erfahrung des Comidio-Teams liegt die Leistungsgrenze bei etwa 15 Teilnehmern, wenn nur ein Teilnehmer seinen Bildschirm teilt oder eine Kamera an ist.
Die Jitsi-Meet-Software selbst skaliert ziemlich gut, was dieser Benchmark auf einem großen Server mit sehr schneller Internet-Anbindung zeigt: https://jitsi.org/Projects/JitsiVideobridgePerformance.
Reicht die Leistung bei vielen Teilnehmern mit Kamera nicht aus, lässt sich die Last der TrutzBox über die Standard-Videoqualität (siehe „Videokonferenz einrichten und starten“) gezielt senken, indem Auflösung und Bildrate reduziert werden.

Externe Verbindungen zum TrutzRTC-Konferenz-Server

Um sich extern, also über Internet mit dem Konferenz-Server der TrutzBox zu verbinden, wird bei den Teilnehmern keine TrutzBox benötigt. Wer den Link kennt (und das evtl. vergebene Passwort), kann an der Konferenz teilnehmen. Das erleichtert vor allem die Nutzung von Webinaren oder spontanen Konferenzen.
Damit der Videokonferenzserver über das Internet erreichbar ist, müssen allerdings auf dem Internet-Router, an dem die TrutzBox angeschlossen ist, diese zwei Ports an die TrutzBox weitergeleitet werden (TrutzRTC Portfreigabe)

Mit dem Link „https://xxxxxx.mytrutzbox.de/trutz-rtc/raumname „kann dann über das Internet dem Raum beigetreten werden.

Falls im Netzwerk in dem die TrutzBox hängt der externe Port 443 schon für andere Anwendungen belegt ist und diese Anwendung auch aus dem Internet erreichbar sein soll, kann auch ein beliebiger anderer externer Port genutzt werden. Dann muss von den Teilnehmern der Videokonferenz jedoch im Aufruf nach dem Domain-Namen dieser Port mit angegeben werden.

Z.B. bei Weiterleitung des Ports 4443 anstatt 443:
„https://xxxxxx.mytrutzbox.de:4443/trutz-rtc/raumname „

Verfügt der Internet-Anschluss über IPv6, ist der Konferenz-Server zusätzlich direkt über die globale IPv6-Adresse der TrutzBox erreichbar, ohne Portweiterleitung, da IPv6 kein NAT kennt. Es genügt dann, am Internet-Router die IPv6-Firewall für die TrutzBox auf den Ports 443 (TCP) und 9083 (UDP) zu öffnen, ohne Umleitung auf Port 9082 wie unter IPv4. Teilnehmer, die selbst nur über IPv6 erreichbar sind (etwa in modernen Mobilfunknetzen), erhalten darüber auch die Medienströme. Näheres unter „IPv6 Unterstützung“.
Die Portfreigabe macht neben den Konferenzräumen auch die Anmeldung am XMPP-Server der TrutzBox aus dem Internet erreichbar (Pfade /xmpp-websocket und /http-bind). Die Videokonferenz braucht diese Anmeldung, denn wer einen Raum eröffnet, meldet sich dort mit TrutzMail-Adresse und

TrutzMail-Passwort an. Über die Freigabe lässt sich das TrutzMail-Passwort damit von außen ausprobieren. Der Angriffsschutz bewacht diese Anmeldung deshalb mit dem Wächter „prosody-auth“: Nach fünf Fehlversuchen innerhalb von 30 Minuten sperrt er die Absenderadresse für sechs Stunden, bei Wiederholung jeweils doppelt so lang bis höchstens eine Woche (Einzelheiten im Kapitel „Angriffsschutz“). Ein starkes Passwort bleibt trotzdem nötig; neue und geänderte Passwörter prüft die TrutzBox deshalb nach einer festen Regel (Abschnitt „Benutzer hinzufügen“). Die Chat-Oberfläche /chat/ gibt die Freigabe dagegen nicht frei, sie ist von unterwegs nur über TrutzVPN erreichbar.

Telefonverbindung von und zum Videokonferenzserver

Da TrutzRTC auf dem Jitsi-Meet-Server basiert, wäre es technisch zwar möglich, sich auch per Telefon in eine Videokonferenz einzuwählen. Es wäre auch möglich, von einer Videokonferenz aus einen Teilnehmer aus dem Telefonnetz anzurufen. Das dafür notwendige Telefonmodul „Jigasi“ (Jitsi Gateway to SIP) ist jedoch derzeit auf der TrutzBox nicht installiert: https://github.com/jitsi/jigasi. SIP ist das Standard-Protokoll der Internet- und Festnetztelefonie, über das sich Telefonteilnehmer in eine solche Konferenz einwählen würden.

Interne TrutzRTC Architektur

Zum tieferen Verständnis hier eine Beschreibung der internen TrutzRTC Architektur.
Das Web-Interface der Videokonferenz wird über einen Apache2-Server bedient. Dessen Konfiguration liegt hier (sollte nicht verändert werden): /usr/share/comidio/trutzrtc/comidio/trutzrtc.apache2.conf

Abweichend vom Original-Jitsi wird von der TrutzBox das jitsi-Konfigurationsdatei dynamisch bei jedem neuen Konferenz-Teilnehmer für den Teilnehmer neu generiert.

Das cgi-Script */usr/share/comidio/trutzrtc/comidio/cgi/rtc-config.cgi*
generiert bei jedem neuen Konferenz-Teilnehmer dynamisch das Konfigurationsdatei trutzbox-config.js (das Konfigurationsdatei geht an jeden Teilnehmer-Browser). Bei der Generierung des Konfigurationsdateis wird unter anderem auch dynamisch der TrutzDynDNS-Name eingesetzt. Welche Konfiguration ein Teilnehmer genau bekommt, kann man mit diesem Link abrufen:
https://**xxxxxx**.mytrutzbox.de/trutz-rtc/config.js
Die Parameter des Konfigurationsdateis sind hier beschrieben: https://community.jitsi.org/t/how-to-how-to-customize-meeting-options/.

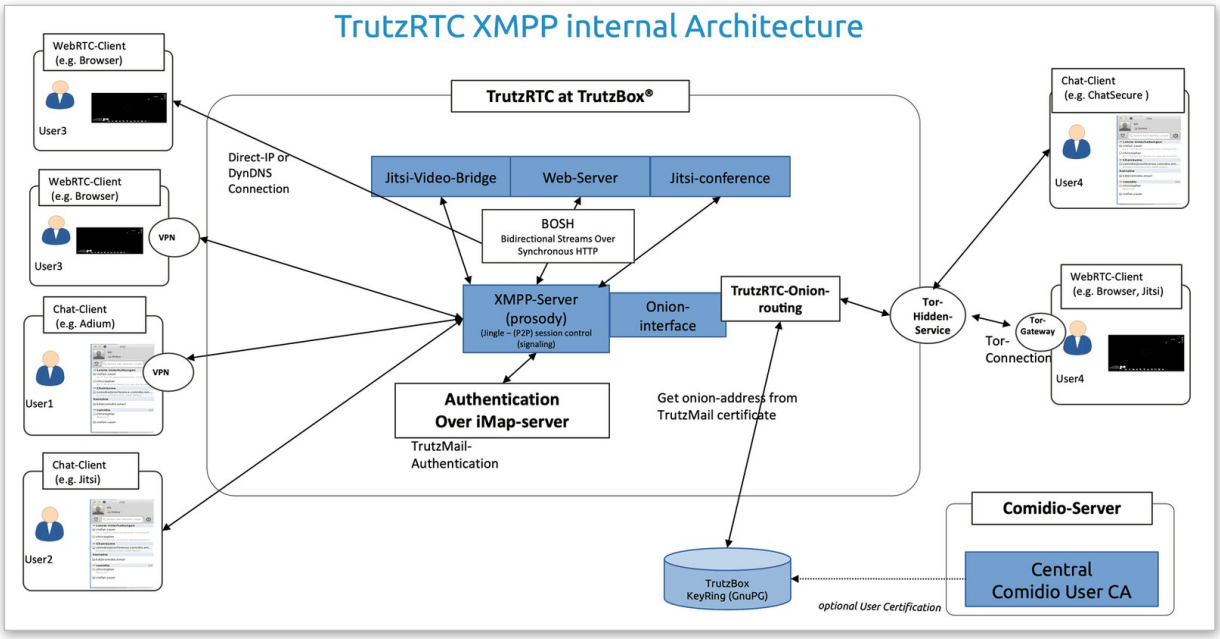
Für den Verbindungsaufbau einer Videokonferenz und für die Chat-Funktion von TrutzRTC wird der XMPP-Server „prosody“[32],[33] genutzt. Prosody ist ein weit verbreiteter Open-Source XMPP-Server, der sich vor allem durch ressourcenschonenden Betrieb und umfangreiche Erweiterbarkeit auszeichnet.
Um beim Chatten über die TrutzMail-Adresse den XMPP-Server (also die TrutzBox) des Kommunikationspartners zu finden, wurde dieser von Comidio um ein spezielles TrutzRTC Onion-

[32] https://prosody.im/

[33] https://de.wikipedia.org/wiki/Prosody

Routing erweitert. Somit ist die TrutzRTC Implementierung in der Lage, sich über Tor-Hidden-Services mit anderen TrutzRTC Servern verschlüsselt und anonym zu verbinden.

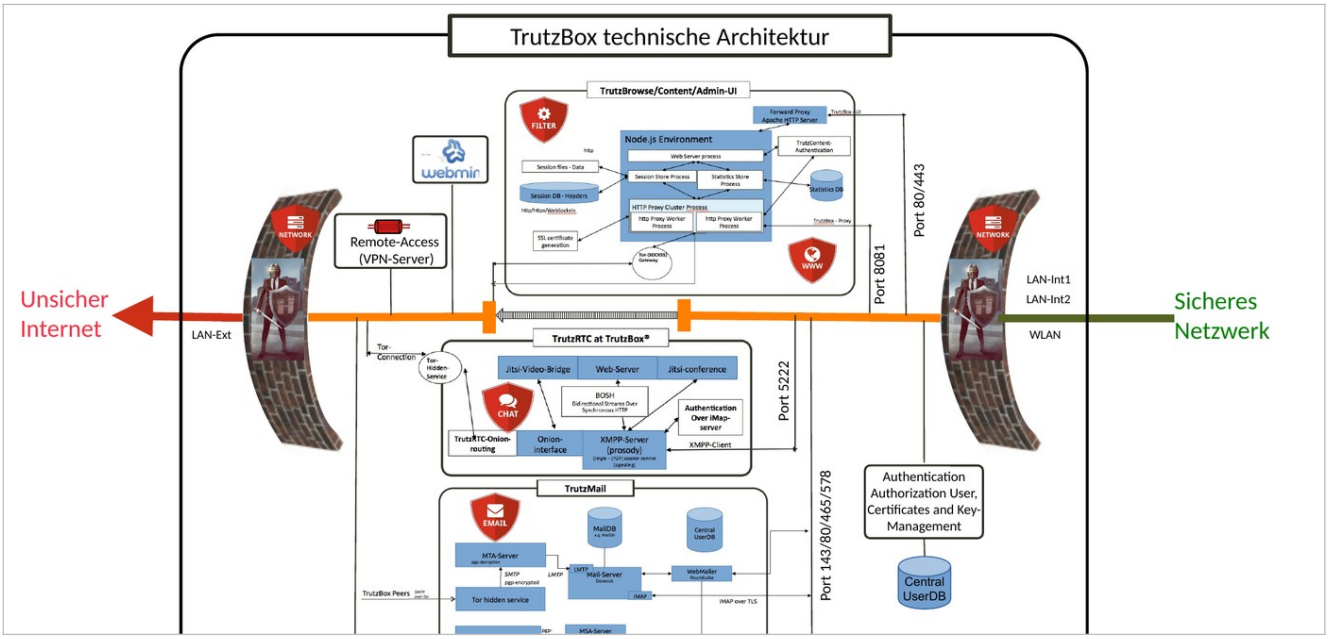
Beim Verbindungsaufbau mit der TrutzBox des Kommunikationspartners wird die entsprechende Signatur der TrutzMail-Adresse überprüft. Dadurch wird verhindert, dass es einem Angreifer gelingen könnte, mit Hilfe einer „gefakten“ TrutzMail-Adresse, die Identität eines anderen zu übernehmen. Damit sich ein TrutzRTC Raum-Administrator mit Hilfe seiner TrutzMail-Adresse authentisieren kann, wird für die XMPP-User-Authentisierung die IMAP-Server-Authentifikation genutzt.



Interne Architektur von TrutzRTC mit XMPP-Server, Konferenz-Server und Anmeldung.
(© 2026 Comidio GmbH)

15 Mehrschichtiger Netzwerk-Schutz (TrutzBase)

Es ist notwendig alles dafür zu tun, dass weder die TrutzBox selbst noch eines der an der TrutzBox angeschlossenen Geräte Opfer eines Hackerangriffs wird. Falls ein Hacker in der Lage wäre die TrutzBox für seine Zwecke zu missbrauchen, könnte das großen Schaden anrichten. Darin unterscheidet sich die TrutzBox wenig von einem Internet-Router. Allerdings befindet sich die TrutzBox im internen Netzwerk, nicht wie der Internet-Router im öffentlichen Netzwerk. Somit ist sie auch zusätzlich durch die Firewall des Internet-Routers geschützt.



Gesamtarchitektur der TrutzBox: Firewall, Proxy, Mail, RTC und VPN mit den jeweils offenen Ports. (© 2026 Comidio GmbH)

Außerdem gilt es, die an die TrutzBox angeschlossenen Netzwerkgeräte auf unterer Netzwerkebene so gut wie technisch möglich zu schützen. Solche angeschlossenen Netzwerkgeräte sind nicht nur PCs, Macs und mobile Geräte wie iPhone, iPad oder Android-Geräte, sondern auch Fernseher sowie schon vorhandene oder zukünftige „Smart Home“-Geräte wie Heizung, Zahnbürste oder Fitness-Armband.

Damit ein einzelner Filter-Mechanismus nicht zur Schwachstelle wird, kombiniert die TrutzBox mehrere Schutzschichten. Auf Anwendungsebene filtert der Proxy URLs und Inhalte, auf Netzwerkebene blockiert ein IP-Blocker mit Firewall und automatischer Angriffs-Sperrung. Beide Schichten greifen ineinander: Was an der einen vorbeigeht, wird von der anderen abgefangen. Folgende Bausteine gehören dazu; sie werden in diesem und im anschließenden Kapitel „Netzwerk“ beschrieben:

- Drei Methoden, Netzwerk-Verkehr zu erkennen und zu blockieren, und warum die TrutzBox mehrere kombiniert
- TrutzBox-Netzwerk (externe und interne Trennung)

- Firewall
- Angriffs-Erkennung und automatische Sperrung
- IP-Blocklisten-Verwaltung, blockierte IP-Adressen und Firewall-Monitor

Wo die einzelnen Schutzfunktionen ansetzen, lässt sich am OSI-Modell zeigen. Das OSI-Modell (Open Systems Interconnection) teilt die Netzwerk-Kommunikation in sieben Schichten ein, von der Übertragung der Bits auf dem Kabel (Schicht 1) bis zur Anwendung, die der Nutzer bedient (Schicht 7). Jede Schicht baut auf der darunter liegenden auf. Die TrutzBox greift auf jeder dieser Schichten ein:

Schicht	Name	Funktionen der TrutzBox
7	Anwendung (Application)	TrutzBrowse (Web-Proxy), TrutzMail, TrutzRTC, Web-Filter und Sperrlisten, Bedienoberfläche
6	Darstellung (Presentation)	Öffnen verschlüsselter Verbindungen mit dem TrutzBox-Stammzertifikat, Sperrseite, Mail-Verschlüsselung (PGP, Autocrypt)
5	Sitzung (Session)	TrutzVPN (OpenVPN, Port 1194), Anmelde- und Sitzungsschutz, Erreichbarkeit über TrutzDynDNS
4	Transport (Transport)	transparenter Proxy (Ports 8081 und 8085), Portfilter, QUIC-Sperre, Erkennung von DoT und DoH
3	Vermittlung (Network)	Firewall (nftables), Router und Gateway, DNS-Filter, Länderzuordnung (GeoIP), Angriffsschutz (fail2ban)
2	Sicherung (Data Link)	interne Netzwerk-Brücke, Geräteerkennung über die MAC-Adresse, WLAN-Zugangspunkt, DHCP
1	Bitübertragung (Physical)	TrutzBox-Hardware, LAN-Anschlüsse, WLAN-Antenne

Die drei Blockier-Methoden aus dem Abschnitt „Drei Methoden, Netzwerk-Verkehr zu erkennen und zu blockieren“ finden sich in dieser Tabelle wieder: die DNS-Blockierung auf Schicht 3, die IP-Blockierung durch die Firewall auf den Schichten 3 und 4, die URL-Filterung des Proxys auf den Schichten 6 und 7. Genau diese Verteilung über mehrere Schichten macht die kombinierte Verteidigung aus.

15.1 Drei Methoden, Netzwerk-Verkehr zu erkennen und zu blockieren

Eine TrutzBox steht zwischen den Geräten im eigenen Netz und dem Internet und entscheidet in Sekundenbruchteilen, ob ein Verbindungsversuch zugelassen oder geblockt wird. Technisch gibt es genau drei Stellen, an denen man so eine Entscheidung treffen kann: am Nameserver, im Netzwerk und im Anwendungsprotokoll. Jede dieser drei Methoden hat charakteristische Stärken, und genauso charakteristische Lücken.

DNS-Blockierung (am Nameserver)

Bei der DNS-Blockierung wird der Aufruf einer Domain bereits verhindert, bevor überhaupt eine Verbindung aufgebaut wird, der Nameserver liefert für unerwünschte Domains schlicht keine IP-Adresse. Bekannte Werkzeuge sind Pi-hole, Firewall-Filter oder das DNS eines Unternehmens. Die Methode ist einfach, schlank und kann flächendeckend ganze Werbe- oder Tracker-Domänen ausschalten.
Sie hat aber drei Schwachstellen: Anwendungen können einen alternativen DNS-Server wie Google oder Cloudflare ansprechen, sie können DNS-Anfragen direkt über HTTPS oder TLS verschlüsseln (DoH bzw. DoT) und damit am lokalen DNS vorbeilaufen, oder sie verwenden gleich eine fest einprogrammierte IP-Adresse und brauchen gar kein DNS. Vor allem aber sieht eine DNS-Sperre nur den Namen. Einzelne Hostnamen lassen sich getrennt behandeln, je nach Werkzeug auch einzelne Geräte oder Gruppen; Pfade, Inhalte und Kopfzeilen innerhalb derselben Verbindung bleiben ihr dagegen verborgen. tracker.example.com und news.example.com sind unterscheidbar, example.com/werbung und example.com/artikel nicht. Bei IPv6 kommen weitere Adressen und Auflösungswege hinzu, die eine DNS-Sperre zusätzlich erschweren.

IP-Blockierung (im Netzwerk)

Die IP-Blockierung greift eine Schicht tiefer: nicht der Domain-Name wird geprüft, sondern die Ziel-IP-Adresse. Das wirkt unabhängig vom Protokoll, egal ob HTTP, HTTPS, QUIC, ein Mail- oder Spiele-Server: Was die Firewall an einer gesperrten IP nicht durchlässt, kommt nicht hindurch. Auch Anwendungen, die DNS umgehen und sich direkt an eine IP-Adresse hängen (typisch für Malware), werden hier abgefangen.
Die Schwierigkeit liegt darin, die Blocklisten aktuell zu halten. Große Anbieter und Cloud-Dienste wechseln ihre IP-Adressen ständig durch (Content Delivery Networks teilen sich oft IP-Blöcke); zudem riskiert man Overblocking, wenn auf einer IP harmlose und unerwünschte Dienste gleichzeitig laufen. Eine reine IP-Blockade ist deshalb pflegeintensiv.

Proxy- bzw. URL-Filterung (im Anwendungsprotokoll)

Bei der Proxy- bzw. URL-Filterung schaut die TrutzBox in den HTTP-/HTTPS-Verkehr hinein und entscheidet pro URL: Diese Seite ja, jene nein. Das ist die feinste Granularität von allen drei Methoden. Man kann gezielt einzelne Tracker-Skripte oder Werbeflächen sperren, ohne den Rest einer Webseite mitzublockieren. Genau das macht die TrutzBox heute mit TrutzContent und TrutzBrowse.
Allerdings kennt der Proxy nur den Verkehr, den er auch sieht. Und genau hier hat sich das Internet in den letzten Jahren entscheidend verändert:

- **QUIC und HTTP/3:** läuft über UDP statt TCP, ist von Anfang an verschlüsselt und lässt sich von einem klassischen HTTP-Proxy nicht aufbrechen; aus Sicht des Proxys ist QUIC ein undurchsichtiger UDP-Strom auf Port 443 (Einzelheiten und Sperr-Schalter im Kapitel „IP-Blocklisten-Verwaltung“).

- **Andere UDP-Anwendungen**: Online-Spiele, Voice- und Video-Telefonie (WebRTC), Smart-TV-Streaming-Apps, viele IoT-Geräte und Telemetrie-Funktionen verschiedener Betriebssysteme nutzen UDP-Protokolle, die kein HTTP sprechen und daher am Proxy vorbeilaufen.
- **Verschlüsselte Tunnel**: ein VPN-Client oder Tor-Client baut eine einzige verschlüsselte Verbindung zu einem externen Server auf, alles weitere passiert in diesem Tunnel. Für den Proxy bleibt das eine einzige nichtssagende Verbindung.
- **Direkte IP-Verbindungen**: sobald eine Anwendung eine IP-Adresse hartcodiert ansteuert, sieht der HTTP-Proxy die Verbindung erst gar nicht.

Anders ausgedrückt: ein Proxy allein ist heute kein vollständiger Schutz mehr. Er deckt zwar das, was er sieht, ausgezeichnet ab, aber er sieht eben längst nicht mehr alles, was über das eigene Netz läuft.

Warum die TrutzBox kombiniert

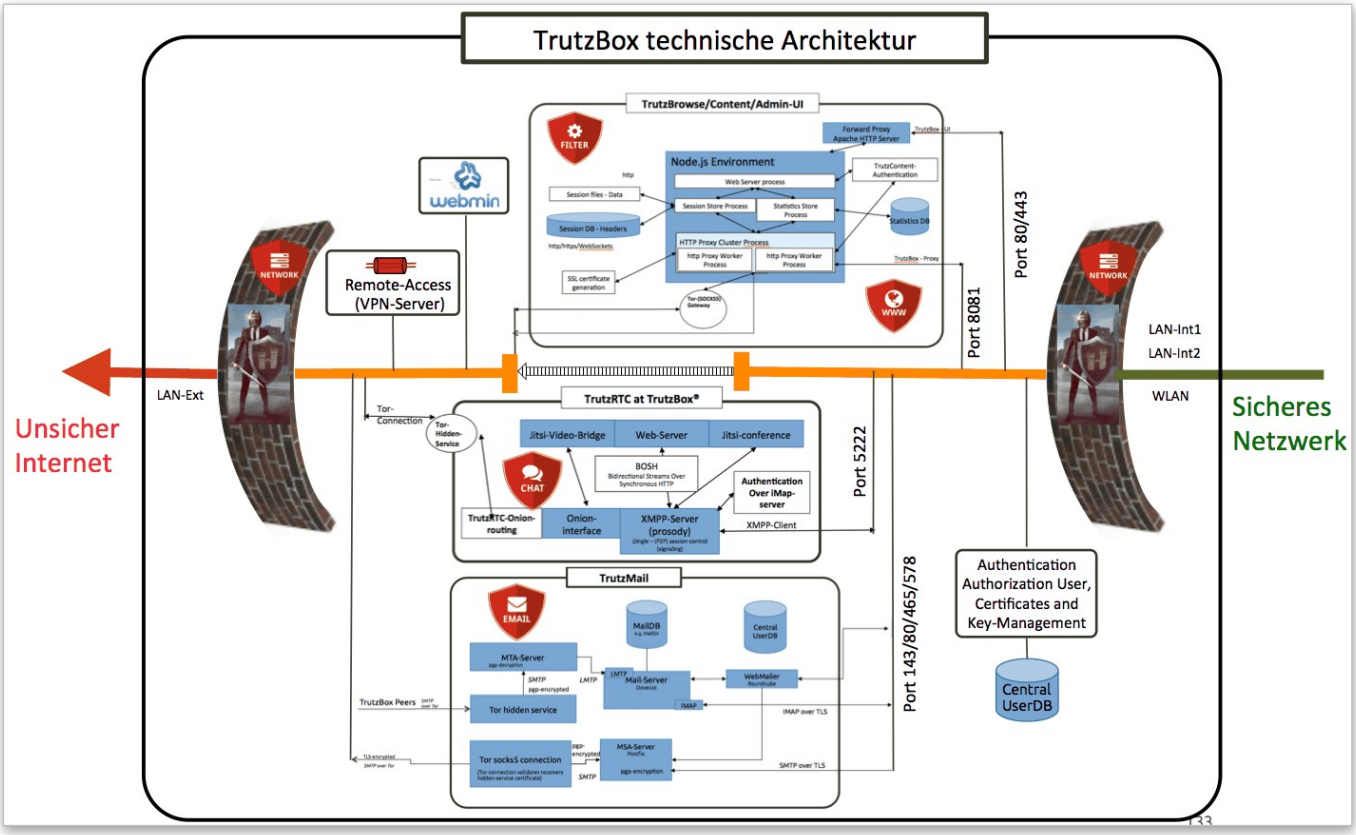
Aus diesen Gründen setzt die TrutzBox die zwei wirksamsten Schichten gemeinsam ein: Proxy/URL-Filterung für alles, was über HTTP/HTTPS läuft, und IP-Blockierung im Netzwerk für alles Übrige: QUIC, UDP-Anwendungen, direkte IP-Verbindungen, Tunnel-Endpunkte. Was die eine Schicht nicht erfassen kann, fängt die andere ab. Die folgenden Abschnitte beschreiben die einzelnen Bausteine dieser kombinierten Verteidigung.
Die folgende Übersicht stellt die drei Methoden noch einmal kompakt gegenüber:

Methode	Vorteile	Nachteile
DNS-Blockierung	Einfach, geringer Overhead, flächendeckende Sperre ganzer Domains.	Umgehung über alternative DNS-Server, DoH/DoT oder direkte IP-Nutzung; keine Subdomain-Granularität; Probleme mit IPv6.
IP-Blockierung	Wirkt unabhängig von DNS und Anwendungsprotokoll; greift auch bei direkter IP-Nutzung und QUIC.	IP-Adressen wechseln häufig (CDN/Cloud); Risiko von Overblocking auf gemeinsam genutzten Servern; Listen müssen gepflegt werden.
Proxy / URL-Filter	**Höchste Granularität:** einzelne URLs sperren, ganze Seite erlauben; gute Transparenz für den Administrator.	Sieht nur HTTP/HTTPS auf Port 80/443; QUIC, andere UDP-Anwendungen und VPN-Tunnel laufen am Proxy vorbei.

(© 2026 Comidio GmbH)

16 Netzwerk

Die TrutzBox funktioniert auf Netzwerk-Ebene wie ein Router. Sie trennt das Netzwerk zwischen dem externen (unsicheren) und dem internen (sicheren) Netzwerk auf. Für Geräte, die über die TrutzBox kommunizieren, werden für alle Ports, für die eine Anwendung auf der TrutzBox bereitsteht (Mail, www-Proxy, Chat, Videokonferenz...), die Zugriffe über den jeweiligen TCP-Port auf die TrutzBox-Anwendung umgeleitet. Somit ist die TrutzBox in der Lage, für diese Anwendungen den Datentransfer in beiden Richtungen zu kontrollieren und unerwünschte Daten zu blockieren oder zu pseudonymisieren.



Die technische Architektur der TrutzBox zwischen unsicherem Internet und sicherem Netzwerk. (© 2026 Comidio GmbH)

16.1 Das TrutzBox externe (unsichere) Netzwerk

Die TrutzBox wird mit dem LAN-Ext-Anschluss per LAN-Kabel am Internet-Router angeschlossen. Beim Hochfahren (Booten) der TrutzBox bezieht sie eine (aus TrutzBox-Sicht) externe IP-Adresse vom DHCP-Server des Routers. Diese kann eine IPv4- oder IPv6-Adresse sein. Dabei teilt sie dem DHCP-Server ihren Host-Namen „trutzbox“ mit.
Beim Setup der TrutzBox kann der TrutzBox am externen Interface auch eine feste IP-Adresse zugewiesen werden; empfohlen wird das jedoch nicht. Im Normalfall sollte die TrutzBox ihre externe Adresse automatisch per DHCP vom Internet-Router beziehen. Diese Einstellung (DHCP oder feste IP-

Adresse, mit Adresse, Netzmaske, Gateway und DNS) kann auch nachträglich unter „Netzwerk → Status“ geändert werden.
Die Zuordnung der Anschlüsse (LAN-Ext zum Router, LAN-Int1 und LAN-Int2 zum internen Netz) ist nicht an feste Gerätenamen gebunden. Bei jedem Start und bei jedem Einstecken eines Netzwerkkabels prüft die TrutzBox die Rollen ihrer Anschlüsse und stellt den Sollzustand wieder her: Jeder Anschluss außer dem Uplink zum Router gehört in die interne Brücke. Den Uplink erkennt sie an einer festen Vorgabe, an der aktiven Standard-Route ins Internet oder an der gemerkten Hardware-Adresse (MAC) des Routers, die sie sich bei jedem fehlerfreien Start einprägt.
Zwei Fehlerbilder behebt die Box damit selbst. Steckt das Kabel zum Router versehentlich in einem der internen Anschlüsse, löst sie den tatsächlichen Uplink aus der Brücke und gibt den frei gewordenen Anschluss an das interne Netz zurück, sofern sie den Router bereits kennt. Wird nachträglich eine WLAN-Karte eingebaut, verschieben sich die internen Namen aller Anschlüsse um eine Position; ohne Korrektur läge der Router-Anschluss in der Brücke (kein Internet), und ein interner Anschluss bliebe ohne Adresse. Die Box erkennt den Router an seiner gemerkten Hardware-Adresse, löst ihn beim nächsten Start aus der Brücke und bindet den verwaisten Anschluss wieder ein. Voraussetzung ist ein fehlerfreier Start vor dem Einbau der Karte, bei dem die Adresse des Routers gemerkt wurde.

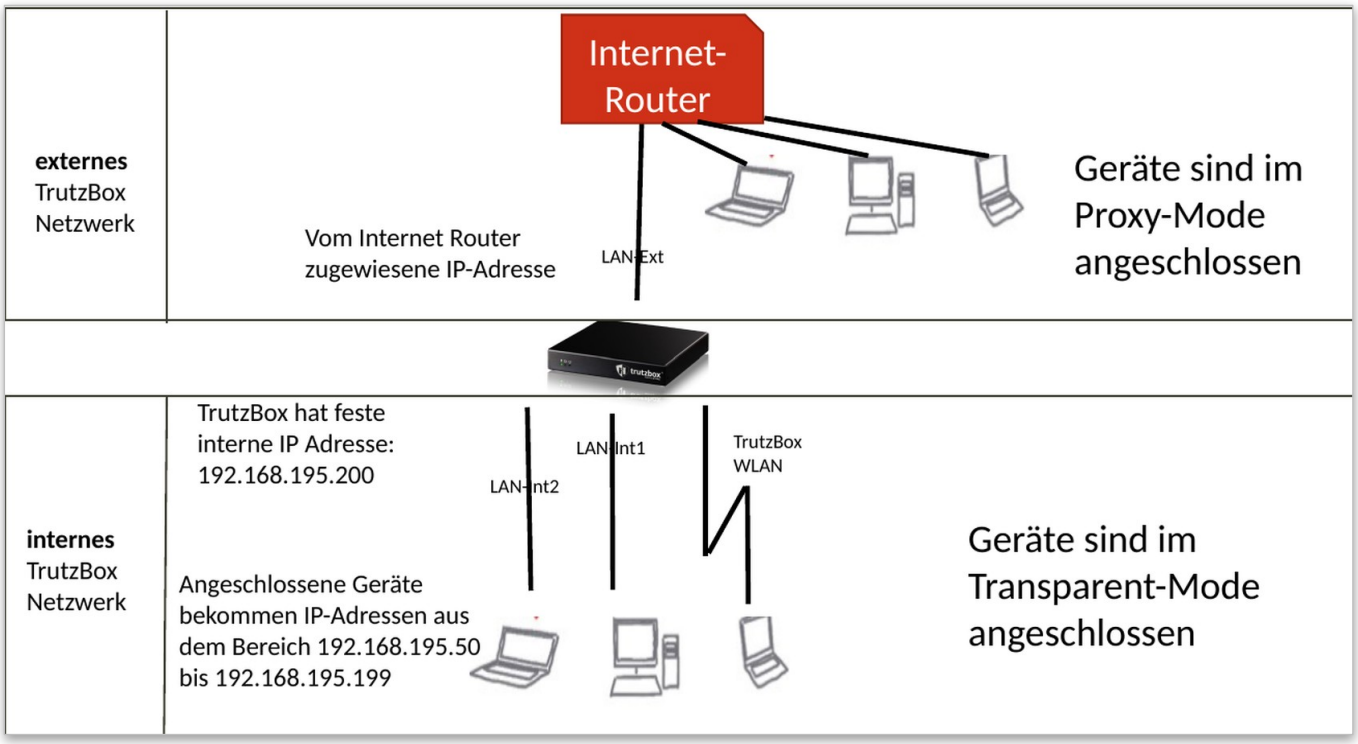
16.2 Das TrutzBox interne (sichere) Netzwerk

Um die an der TrutzBox angeschlossenen Geräte zusätzlich abzusichern, baut die TrutzBox ein eigenes, vom Internet-Router getrenntes internes (sicheres) Netzwerk auf. Die TrutzBox stellt drei Netzwerk-Interfaces zur Verfügung, über die Geräte an das interne Netzwerk angeschlossen werden können: WLAN (optional), LAN-Int1 und LAN-Int2. Diese drei Netzwerk-Anschlüsse sind in einer Netzwerk-Bridge zusammengeschaltet. Sie bilden somit zusammen ein einzelnes Netzwerk. Alle daran angeschlossenen Geräte können ungehindert untereinander kommunizieren.
Falls eine VPN-Verbindung zur TrutzBox aufgebaut wird, dann endet dieses Netzwerk ebenfalls in der Bridge, also im internen Netzwerk.

Falls mehr LAN-Anschlüsse benötigt werden, können diese Netzwerk-Anschlüsse auch durch Router, Hubs, Switches oder WLAN-Router erweitert werden. Durch einen DHCP-Server bekommen die angeschlossenen Geräte (die Geräte, die im Transparent-Modus angeschlossen sind) eine neue IP-Adresse aus dem Bereich 192.168.195.50 bis 192.168.195.199. Ein eigener DNS-Server (dnsmasq) beantwortet dabei die Namensauflösung für die angeschlossenen Geräte; was er nicht lokal beantworten kann, leitet die TrutzBox verschlüsselt per DoT an den unter „Netzwerk → DNS-Auflösung“ gewählten DNS-Anbieter weiter (siehe Kapitel „DNS-Auflösung“). Die TrutzBox vergibt im internen Netzwerk nur IPv4-Adressen, keine IPv6-Adressen.

Die TrutzBox übernimmt das Routing zwischen dem TrutzBox internen Netzwerk (WLAN, LAN-Int1 und LAN-Int2) und dem TrutzBox externen Netzwerk (LAN-Anschluss „LAN-Ext“).

Die TrutzBox selbst hat im internen Netzwerk immer die IP-Adresse 192.168.195.200.



Externes und internes Netz: im Proxy-Modus am Router, im Transparent-Modus hinter der TrutzBox. (© 2026 Comidio GmbH)

Einem angeschlossenen Gerät kann auch eine fest zugeordnete (statische) IP-Adresse gegeben werden, und zwar außerhalb des Bereichs, den der DHCP-Server selbst vergibt: 192.168.195.2 bis 192.168.195.49 oder 192.168.195.201 bis 192.168.195.254. Eine feste Adresse aus 192.168.195.50 bis 192.168.195.199 würde früher oder später ein zweites Mal vergeben. Die Subnetzmaske ist dann 255.255.255.0, die Router- und DNS-Server-IP-Adresse ist 192.168.195.200.

Geräte, die am Internet-Router hängen (etwa ein Drucker oder ein Netzwerkspeicher), lassen sich aus dem internen Netz auch mit ihrem kurzen Namen ansprechen, also „drucker“ statt „drucker.fritz.box“. Ein Name ohne Punkt gehört zu keiner bekannten Domäne. Die TrutzBox leitet solche Namen deshalb gezielt an den Router weiter, der seine eigenen Geräte kennt. Die Namen „wpad“ und „isatap“ nimmt sie davon aus: Über diese beiden Namen könnte sich sonst ein Gerät am Router als Proxy-Verteiler für das interne Netz ausgeben. Die Adresse des Routers hält die Box bei jedem Wechsel ihrer externen Adresse aktuell. Die Einstellung wird beim nächsten Start der internen Netzwerk-Brücke wirksam, in der Regel also nach einem Neustart der TrutzBox. Ein Neustart der Brücke im laufenden Betrieb würde alle LAN- und WLAN-Geräte kurz trennen und unterbleibt deshalb.
Eine Besonderheit gilt für Windows. Windows fragt einen Namen ohne Punkt nie unverändert ab, sondern hängt die per DHCP erhaltene Suchdomäne des internen Netzes an („drucker.sec“). Diese Anfrage kann die TrutzBox nicht beantworten, weil „.sec“ nur für Geräte hinter der Box steht. Unter

Windows ist deshalb der lange Name mit der Domäne des Routers zu verwenden, zum Beispiel „\\ds920.fritz.box\freigabe“. macOS, Linux und die meisten anderen Systeme kommen mit dem kurzen Namen zurecht.

Die TrutzBox im Netz finden: trutzbox.local (mDNS)

Seit September 2026 ist die TrutzBox außer unter ihrem Netzwerknamen auch unter diesem Namen mit der Endung .local erreichbar, ab Werk also unter trutzbox.local. Dahinter steht Multicast-DNS (mDNS) mit der Dienstsuche DNS-SD nach RFC 6762 und RFC 6763; Apple nennt das Verfahren „Bonjour“. Ein Gerät fragt dabei keinen Namensserver, sondern stellt die Frage per Multicast in das lokale Netz, und das Gerät, dem der Name gehört, antwortet selbst. Die TrutzBox antwortet mit ihrer Adresse auf der jeweiligen Seite: im internen Netz mit 192.168.195.200, im Netz des Internet-Routers mit ihrer Adresse an LAN-Ext.

http://trutzbox bleibt der Standardweg: Im internen Netz beantwortet die TrutzBox ihren Namen selbst, im Netz des Routers tut das der Router, weil die TrutzBox ihm den Namen bei der Adressvergabe (DHCP) meldet. Die Adresse mit .local ist der Rückfall, wenn das nicht klappt, etwa weil der Router seine Geräte nicht mit Namen kennt. iPhone, iPad und Mac, Windows 10 und 11 sowie Linux mit avahi lösen .local-Namen auf; Browser unter Android tun das nicht auf jedem Gerät.

Wo die TrutzBox sich ankündigt: Angekündigt wird auf der internen Brücke und an LAN-Ext, nie auf den Tunneln des Fernzugriffs. mDNS überquert weder einen Router noch einen Tunnel. Wer über den Fernzugriff verbunden ist, erreicht die TrutzBox deshalb über ihre feste Adresse im Tunnel, 10.9.0.1 bei WireGuard und 10.8.0.1 bei OpenVPN. Antworten bekommen nur Absender aus dem Netz der jeweiligen Seite.

Dienst für Suchprogramme: Neben dem Namen kündigt die TrutzBox einen Dienst vom Typ _https._tcp an. Er heißt „TrutzBox“ und zeigt auf Port 443; über ihn führen Suchprogramme, etwa die Netzwerkansicht mancher Linux-Dateimanager, die TrutzBox auf. Im internen Netz steht er immer bereit, im Netz des Routers nur während der Einrichtung.

Zwei TrutzBoxen mit demselben Namen: Stehen zwei TrutzBoxen mit gleichem Netzwerknamen im selben Netz, etwa beide ab Werk als trutzbox, weicht die mit der kleineren Adresse auf <Name>-2.local aus, im Beispiel trutzbox-2.local. Eindeutige Netzwerknamen (Kapitel „Allgemeine Einstellungen“) vermeiden das.

> **Technischer Hintergrund:** Die Ankündigung übernimmt ein eigener Dienst der Verwaltungssoftware (MdnsService); ein Zusatzprogramm wie avahi braucht die TrutzBox dafür nicht. Die Firewall der TrutzBox erlaubt mDNS (UDP-Port 5353 an die Multicast-Adresse 224.0.0.251) aus dem internen Netz und aus dem Netz des Routers.

16.3 Status (Netzwerk)

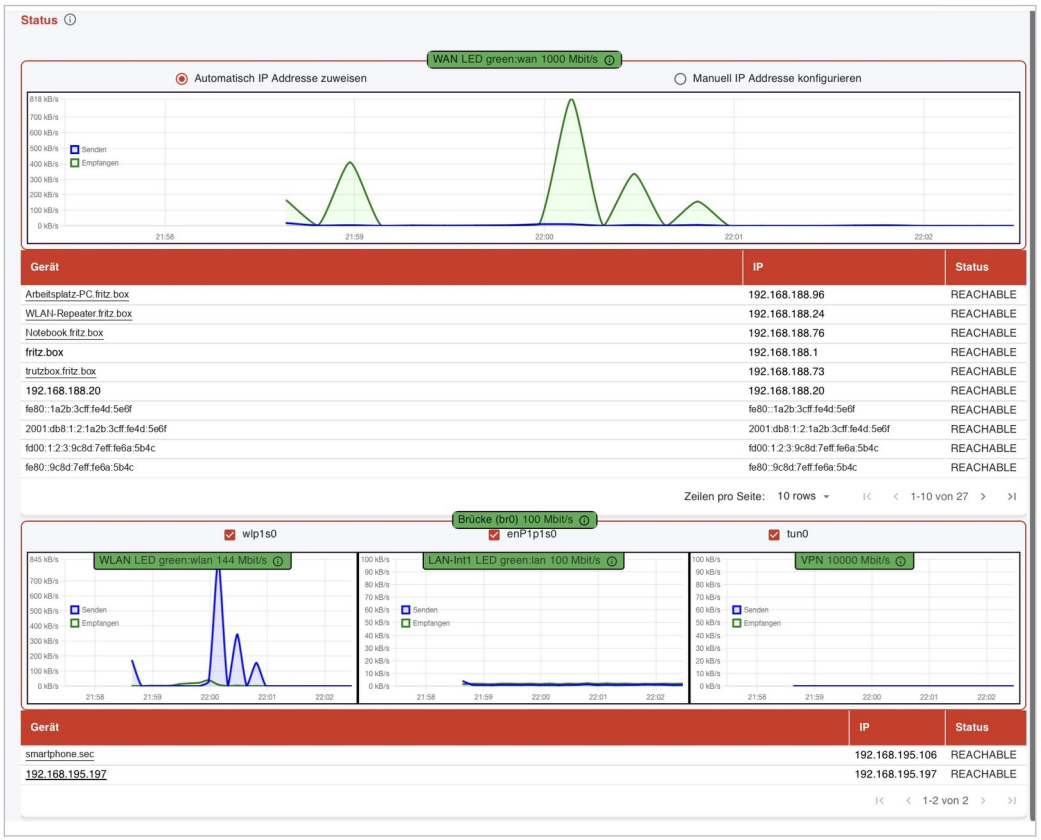
Die Seite „Status“ (Menü „Netzwerk → Status“) zeigt den Zustand der Netzwerk-Schnittstellen der TrutzBox und erlaubt die Einstellung der externen IP-Adresse. Sie ist in drei Bereiche gegliedert: das externe Interface „LAN-Ext“, die interne Netzwerk-Brücke „br0“ und den VPN-Tunnel „tun0“. Darüber steht, sobald Fernzugriff oder Videokonferenz laufen, die Erreichbarkeit von außen (siehe unten).

Der zusätzliche Bereich „Tunnel (tun0)“ ist für die Fehlersuche gedacht und zeigt den Verkehr der VPN-Einwahl. Wird die externe Adresse zwischen automatischem Bezug und fester Einstellung umgeschaltet, begleitet ein Fenster „IP-Konfiguration ändern“ den Vorgang: Es meldet, wann die neue Einstellung angewendet wird, prüft anschließend die Erreichbarkeit und bietet, falls die Oberfläche danach unter einer anderen Adresse liegt, den Verweis dorthin an.

- LAN-Ext (z. B. enp2s0): das zum Internet-Router gerichtete externe Interface. Über die Auswahl „Automatisch IP Adresse zuweisen“ (DHCP, Voreinstellung) bzw. „Manuell IP Adresse konfigurieren“ wird festgelegt, wie die TrutzBox ihre externe Adresse bezieht. Bei manueller Konfiguration werden Adresse, Netzmaske, Gateway und DNS eingetragen; empfohlen bleibt die DHCP-Voreinstellung (siehe Abschnitt „Das TrutzBox externe (unsichere) Netzwerk“). Darunter zeigt ein Live-Diagramm die gesendete und empfangene Datenrate, eine Tabelle listet die am Router erreichbaren Geräte mit Gerätename, IP und Status (REACHABLE, STALE oder FAILED), seitenweise blätterbar.
- **Brücke (br0):** das interne (sichere) Netzwerk. Es fasst die internen Schnittstellen zusammen: WLAN (z. B. wlp1s0), VPN (tun0) und die internen LAN-Anschlüsse (z. B. enp3s0 und enp4s0). Sie lassen sich einzeln über Kontrollkästchen ein- und ausblenden und besitzen je ein eigenes Live-Diagramm. Eine weitere Tabelle listet die am internen Netzwerk angeschlossenen Geräte.

Zu jeder Schnittstelle lassen sich über einen Detail-Dialog die technischen Netzwerkdaten (ifconfig) einsehen.

Menüpfad: Netzwerk → Status



Die Seite „Status“ mit der Adressvergabe für LAN-Ext und den erkannten Geräten je Anschluss. (© 2026 Comidio GmbH)

Erreichbarkeit von außen

Läuft der Fernzugriff oder die Videokonferenz, steht ganz oben auf der Seite „Status“ der Abschnitt „Erreichbarkeit von außen“. Er nennt für jeden der beiden Dienste, ob die TrutzBox aus dem Internet erreichbar ist: „erreichbar“, „erreichbar, nur über IPv4“, „nur über IPv6 erreichbar“, „nicht erreichbar“ oder „nicht prüfbar“. Fehlt eine Freigabe, steht darunter, was am Internet-Router einzutragen ist, zum Beispiel „UDP 9083 an 192.168.178.20“. Läuft keiner der beiden Dienste, erscheint der Abschnitt nicht.
„Erreichbar, nur über IPv4“ ist ein Hinweis und kein Fehler: Der Dienst kommt an, der Name der TrutzBox trägt aber auch die IPv6-Adresse, und über die kommt bei diesem Dienst nichts an. Darunter steht, für welchen Anschluss am Internet-Router die IPv6-Freigabe fehlt. Die meisten Browser weichen dann von selbst auf IPv4 aus, manche Apps nicht. Die Anzeige erscheint nur, wenn ein anderer Dienst über IPv6 ankommt und die TrutzBox die IPv6-Adresse deshalb im Namen lässt.
Das Wort „Details“ daneben klappt auf, was die TrutzBox gemessen hat. Eine Tabelle nennt je Dienst den Anschluss am Internet-Router und den an der TrutzBox und daneben, ob die Testpakete über IPv4 und über IPv6 angekommen sind; die Zahl in Klammern ist die gezählte Anzahl (der Server schickt je UDP-Anschluss drei Testpakete und versucht je TCP-Anschluss zwei Verbindungen). Im Kopf der beiden Spalten stehen die Adressen, an die die Testpakete gingen. Darunter fasst der Block „Anschluss“

zusammen, was die TrutzBox über ihren Anschluss weiß: den TrutzDynDNS-Namen und die Adressen, die er gerade trägt, die öffentliche IPv4-Adresse, die IPv6-Adresse der TrutzBox samt der Interface-ID für IPv6-Freigaben am Router, die Adresse der TrutzBox im Netz des Internet-Routers, die Adressen des Servers, von denen die Testpakete kamen, und den Anlass der Messung. Die letzte Zeile ordnet das Ergebnis ein: Kommt über IPv4 nichts an, spricht das für einen Anschluss ohne eigene IPv4-Adresse (DS-Lite) oder für fehlende Freigaben am Internet-Router. Dieselben Angaben stehen im „Bericht an Support“ (Kapitel „TrutzBox-Betriebszustand“).
Wie die Prüfung technisch abläuft und wie die TrutzBox aus dem Ergebnis die veröffentlichten Adressen ableitet, beschreibt das Kapitel „TrutzDynDNS: Erreichbarkeit aus dem Internet“ in den Abschnitten „Prüfung der Erreichbarkeit von außen“ und „Nur IPv6 oder nur IPv4 veröffentlichen“.

16.4 Firewall

Wie im Kapitel „Mehrschichtiger Netzwerk-Schutz (TrutzBase)“ beschrieben, schützt die TrutzBox auf zwei Ebenen: Domain-/URL-Sperren im HTTP/S-Proxy (TrutzContent) und IP-Sperren in der nftables-Firewall. Die folgende Übersicht zeigt die praktischen Unterschiede der beiden Mechanismen:

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Eigenschaft	Domain-Sperre (TrutzContent über den HTTP/S-Proxy)	IP-Sperre (Firewall, nftables)
Was wird gesperrt	Hostnamen und URLs, beispielsweise tracker.example.com.	IP-Adressen und ganze Adressbereiche in CIDR-Notation, beispielsweise 192.0.2.0/24. Die Zahl hinter dem „/“ gibt an, wie viele führende Bits das Netz bestimmen und damit, wie groß der Adressbereich ist (bei „/24“ etwa 256 Adressen).
Wo eingestellt	Im Menü „Verwaltung → Filterlisten“ und „Filtergruppen“.	Im Menü „Netzwerk → Angriffsschutz“, Reiter „Sperrlisten“.
Granularität	Pro Gerät bzw. Filtergruppe einstellbar; jedes Gerät kann seine eigenen Regeln haben.	Wirkt global für die gesamte TrutzBox und damit für alle Geräte gleichermaßen.
Was das Gerät sieht	Eine TrutzBox-Sperrseite mit dem HTTP-Status 450. Der Browser zeigt klar, dass die Verbindung blockiert wurde, und nennt den Grund.	Der Verbindungsaufbau wird mit TCP-Reset oder ICMP-Antwort abgewiesen. Das Gerät meldet einen Verbindungsfehler ohne weitere Erklärung.
Risiko falscher Sperren	Niedrig, weil die Sperre genau die unerwünschte Domain trifft.	Höher, weil viele Webseiten heute IP-Adressen großer Cloud-Anbieter teilen (Shared Hosting, CDN); dabei können auch erwünschte Seiten mitgesperrt werden.
Bedienbarkeit für Laien	Gut zugänglich; die Filterlisten lassen sich auch ohne tiefes Netzwerkwissen verwalten.	Eher für technisch versierte Administratoren; Treffer sind ohne Werkzeuge schwer zu untersuchen.

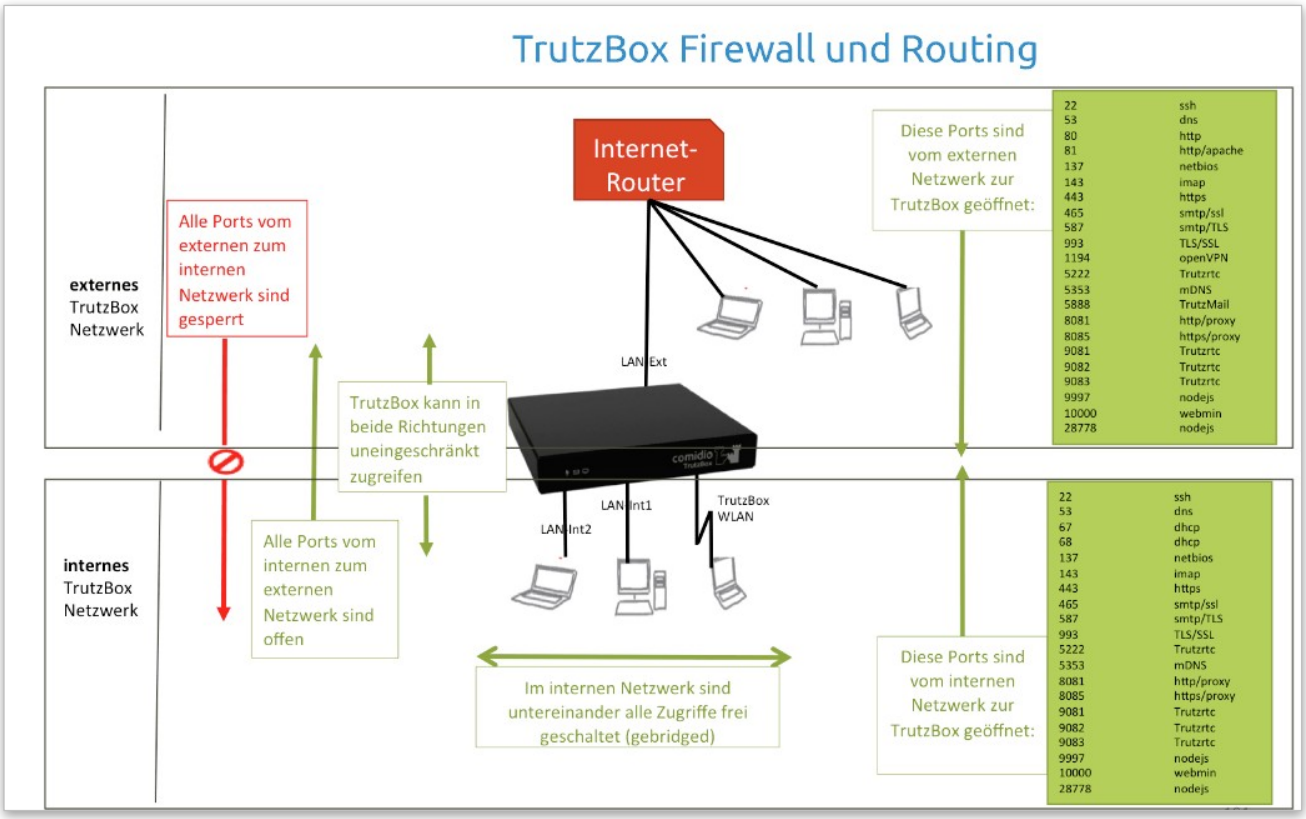
(© 2026 Comidio GmbH)

Die Domain-Sperre ist das passende Werkzeug für die alltägliche Steuerung, etwa um Tracker, Werbung oder für Kinder und Jugendliche ungeeignete Inhalte gezielt pro Gerät zu blockieren. Die IP-Sperre ergänzt sie dort, wo Verkehr am Proxy vorbeiläuft (siehe Kapitel TrutzBase). Die folgenden Abschnitte beschreiben, wie die Firewall die IP-Sperre konkret umsetzt.

Um sowohl die TrutzBox als auch alle Geräte, die am internen Netzwerk angeschlossen sind, zu schützen, hat die TrutzBox eine Stateful Packet Inspection Firewall (SPI). Diese schützt nicht nur die TrutzBox selbst vor unbefugtem Zugriff auf der Netzwerkseite, sondern blockiert auch Angreifer von außen. Zusätzlich schützt die Firewall alle angeschlossenen Netzwerkgeräte über entsprechende Portfreigaben vor unkontrolliertem Netzwerkzugriff.
Somit werden alle Netzwerk-Verbindungen durch die Firewall kontrolliert und geschützt. Verbindungen über Port 80/443 werden zusätzlich durch den Proxy abgesichert.

Die verwendete Firewall ist eine Stateful Packet Inspection Firewall (SPI), d. h. jedes Datenpaket wird einer bestimmten aktiven Verbindung (Session) zugeordnet:

- Alle am internen Netzwerk angeschlossenen Geräte sind untereinander gebridged, sodass diese uneingeschränkt miteinander kommunizieren können.
- Alle angeschlossenen Geräte können auf allen Ports Verbindungen nach „extern“ (LAN-Ext) aufbauen, wenn die IP-Adresse nicht in der IP-Blocklisten-Verwaltung aufgeführt ist.
  Alle Verbindungen über Port 80/443 werden dabei automatisch über den TrutzBox Proxy (Filter) geleitet, der dann die ein- und ausgehenden Daten zusätzlich kontrolliert.
- Ein Verbindungsaufbau von extern zur TrutzBox ist nur für spezielle Ports freigeschaltet, falls ein Programm auf der TrutzBox auf diesen Port die Verbindung abfängt.
- Ein Verbindungsaufbau vom externen Netzwerk nach intern ist nicht freigeschaltet und somit nicht erlaubt.



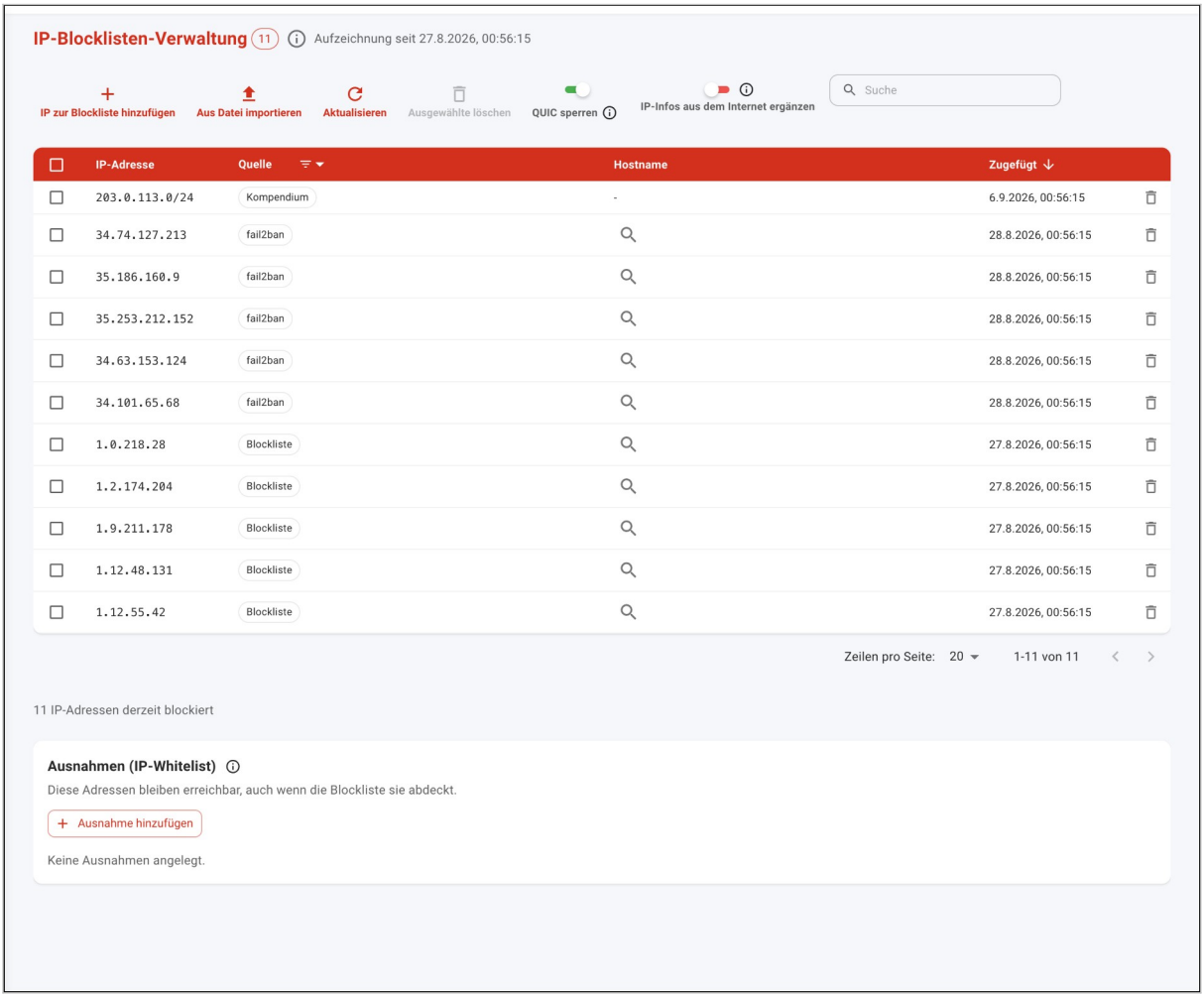
Regeln der Firewall: nach außen erlaubt, von außen nur für freigegebene Ports.
(© 2026 Comidio GmbH)

Als Basis für die Firewall wird die Debian-Standard-Firewall (nftables) verwendet.

16.5 IP-Blocklisten-Verwaltung

Mit der IP-Blocklisten-Verwaltung werden IP-Adressen und Bereiche verwaltet, die auf Netzwerkebene blockiert werden sollen, protokollunabhängig, also für alle Verbindungsarten (nicht nur HTTP/HTTPS). Zu finden ist die Verwaltung als Reiter „Sperrlisten“ auf der Seite „Netzwerk → Angriffsschutz“.
Der TrutzBox-Administrator kann einzelne IP-Adressen oder Bereiche hier selbst eintragen. Oder öffentlich verfügbare IP-Blockinglisten mit bekannten schädlichen Internet-Adressen, wie z. B. Listen von Firehol nachladen: https://iplists.firehol.org/?ipset=firehol_level1

Menüpfad: Netzwerk → Angriffsschutz → Sperrlisten



Die IP-Blocklisten-Verwaltung mit Einträgen, Import und QUIC-Sperre.
(© 2026 Comidio GmbH)

Die Abbildung zeigt nur wenige Einträge; im Betrieb sind es je nach eingespielter Blockliste einige tausend. Jeder Eintrag zeigt die IP-Adresse bzw. den CIDR-Bereich (z. B. 1.10.16.0/20) und optional den zugehörigen Hostnamen.

- **IP zur Blockliste hinzufügen:** Einzelne IP-Adresse oder IP-Bereich in CIDR-Notation manuell eintragen.
- **Aus Datei importieren:** Importiert eine Liste von IP-Adressen/Bereichen aus einer Textdatei.
- **Aktualisieren:** Lädt die angezeigte Liste neu.
- **Ausgewählte löschen:** Über die Auswahlkästchen ganz links lassen sich mehrere Einträge markieren und in einem Schritt gemeinsam aus der Blockliste entfernen.
- **Einzeln löschen:** Jeder Eintrag kann über das Papierkorb-Symbol einzeln entfernt werden.

- **QUIC sperren:** Dieser Schalter (standardmäßig eingeschaltet) blockiert auf Netzwerkebene das QUIC-Protokoll.

QUIC ist ein neueres, von Google entwickeltes Transportprotokoll (Grundlage von HTTP/3), das über UDP läuft und von Anfang an verschlüsselt ist. Es wird u. a. von Chrome, Edge, vielen Android-Apps und Diensten wie YouTube, Gmail oder Facebook genutzt. Für den HTTP/S-Proxy der TrutzBox ist QUIC eine nicht aufbrechbare „Blackbox“ auf UDP-Port 443; TrutzContent und TrutzBrowse können solchen Verkehr also nicht filtern. Wird QUIC gesperrt, fallen Browser und die meisten Apps auf herkömmliches HTTPS (über TCP) zurück, das wieder über den Proxy läuft und damit gefiltert werden kann; einzelne Apps ohne diesen Rückfall können dann keine Verbindung aufbauen. Deshalb ist die Sperre standardmäßig aktiv.
Die Blockierung erfolgt für IPv4- und IPv6-Adressen gleichermaßen; IPv6-Bereiche werden ebenfalls in CIDR-Notation eingetragen. Auch der Angriffsschutz trägt erkannte Angreifer-Adressen automatisch hier ein (Einzelheiten im Kapitel „Angriffsschutz“). Einzelne Adressen zeigt die Liste ohne den technischen Zusatz /32 beziehungsweise /128, der sich fälschlich wie ein Adressbereich las. Eine Firewall-Ausnahme hat Vorrang vor der Blockliste, ohne deren Eintrag zu verändern (siehe folgender Abschnitt).

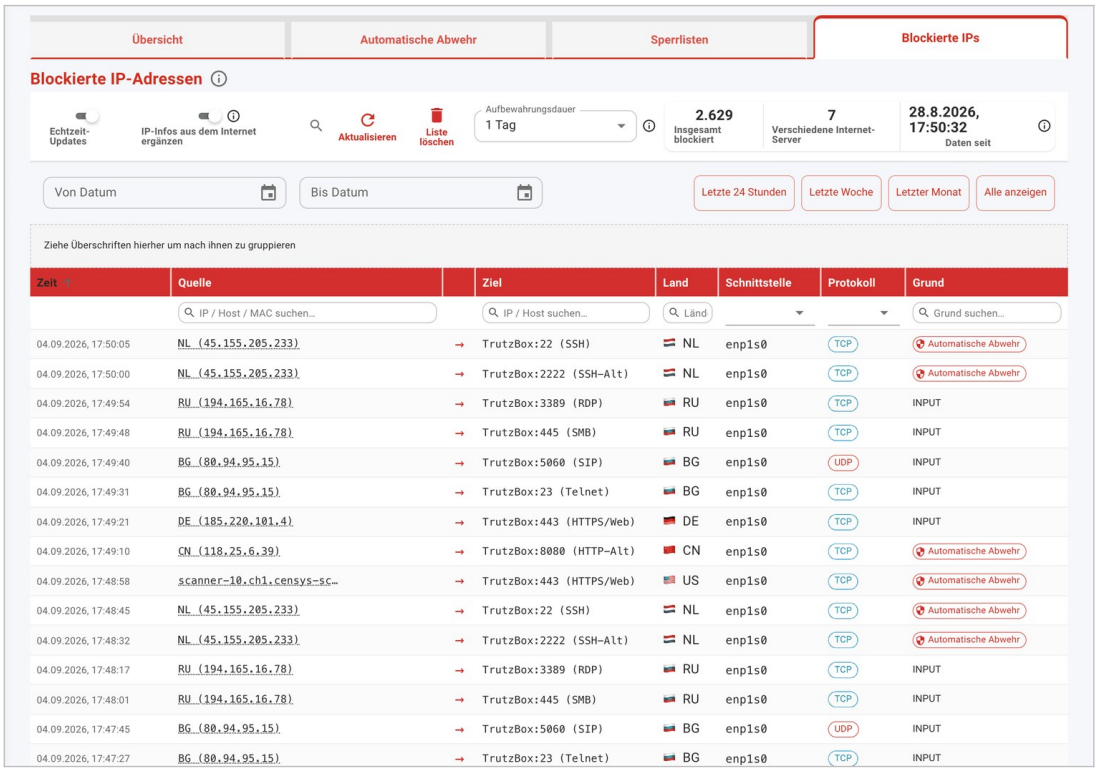
16.6 Firewall-Ausnahmen

Unterhalb der Blockliste führt die Seite den Abschnitt „Ausnahmen (IP-Whitelist)“: Eine Ausnahme ist eine ausdrückliche Freigabe für eine IP-Adresse oder einen Adressbereich, die die IP-Blockliste überstimmt, ohne deren Eintrag zu löschen. Das ist der entscheidende Unterschied zum früheren Verhalten, bei dem ein Freigeben den deckenden Eintrag (bei einem Adressbereich gleich den ganzen Bereich) aus der Blockliste entfernte und die nächtliche Aktualisierung ihn stillschweigend wieder eintrug; als eigenständige Ausnahme bleibt die Freigabe dauerhaft bestehen. Wann eine solche Ausnahme nach einer Domain-Freigabe nötig ist, beschreibt das Kapitel „Eigene Sperren und Ausnahmen“.
Jede Ausnahme führt einen eigenen Trefferzähler, an dem sich ablesen lässt, ob sie überhaupt gebraucht wird. Nicht jede Freigabe wird angenommen: Ausnahmen auf reservierte Adressbereiche, auf zu große Bereiche und auf eine gerade aktive Sperre des Angriffsschutzes lehnt die TrutzBox ab. Der Angriffsschutz hätte sonst keine Wirkung mehr, sobald eine einzige zu weit gefasste Ausnahme besteht.

16.7 Blockierte IP-Adressen

Die Ansicht „Blockierte IP-Adressen“ zeigt alle Verbindungsversuche, die von der Firewall auf Netzwerkebene blockiert wurden. Zu finden ist sie als Reiter „Blockierte IPs“ auf der Seite „Netzwerk → Angriffsschutz“. Die Lupe der Werkzeugleiste durchsucht dabei serverseitig den gesamten Datenbestand (IP, Host, MAC, Ports, Grund); Dienstnamen wie „https“ finden auch die zugehörige Portnummer, und gesucht werden kann direkt nach den angezeigten deutschen Grund-Texten (etwa „Eingehend verworfen“). Ports erscheinen in den Spalten mit Dienstnamen („443 (HTTPS)“).

Menüpfad: Netzwerk → Angriffsschutz → Blockierte IPs



Der Reiter „Blockierte IPs“ mit den von der Firewall abgewiesenen Verbindungsversuchen. (© 2026 Comidio GmbH)

- **Echtzeit-Updates:** Die Liste aktualisiert sich automatisch. Der Aufbewahrungszeitraum ist konfigurierbar (Standard: 31 Tage).
- **Zeitfilter:** Letzte 24 Stunden, Letzte Woche, Letzter Monat oder Alle anzeigen.
- **Spalten:** Zeit, Quelle, Ziel (IP:Port), Schnittstelle, Protokoll (UDP/TCP), Land sowie Grund (z. B. „Lokal verweigert“).
- **Suche und Gruppierung:** Je Spalte (Quelle, Ziel, Land, Grund) kann gesucht werden; Spalten lassen sich zudem per Drag & Drop als Gruppierspalte verwenden.
- **CSV-Export:** Die angezeigten Einträge lassen sich als CSV-Datei exportieren. Oberhalb der Liste fassen zudem Kennzahlen die Gesamtzahl der Blockierungen und die Zahl der eindeutigen Server zusammen.

16.8 Angriffsschutz

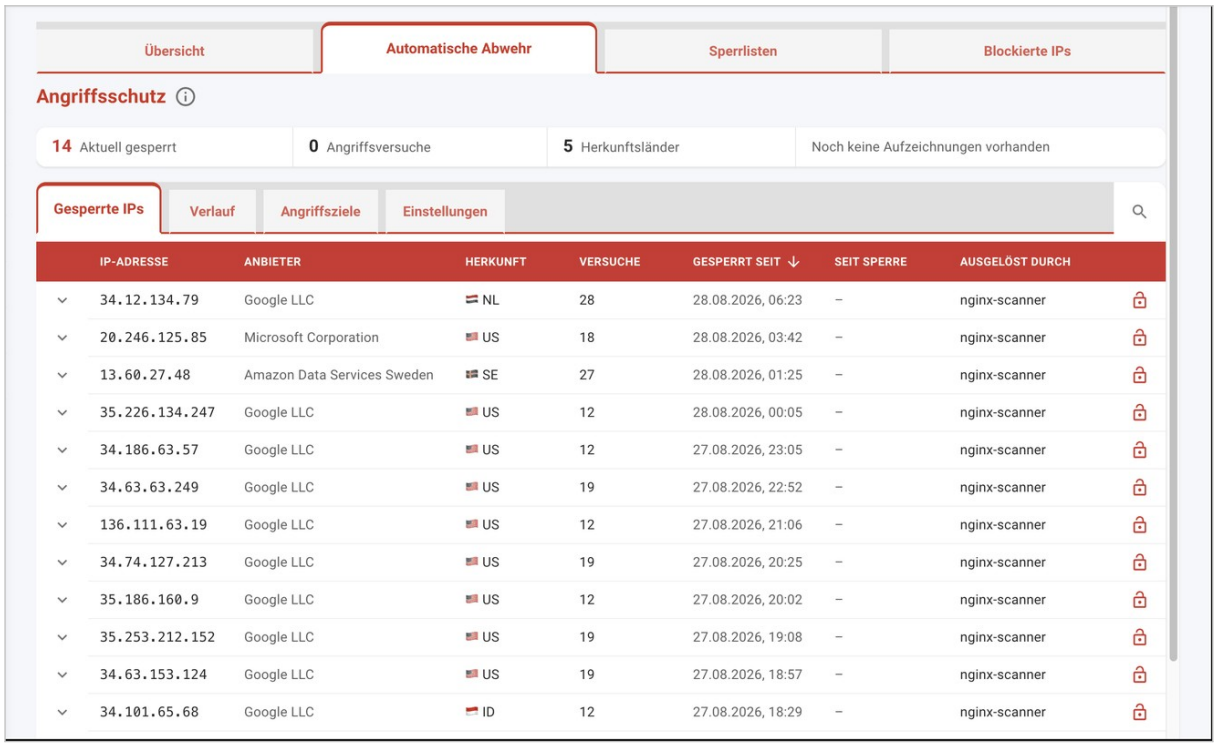
Die Seite „Netzwerk → Angriffsschutz“ zeigt die automatische Abwehr von Angriffen aus dem Internet. Die von außen erreichbaren Dienste der TrutzBox (etwa der Web-Zugang für Fernzugriff und Videokonferenz) werden ständig von automatisierten Scannern angetastet, die im ganzen Internet nach verwundbaren Systemen suchen. Der Angriffsschutz (technisch: „fail2ban“) erkennt IP-Adressen, die

wiederholt solche Zugriffsversuche unternehmen, und trägt sie automatisch und dauerhaft in die IP-Blockliste ein (siehe „IP-Blocklisten-Verwaltung“). Geräte im eigenen Netz werden dabei grundsätzlich nie gesperrt. fail2ban ist ein bewährter quelloffener Schutzdienst: Er liest im Hintergrund fortlaufend die Protokolle der von außen erreichbaren Dienste mit und sperrt eine Adresse, sobald sich von ihr zu viele fehlgeschlagene oder auffällige Zugriffe häufen. Diese Schutzregel kennt auch alle internen IPv6-Adressbereiche, sodass eine Adresse aus dem eigenen Netz auch dann nicht auf der Sperrliste landen kann, wenn das eigene Netz mit IPv6 arbeitet.

Die Seite „Netzwerk → Angriffsschutz“ bündelt vier Reiter: „Übersicht“ (der Firewall-Monitor, siehe folgendes Kapitel), „Automatische Abwehr“ (die hier beschriebene automatische Sperrung angreifender Adressen), „Sperrlisten“ (die IP-Blocklisten-Verwaltung) und „Blockierte IPs“ (die gleichnamige Ansicht; beide in den vorangegangenen Kapiteln beschrieben).

Im Reiter „Automatische Abwehr“ fassen drei Kennzahlen die Lage zusammen: die Zahl der aktuell gesperrten Adressen, die Zahl der Angriffsversuche und die Herkunftsländer. Darunter gliedert sich die Ansicht in vier weitere Reiter:

Menüpfad: Netzwerk → Angriffsschutz → Automatische Abwehr



Der Reiter „Automatische Abwehr“ mit gesperrten Adressen, Angriffsversuchen und Herkunftsländern. (© 2026 Comidio GmbH)

- **Gesperrte IPs:** listet die derzeit gesperrten Adressen mit dem Namen des Anbieters (aus Reverse-DNS und WHOIS) statt nur der nackten IP-Adresse, dazu Herkunftsland (Flagge), Zahl der Versuche, Sperrzeitpunkt und der Dienst, der die Sperre ausgelöst hat:

- **Sortieren und Suchen:** Alle Spalten sind sortierbar. Die Lupe neben der Reiter-Leiste durchsucht die Tabellen als Volltext, auch die aufklappbaren Angriffsziele mit Pfaden, Kategorien und Erklärungen, sodass etwa „.env“ oder „VPN“ die passenden Sperren findet.
- **Angriffsziele:** Der Pfeil am Zeilenanfang klappt die Angriffsziele der Adresse auf: je Zugriff Kategorie, angefragter Pfad und eine Klartext-Erklärung (etwa „Umgebungsdatei mit Passwörtern und API-Schlüsseln“).
- **Entsperren:** Über das Schloss-Symbol rechts lässt sich eine Adresse manuell entsperren.
- **Abgewehrte Zugriffe:** Zu jeder gesperrten Adresse steht außerdem, wie viele Zugriffsversuche seit der Sperre abgewehrt wurden. Diese Zahl kommt unmittelbar aus den Zählern der Firewall, und frisch gesperrte Adressen werden von der ersten Sekunde an mitgezählt.
- **Seit der Sperre geblockt:** Ein eigener Bereich schlüsselt diese Versuche auf: Er nennt die Zahl der Pakete, die die gesperrte Adresse seither noch geschickt hat, und die Ports, die sie dabei angesteuert hat, bezogen auf die letzten 24 Stunden des Firewall-Protokolls. Bleibt der Bereich leer, hat die Gegenstelle es seit der Sperre nicht mehr versucht.
- **Seitenkopf:** Er nennt zusätzlich, seit wann die Daten aufgezeichnet werden.
- **Verknüpfte Register:** Die vier Register sind untereinander verknüpft. Von einer gesperrten Adresse führt ein Klick direkt zu ihren Einträgen in den anderen Registern, wobei abgewehrte Zugriffe als solche gekennzeichnet sind.
- **Verlauf:** zeigt Sperrungen („Gesperrt“) und Freigaben („Freigegeben“) chronologisch, neueste zuerst, ebenfalls mit Anbieter-Name und Herkunft je Adresse.
- **Angriffsziele:** zeigt in Alltagssprache, wonach die gesperrten Angreifer gesucht haben, etwa Zugangsdaten und Schlüssel (private SSH-Schlüssel, Passwort-Dateien), Router-Zugänge, Exchange-/Webmail-Server, VPN-Portale, Überwachungskameras, WordPress- oder Datenbank-Verwaltungen. Wichtig zur Einordnung: Keiner dieser Dienste läuft auf der TrutzBox; die Liste zeigt lediglich, wonach automatisierte Scanner überall im Internet suchen.

Menüpfad: Netzwerk → Angriffsschutz → Automatische Abwehr



Angriffsziele in Alltagssprache: wonach die gesperrten Angreifer gesucht haben.
(© 2026 Comidio GmbH)

- **Einstellungen:** Hier lassen sich die Sperrdauer (auf Wunsch „dauerhaft“), der Beobachtungszeitraum und die Zahl der Versuche bis zur Sperre anpassen:
- **Ausnahmen:** Die Standard-Ausnahmen (das Netz der TrutzBox und die eigene Internet-Adresse) sind fest hinterlegt und können nicht entfernt werden. Eigene zusätzliche Ausnahmen können ergänzt werden.
- **Sperrdauer:** Sie gilt für Angriffsmuster (etwa das Absuchen der Box nach Lücken).
- **Fehlgeschlagene Anmeldungen:** Diese sperrt die TrutzBox dagegen nie dauerhaft: Die erste Sperre dauert sechs Stunden, jede weitere derselben Adresse doppelt so lang (12, 24, 48, 96 Stunden), höchstens eine Woche. Die Sperrdauer lässt sich für Anmeldungen nicht einstellen. Dahinter steckt meist ein eigenes Gerät mit einem alten Passwort, das sich sonst dauerhaft selbst aussperren würde. Bei der Anmeldung an der Kommandozeile (SSH) dauert die erste Sperre nur eine Stunde, jede weitere ebenfalls doppelt so lang, höchstens eine Woche. Dort sitzt ein Mensch an der Tastatur und kein Programm, das mit einem alten Passwort immer wieder anklopft; wer sich unterwegs vertippt, soll nicht einen halben Tag warten müssen.
- **Beobachtungszeitraum und Versuche:** Beide gelten für Angriffsmuster und Anmeldungen, bei Anmeldungen aber nur in die strengere Richtung: Mehr als fünf Versuche oder ein kürzerer Zeitraum als 30 Minuten werden dort nicht übernommen. In der Spalte „Ausgelöst durch“ erscheint neben dem Scanner-Wächter („nginx-scanner“) entsprechend auch die Anmelde-Wächter für den Chat („prosody-auth“) und für TrutzMail („trutzmail-auth“). Seit Oktober 2026 kommt der Anmelde-Wächter für die Kommandozeile („sshd“) hinzu.
- **Zahl im Ereignis-Dialog:** Das ist die Zahl der protokollierten Abweisungen, nicht die Zahl aller abgewehrten Pakete. Blockiert wird jedes Paket, nur das Mitschreiben ist je Absender begrenzt (Einzelheiten im Kapitel „Wie der Monitor die Daten vorhält“).

Der Zustand des Angriffsschutzes ist zusätzlich als Kachel auf der Seite „TrutzBox-Betriebszustand“ sichtbar.
Ab Werk gelten vier Wächter mit unterschiedlichen Standardwerten:

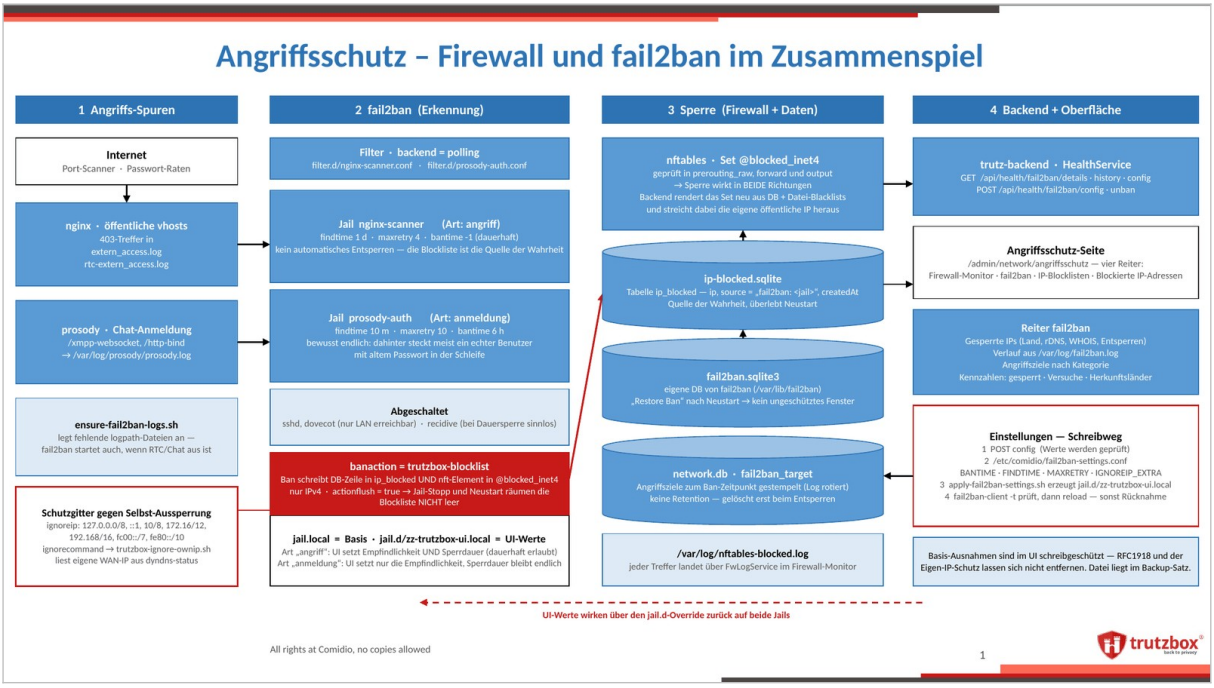
Wächter	Beobachtet	Versuche	Beobachtungszeitraum	Sperrdauer
Web-Scanner („nginx-scanner“)	abgewiesene Anfragen am Web-Zugang von außen	3	24 Stunden	dauerhaft
Chat-Anmeldung („prosody-auth“)	fehlgeschlagene Anmeldungen am Chat	5	30 Minuten	6 Stunden, wachsend bis 1 Woche
TrutzMail-Anmeldung („trutzmail-auth“)	fehlgeschlagene Anmeldungen an Postfach und Mail-Versand (IMAP, POP3, SMTP) von außen	5	30 Minuten	6 Stunden, wachsend bis 1 Woche
SSH-Anmeldung („sshd“)	fehlgeschlagene Anmeldungen an der Kommandozeile (SSH)	5	30 Minuten	1 Stunde, wachsend bis 1 Woche

Der lange Beobachtungszeitraum des Scanner-Wächters ist auf verteiltes Absuchen mit wenigen Zugriffen je Adresse zugeschnitten; eine dauerhafte Sperre ist hier unbedenklich, weil ein eigenes Gerät dieses Muster nicht erzeugt. Beim Anmelde-Wächter steckt hinter Fehlversuchen meist ein eigenes Gerät mit einem alten Passwort; die Sperre endet deshalb von selbst. Im Reiter „Einstellungen“ lassen sich beim Scanner-Wächter Empfindlichkeit und Sperrdauer ändern, bei den Anmelde-Wächtern nur die Empfindlichkeit, und die nur strenger als ab Werk.

Wie Erkennung und Sperre intern zusammenspielen

Hinter der Seite steckt ein bewusst einfach gehaltenes Zusammenspiel aus dem Erkennungsdienst fail2ban, der nftables-Firewall und der TrutzBox-Datenhaltung. Die Übersicht zeigt den Weg eines Angriffs in vier Bahnen, von der Spur im Log über die Erkennung und die Sperre bis zur Anzeige in der Oberfläche:

> **Technischer Hintergrund:** Wonach ein Angreifer gesucht hat, hält die Box im Moment der Sperre fest, nicht erst beim Betrachten. Der Grund ist die Haltbarkeit der Belege: Die Sperre gilt dauerhaft, der Nachweis steht aber im Zugriffsprotokoll des Web-Zugangs, und das wird regelmäßig rotiert. Würde die Oberfläche die Angriffsziele erst beim Aufruf aus dem Protokoll suchen, stünde bei älteren Sperren nichts mehr da. Deshalb schreibt die Box die gesuchten Pfade beim Bann neben den Eintrag.



Zusammenspiel von fail2ban, Firewall und Datenhaltung beim Sperren eines Angreifers. (© 2026 Comidio GmbH)

Erkannt wird ausschließlich aus Logzeilen der von außen erreichbaren Dienste: Der Web-Zugang (nginx) protokolliert abgewiesene Scanner-Anfragen, die Chat-Anmeldung (prosody) und die Mail-Dienste (Dovecot, Postfix) fehlgeschlagene Logins. Getrennte fail2ban-Wächter werten diese Logs aus: der Scanner-Wächter mit langem Beobachtungsfenster und Dauersperre, die Anmelde-Wächter bewusst mit endlicher Sperrdauer, denn hinter Fehlversuchen steckt meist ein eigenes Gerät mit einem alten Passwort (siehe Reiter „Einstellungen“ oben). Seit Oktober 2026 wertet ein weiterer Anmelde-Wächter die Anmeldungen an der Kommandozeile aus (SSH, Protokoll /var/log/auth.log): Ein falsches Passwort zählt einmal, ein unbekannter Benutzername doppelt, eine gelungene Anmeldung gar nicht.

Das Kernprinzip: fail2ban erkennt nur; gesperrt wird ausschließlich über die TrutzBox-Blockliste und das Firewall-Set. Ein automatischer Bann landet damit an genau derselben Stelle wie eine von Hand eingetragene Adresse (Reiter „Sperrlisten“) und wirkt in beide Richtungen, geprüft noch bevor NAT oder Proxy-Umleitung greifen. So gibt es keine zwei getrennten Sperrwelten (eine sichtbare in der Oberfläche und eine unsichtbare daneben).

Quelle der Wahrheit ist die Datenbank, nicht der Kernel-Zustand: Das Firewall-Set wird stets vollständig aus der Blocklisten-Datenbank neu erzeugt und überlebt so jeden Neustart; fail2ban stellt seine Sperren nach einem Neustart aus der eigenen Datenbank wieder her, sodass kein ungeschütztes Zeitfenster entsteht. Die Angriffsziele eines Angreifers werden bereits beim Sperren festgeschrieben, damit ihre Begründung auch nach der Log-Rotation erhalten bleibt.

Gegen Selbst-Aussperrung sichern zwei Schichten: Vor jeder Sperr-Entscheidung greifen feste Ausnahmen (alle privaten Netzbereiche und die eigene Internet-Adresse), und beim Erzeugen des Firewall-Sets wird die eigene öffentliche Adresse zusätzlich herausgefiltert, unabhängig davon, aus welcher Quelle sie eingetragen wurde. Diese Basis-Ausnahmen lassen sich über die Oberfläche bewusst nicht entfernen.

Auch der Schreibweg ist abgesichert: Einstellungen aus der Oberfläche verändern die Paket-Konfiguration nie direkt. Sie werden geprüft, in einer eigenen Einstellungsdatei abgelegt und als Überschreib-Ebene über die Basis-Konfiguration gelegt; erst wenn die Prüfung der neuen Konfiguration gelingt, wird der Angriffsschutz neu geladen. Andernfalls wird die Änderung zurückgenommen.

16.9 Verkehr ohne sichtbaren Domain-Namen

DNS-Sperre und URL-Filter setzen voraus, dass der Domain-Name einer Verbindung sichtbar ist (die drei Blockier-Methoden im Vergleich zeigt das Kapitel „Mehrschichtiger Netzwerk-Schutz (TrutzBase)“). Genau das ist nach Beobachtung im Monitor immer seltener der Fall; ein wachsender Anteil des Verkehrs lässt keinen Domain-Namen mehr erkennen:

- Viele Smart-TVs, Sprachassistenten und Konsolen ignorieren den heimischen Resolver und fragen fest eingetragene DNS-Server (Google, Cloudflare) direkt an; der Schutz vor DNS-Umgehung fängt das ab (Einzelheiten im Kapitel „DNS-Auflösung“).
- Browser und Apps verschlüsseln ihre Adress-Anfragen zunehmend selbst (DoH/DoT); ein Filter im eigenen Netz sieht davon nichts mehr. Die TrutzBox blockiert deshalb bekannte DoH-Anbieter und erzwingt den eigenen Auflösungsweg (Einzelheiten im Kapitel „DNS-Auflösung“).
- Mit Encrypted Client Hello (ECH) ist bei Servern, die das Verfahren unterstützen, auch der Server-Name im TLS-Handshake verschlüsselt; auf Netzwerkebene bleibt dann nur die IP-Adresse übrig. Die IP-Blocklisten des Angriffsschutzes sperren genau dort, und das Server-Detail im Monitor liefert Betreiber, Land und WHOIS-Angaben zur Einordnung.
- Rund jede fünfte Web-Verbindung nutzt inzwischen HTTP/3 (QUIC über UDP 443) und läuft damit am HTTP/S-Proxy vorbei; der Schalter „QUIC sperren“ schließt diesen Weg (Einzelheiten im Kapitel „IP-Blocklisten-Verwaltung“).
- Push-Dienste von Betriebssystemen verbinden sich nach Beobachtung im Monitor teilweise mit fest hinterlegten Server-Adressen ohne vorherige DNS-Abfrage. Solche Verbindungen sieht und steuert nur eine IP-basierte Firewall; im Monitor erscheinen sie als direkte Verbindungen, benannt über den PTR-Namen des Betreibers.

Zwei der drei Methoden brauchen also den Domain-Namen, und der verschwindet zusehends aus dem Netzwerkverkehr. Die TrutzBox kombiniert deshalb ihre beiden Ebenen: Der Proxy filtert präzise, wo er Namen und URL sieht; der Angriffsschutz blockiert anhand der IP-Adresse, wo kein Name mehr sichtbar ist. Der Monitor macht beides sichtbar und bietet zu jeder Verbindung die passende Aktion an („Domain sperren/erlauben“, „IP blockieren“).

16.10 Firewall-Monitor

Der Firewall-Monitor bildet den Reiter „Übersicht“ der Seite „Netzwerk → Angriffsschutz“.
Der Firewall-Monitor ist die Live-Sicht der nftables-Firewall auf alle Verbindungsversuche, die auf Netzwerk-Ebene blockiert wurden, also unabhängig vom HTTP/S-Proxy. Während der Proxy nur die

Ports 80 und 443 sieht, erfasst die Firewall jeden Verbindungsversuch über beliebige Ports und Protokolle (TCP wie UDP). Besonders sichtbar werden dadurch unaufgeforderte Scan- und Zugriffsversuche aus dem Internet; die blockierten Ereignisse werden zusammengefasst und nach Schweregrad (hoch, mittel, niedrig) eingestuft.

> **Technischer Hintergrund:** Für die Zuordnung liest die Box den Regelsatz der Firewall maschinenlesbar aus und vergleicht jede blockierte Verbindung mit den Regeln. So kann sie zu einem Treffer die zugrundeliegende Regel benennen. Zusätzlich prüft sie, ob zu einer von außen abgewiesenen Verbindung eine passende Sitzung aus dem eigenen Netz gehört; ist das der Fall, stuft sie den Vorgang als harmlos ein, weil es sich dann um eine Antwort auf eigenen Verkehr handelt und nicht um einen fremden Zugriffsversuch.

Die Kopfzeile fasst die wichtigsten Kennzahlen zusammen: die Anzahl der blockierten Verbindungen, die Zahl der beteiligten Geräte, die Anzahl aktiver Firewall-Regeln, den abgedeckten Logzeitraum sowie die am Internet-Router freigegebenen Ports (z. B. UDP/1194 für den VPN-Fernzugriff und TCP/443 für die Videokonferenz). Dazu bietet sie diese Funktionen:

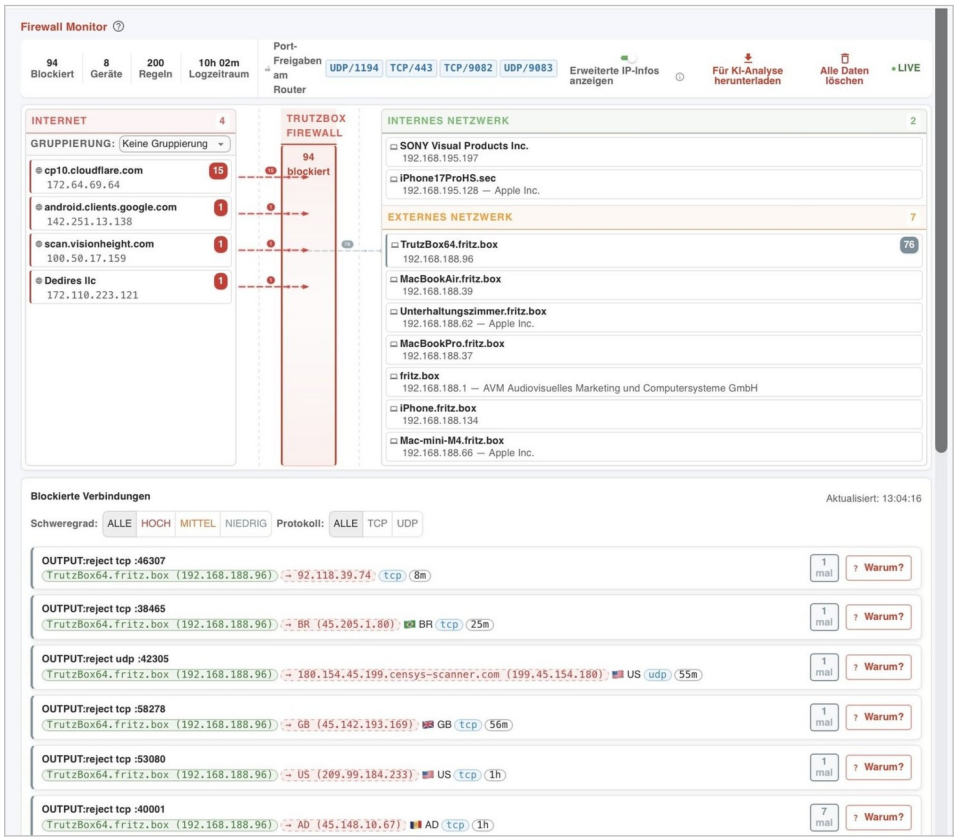
- **„IP-Infos aus dem Internet ergänzen“:** ergänzt zu jeder Adresse Land und Betreiber.
- **„Für KI-Analyse herunterladen“:** stellt die Daten als Datei für eine externe Auswertung zusammen, die der Administrator selbst prüft und weitergibt (die TrutzBox kontaktiert keine Threat-Intelligence-Dienste von sich aus). Die Datei enthält IP-Adressen und Gerätenamen, also personenbezogene Daten, was vor einer Weitergabe an externe Dienste zu berücksichtigen ist.
- **„Alle Daten löschen“:** leert das Protokoll.
- **Lupe:** durchsucht Diagramm und Liste gemeinsam als Volltext (IP, Name, Port, Dienst, Land, Grund; mit Trefferzähler „X von Y Verbindungen“).

Auf den Angreifer-Kacheln der Internet-Spalte steht zudem der am häufigsten angegriffene Ziel-Port mit Dienstnamen, etwa „Port 443 (HTTPS) +3“.

- **Port-Freigaben am Router:** Die Kopfzeile führt außerdem auf, welche Port-Weiterleitungen am Internet-Router gerade eingerichtet sind. Die TrutzBox fragt sie beim Router per UPnP-IGD ab und nennt zu jedem Eintrag die Quelle der Angabe und den Zeitpunkt der letzten Prüfung. Antwortet der Router nicht darauf, steht dort „nicht ermittelbar“.
- **Endpunkt-Details:** Ein Klick auf eine Kachel öffnet die „Endpunkt-Details“ mit der Block-Statistik dieser Gegenstelle: die Zahl der Blockierungen insgesamt, die eingeschätzte Bedrohungsstufe und die zuletzt blockierten Verbindungen. Zu jeder Zeile lässt sich die zugrundeliegende Firewall-Regel einblenden; steht dort kein Regel-Treffer, kam die Blockierung nicht von der Firewall, sondern etwa vom Web-Inhaltsfilter.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Menüpfad: Netzwerk → Angriffsschutz → Übersicht



Der Firewall-Monitor mit Angreifern, Zielen und den blockierten Verbindungen.
(© 2026 Comidio GmbH)

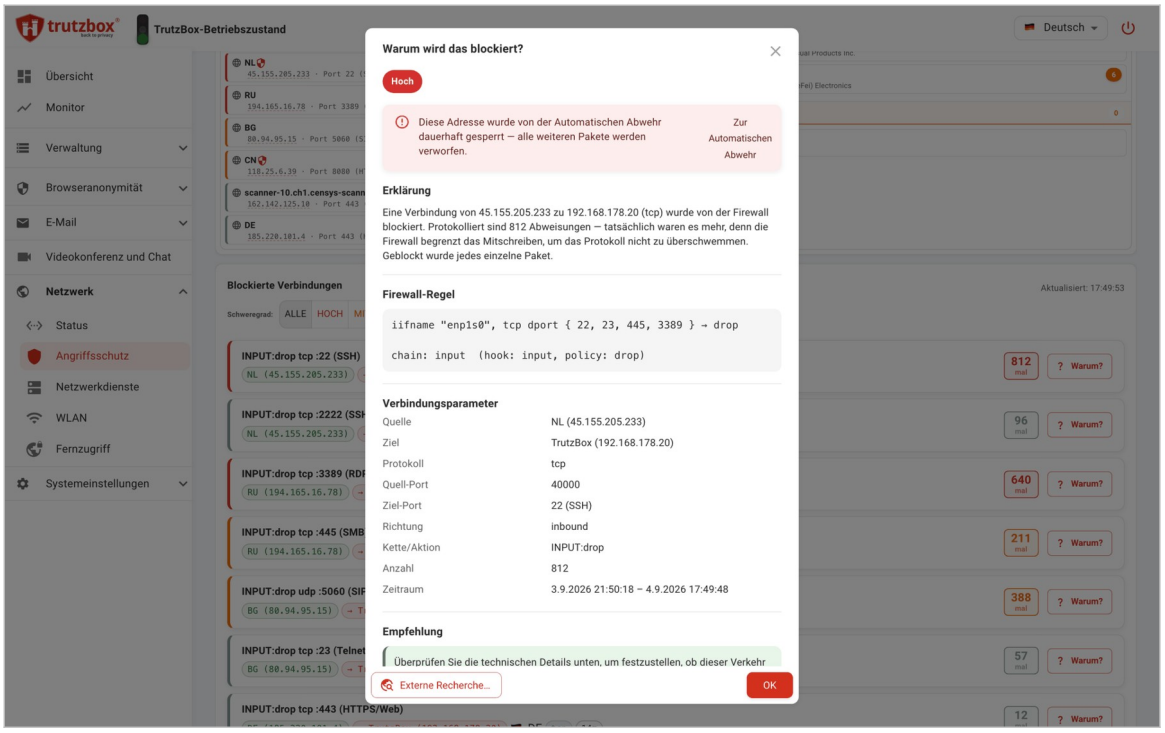
Die Darstellung ist, wie beim Monitor, dreispaltig: links die kontaktierten bzw. blockierten Internet-Server, in der Mitte die TrutzBox-Firewall mit der Zahl der blockierten Versuche, rechts die Geräte, getrennt nach internem Netzwerk (direkt an der TrutzBox) und externem Netzwerk (am Internet-Router). Rot gestrichelte Linien markieren die blockierten Verbindungen.

Blockierte Verbindungen im Detail

Unterhalb der Grafik listet „Blockierte Verbindungen“ jeden Versuch einzeln auf. Die Liste lässt sich nach Schweregrad (Hoch, Mittel, Niedrig) und Protokoll (TCP, UDP) filtern. Jeder Eintrag nennt die Firewall-Aktion (z. B. „OUTPUT:reject“ oder „net2fw:DROP“), Quelle und Ziel mit Port, Land und Protokoll sowie wie oft und über welchen Zeitraum der Versuch auftrat.
Über die Schaltfläche „Warum?“ öffnet sich zu jedem Eintrag eine Erklärung in Klartext. Sie nennt den Schweregrad, fasst zusammen, worum es sich vermutlich handelt (etwa ein Port-Scan oder ein unbefugter Zugriffsversuch aus dem Internet), zeigt die zugrunde liegende Firewall-Regel sowie die vollständigen Verbindungsparameter (Quelle, Ziel, Protokoll, Quell- und Ziel-Port, Richtung, Kette/Aktion) und gibt eine Handlungsempfehlung. In den meisten Fällen ist keine Maßnahme erforderlich, denn die Firewall schützt das Netzwerk, indem sie unaufgeforderte eingehende Verbindungen blockiert.

Zu jeder Adresse bietet der Dialog außerdem „Externe Recherche“: kuratierte Links zu Diensten wie AbuseIPDB und GreyNoise sowie das Kopieren der Adresse in die Zwischenablage. Auch diese ruft die TrutzBox nicht selbst auf; sie öffnet lediglich den Link; ob recherchiert wird, entscheidet der Administrator. Über den Regel-Browser lässt sich zudem der vollständige nftables-Regelsatz, gegliedert nach Kette, Hook und Policy, schreibgeschützt einsehen.

Menüpfad: Netzwerk → Angriffsschutz → Übersicht



Der Dialog „Externe Recherche“ mit kuratierten Links und Angabe, was gesendet wird. (© 2026 Comidio GmbH)

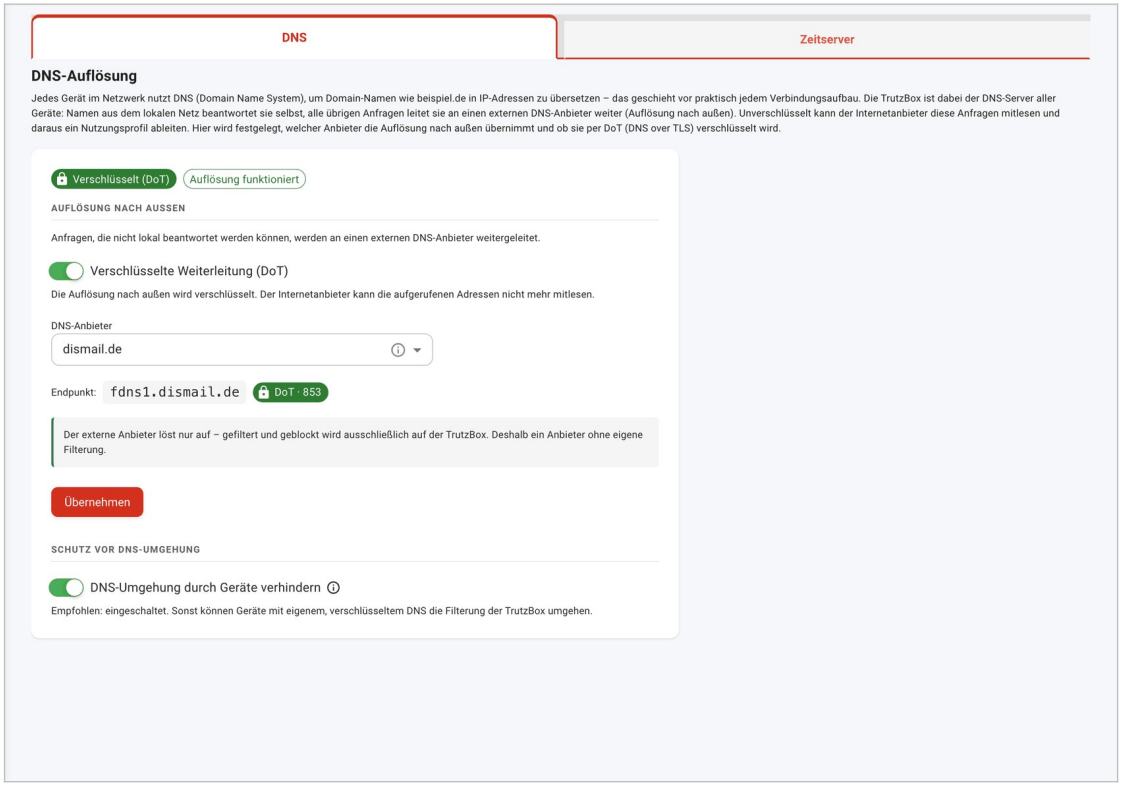
Die interaktiven Bedienelemente, also Verbindungslinien, Gruppierung der Server und die Steuerung des Zeitraums, funktionieren wie im Kapitel „Monitor“ beschrieben.

16.11 DNS-Auflösung

Jedes Gerät im Netzwerk nutzt DNS (Domain Name System), um Domain-Namen wie beispiel.de in IP-Adressen zu übersetzen. Diese Anfragen verraten viel über die Nutzung: Wer sie mitlesen kann, sieht, welche Webseiten und Dienste im Haushalt aufgerufen werden. Der Reiter „DNS“ der Seite „Netzwerk → Netzwerkdienste“ legt fest, wie die TrutzBox mit diesen Anfragen umgeht.
Anfragen aus dem eigenen Netz beantwortet die TrutzBox zunächst selbst. Nur was sie nicht lokal beantworten kann, leitet sie unter „Auflösung nach außen“ an einen externen DNS-Anbieter weiter.
Verschlüsselte Weiterleitung (DoT): Mit diesem Schalter wird die Auflösung nach außen verschlüsselt (DNS über TLS, kurz „DoT“). Der Internetanbieter kann die aufgerufenen Adressen dann nicht mehr mitlesen. Zwei Status-Anzeigen zeigen den aktuellen Zustand: „Verschlüsselt (DoT)“ bzw. „Unverschlüsselt“ sowie „Auflösung funktioniert“ bzw. „Auflösung gestört“. Die verschlüsselte

Weiterleitung ist die Standardeinstellung: Die TrutzBox schaltet sie selbsttätig ein und prüft die Verbindung dabei selbst. Lässt das Netz DoT nicht zu, bleibt die Auflösung unverschlüsselt, und die Box wiederholt den Versuch in der ersten Stunde alle fünf Minuten, danach alle 30 Minuten, etwa bis der Router den Port wieder freigibt oder die Box in ein anderes Netz umzieht. Fällt die Verschlüsselung im laufenden Betrieb aus, schaltet die Box binnen etwa einer Minute auf unverschlüsselt um, damit die Geräte Internet behalten. „Verschlüsselt (DoT)“ zeigt die Seite nur an, wenn keine Anfrage mehr unverschlüsselt über den Router läuft. Eine bewusste Abschaltung durch den Administrator bleibt dagegen dauerhaft bestehen.

Menüpfad: Netzwerk → Netzwerkdienste → DNS



Die Seite „Netzwerkdienste“, Reiter „DNS“, mit verschlüsselter Weiterleitung und Anbieterwahl. (© 2026 Comidio GmbH)

DNS-Anbieter: Zur Auswahl stehen geprüfte Anbieter, jeweils mit einer kurzen Einordnung zu Betreiber und Rechtsraum: „DNS4EU“ (EU-gefördertes Projekt ohne eigene Filterung, empfohlen), „Quad9“ (gemeinnützige Schweizer Stiftung; verwendet wird der ungefilterte Dienst 9.9.9.10), „Cloudflare“ und „Google“ (beide US-Unternehmen) sowie „Benutzerdefiniert“ für einen eigenen DoT-Server (Hostname für die Zertifikatsprüfung plus eine bis vier IPv4-Adressen).

- **Eigener Anbieter:** Über „Benutzerdefiniert …“ lässt sich ein selbst betriebener oder ein anderer DoT-Server eintragen. Erforderlich sind der DoT-Hostname für die Zertifikatsprüfung (etwa dot.example.org) und ein bis vier IPv4-Adressen. Das Zertifikat des Servers muss zum angegebenen Hostnamen passen, sonst kommt keine Verbindung zustande.

Wichtig zur Einordnung: Der externe Anbieter löst nur auf; gefiltert und geblockt wird ausschließlich auf der TrutzBox. Deshalb wird ein Anbieter ohne eigene Filterung empfohlen; die Kontrolle bleibt vollständig bei der Box.
Schutz vor DNS-Umgehung: Der Schalter „DNS-Umgehung durch Geräte verhindern“ (empfohlen: eingeschaltet) sorgt dafür, dass Geräte die Filterung nicht umgehen, indem sie an der TrutzBox vorbei auflösen:

- **Klassisches DNS:** Anfragen an fremde Server beantwortet die TrutzBox transparent selbst.
- **Verschlüsseltes DNS:** Verbindungen (DoH/DoT) zu bekannten Anbietern wie Google oder Cloudflare werden blockiert, sodass die Geräte auf die TrutzBox zurückfallen.
- **Apple Private Relay:** Es wird im eigenen Netz durch die Sperre der zugehörigen Server unterbunden (betroffene Apple-Geräte zeigen dazu nach Beobachtung des Comidio-Teams einen Hinweis an).
- **Gerät ohne Namensauflösung:** Kann ein Gerät mit fest eingetragenem verschlüsseltem DNS danach keine Namen mehr auflösen, entfernt man diese Einstellung auf dem Gerät oder schaltet notfalls den Schalter aus.
- **DNS4EU:** Die Sperrliste dieses Schutzes kennt sämtliche Varianten des europäischen DNS-Dienstes DNS4EU, also auch die Ausführungen mit Werbe- und Kinderschutzfilter. Geräte, die einen dieser Server unmittelbar ansprechen, werden wie bei allen anderen Anbietern abgefangen.
- **Mitschreiben:** Auch hier ist das Mitschreiben je Gerät begrenzt, damit ein Gerät, das es im Sekundentakt versucht, die Box nicht ausbremst. Der Schutz selbst greift unverändert bei jeder einzelnen Anfrage.
- **Im Monitor:** Die betroffenen Adressen erscheinen mit ihrem Namen, und die abgefangene Anfrage wird der TrutzBox zugeordnet, weil sie sie selbst beantwortet hat.

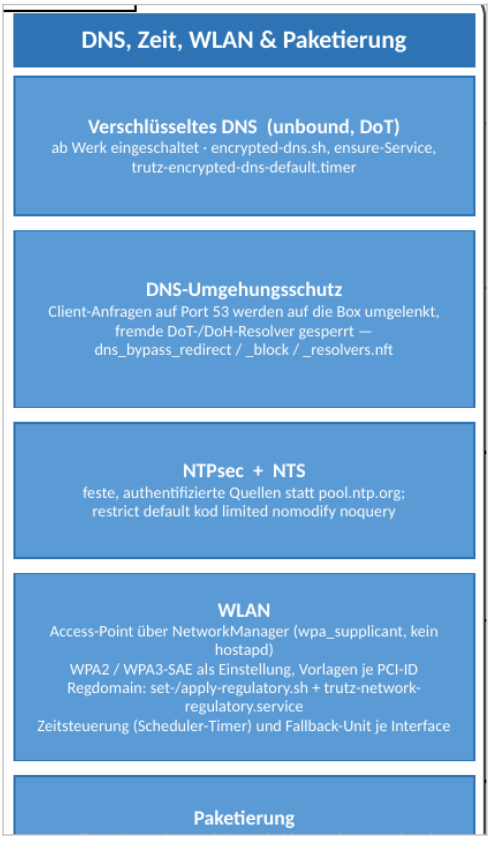
Über „Übernehmen“ wird die Einstellung aktiv. Die TrutzBox prüft die Umschaltung dabei selbst; das kann bis zu einer Minute dauern. Schlägt die Prüfung fehl, stellt sie automatisch den vorherigen Zustand wieder her, damit die Namensauflösung im eigenen Netz nicht ausfällt.
Ob der DNS-Verkehr tatsächlich verschlüsselt läuft, lässt sich im Monitor nachprüfen: Das Verbindungs-Detail zeigt unter „DNS-Verschlüsselung“, ob ein DNS-Server über TLS (DoT), über HTTPS (DoH) oder unverschlüsselt (Port 53) angesprochen wird.
Der Schutz vor DNS-Umgehung arbeitet mit vier Mitteln, die ineinandergreifen; hinzu kommt die Behandlung im VPN:

- **Umlenken:** Unverschlüsselte DNS-Anfragen an fremde Server lenkt die TrutzBox auf ihren eigenen Namensdienst um; das Gerät bemerkt davon nichts.
- **Abweisen:** Verschlüsselte DNS-Verbindungen (DoT auf Port 853 sowie DoH über Port 443 zu bekannten Anbietern) weist sie ab, sodass das Gerät auf den per DHCP mitgeteilten Namensdienst der Box zurückfällt.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

- **Namen verweigern:** Die Namen bekannter DoH-Anbieter beantwortet die Box nicht, damit ein Gerät deren Adresse gar nicht erst ermitteln kann.
- **Firefox-Prüfdomäne:** Firefox prüft vor dem Einschalten seines eigenen verschlüsselten DNS eine bestimmte Prüfdomäne; bleibt sie ohne Antwort, wertet Firefox das als Vorgabe des Netzbetreibers und schaltet sein verschlüsseltes DNS selbst ab. Genau diese Antwort verweigert die TrutzBox.
- **TrutzVPN:** Über TrutzVPN verbundene Geräte erhalten den Namensdienst der Box mit der VPN-Verbindung. Unverschlüsselte Anfragen an bekannte fremde Anbieter werden auch im VPN abgewiesen, sodass diese Geräte ebenfalls über die Box auflösen.

Der eigene Verkehr der TrutzBox ist nie betroffen; als Anbieter für die Auflösung nach außen funktioniert auch Google bei eingeschaltetem Schutz.
Der Schutz hat Grenzen. Er erkennt verschlüsselte DNS-Anfragen an Adresse und Port, nicht am Inhalt. Ein privater oder unbekannter DoH-Server ist von einer gewöhnlichen HTTPS-Verbindung nicht zu unterscheiden und wird nicht erkannt. Unverschlüsselte IPv6-Anfragen an unbekannte Server werden nicht umgeleitet. Abgefangene Versuche erscheinen im Firewall-Monitor in der Kategorie „DNS-Umgehung“.



Bausteine der DNS-Auflösung: verschlüsseltes DNS (DoT), Umgehungsschutz für Port 53 und fremde DoT/DoH-Server.
(© 2026 Comidio GmbH)

16.12 Zeitserver

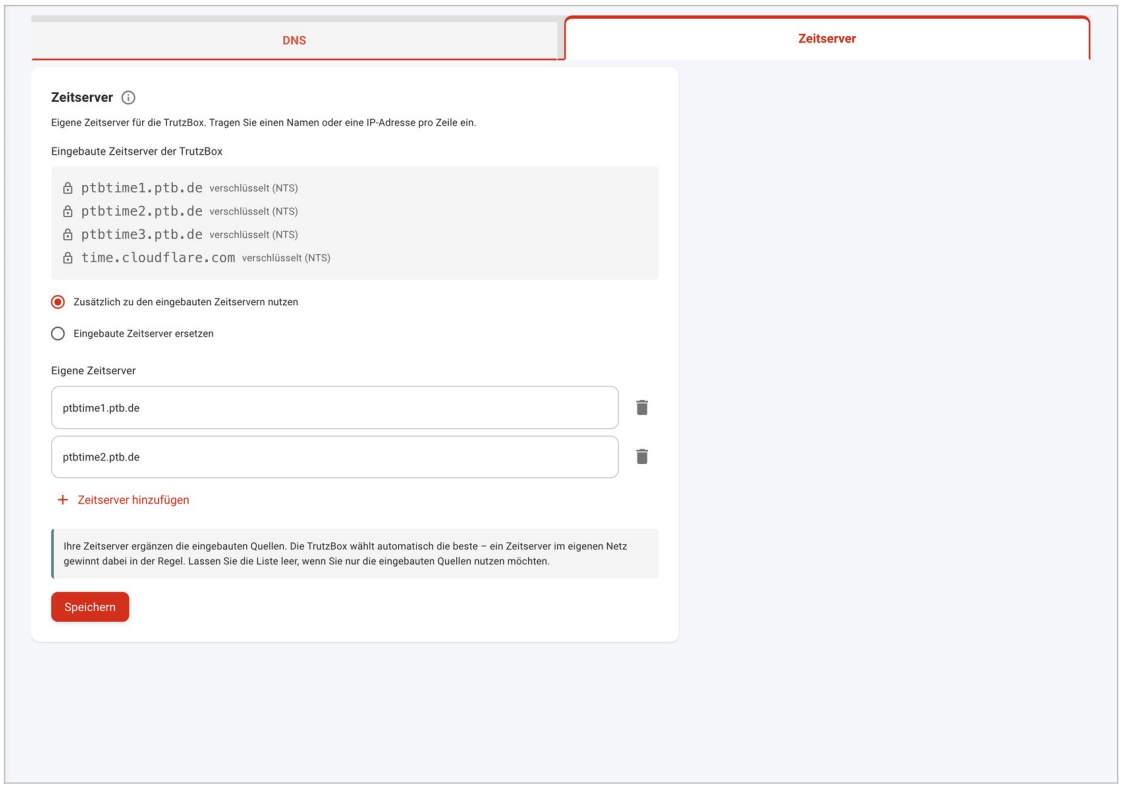
Der zweite Reiter der Seite „Netzwerk → Netzwerkdienste“ verwaltet die Zeitquellen der TrutzBox. Die Box holt ihre Uhrzeit verschlüsselt von vertrauenswürdigen Quellen: der deutschen Atomuhr über die Physikalisch-Technische Bundesanstalt (PTB) und Netnod. NTS (Network Time Security) ist dabei die verschlüsselte, manipulationssichere Variante des NTP-Zeitabgleichs.
Zusätzlich lassen sich bis zu acht eigene Zeitserver eintragen (Name oder IP-Adresse), zum Beispiel ein NTP-Server im eigenen Netz:

- **Ergänzung statt Ersatz:** Eigene Server ergänzen die eingebauten Quellen, sie ersetzen sie nicht. Die TrutzBox wählt automatisch die beste Quelle; ein Zeitserver im eigenen Netz gewinnt dabei in der Regel.
- **Leere Liste:** Bleibt die Liste leer, nutzt die Box nur die eingebauten Quellen.
- **Sonderfall falsche Uhr:** Ein Sonderfall ist der Start mit falsch gehender Uhr. Die verschlüsselte Zeitabfrage (NTS) braucht ein gültiges Zertifikat, und die Gültigkeitsprüfung eines Zertifikats braucht ihrerseits eine halbwegs richtige Uhr.
- **Folge:** Liegt die Uhr beim Start weit in der Vergangenheit, etwa nach einem leeren Puffer der Hardware-Uhr, beißt sich das: Zeitabfrage, Aktualisierungen, Zertifikate und verschlüsselte Anmeldungen scheitern gemeinsam, und die Box kann sich nicht mehr selbst heilen.
- **Prüfung beim Start:** Deshalb prüft die TrutzBox beim Start, ob die Uhr beweisbar falsch geht. Ist das der Fall, holt sie sich einmalig die Zeit, zuerst beim eigenen Internet-Router, und schreibt sie in die Hardware-Uhr; danach läuft die normale, verschlüsselte Zeitabfrage wieder.

Eine Box mit richtig gehender Uhr erzeugt dabei keinerlei Netzverkehr.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Menüpfad: Netzwerk → Netzwerkdienste → Zeitserver



Der Reiter „Zeitserver“ mit den eingebauten und den eigenen Zeitservern.
(© 2026 Comidio GmbH)

Wie einzelne Geräte ihre Zeitabfragen über die TrutzBox leiten, ist im Kapitel „Geräte“ beschrieben. Warum es den Schalter „NTP über TrutzBox leiten“ je Gerät gibt, erklärt ein Blick auf das Verhalten der Betriebssysteme. Der DHCP-Server der TrutzBox teilt allen Geräten den Zeitserver der Box mit (DHCP-Option 42, ein Standard aus RFC 2132). Diese Angabe beachten aber nur wenige Systeme:

- **Übernehmen automatisch:** Linux, BSD, OpenWrt sowie Drucker, Access-Points, IP-Telefone und viele IoT-Geräte.
- **Windows und macOS:** Sie ignorieren die Option und fragen fest bei time.windows.com beziehungsweise time.apple.com. Dort lässt sich der Zeitserver zwar von Hand ändern, aber nicht zentral über das Netz.
- **Android und iOS:** Android (time.android.com bei Google) und iOS (time.apple.com) ignorieren die Option ebenfalls und bieten keine Einstellung. iOS ist nur über ein Verwaltungsprofil (MDM) umstellbar, Android nur mit Entwicklerwerkzeugen.

Für einen Haushalt ist das praktisch nicht machbar.

Gerät / System	Standard-Zeitserver	Beachtet DHCP-Option 42	Selbst änderbar
Linux, BSD, OpenWrt	Distribution / Pool	ja	ja

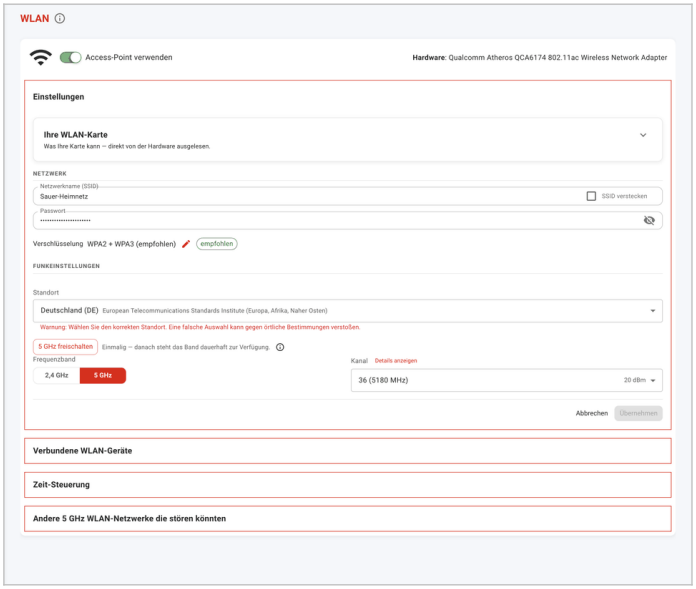
Gerät / System	Standard-Zeitserver	Beachtet DHCP-Option 42	Selbst änderbar
Drucker, Access-Points, IP-Telefone, viele IoT-Geräte	herstellerabhängig	meist ja	ja
Windows	time.windows.com	nein	ja, von Hand
macOS	time.apple.com	nein	ja, von Hand
Android	time.android.com (Google)	nein	nur eingeschränkt (Entwicklerwerkzeuge)
iOS / iPadOS	time.apple.com	nein	nein (nur per MDM-Profil)

Der einzige Weg, alle Geräte im eigenen Netz zu halten, ist deshalb die Umleitung: Die TrutzBox lenkt die Zeitanfragen des Geräts (UDP-Port 123) transparent auf ihren eigenen Zeitdienst um. Das funktioniert auch bei Geräten ohne Einstellmöglichkeit, weil gewöhnliches NTP unverschlüsselt ist. Das Gerät kann die Antwort der Box nicht von der des Herstellers unterscheiden und übernimmt die Zeit. Microsoft, Apple und Google erfahren dann nicht mehr, wann und von welcher Adresse aus das Gerät online ist. Nicht erfasst werden Geräte, die ihre Zeit verschlüsselt per NTS beziehen; kein verbreitetes Endgeräte-System tut das ab Werk. Die Umleitung wirkt nur für Geräte, deren Verkehr über die TrutzBox läuft. Die Box selbst holt ihre Zeit weiterhin verschlüsselt von den oben genannten Quellen.

16.13 WLAN

Das WLAN-Menü erscheint nur bei entsprechend ausgestatteter Hardware. Abhängig von der WLAN-Hardware stehen unterschiedliche Funktionen bereit. Welche Bänder und Einstellungen angeboten werden, hängt von der jeweils eingebauten WLAN-Karte ab. Die Bedienoberfläche erkennt das und weist darauf hin.

Menüpfad: Netzwerk → WLAN



Das WLAN-Menü mit Netzname, Verschlüsselung, Band und Kanalwahl.
(© 2026 Comidio GmbH)

Funkeinstellungen

Über den Schalter „Access-Point verwenden“ wird die TrutzBox als WLAN-Zugangspunkt aktiviert. Im Kopfbereich des Menüs zeigt die Box den eingebauten Funkadapter (etwa Qualcomm Atheros 802.11ac); der angezeigte Funktionsumfang richtet sich nach dieser Hardware. Die Seite gliedert sich in aufklappbare Bereiche: „Einstellungen“, „Verbundene WLAN-Geräte“, „Zeit-Steuerung“ und die Übersicht der WLANs in der Umgebung. Die Karte „Ihre WLAN-Karte“ (im Bereich „Einstellungen“) zeigt vorab, was die eingebaute Hardware kann: WPA3, 5-GHz-Band, Geschwindigkeit (Wi-Fi-Generation), zwei Funknetze gleichzeitig. Außerdem nennt sie den Dienst, der die Karte verwaltet.
Unter „Netzwerk“ werden der WLAN-Name (SSID) und das Passwort festgelegt. Mit „SSID verstecken“ lässt sich der Netzwerkname aus der öffentlichen Sichtbarkeit nehmen, sodass er nicht in den Netzwerklisten anderer Geräte erscheint.
Unter dem Passwort wählt die Auswahl „Verschlüsselung“ (Stift-Symbol) den Sicherheitsstandard: „WPA2 + WPA3 (empfohlen)“ (der Übergangsmodus, in dem ältere und neue Geräte gleichzeitig funktionieren), „Nur WPA3“ (höchste Sicherheit, sehr alte Geräte bleiben außen vor) oder „Nur WPA2“. Je nach Auswahl wechselt die TrutzBox den zugrunde liegenden Access-Point-Dienst selbständig (NetworkManager bzw. hostapd); ein Eingriff ist dazu nicht nötig.
Die Funkeinstellungen legen das Frequenzband (2,4 GHz und, je nach Hardware, 5 GHz) und den verwendeten Kanal fest. Über den Standort wird die zuständige Funkregulierung gewählt (etwa Deutschland/ETSI für Europa). Die Auswahl bestimmt, welche Kanäle und Sendeleistungen am Aufstellort überhaupt zulässig sind, und sollte unbedingt korrekt gesetzt werden, da eine falsche Angabe gegen örtliche Funkvorschriften verstoßen kann. In der Voreinstellung wählt „Autokanal“ selbständig den am wenigsten belegten Kanal; wer manuell wählt, sieht je Kanal Frequenz, Sendeleistung und Besonderheiten (etwa DFS-Kanäle, die auf Wetter-Radar Rücksicht nehmen).
Hinweis zu selbstverwalteten Funkkarten: Manche WLAN-Adapter regeln die Funkregulierung in ihrer eigenen Firmware („self-managed“) und ignorieren die Software-Auswahl teilweise. In diesem Fall zeigt die TrutzBox eine Warnung und meldet gegebenenfalls eine andere tatsächlich aktive Regulierung als die gewählte. Beim Ändern des Standorts startet die Box das WLAN intern kurz neu, damit die Einstellung zuverlässig übernommen wird.

5-GHz-Kanäle und Funkregulierung

Ob die 5-GHz-Kanäle zur Verfügung stehen, hängt von der jeweils eingebauten WLAN-Karte ab. Manche Karten geben das Band für den Betrieb als Zugangspunkt frei, andere nicht; die Karte „Ihre WLAN-Karte" zeigt, was das verbaute Modul beherrscht. Bietet die Oberfläche nur 2,4 GHz an, gibt die Karte das 5-GHz-Band für diesen Betrieb nicht frei.
Unabhängig davon bestimmt der eingestellte Aufstellort, welche Kanäle und Sendeleistungen zulässig sind.

Verbundene WLAN-Geräte

Der Bereich „Verbundene WLAN-Geräte“ listet alle aktuell am TrutzBox-WLAN angemeldeten Geräte, jeweils mit Namen aus der Geräteliste, IP-Adresse, Signalstärke (dBm), aktueller Empfangs- und Sende-

Datenrate sowie der Dauer der Verbindung. So ist auf einen Blick erkennbar, wer das WLAN nutzt und wie gut der Empfang am jeweiligen Standort ist.

Zeit-Steuerung

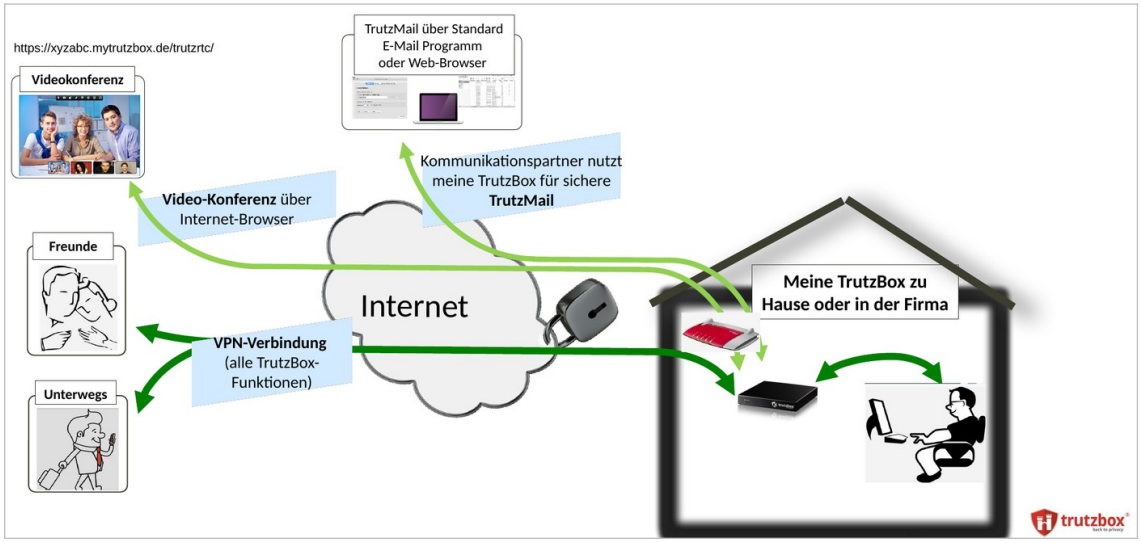
Die Zeit-Steuerung schaltet den Access-Point nach einem festen Wochenplan automatisch ein und aus. Im 24-Stunden-Raster werden pro Wochentag die aktiven Zeitfenster grün dargestellt; in den grau hinterlegten Zeiträumen ist das Funkmodul ausgeschaltet. Über die Schaltfläche „Einstellen“ lassen sich die Zeitfenster anpassen. Der Schalter „Access-Point verwenden“ hat dabei Vorrang: Schaltet man das WLAN von Hand ein oder aus, gilt diese manuelle Entscheidung bis zum nächsten im Plan hinterlegten Schaltzeitpunkt; erst dann übernimmt die Zeit-Steuerung wieder.
Ab Werk ist kein Zeitplan aktiv. Wer einen einrichtet, bekommt als Vorschlag täglich 07:00 bis 22:00. Außerhalb dieser Zeiten verbraucht das Funkmodul keinen Strom und sendet keine Funkwellen. Das senkt den Stromverbrauch und die Funkaktivität im Haushalt, ohne dass jeden Abend ein Knopf gedrückt werden muss.

Andere WLANs in der Umgebung

Im unteren Bereich des Menüs zeigt die TrutzBox einen Scan der WLANs in Funkreichweite, die das eigene Netz stören könnten. Aufgeführt werden je gefundenem Netz die Signalstärke in Prozent, der belegte Kanal mit Frequenz, die maximal angekündigte Brutto-Datenrate und die unterstützten Verschlüsselungsstandards (etwa WPA2 oder WPA3). Der Scan steht auch zur Verfügung, während die TrutzBox selbst als Zugangspunkt sendet; angezeigt werden die Netze des gerade aktiven Frequenzbands.
Anhand dieser Übersicht lässt sich erkennen, welche Kanäle in der Nachbarschaft bereits stark belegt sind. Im Idealfall wird für das eigene WLAN ein Kanal gewählt, der von keinem starken Nachbarnetz genutzt wird. Bei 2,4 GHz empfiehlt sich erfahrungsgemäß einer der nicht überlappenden Kanäle 1, 6 oder 11.

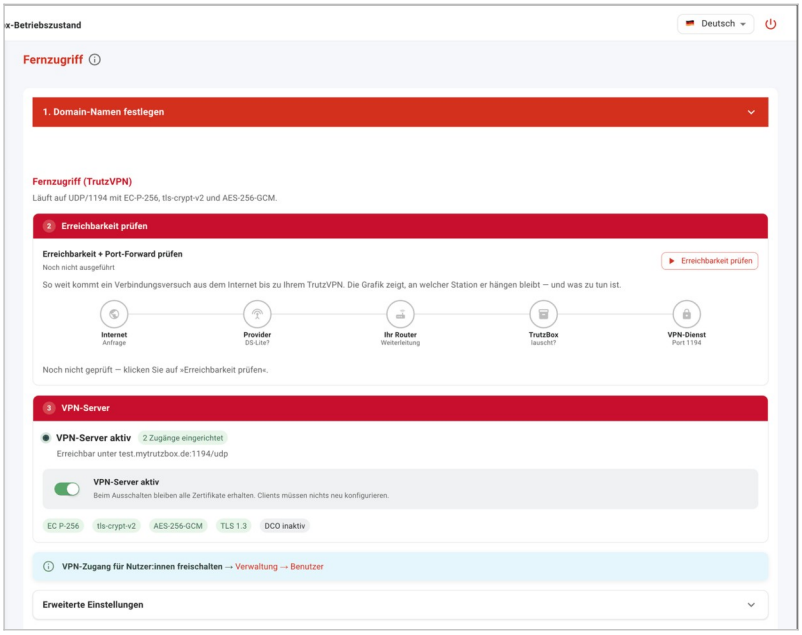
16.14 Fernzugriff: VPN (Virtual Private Network)

Die TrutzBox steht typischerweise zu Hause oder in einer Firma. Um die TrutzBox Funktionen auch unterwegs nutzen zu können sollte man die TrutzBox nicht mitnehmen, sondern den Fernzugriff auf der TrutzBox aktivieren. Der Fernzugriff auf die TrutzBox wird durch ein VPN realisiert.



Nutzung von unterwegs über TrutzDynDNS: VPN, Videokonferenz und TrutzMail erreichen die TrutzBox über den Internet-Router.
(© 2026 Comidio GmbH)

Menüpfad: Netzwerk → Fernzugriff



Die Seite „Fernzugriff“ mit TrutzDynDNS-Namen, VPN-Server und Erreichbarkeitstest.
(© 2026 Comidio GmbH)

VPN bedeutet „virtual private network“. Ein VPN verbindet ein Gerät über ein unsicheres Netzwerk (das Internet) mit einem privaten Netzwerk (z. B. Firmen- oder Heimnetzwerk). Es ermöglicht einem Computer über ein öffentliches Netzwerk Daten auszutauschen, als wäre der Computer direkt mit dem Firmen- oder Heimnetzwerk verbunden. Über einen solchen VPN Zugang können TrutzBox Nutzer die

gesamte TrutzBox Funktionalität auch von außerhalb des eigenen Netzes nutzen, z. B. von unterwegs mit dem Smartphone.
Dadurch bietet dieser Zugang die gleiche Funktionalität, Sicherheit und Kontrollmechanismen wie aus dem privaten Netzwerk zu Hause oder in der Firma. Eine VPN-Verbindung wird erreicht, indem eine virtuelle Punkt-zu-Punkt Verbindung vom Endgerät, über das Internet, zu der TrutzBox, mit entsprechender Authentisierung und Verschlüsselung aufgebaut wird. Eine VPN-Verbindung kann auch aus dem lokalen Netzwerk heraus aufgebaut werden.

Mit VPN ist es dem TrutzBox Besitzer auch möglich, anderen (z. B. Freunden, Verwandten oder Mitarbeitern) Zugriff auf eine TrutzBox zu geben und diese mitzubenutzen. Die TrutzBox ermöglicht diese Mitbenutzung zwar, aber Comidio empfiehlt das Mitbenutzen der TrutzBox nur dann, wenn die Mitbenutzer Vertrauen in den TrutzBox-Administrator haben. Der Administrator der TrutzBox wäre zumindest technisch in der Lage, diese Nutzer zu überwachen und auf vertrauliche Informationen zuzugreifen. Für die Mitbenutzung durch Dritte gilt der rechtliche Hinweis am Anfang dieses Dokuments. Für die Mitbenutzung durch Dritte gilt der rechtliche Hinweis am Anfang dieses Dokuments.

Des Weiteren sollte man bei Nutzung von VPN darauf achten, dass die eigene Internet-Verbindung (vor allem die Upload Geschwindigkeit) genügend Durchsatz bietet.
Um den Fernzugriff nutzen zu können, muss der eigene Internet-Anschluss vom Internet aus erreichbar sein. Leider ist das nicht immer der Fall. Meist sind z. B. Mobilfunkverbindungen vom Internet aus nicht erreichbar. Auch kommt es immer öfter vor, dass der private Internet-Provider keine echte, eindeutige IPv4 Adresse dem eigenen Internet-Anschluss zuordnet, sondern lediglich einen „Dual-Stack Lite“ Anschluss zur Verfügung stellt. In diesem Fall wird die lokale externe IPv4-Adresse durch ein IPv6-Netzwerk geroutet und die IPv4-Adresse ist nicht eindeutig und nicht von außen erreichbar.

Hängt die TrutzBox z. B. über eine Mobilfunkverbindung am Internet, ist sie über VPN meist nicht erreichbar. An einem „Dual-Stack Lite“-Anschluss ist sie über IPv4 gar nicht erreichbar; TrutzVPN lässt sich dort nur über IPv6 nutzen (siehe Abschnitt „Erreichbarkeit der TrutzBox-Dienste über IPv6“).
Welche Anschlussarten von außen erreichbar sind, fasst der Abschnitt „Welche Anschlüsse von außen erreichbar sind“ im Kapitel „TrutzDynDNS: Erreichbarkeit aus dem Internet“ zusammen.

TrutzBox auf Fernzugriff vorbereiten und Internet-Router freischalten

Um von unterwegs, z. B. Hotel, auf die TrutzBox zugreifen zu können, muss das Netz, an dem die TrutzBox angeschlossen ist, über einen Domain-Namen erreichbar sein.
Da das VPN-Zertifikat auf den Domain-Namen ausgestellt wird, kann man erst nachdem ein Domain-Name angegeben wurde, den Fernzugriff auf die TrutzBox aktivieren.

Die eingesetzte VPN Lösung auf der TrutzBox (VPN-Server) basiert auf OpenVPN. Um VPN (Fernzugriff) nutzen zu können, müssen auf der TrutzBox unter „Netzwerk“ → Fernzugriff“ zunächst zwei Schritte durchgeführt werden:

1. „TrutzDynDNS“ aktivieren, das Zertifikat muss für den VPN Zugriff nicht aktiviert werden.
2. „VPN-Server aktivieren und warten, bis die VPN-Server-Schlüssel generiert wurden
Bei der Aktivierung des Fernzugriffs wird der VPN-Server auf der TrutzBox eingerichtet. Dabei wird auch ein sicherer OpenVPN-Server-Schlüssel auf der TrutzBox generiert (Dauer ca. 15 Sekunden).

Um auf die TrutzBox von außen über das VPN-Protokoll zugreifen zu können, muss auf dem Internet-Router der UDP-Port 1194 (TrutzBox-VPN Portfreigabe) zur TrutzBox weitergeleitet werden.
Als zweiter Tunnel steht WireGuard zur Wahl; beide teilen sich UDP-Port 1194, und es läuft immer nur einer von ihnen (siehe Abschnitt „Zweiter Tunnel: WireGuard“).

Die Fernzugriff-Seite im Detail

Die Seite „Fernzugriff“ ist in mehrere Abschnitte gegliedert. Der VPN-Server läuft auf UDP/1194 und verwendet moderne Verschlüsselung (EC P-256, tls-crypt-v2, AES-256-GCM, TLS 1.3). tls-crypt-v2 ist dabei eine OpenVPN-Funktion, die den TLS-Handshake zusätzlich mit einem eigenen Schlüssel je Client verschleiert und schützt; das verbirgt den VPN-Zugang vor Scannern und erschwert Überlastungsangriffe.

- 1. Domain-Namen festlegen: Über den Schalter „TrutzDynDNS“ erhält die TrutzBox einen festen Domain-Namen unter *.mytrutzbox.de; angezeigt werden der TrutzDynDNS-Name und die erkannte IP-Adresse des Internet-Anschlusses. Darunter stehen die IPv6-Adresse und die „IPv6-Interface-ID (für Freigaben am Router)“ sowie der Schalter „TrutzDynDNS nur mit IPv6 (Anschluss ohne eigene IPv4-Adresse, DS-Lite)“ (Abschnitt „Erreichbarkeit der TrutzBox-Dienste über IPv6“); den Schalter setzt die TrutzBox auch von selbst (Abschnitt „Erreichbarkeit von außen“ im Kapitel „Status (Netzwerk)“). Unter TrutzDynDNS folgt die Karte für einen eigenen Namen (Abschnitt „Eigener Name neben TrutzDynDNS“).

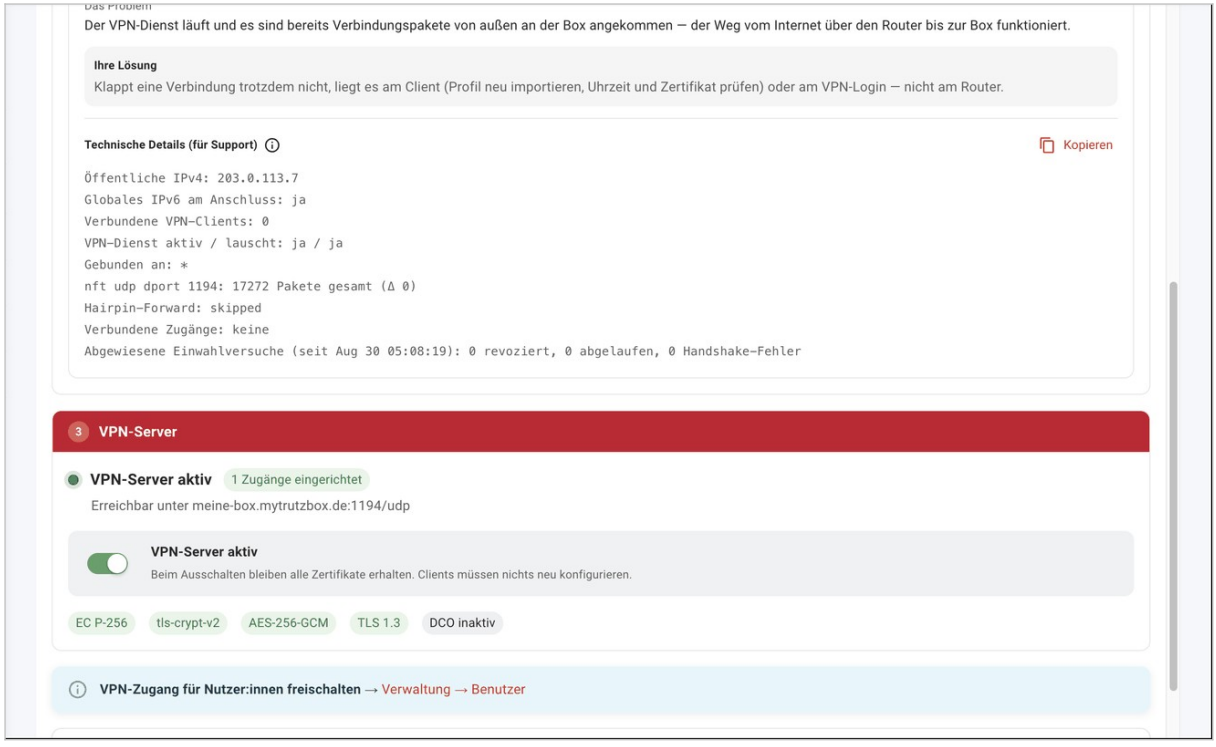
- **Erreichbarkeit prüfen:** Über „Test starten“ prüft die TrutzBox, ob sie aus dem Internet erreichbar ist, und zwar in fünf Stationen: Internet, Provider, Ihr Router, TrutzBox und VPN-Dienst. Weil sich von der Box aus nicht zuverlässig feststellen lässt, ob ein Paket von außen wirklich ankommt, wartet der Test nach dem Start auf einen echten Einwahlversuch: Die Seite fordert dazu auf, jetzt ein Gerät von außen zu verbinden, etwa ein Smartphone über Mobilfunk statt über das eigene WLAN, und zählt dabei die verbleibende Zeit herunter. Sobald der Versuch an der Box ankommt, wird die Station grün, auch wenn die Verbindung selbst noch nicht zustande kommt. So trennt der Test sauber die Frage, ob der Weg von außen überhaupt offen ist, von der Frage, ob Zertifikat und Zugangsdaten stimmen.

- **Geführte Erreichbarkeits-Diagnose:** Die Seite zeigt den Weg einer Verbindung aus dem Internet als Kette an (Internet → Provider → Ihr Router → TrutzBox → VPN-Dienst) und macht so sichtbar, an welcher Station es hängt:

- **Echter Verkehr:** Die Box misst echten Verkehr statt einer reinen Selbst-Probe. Sie prüft, ob der VPN-Dienst lauscht und ob sie über ihre eigene öffentliche Adresse zu sich selbst zurückfindet, und zählt eingehende VPN-Pakete mit.

- **Verbindung von außen:** Verbinden Sie sich dazu einmal von außen (etwa mit dem Smartphone über Mobilfunk). Steigt der Zähler oder ist ein Client verbunden, ist die Erreichbarkeit zweifelsfrei bewiesen; so lässt sich ein fehlendes Port-Forwarding im Router sicher von einem stillen Server unterscheiden.
- **Abgewiesene Einwahlen:** Die Diagnose zeigt zusätzlich die abgewiesenen Einwahlversuche der letzten sieben Tage mit Grund (gesperrtes oder abgelaufenes Zertifikat), die aktuell verbundenen Zugänge und den Hinweis, ob dieselbe Verbindungs-Kennung gleichzeitig von mehreren Geräten benutzt wurde. Beides ist wichtig, weil das abgewiesene Gerät selbst keine Fehlermeldung bekommt und weil sich Geräte mit gleicher Kennung gegenseitig ohne jede Meldung aus der Verbindung werfen.
- **Hilfetext:** Ein Hilfetext erklärt die technischen Angaben.
- **Experten-Ansicht:** Ein Schalter „Experten-Ansicht“ klappt darunter die technischen Werte auf, die sich mit einem Klick für den Support kopieren lassen: die öffentliche IPv4-Adresse, ob der Anschluss ein globales IPv6 hat, die Zahl der verbundenen Clients, ob der Dienst läuft und lauscht, die Adresse, auf der er gebunden ist, der Paketzähler der Firewall für UDP 1194 samt Zuwachs während des Tests, das Ergebnis des Hairpin-Selbsttests, die verbundenen Zugänge mit Beginn der Sitzung und schließlich die abgewiesenen Einwahlversuche seit einem genannten Zeitpunkt, aufgeschlüsselt nach gesperrtem Zertifikat, abgelaufenem Zertifikat und Handshake-Fehler.

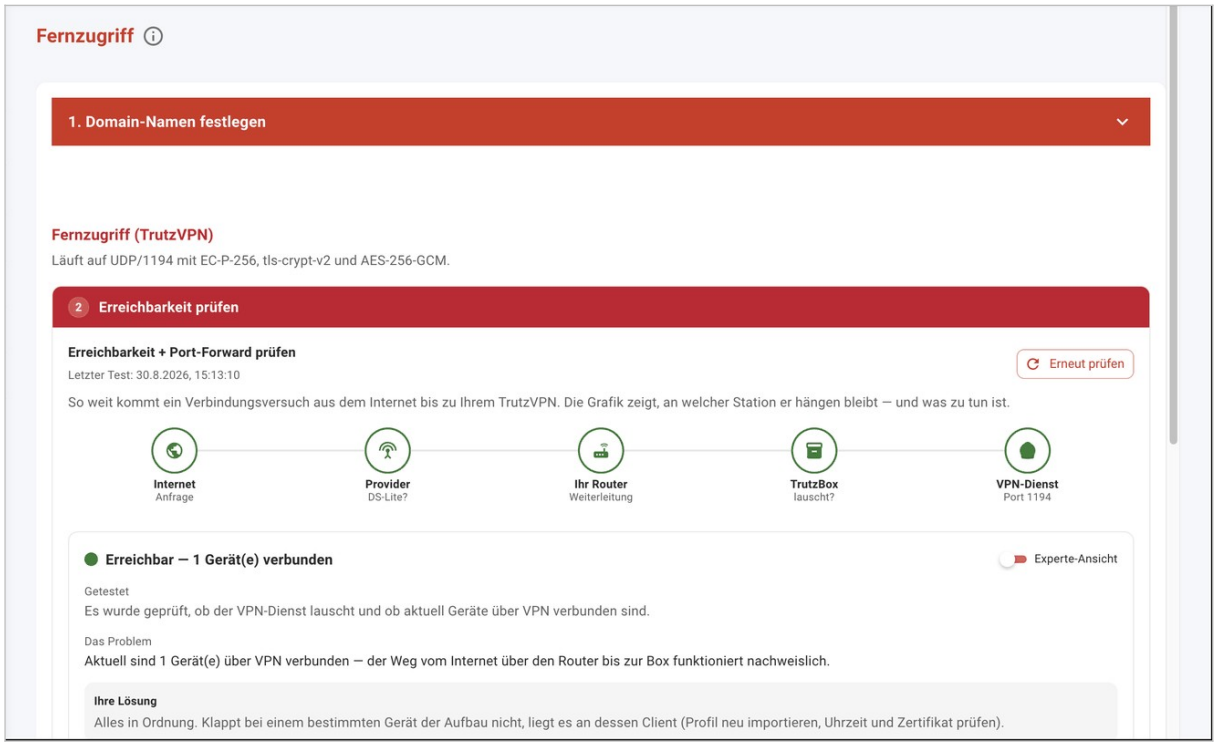
Menüpfad: Netzwerk → Fernzugriff



Die Experten-Ansicht mit den technischen Werten für den Support.
(© 2026 Comidio GmbH)

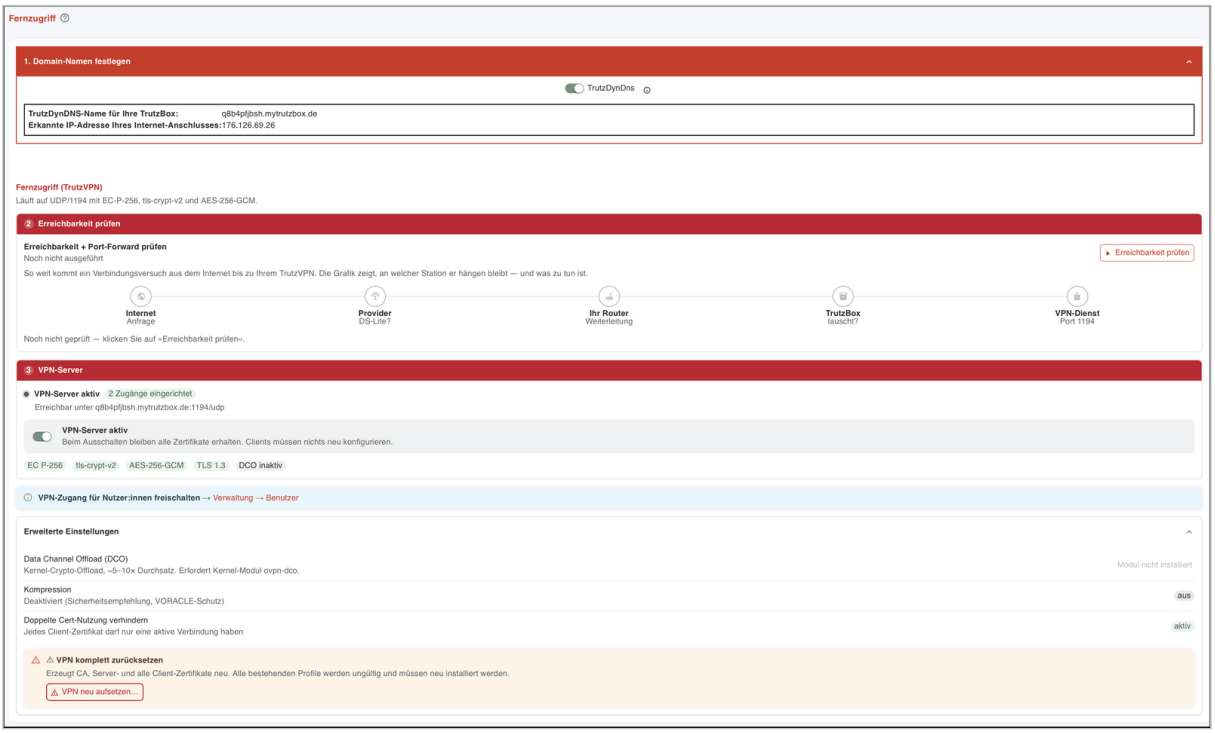
- **VPN-Server:** zeigt den Status (z. B. „VPN-Server aktiv, 1 Client verbunden“) und die Adresse, unter der der Server erreichbar ist. Mit dem Schalter „VPN-Server aktiv“ wird der Dienst ein- oder ausgeschaltet; beim Ausschalten bleiben alle Zertifikate erhalten, sodass Clients nichts neu konfigurieren müssen. Der Hinweis „VPN-Zugang für Nutzer freischalten“ verweist auf „Verwaltung → Benutzer“, wo der Zugang je Benutzer aktiviert wird. Kurze Aussetzer der Internetleitung führen nicht sofort zum Verbindungsabbruch: Die TrutzBox wartet bis zu zwei Minuten, bevor sie eine VPN-Verbindung für tot erklärt und neu aufbaut.
- **Erweiterte Einstellungen:** „VPN auch über IPv6 anbieten“ (ab Werk aus; nur schaltbar, wenn der VPN-Server läuft und die Box eine globale IPv6-Adresse hat; Einzelheiten im Abschnitt „Erreichbarkeit der TrutzBox-Dienste über IPv6“), „Data Channel Offload (DCO)“ (Kernel-Crypto-Offload für höheren Durchsatz; nur verfügbar, wenn das passende Kernel-Modul installiert ist), „Kompression“ (aus Sicherheitsgründen standardmäßig deaktiviert) und „Doppelte Cert-Nutzung verhindern“ (jedes Client-Zertifikat darf nur eine aktive Verbindung haben). Über „VPN neu aufsetzen…“ lassen sich CA-, Server- und alle Client-Zertifikate neu erzeugen; alle bestehenden Profile werden dadurch ungültig und müssen neu installiert werden.

Menüpfad: Netzwerk → Fernzugriff



Die Erreichbarkeits-Diagnose zeigt in fünf Stationen, an welcher Stelle der Fernzugriff hängt. (© 2026 Comidio GmbH)

Menüpfad: Netzwerk → Fernzugriff



Die erweiterten VPN-Einstellungen mit Offload, Kompression und doppelter Zertifikatsnutzung.
(© 2026 Comidio GmbH)

Zweiter Tunnel: WireGuard

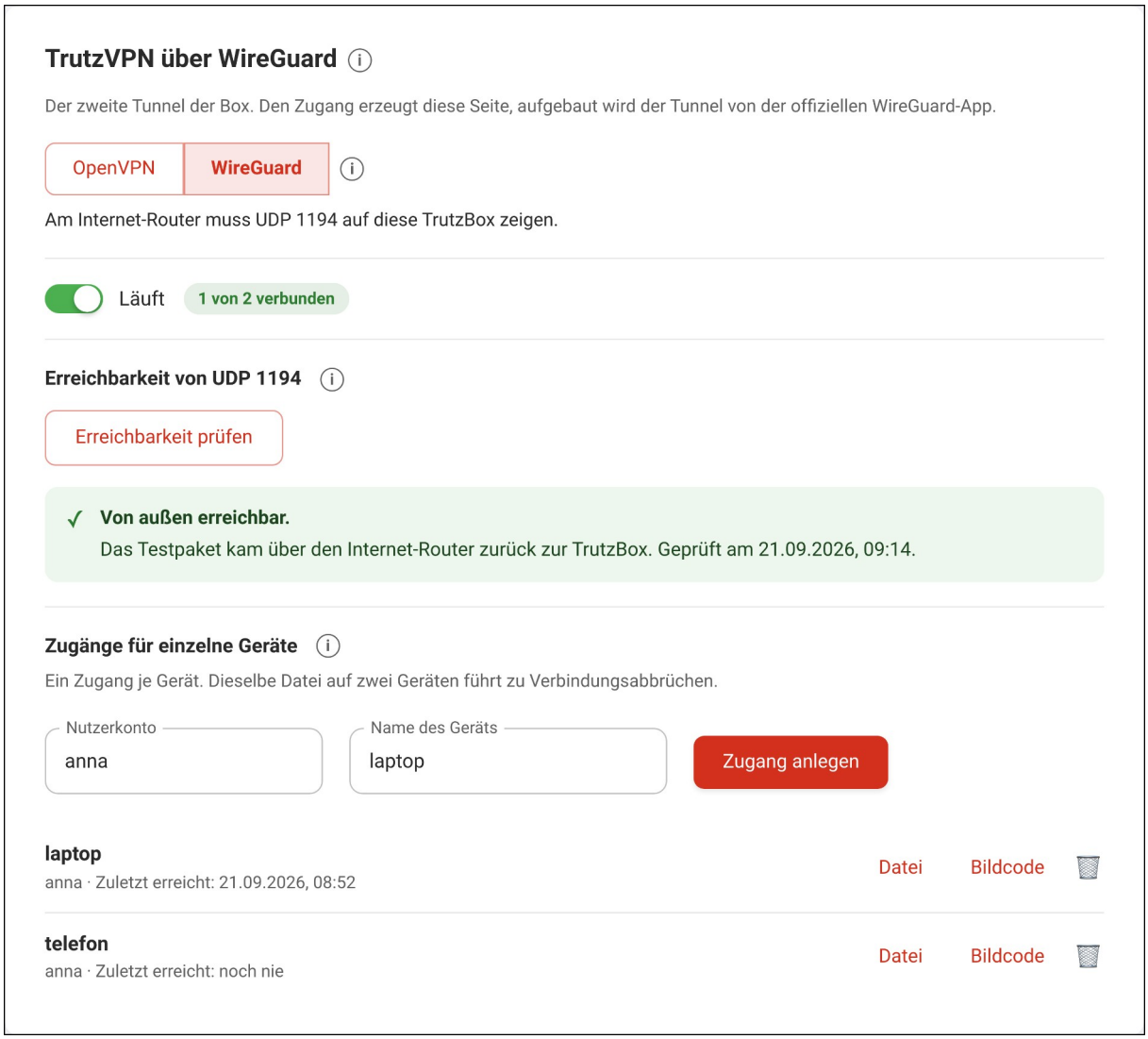
Neben OpenVPN bietet die TrutzBox seit September 2026 einen zweiten Tunnel an: WireGuard. WireGuard ist deutlich schlanker als OpenVPN, baut eine Verbindung nach einem Netzwechsel, etwa vom WLAN in den Mobilfunk, in wenigen Sekunden neu auf und schont auf Telefonen den Akku. Beide Tunnel verschlüsseln gleich stark. WireGuard verwendet dabei feste, moderne Verfahren (Curve25519 für den Schlüsselaustausch, ChaCha20-Poly1305 für die Daten), statt sie mit jeder Gegenstelle auszuhandeln.

Ein Anschluss, immer nur ein Tunnel: Beide Tunnel benutzen denselben Anschluss, UDP-Port 1194. Die Portweiterleitung im Internet-Router bleibt beim Wechsel deshalb unverändert, ebenso eine IPv6-Freigabe. Weil ein Anschluss nur einem Dienst gehören kann, läuft immer genau einer der beiden Tunnel. Welcher, bestimmt der Umschalter oben in der Karte „TrutzVPN über WireGuard“ auf der Seite „Fernzugriff“. Ab Werk läuft OpenVPN, damit bestehende Profile weiter funktionieren.

Was beim Umschalten geschieht: Beim ersten Wechsel auf WireGuard richtet die Box den Tunnel selbst ein. Sie erzeugt ein Schlüsselpaar für den Server, legt das Tunnelnetz 10.9.0.0/24 an und installiert bei Bedarf das Werkzeug wireguard-tools aus dem TrutzBox-Repository. Erst danach hält sie OpenVPN an und übergibt den Anschluss. Kommt WireGuard nicht hoch, startet OpenVPN sofort wieder, sodass nie eine Lücke ohne Fernzugriff entsteht. Gelöscht wird beim Umschalten nichts: Ausgestellte OpenVPN-Profile und angelegte WireGuard-Zugänge bleiben erhalten und gelten wieder, sobald zurückgeschaltet wird. Solange WireGuard läuft, kommen OpenVPN-Profile allerdings nicht durch, und

umgekehrt. Läuft die Sitzung, in der umgeschaltet wird, selbst über einen der beiden Tunnel, warnt die Oberfläche vorher, denn mit dem Umschalten bricht genau diese Verbindung ab.

Menüpfad: Netzwerk → Fernzugriff



Die Karte „TrutzVPN über WireGuard“: Umschalter, Zustand, Erreichbarkeitsprüfung und die Zugänge der einzelnen Geräte.
(© 2026 Comidio GmbH)

Zugänge für einzelne Geräte: WireGuard kennt keine Anmeldung mit Nutzername und Kennwort. Jedes Gerät trägt stattdessen ein eigenes Schlüsselpaar. Den Zugang legt der Administrator in der Karte unter „Zugänge für einzelne Geräte“ an: Nutzerkonto wählen, Namen des Geräts eintragen, „Zugang anlegen“. Die Box erzeugt dazu das Schlüsselpaar und eine feste Adresse im Tunnelnetz und zeigt die fertige Konfiguration auf zwei Wegen: als Bildcode, den die WireGuard-App auf Telefonen direkt einliest, und als Datei (.conf), die sich am Rechner importieren lässt. Der Zugang bleibt gespeichert und lässt sich jederzeit erneut anzeigen oder entfernen; entfernt verliert nur dieses eine Gerät den Zugang.

Eine Konfiguration gehört zu genau einem Gerät. Steckt dieselbe Datei in zwei Geräten, beanspruchen beide dieselbe Adresse im Tunnel, und die Verbindungen reißen ständig ab.

Menüpfad: Netzwerk → Fernzugriff



Der Zugang eines Geräts: Bildcode für das Telefon, derselbe Inhalt als Text, dazu die Datei für den Rechner.
(© 2026 Comidio GmbH)

Der Text eines Zugangs enthält den geheimen Schlüssel des Geräts. Er gehört deshalb weder in eine Mail noch in einen Chat; der Dialog weist ausdrücklich darauf hin. Der geheime Schlüssel des Servers verlässt die Box nie.

Erreichbarkeit prüfen: Die Karte hat eine eigene Prüfung, die derselben Kette folgt wie die Erreichbarkeits-Diagnose von OpenVPN. Die Box schickt sich selbst ein Testpaket über den Internet-Router auf UDP-Port 1194 und zählt an der Firewall, ob es zurückkommt. Das ist bei WireGuard besonders wichtig, weil die WireGuard-App bei einem Fehlschlag keine Meldung zeigt, sondern still weiter versucht. Kommt das Paket nicht zurück, prüft die Box zusätzlich einen zweiten, am Router freigegebenen Anschluss. Kommt der durch, zeigt die Weiterleitung von UDP-Port 1194 auf ein anderes Gerät, etwa auf eine zweite TrutzBox am selben Router. Kommt auch der nicht durch, kann der Router seine eigene öffentliche Adresse aus dem lokalen Netz nicht erreichen (fehlendes Hairpin-NAT); dann entscheidet nur ein Versuch von außen, etwa über Mobilfunk. Nach dem Umschalten auf WireGuard startet die Prüfung von selbst.

Firewall: UDP-Port 1194 steht in der Firewall der TrutzBox nur offen, solange einer der beiden Tunnel tatsächlich läuft. Beim Umschalten wandert die Freigabe mit; ein angehaltener Tunnel hinterlässt keinen offenen Port.

Auf den Geräten: Den Tunnel baut auf jedem Gerät die offizielle, kostenlose WireGuard-App auf: für Windows von wireguard.com, für macOS, iPhone und iPad aus dem App Store, für Android aus dem

Play Store. Unter Linux genügt das Paket wireguard. Die Schritte je System beschreibt das TrutzBox-Handbuch im Abschnitt „Ihre Geräte einrichten“.
Grenzen: Anders als OpenVPN führt WireGuard keine Sperrliste abgelaufener Zertifikate; ein verlorenes Gerät wird gesperrt, indem sein Zugang in der Karte entfernt wird. Für den Weg über IPv6 gilt dasselbe wie bei OpenVPN: Er braucht eine IPv6-Freigabe für UDP-Port 1194 auf die Interface-ID der TrutzBox (siehe Abschnitt „Erreichbarkeit der TrutzBox-Dienste über IPv6“).
Eigener Name: Wie die TrutzBox neben dem TrutzDynDNS-Namen auch unter einem eigenen Namen erreichbar wird, steht im Abschnitt „Eigener Name neben TrutzDynDNS“ im Kapitel „TrutzDynDNS: Erreichbarkeit aus dem Internet“.

Sonderfall: VPN aus dem eigenen Netz heraus

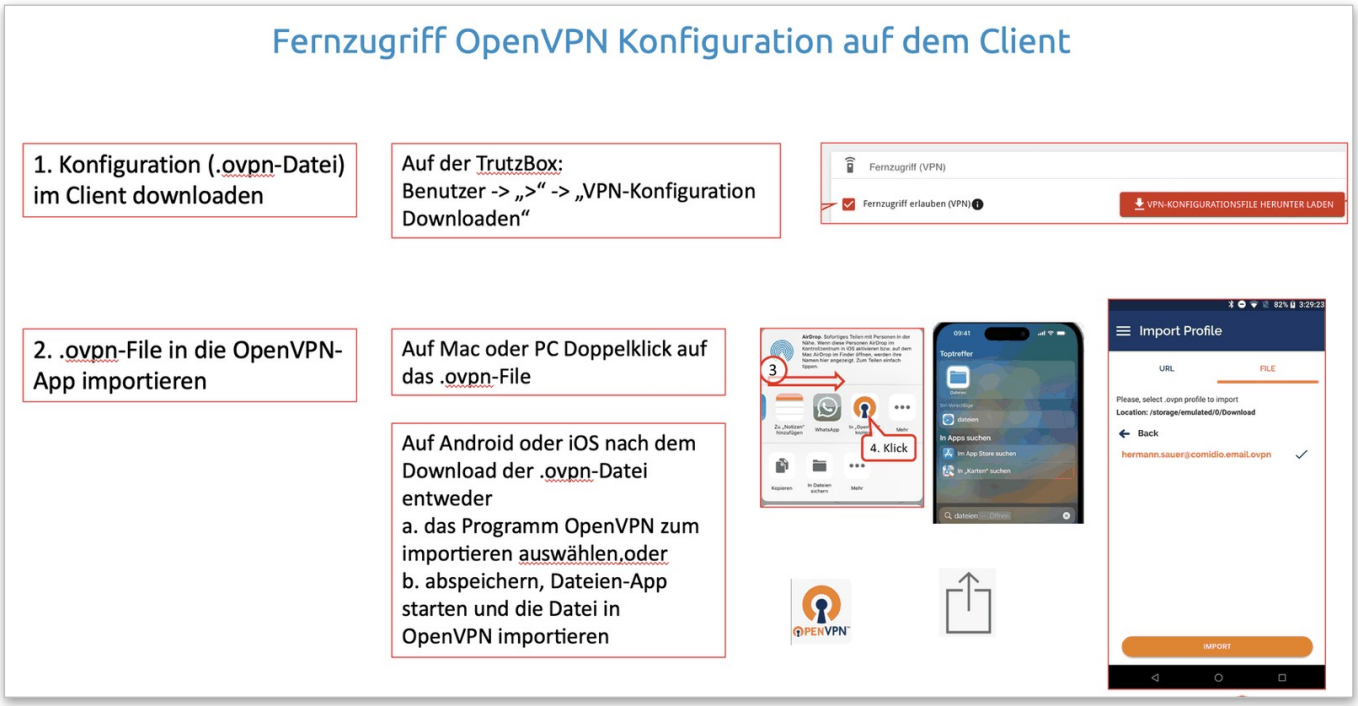
Comidio empfiehlt TrutzVPN als einfachsten Weg für mobile Geräte: Wer kein WLAN an der TrutzBox hat, müsste sonst auf jedem Gerät einen Proxy eintragen und ihn beim Verlassen des Hauses wieder herausnehmen. Ein Schalter für die VPN-Verbindung erspart das. Genau daraus ergibt sich aber eine Eigenheit, die zunächst wie ein Fehler der TrutzBox aussieht.
Das mobile Gerät ruft die TrutzBox immer über ihren öffentlichen TrutzDynDNS-Namen. Unterwegs ist das der richtige Weg. Hängt das Gerät dagegen im WLAN des Internet-Routers, also im selben Netz wie die TrutzBox, dann zeigt dieser Name auf die eigene Anschlussadresse: Das Paket verlässt den Router und muss sofort wieder hereinkommen. Fachleute nennen das Hairpin oder NAT-Loopback, weil der Weg wie eine Haarnadel kehrtmacht.
Viele Router beherrschen das für UDP nur unzuverlässig. Die Zuordnung von Adresse und Port, die der Router für die Rückrichtung führt, verfällt vorzeitig, die Antwort der TrutzBox findet den Weg zurück nicht mehr, und der VPN-Client bricht nach wenigen Sekunden ab und baut mit einem neuen Quell-Port neu auf. Auf dem Gerät sieht das nach einer stehenden Verbindung aus, tatsächlich wird sie im Sekundentakt erneuert. Dasselbe Gerät hält im Mobilfunk dagegen in der Regel über Stunden.
Daran ist weder die TrutzBox noch das VPN-Profil schuld, sondern der Router. Wer den Fall vermeiden will, hat zwei Möglichkeiten: das VPN im eigenen Netz gar nicht erst einzuschalten, dort ist das Gerät ohnehin schon hinter der TrutzBox, oder den Router so einzurichten, dass er den TrutzDynDNS-Namen intern auf die lokale Adresse der TrutzBox auflöst. Aus demselben Grund fordert die Erreichbarkeitsprüfung ausdrücklich dazu auf, für den Test ein Smartphone über Mobilfunk zu verwenden und nicht das eigene WLAN, und führt in der Experten-Ansicht einen eigenen Hairpin-Selbsttest.
Die Zugangsdateien enthalten deshalb den Netzwerknamen der Box als ersten Verbindungsweg: Hängt das Gerät im selben Router-Netz, verbindet es sich direkt über den lokalen Namen, und der Hairpin-Weg entfällt. Wird der Netzwerkname der Box später geändert, passt die TrutzBox die gespeicherten Zugangsdateien an und weist auf der Fernzugriff-Seite darauf hin, wenn Dateien nicht den aktuellen Namen tragen. Die betroffenen Nutzer laden ihre Zugangsdatei unter „Benutzer“ neu herunter und importieren sie in ihrer VPN-App neu; ein Knopf „Profile neu erzeugen“ zieht alle gespeicherten Dateien auf den aktuellen Stand.
Die Erreichbarkeit von außen muss vor der Einrichtung übrigens nicht bestätigt sein: Der Server lässt sich einrichten und anschließend mit einem Verbindungsversuch von außen prüfen. Auch ganz ohne

Zugriff von außen ist TrutzVPN sinnvoll: Geräte im selben Router-Netz erreichen die Box über ihren Netzwerknamen und laufen damit über den Filter.

Mobiles Gerät für den Fernzugriff vorbereiten

Nachdem der Fernzugriff auf der TrutzBox aktiviert wurde, steht für jeden eingerichteten TrutzBox Benutzer, der eine TrutzMail-Adresse hat, unter dem Menüpunkt „Benutzer verwalten“ eine neue Option „Fernzugriff“ zur Verfügung. Wenn diese Option für einen Benutzer aktiviert wird, bekommt der Benutzer ein OpenVPN-Client Konfigurationsdatei generiert. Das kann dann auf dem Endgerät heruntergeladen werden. Dieses OpenVPN-Konfigurationsdatei (.ovpn) kann dieser dann auf allen seinen mobilen Geräten im OpenVPN-Programm importieren.

Als VPN-Client-Programm für iPhone, Android und Windows hat sich dazu „openvpn“ (openvpn.net) und für den Mac Tunnelblick (tunnelblick.net) bewährt. Eine Liste von VPN-Clients ist hier zu finden: https://de.wikipedia.org/wiki/OpenVPN#Frontends.
Danach kann unterwegs von einem beliebigen Internet-Anschluss auf die TrutzBox im Unternehmen oder zu Hause zugegriffen und alle Funktionen der TrutzBox genutzt werden.



Die Konfigurationsdatei herunterladen und in die OpenVPN-App des Geräts importieren.
(© 2026 Comidio GmbH)

IPv6 Unterstützung

Grundsätzlich unterstützt die TrutzBox auch IPv6 auf dem externen Netzwerk. Aufgrund der Eigenarten von IPv6, gerade in Kombination mit IPv4, ist jedoch einiges zu beachten.
Dabei muss man drei Netzwerke unterscheiden:

- Die IP-Adresse des Internet-Anschlusses am Internet-Router (z. B. FRITZ!Box): hier ist IPv6 in Verbindung mit der TrutzBox nutzbar, wobei die IPv6-Adresse der Internet-Service-Provider liefert. Hat der Anschluss keine eigene öffentliche IPv4-Adresse (DS-Lite-Tunnel), ist TrutzVPN von außen nur über IPv6 nutzbar (Schalter „VPN auch über IPv6 anbieten“ und eine IPv6-Freigabe am Internet-Router); Näheres im Abschnitt „Erreichbarkeit der TrutzBox-Dienste über IPv6“ weiter unten.
- Internes Netzwerk, also Ihre Geräte, die mit dem Internet-Router verbunden sind. Dazu gehört dann auch die TrutzBox, die per LAN-Kabel an den Internet-Router angeschlossen wird. Hier kann die TrutzBox vom Internet-Router eine IPv6-Adresse bekommen, was uneingeschränkt funktioniert. Geräte, die die TrutzBox nutzen sollen, können am internen Netzwerk verbleiben (also am Internet-Router, „Proxy-Modus“). Diese Geräte können auch eine IPv6-Adresse bekommen. Da die TrutzBox unter IPv6 den Hostnamen eines angeschlossenen Geräts in der Regel nicht ermitteln kann, empfiehlt Comidio, Geräte im Proxy-Modus mit IPv4 zu betreiben (kann i.d.R. im angeschlossenen Gerät eingestellt werden).
- Da die TrutzBox wie ein Router funktioniert, können auch Geräte an das interne TrutzBox-Netzwerk angeschlossen werden (Transparent-Modus). In diesem Fall muss in dem angeschlossenen Gerät kein Proxy konfiguriert werden. Geräte die am TrutzBox internen Netzwerk angeschlossen sind, werden im „Transparent-Modus“ betrieben. Da die TrutzBox lediglich IPv4 Adressen auf ihrem internen Netzwerk vergibt, können solche Geräte nur mit IPv4 betrieben werden.

Um das Thema IPv6-Unterstützung etwas einfacher zusammenzufassen, gilt Folgendes: Die IP-Adresse des Internet-Service-Providers kann eine IPv6-Adresse sein. Für den Betrieb mit der TrutzBox empfiehlt Comidio im internen Netzwerk IPv4, da Geräteerkennung und Filterung darauf ausgelegt sind.

Erreichbarkeit der TrutzBox-Dienste über IPv6

Bezieht die TrutzBox an ihrem externen Netzwerk eine globale IPv6-Adresse (eine sogenannte GUA, die ihr der Internet-Router aus dem Präfix des Providers zuweist), so sind ihre nach außen angebotenen Dienste (Videokonferenz und Chat, auf Wunsch auch der Fernzugriff per TrutzVPN) nicht nur über IPv4, sondern auch direkt über IPv6 erreichbar. Anders als bei IPv4 gibt es unter IPv6 keine Adressumsetzung (kein NAT): Die globale Adresse der TrutzBox ist zugleich ihre öffentlich erreichbare Adresse, eine Portweiterleitung im klassischen Sinn entfällt.
Das Nötige erledigt die TrutzBox weitgehend selbst: TrutzDynDNS veröffentlicht neben der IPv4-Adresse (A-Eintrag) automatisch auch die IPv6-Adresse (AAAA-Eintrag), damit der feste Domainname auch unter IPv6 auf die TrutzBox zeigt. Das gilt, solange die Prüfung der Erreichbarkeit von außen nichts anderes ergibt (Abschnitt „Erreichbarkeit von außen“ im Kapitel „Status (Netzwerk)“). Der Videokonferenz-Server bietet seine globale IPv6-Adresse als Medien-Kandidaten an, sodass auch Teilnehmer, die nur über IPv6 verfügen, nicht nur die Signalisierung, sondern auch Ton und Bild erhalten.
TrutzVPN nutzt diesen Weg nur auf Wunsch: Der VPN-Server nimmt Verbindungen zwar immer über IPv4 und IPv6 an, welchen Weg eine VPN-App wählt, legt aber ihre Zugangsdatei (.ovpn) fest. Darin stehen mehrere Adresszeilen, die die App der Reihe nach probiert. Ab Werk sind es zwei, beide über IPv4: zuerst der Netzwerkname der Box im lokalen Netz, dann der TrutzDynDNS-Name. Mit dem

Schalter „VPN auch über IPv6 anbieten“ (Netzwerk → Fernzugriff, aufklappbarer Bereich „Erweiterte Einstellungen“, erste Zeile) kommt an zweiter Stelle der TrutzDynDNS-Name über IPv6 hinzu, der TrutzDynDNS-Name über IPv4 rückt als Rückfall an die dritte Stelle. Im lokalen Netz verbindet die App deshalb weiterhin über IPv4 und den Netzwerknamen; den IPv6-Weg nimmt sie nur unterwegs, etwa im Mobilfunk, der IPv6 bevorzugt. Der Tunnel selbst bleibt in jedem Fall IPv4 (Adressbereich 10.8.0.0/24), IPv6 ist nur der Transportweg bis zur Box.

Der Schalter ist ab Werk aus. Umlegen lässt er sich nur, wenn der VPN-Server läuft und die Box eine globale IPv6-Adresse hat; fehlt diese, steht dort „Nicht verfügbar: Die Box hat keine globale IPv6-Adresse.“ Beim Umschalten schreibt die TrutzBox alle Zugangsdateien neu. Profile, die bereits in eine VPN-App importiert sind, bleiben davon unberührt: Jeder Nutzer lädt seine Zugangsdatei unter „Verwaltung → Benutzer“ neu herunter, löscht in der App das alte Profil und importiert das neue. Einschalten sollte man ihn erst, wenn am Internet-Router die IPv6-Freigabe für UDP-Port 1194 eingerichtet ist (siehe nächster Absatz). Fehlt sie, probieren Smartphones zuerst die IPv6-Zeile und fallen erst nach bis zu einer Minute auf IPv4 zurück. TrutzDynDNS veröffentlicht die Adressen so, wie die TrutzBox sie meldet. Ob die IPv6-Adresse von außen erreichbar ist, prüft die TrutzBox selbst (Abschnitt „Erreichbarkeit von außen“ im Kapitel „Status (Netzwerk)“); kommt über IPv6 bei keinem Dienst etwas an, meldet sie nur noch die IPv4-Adresse. Dass der Schalter nicht von vornherein an ist, hat einen Grund: OpenVPN Connect bricht auf iPhone und iPad bei einer IPv6-Zeile ohne erreichbares Ziel teils ganz ab. Ob TrutzVPN auch über IPv6 angeboten wird, entscheidet deshalb der Administrator.

Eine Voraussetzung verbleibt beim Anwender: Am Internet-Router muss die IPv6-Firewall die TrutzBox für die benötigten Ports nach außen öffnen. Benötigt werden diese Freigaben (Videokonferenz: TCP-Port 443 und UDP-Port 9083, ohne Umleitung auf Port 9082 wie unter IPv4; Fernzugriff: UDP-Port 1194). Für TrutzVPN kommt die IPv6-Freigabe zur bestehenden IPv4-Portweiterleitung von UDP-Port 1194 hinzu. Die Interface-ID ist die hintere Hälfte der IPv6-Adresse. Sie wird nach dem Verfahren EUI-64 aus der Hardware-Adresse der Box gebildet, bleibt also gleich, wenn der Provider die vordere Hälfte (das Präfix) wechselt, und steht auf der Seite „Fernzugriff“ im Domain-Bereich als „IPv6-Interface-ID (für Freigaben am Router)“. Wie die Freigabe in einer FRITZ!Box angelegt wird, zeigt die folgende Schrittfolge. Gerade an Anschlüssen ohne echte öffentliche IPv4-Adresse (etwa bei DS-Lite, wo eingehende IPv4-Verbindungen gar nicht möglich sind) ermöglicht erst dieser IPv6-Weg den Zugang von außen zur Videokonferenz und zu TrutzVPN. Unterwegs gelingt die VPN-Verbindung dann allerdings nur aus Netzen, die selbst IPv6 bieten: im Mobilfunk meist, in manchen Hotel- und Gäste-WLANs dagegen nicht, weil sie nur IPv4 kennen. Als Alternative bleibt eine echte öffentliche IPv4-Adresse, die viele Anbieter auf Anfrage einrichten.

Schrittfolge für eine FRITZ!Box (FRITZ!OS 7.5 und neuer; ältere Fassungen führen zum selben Ziel, die Menüpunkte heißen teils anders):

1. In der Benutzeroberfläche der FRITZ!Box „Internet“ öffnen, dann „Freigaben“ und den Reiter „Portfreigaben“.
2. „Gerät für Freigaben hinzufügen“ anklicken und die TrutzBox aus der Liste wählen. Steht sie dort mehrfach, zählt der Eintrag mit der Adresse, die im lokalen Netz zur TrutzBox gehört.
3. Im Feld „IPv6-Interface-ID“ den Wert von der Seite „Fernzugriff“ eintragen. Die FRITZ!Box schlägt sonst eine eigene Kennung vor; sie muss mit dem Wert der TrutzBox überschrieben werden, sonst zeigt die Freigabe ins Leere.

4. „Neue Freigabe“ anklicken, „Freigabe für andere Anwendungen“ wählen, Protokoll und Port eintragen und den Haken „Internetzugriff über IPv6“ setzen: für TrutzVPN UDP 1194 (oder der eingetragene „Port von außen für VPN“), für Videokonferenz und Chat als zwei weitere Freigaben TCP 443 und UDP 9083, ohne Umleitung auf einen anderen Port.
5. Mit „OK“ und „Übernehmen“ sichern.

Der grüne Punkt neben der Freigabe sagt nur, dass die Regel aktiv ist, nicht, dass die TrutzBox von außen antwortet; das zeigt erst die Erreichbarkeitsprüfung oder ein Verbindungsversuch über Mobilfunk. Eine zweite TrutzBox am selben Router bekommt eine eigene Freigabe mit ihrer eigenen Interface-ID; beide dürfen denselben Port benutzen, weil IPv6 ohne Umsetzung auf eine gemeinsame Adresse auskommt.

Anschluss ohne eigene IPv4-Adresse (DS-Lite): Hier hilft der Schalter „TrutzDynDNS nur mit IPv6“. Wie er arbeitet und wann die TrutzBox ihn selbst setzt, beschreibt der Abschnitt „Nur IPv6 oder nur IPv4 veröffentlichen“ im Kapitel „TrutzDynDNS: Erreichbarkeit aus dem Internet“.

Mehrere TrutzBoxen hinter einem Router: Sie teilen sich die öffentliche IPv4-Adresse des Anschlusses, und UDP-Port 1194 lässt sich über IPv4 nur an eine von ihnen weiterleiten. Jede weitere TrutzBox ist von außen nur über IPv6 erreichbar: Bei ihr muss der Schalter „VPN auch über IPv6 anbieten“ eingeschaltet sein, und sie braucht am Router eine eigene IPv6-Freigabe mit ihrer eigenen Interface-ID. Landet ein Profil über IPv4 trotzdem bei der falschen Box, weist diese es ab, ohne dass die VPN-App eine verständliche Fehlermeldung zeigt.

TrutzBox an einem reinen IPv6-Anschluss

Die zuvor beschriebene Erreichbarkeit über IPv6 betrifft den Weg von außen zur TrutzBox, also ihre eigenen Dienste. Davon zu unterscheiden ist der entgegengesetzte Weg: Für die angeschlossenen Geräte baut die TrutzBox die Verbindungen zu den Internet-Servern selbst auf und filtert sie dabei (TrutzContent und TrutzBrowse). Das interne Netzwerk bleibt dabei IPv4; die Geräte erreichen den Proxy also unverändert.

Solange der Internet-Anschluss in irgendeiner Form IPv4 bereitstellt (bei üblichen Anschlüssen mit Dual-Stack oder DS-Lite praktisch immer der Fall), arbeitet der Proxy unverändert weiter. Die IPv6-Erreichbarkeit der Box-Dienste ändert daran nichts.

Anders verhält es sich, wenn die TrutzBox ausschließlich eine IPv6-Adresse erhält und gar kein IPv4 mehr zur Verfügung steht: Ein großer Teil der Internet-Server ist weiterhin nur über IPv4 erreichbar. Um diese von einer reinen IPv6-Box aus zu erreichen, wäre eine Übersetzung im Netz (NAT64/DNS64) nötig, die die TrutzBox selbst nicht vornimmt. Der Proxy käme dann nur noch an rein IPv6-fähige Ziele; ein reiner IPv6-Anschluss wird daher derzeit nicht unterstützt.

Für den Mobilfunk-Betrieb ist das in der Regel unkritisch: Hängt die TrutzBox hinter einem LTE- oder 5G-Router bzw. einem Hotspot, übersetzen diese Geräte intern (Stichwort 464XLAT) und geben der TrutzBox ein normales IPv4-Netzwerk, auch wenn der Mobilfunk-Anschluss nach außen nur IPv6 nutzt. Die Einschränkung greift erst, wenn die TrutzBox direkt, ohne einen solchen Router, eine reine IPv6-Adresse bekäme.

16.15 Portübersicht: was der Internet-Router durchlassen muss

Die TrutzBox kommt mit wenigen Verbindungen nach außen aus, und die meisten Internet-Router lassen ausgehende Verbindungen ohnehin ungehindert durch. Die folgende Übersicht ist für zwei Fälle gedacht: Am Router sind ausgehende Verbindungen eingeschränkt, etwa über eine Kindersicherung oder eigene Filterregeln, oder eine Funktion der TrutzBox soll von unterwegs erreichbar sein.
Ausgehend, von der TrutzBox ins Internet:

Port	Wofür
53 (UDP und TCP)	Namensauflösung über den Internet-Router. Ist die verschlüsselte Weiterleitung eingeschaltet, laufen darüber nur noch kurze Gerätenamen, die Namen im Netz des Routers (etwa fritz.box) und der Rückfall, wenn DoT gerade nicht funktioniert.
853 (TCP)	Verschlüsselte Namensauflösung (DoT) zum gewählten DNS-Anbieter, ab Werk DNS4EU. Sperrt der Router diesen Port, löst die TrutzBox unverschlüsselt auf und meldet das im Betriebszustand.
123 (UDP)	Abgleich der Uhrzeit (NTP).
4460 (TCP)	Schlüsselaustausch für die verschlüsselte Uhrzeit (NTS) mit der Physikalisch-Technischen Bundesanstalt und Netnod.
80 und 443 (TCP)	Software-Updates, Filterlisten und die Verbindung zum Kontoserver von Comidio (Vertrag, TrutzDynDNS, Zertifikate).
43 (TCP)	Auskunft über den Inhaber eines Servers im Monitor (WHOIS).
je nach Anbieter, meist 465 oder 587 (TCP)	Versand an normale E-Mail-Adressen über das Mail-Konto, das für einen Benutzer hinterlegt ist.
wechselnd, meist 443 und 9001 (TCP)	Tor-Netzwerk: Anonymität für Geräte, die über Tor surfen, sowie TrutzMail und TrutzChat zwischen TrutzBoxen.

(© 2026 Comidio GmbH)

Eingehend, vom Internet auf die TrutzBox. Freigaben braucht es nur für Funktionen, die von außen genutzt werden; eingerichtet werden sie am Internet-Router:

Funktion	Freigabe am Internet-Router
Fernzugriff (TrutzVPN)	UDP-Port 1194 an die TrutzBox weiterleiten. Für TrutzVPN über IPv6 (Schalter „VPN auch über IPv6 anbieten“ an) zusätzlich eine IPv6-Freigabe für UDP-Port 1194 auf die Interface-ID der TrutzBox einrichten. Denselben Port nutzt WireGuard, wenn es statt OpenVPN läuft; aktiv ist immer nur einer der beiden Tunnel. Ist unter „Fernzugriff“ ein anderer „Port von außen für VPN“ eingetragen, nennen die Zugangsdateien diesen Port, die Freigabe am Router lautet auf ihn, und die Firewall der TrutzBox leitet ihn auf den Tunnel-Port um, unter IPv4 wie unter IPv6.
Videokonferenz von außen	TCP-Port 443 (extern) auf Port 9082 der TrutzBox und UDP-Port 9083 auf Port 9083 weiterleiten. Unter IPv6 genügt es, TCP 443 und UDP 9083 in der IPv6-Firewall des Routers für die TrutzBox zu öffnen, ohne Umleitung auf Port 9082. Die Freigabe macht auch die Chat-Anmeldung (XMPP) mit dem TrutzMail-Passwort aus dem Internet erreichbar, die der Angriffsschutz bewacht; die Chat-Oberfläche /chat/ gibt sie nicht frei.
Chat und E-Mail von unterwegs	Keine eigene Freigabe. Web-Chat, Chat-Programme und Mail-Programme erreichen die TrutzBox von unterwegs über den Fernzugriff (VPN); Port 5222 wird am Router nicht freigegeben. Wer die Mail-Ports 993, 465 oder 587 trotzdem freigibt, dessen Mail-Anmeldungen bewacht der Angriffsschutz („trutzmail-auth“).
TrutzMail und TrutzChat zwischen TrutzBoxen	Keine Freigabe nötig, beides läuft über das Tor-Netzwerk.
Finden im lokalen Netz (mDNS)	Keine Freigabe. mDNS (UDP-Port 5353 an die Multicast-Adresse 224.0.0.251) bleibt im lokalen Netz, der Router gibt es nicht ins Internet weiter. Die Firewall der TrutzBox lässt es aus dem internen Netz und aus dem Netz des Routers zu, damit Geräte die TrutzBox unter trutzbox.local finden (Abschnitt „Die TrutzBox im Netz finden: trutzbox.local (mDNS)“).

(© 2026 Comidio GmbH)

Geräte im internen Netz dürfen verschlüsselte Namensauflösung (DoT auf Port 853 und DNS über HTTPS zu bekannten Anbietern) absichtlich nicht selbst nutzen, damit sie die Filter der TrutzBox nicht umgehen (siehe Abschnitt „DNS-Auflösung“). Ob der Router Port 853 durchlässt, lässt sich deshalb nicht von einem Gerät im internen Netz aus prüfen. Auskunft gibt die Karte „DNS für Geräte“ im Betriebszustand.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

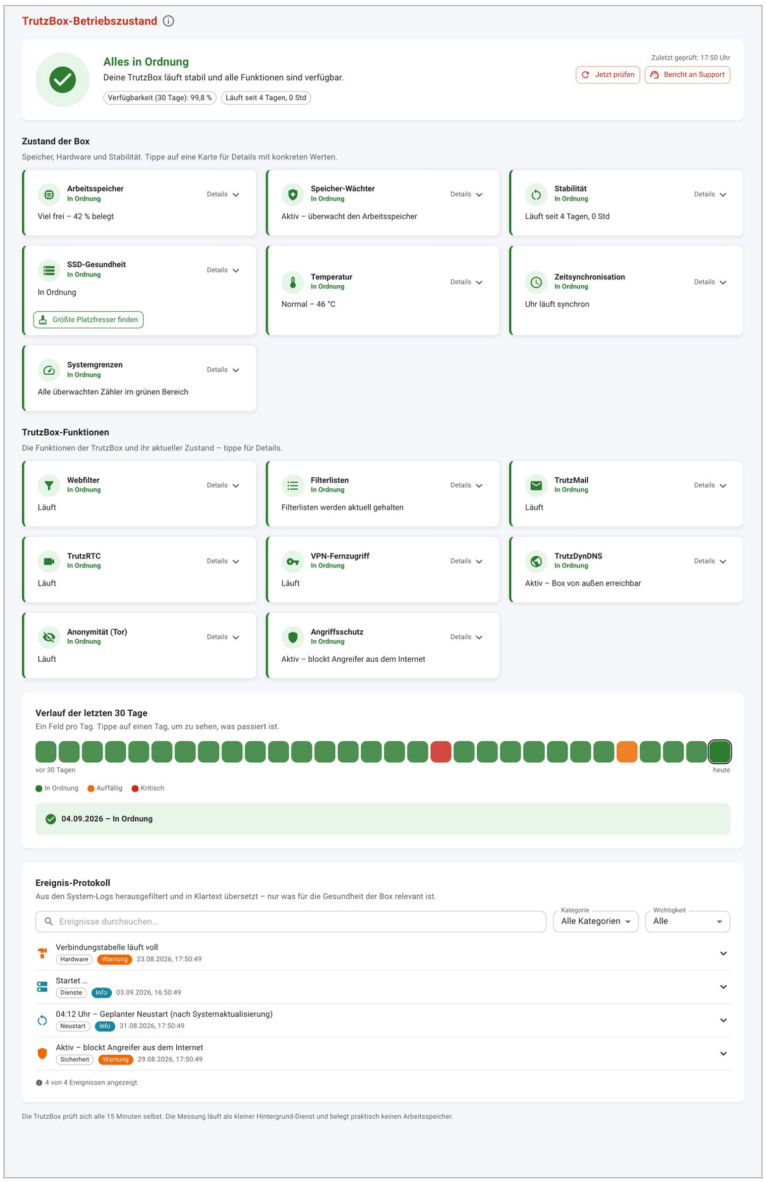
17 Systemeinstellungen

17.1 TrutzBox-Betriebszustand

Die Seite „TrutzBox-Betriebszustand“ (Menü „Systemeinstellungen → Betriebszustand“) fasst auf einen Blick zusammen, ob die TrutzBox stabil läuft und alle Funktionen verfügbar sind. Sie ist als schnelle Selbstdiagnose gedacht: Statt einzelne System-Logs zu durchsuchen, sieht der Administrator hier in Klartext, ob Hardware, Speicher und die TrutzBox-Dienste in Ordnung sind.
Ganz oben zeigt ein Ampel-Status den Gesamtzustand an (z. B. „Alles in Ordnung“), zusammen mit der Verfügbarkeit der letzten 30 Tage und der Laufzeit seit dem letzten Neustart. Über „Jetzt prüfen“ lässt sich eine sofortige Überprüfung anstoßen, und mit „Ampel auf Grün stellen“ können bereits zur Kenntnis genommene Hinweise quittiert werden. „Bericht an Support“ stellt die relevanten Informationen für eine Support-Anfrage zusammen und öffnet einen Dialog, in dem sich der Bericht als Klartext einsehen, kopieren, per E-Mail-Programm versenden oder als Datei herunterladen lässt. Laufen Fernzugriff oder Videokonferenz, enthält der Bericht auch den Block „Erreichbarkeit von außen“ mit dem Ergebnis der letzten Prüfung je Dienst und Anschluss und den Angaben zum Anschluss (Abschnitt „Erreichbarkeit von außen“ im Kapitel „Status (Netzwerk)“).
Die Ampel kennt vier Zustände: grün (in Ordnung), gelb (Beachtung ratsam), rot (ein konkreter, erkennbarer Fehler) und neutral für Funktionen, die der Administrator bewusst abgeschaltet hat; eine bewusst deaktivierte Funktion zieht die Ampel also nicht auf Gelb oder Rot. Dieselbe Ampel erscheint auch in der App-Leiste jeder Admin-Seite und verlinkt auf diese Übersicht. Solange die Box Aktualisierungen einspielt oder Paketlisten holt, meldet die betroffene Kachel „aktualisiert gerade“ statt eines Fehlers. Auch eine Uhr, die sich nach dem Start noch einpendelt, gilt nicht als Störung.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Menüpfad: Systemeinstellungen → Betriebszustand



Der TrutzBox-Betriebszustand mit Ampel, Zustand der Box und den Funktionen.
(© 2026 Comidio GmbH)

Zustand der Box

Der Abschnitt „Zustand der Box“ bündelt Speicher, Hardware und Stabilität. Jede Kachel zeigt einen Kurzstatus; ein Tippen auf die Kachel öffnet die Details mit konkreten Messwerten:

- **Arbeitsspeicher:** aktuelle Auslastung des Arbeitsspeichers (Beispielwert in der Bildschirmkopie: 42 % belegt). Der Detail-Dialog schlüsselt zusätzlich den Heap-Speicher von Webfilter (Proxy) und Web-Server einzeln auf und nennt die Warnschwelle beim freien Speicher, ab der der Speicher-Wächter eingreift.

- Speicher-Wächter: überwacht den Arbeitsspeicher und hält bei Knappheit gezielt erst TrutzRTC, dann TrutzMail an, um ein Einfrieren der Box zu verhindern. Ist wieder genug Speicher frei, startet er den Dienst selbst wieder, höchstens einmal in 24 Stunden; bis dahin steht die Kachel des Dienstes neutral auf „Vom Speicher-Wächter angehalten“ statt rot. Muss er binnen eines Tages ein zweites Mal eingreifen, bleibt der Dienst aus, bis der Administrator ihn wieder einschaltet (TrutzRTC auf der Seite „Videokonferenz und Chat“, TrutzMail auf der Übersicht). Die Kachel nennt dazu den gestoppten Dienst, den freien Speicher im Moment des Eingriffs und den Zeitpunkt des Wiederanlaufs.
- **Stabilität:** Laufzeit seit dem letzten Neustart.
- **SSD-Gesundheit:** Ergebnis des SSD-Selbsttests; über „Größte Platzfresser finden“ lassen sich die speicherintensivsten Daten aufspüren (der zugehörige Dialog kann zusätzlich alte Kernel-Versionen aufräumen). Über „SSD-Details anzeigen“ öffnet sich ein Dialog mit Modell, Kapazität, Firmware, Selbsttest-Ergebnis und einzelnen SMART-Werten, jeweils mit Ampelbewertung. SMART bezeichnet die Selbstdiagnose-Werte, die moderne SSDs und Festplatten selbst führen; an ihnen lässt sich ein drohender Ausfall oft früh erkennen.
- **Temperatur:** aktuelle Betriebstemperatur der Hardware (Beispielwert in der Bildschirmkopie: 46 °C).
- **Zeitsynchronisation:** zeigt, ob die Uhr der Box synchron läuft, mit welcher Quelle sie abgeglichen wird und welche Uhrzeit die Box selbst führt. Weicht die Uhr der Box deutlich von der Uhr des Browsers ab, taucht dieser Befund auch im Support-Bericht auf.
- **Systemgrenzen:** Früherkennung für langsam volllaufende Betriebsmittel, von Datei-Handles über die Verbindungstabelle der Firewall bis zur Platten-Latenz. Details im Abschnitt „Systemgrenzen: stille Engpässe früh erkennen“ weiter unten.

TrutzBox-Funktionen

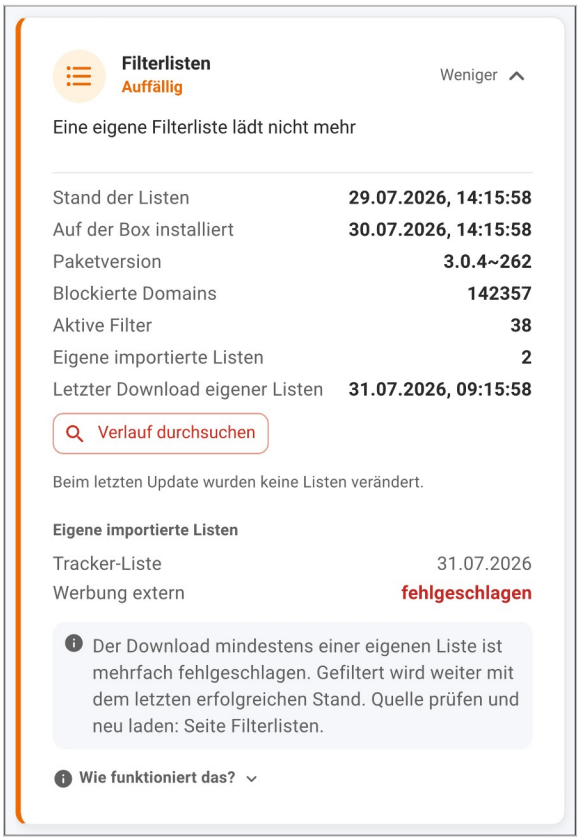
Der Abschnitt „TrutzBox-Funktionen“ zeigt für jede zentrale Funktion, ob sie aktuell läuft. Im Normalfall stehen alle auf „In Ordnung“:

- **Webfilter:** TrutzContent und TrutzBrowse, der Anonymisierungs-Proxy.
- **Filterlisten:** Sperrlisten werden aktuell gehalten. Die Kachel zeigt zusätzlich:
- **Letzte Aktualisierung:** wann die Listen zuletzt aktualisiert wurden und wie viele Listen sich dabei verändert haben.
- **Verlauf durchsuchen:** Über „Verlauf durchsuchen“ öffnet sich der Filterlisten-Verlauf. Nach Eingabe eines Listennamens zeigt er je Liste, wann sie aktualisiert wurde, wie viele Einträge sie enthält und was sich gegenüber dem vorherigen Stand geändert hat.

- **Warnung:** Bietet der Update-Server neuere Filterlisten an, die die Box seit über zwei Tagen nicht übernommen hat, warnt die Kachel orange („Neuere Filterlisten stehen bereit, sind aber nicht installiert“) und nennt „Verfügbare Version“ und „Zurück seit“; gefiltert wird unverändert weiter.
- **Überschneidung:** Im Verlauf lässt sich zu jeder eigenen importierten Liste über „Überschneidung anzeigen“ die beim letzten Update ermittelte Überschneidung mit den vorhandenen Listen abrufen.
- **TrutzMail:** der verschlüsselte E-Mail-Dienst.
- **TrutzRTC:** Videokonferenz und Chat. Die Kachel prüft zusätzlich die Videobrücke selbst: Laufen zwar alle Dienste, antwortet die Brücke aber nicht, meldet sie „Läuft, aber gestört“ samt Handlungsempfehlung (TrutzRTC aus- und wieder einschalten).
- **VPN-Fernzugriff:** sicherer Zugang zur TrutzBox von unterwegs.
- **TrutzDynDNS:** macht die Box unter einem festen Namen von außen erreichbar.
- **Anonymität (Tor):** Anbindung an das Tor-Netzwerk.
- **Angriffsschutz (fail2ban):** sperrt automatisch angreifende Internet-Adressen (Einzelheiten im Kapitel „Angriffsschutz“). Ein Detail-Dialog zeigt die gebannten Adressen mit Länderkennung und die betroffenen Angriffsziele.

Wie viel hinter einer einzelnen Kachel steckt, zeigt das Beispiel „Filterlisten“ mit aufgeklappten Details: Stand und Installationszeitpunkt der Listen, Paketversion, Zahl der blockierten Domains und der aktiven Filter, die eigenen importierten Listen mit ihrem letzten Abruf-Ergebnis, dazu „Verlauf durchsuchen“ und bei Störungen eine konkrete Handlungsempfehlung:

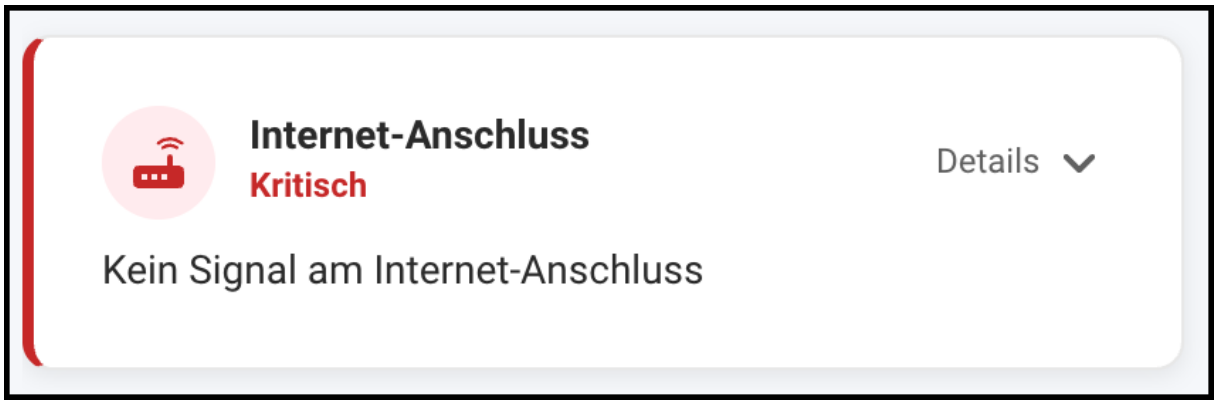
Menüpfad: Systemeinstellungen → Betriebszustand



Die Kachel „Filterlisten“ aufgeklappt, mit Stand, Paketversion und eigenen Listen.
(© 2026 Comidio GmbH)

Internet-Anschluss: der stille Wächter

Eine Karte bleibt im Normalbetrieb unsichtbar. Die Karte „Internet-Anschluss" prüft die Leitung zum Internet-Router in drei Stufen: das Signal am Anschluss, die Adressvergabe und den Router selbst sowie das Internet dahinter, wobei die Abfrage der öffentlichen Adresse für TrutzDynDNS zugleich als Prüfung dient. Solange alles in Ordnung ist, wird die Karte ausgeblendet; sie erscheint erst, wenn eine dieser Stufen ausfällt.
Der Zeitpunkt stammt dabei nicht aus dem Moment des Aufrufs, sondern aus einer eigenen Zustandsdatei: „Ohne Signal seit 20:10" nennt den Augenblick, in dem das Kabel gezogen wurde. Aufgeklappt zeigt die Karte den benutzten Anschluss, die ausgehandelte Geschwindigkeit samt Duplex-Betrieb, die Adresse der Box und die des Routers sowie den letzten erfolgreichen Internet-Test.



(© 2026 Comidio GmbH)

Fällt der Anschluss aus, melden auch Uhrzeit, TrutzDynDNS, Fernzugriff, Filterlisten, Mail, Videokonferenz und die Tor-Anbindung Probleme. Damit der Administrator nicht sieben Ursachen nachgeht, kennzeichnet die TrutzBox diese Karten als Folge des fehlenden Anschlusses.

DNS für Geräte: die zweite stille Karte

Nach demselben Prinzip arbeitet die Karte „DNS für Geräte“. Sie prüft die Namensauflösung auf zwei Wegen: Ein Testname wird über die Adresse der Box im internen Netz aufgelöst, also so, wie die Geräte fragen, und über 127.0.0.1, also so, wie die Box selbst für Updates, TrutzDynDNS und Mailversand fragt. Solange beide Wege antworten, bleibt die Karte ausgeblendet; im Support-Bericht steht sie immer. Anlass war ein Fall, der sonst kaum auffällt: Die Geräte im internen Netz kommen nicht mehr ins Internet, die Ampel steht aber auf Grün, weil die Box selbst weiter Namen auflöst. Typisch ist, dass Webseiten nicht laden, während Programme, die direkt mit IP-Adressen arbeiten, etwa manche Messenger oder ein fremder VPN-Tunnel, weiterlaufen. Genau dann erscheint die Karte. Sie kennt fünf Zustände:

- **Geräte im LAN bekommen keine Namensauflösung** (rot): Nur der Weg der Geräte ist tot. Erste Hilfe: unter „Netzwerk“ → „Netzwerkdienste“ auf der Seite „DNS“ die verschlüsselte Weiterleitung aus- und wieder einschalten.
- **Die Box selbst löst keine Namen auf** (orange): Die Geräte haben Internet, Updates, TrutzDynDNS und Mailversand der Box scheitern.
- **Keine Namensauflösung, weder für Geräte noch für die Box** (rot): meist fehlt der Internet-Anschluss, oder der Router antwortet nicht.
- **Verschlüsselung kurz unterbrochen, Auflösung solange unverschlüsselt** (grün): Die Box erreicht ihren DNS-Anbieter gerade nicht verschlüsselt, etwa während einer Wartung beim Anbieter. Sie löst in dieser Zeit unverschlüsselt auf, damit die Geräte Internet haben, versucht es alle fünf Minuten erneut und schaltet von selbst zurück. Die Ampel bleibt grün; Beginn und Ende stehen als Hinweis in der Ereignisliste.

- **Verschlüsselung zum DNS-Anbieter nicht möglich, Auflösung unverschlüsselt** (orange): Derselbe Zustand, aber seit über einer Stunde, etwa weil der Router Port 853 sperrt. Die Box löst weiter unverschlüsselt auf und versucht es alle 30 Minuten erneut; Filter und Sperren arbeiten unverändert.

Aufgeklappt nennt die Karte den Testnamen, die Antwortzeit beider Wege und den Stand der Verschlüsselung samt Anbieter. Melden andere Karten gleichzeitig Probleme, die auf fehlende Namensauflösung zurückgehen, etwa TrutzDynDNS, Filterlisten, Mail, Tor oder die Zeitsynchronisation, verweisen sie auf diese Karte, statt eigene Ursachen zu nennen.

Systemgrenzen: stille Engpässe früh erkennen

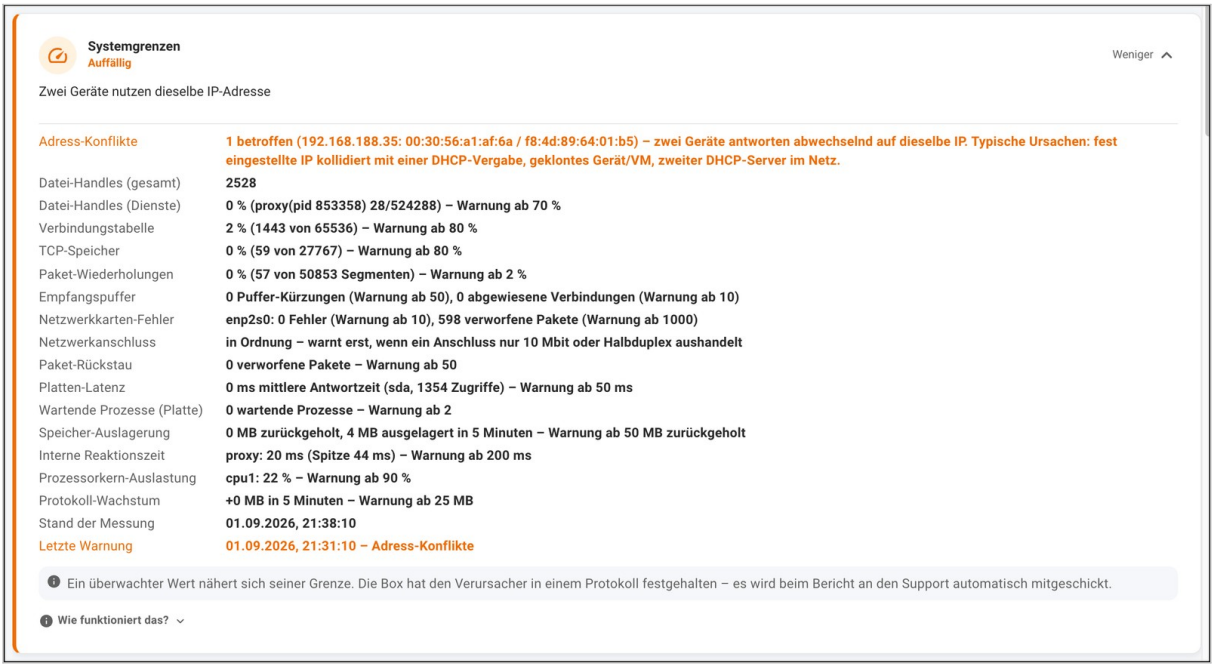
Manche Betriebsmittel der Box sind begrenzt: Datei-Handles, die Verbindungstabelle der Firewall, der TCP-Speicher des Kernels, die Antwortzeit der SSD. Läuft eines davon langsam voll, wird die Box spürbar langsamer, während Prozessor und Arbeitsspeicher weiter unauffällig aussehen. Genau solche Fälle sind im Nachhinein kaum aufzuklären, weil die Belege beim nächsten Neustart verschwunden sind. Die Kachel „Systemgrenzen“ schließt diese Lücke.
Ein kleiner Hintergrund-Dienst misst alle fünf Minuten mit niedrigster Priorität: Er kommt nur zum Zug, wenn Prozessor und Platte gerade nichts anderes zu tun haben, und kann die Box dadurch nie ausbremsen. Aufgeklappt zeigt die Kachel jeden überwachten Zähler mit seinem aktuellen Wert und der zugehörigen Warnschwelle, etwa „2 % (1443 von 65536), Warnung ab 80 %“. Überwacht werden unter anderem:

- **Datei-Handles, gesamt und je Dienst:** Ein Handle-Leck im Webfilter bremst jeden Download, lange bevor der Dienst ausfällt
- die Verbindungstabelle der Firewall (conntrack) und der TCP-Speicher des Kernels
- Paket-Wiederholungen (TCP) und die Empfangspuffer, beides Frühzeichen für eine überlastete oder gestörte Strecke
- Fehler und verworfene Pakete der Netzwerkkarten, Paket-Rückstau im Kernel sowie der Netzwerkanschluss selbst, der erst warnt, wenn ein Anschluss nur noch 10 Mbit oder Halbduplex aushandelt
- Platten-Latenz und Prozesse, die auf die Platte warten
- die Speicher-Auslagerung: Gewarnt wird nur, wenn ausgelagerte Seiten laufend zurückgeholt werden; das planmäßige Auslagern kalter Daten in den komprimierten Speicher zählt nicht
- die interne Reaktionszeit von Webfilter und Web-Server sowie die Auslastung einzelner Prozessorkerne: Beides deckt den Fall ab, dass ein einzelnes Programm stockt oder ein einzelner Kern am Anschlag läuft, während die Gesamtauslastung entspannt wirkt

- **Adress-Konflikte:** zwei Geräte beanspruchen abwechselnd dieselbe IP-Adresse; typisch, wenn eine fest eingestellte IP mit einer DHCP-Vergabe kollidiert, ein Gerät geklont wurde oder ein zweiter DHCP-Server im Netz steht
- das Wachstum der Protokolldateien: Ein Log-Sturm belastet die SSD

Überschreitet ein Zähler seine Schwelle, wird die Kachel gelb, die Überschrift benennt das Problem im Klartext (etwa „Ausgelagerter Speicher wird laufend zurückgeholt“ oder „Zwei Geräte nutzen dieselbe IP-Adresse“), und die auslösenden Zeilen sind orange markiert. Bei schwankenden Zählern gilt eine Bestätigungsregel: Erst zwei Messungen nacheinander über der Schwelle lösen aus, damit ein einmaliger Lastberg, etwa ein Paket-Update, keinen Fehlalarm erzeugt. Jede Überschreitung erscheint zusätzlich im Ereignis-Protokoll.
Im Moment der Überschreitung hält die Box den Verursacher in einem Protokoll fest, je nach Zähler etwa die Prozesse mit den meisten Datei-Handles, die größten Schreiber auf die Platte oder die beteiligten Geräte eines Adress-Konflikts. Diese Verursacher-Protokolle bleiben 30 Tage erhalten und wandern beim „Bericht an Support“ automatisch mit. Nach einer Warnung bleibt die Kachel noch sechs Stunden gelb, damit ein nächtliches Ereignis nicht unbemerkt verschwindet; „Ampel auf Grün stellen“ beendet diese Nachwirkung sofort. Ein Zähler, der akut über seiner Schwelle liegt, lässt sich dagegen nicht wegklicken.

Menüpfad: Systemeinstellungen → Betriebszustand

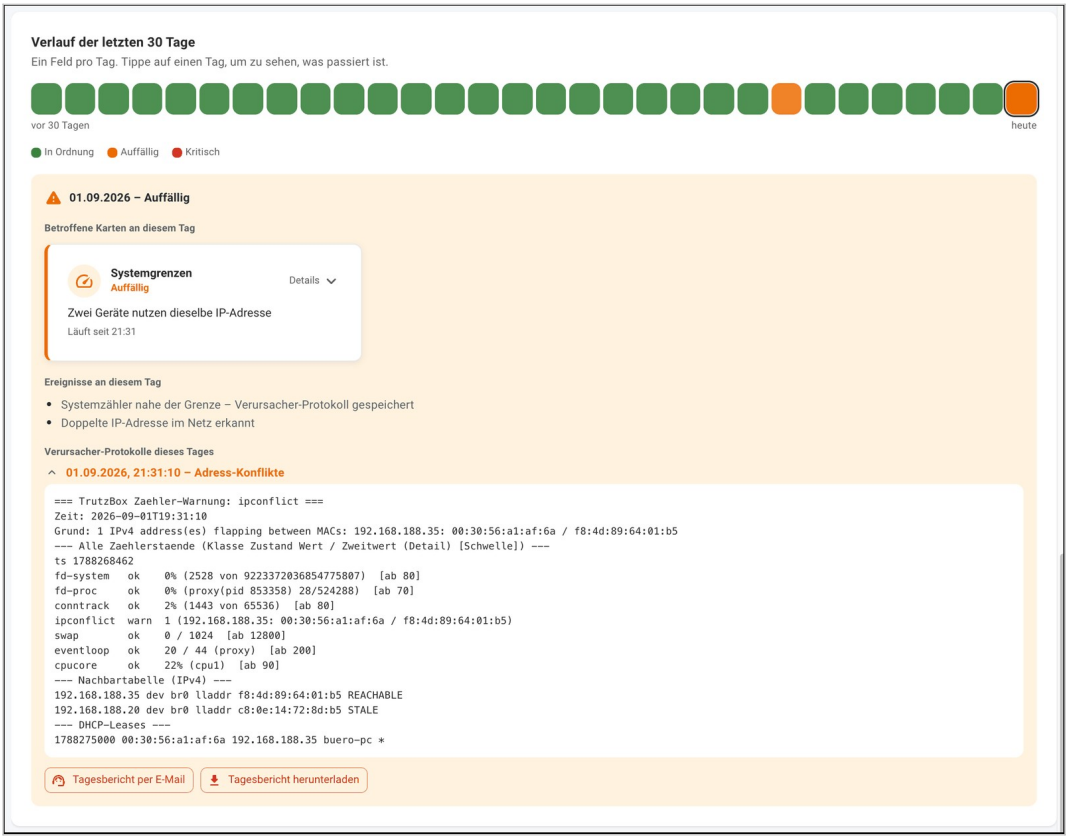


Die Kachel „Systemgrenzen“ aufgeklappt: alle überwachten Zähler mit ihren Warnschwellen. (© 2026 Comidio GmbH)

Verlauf der letzten 30 Tage

Jede Tageskarte nennt unter „Aufgetreten:“ den Zeitraum der Störung (erste bis letzte Sichtung der 15-Minuten-Prüfungen, etwa „16:12 bis 17:45“); die Ereignisse und Neustarts des Tages stehen unter der eigenen Überschrift „Ereignisse an diesem Tag“.
Eine Zeile mit einem Feld pro Tag visualisiert die letzten 30 Tage. Die Farbe steht für den Tagesstatus: grün „In Ordnung“, orange „Auffällig“, rot „Kritisch“. Ein Tippen auf einen Tag zeigt, was an diesem Tag passiert ist.
Bei einem orangen oder roten Tag zeigt die Tagesansicht zusätzlich die Verursacher-Protokolle dieses Tages: Zeitpunkt und betroffener Zähler, der volle Protokolltext lässt sich aufklappen. Diese Protokolle entstehen unabhängig davon, ob die Oberfläche geöffnet war; damit lässt sich auch ein Tag untersuchen, an dem niemand hingesehen hat. Zwei Knöpfe stellen einen Bericht nur für diesen Tag zusammen, „Tagesbericht per E-Mail“ und „Tagesbericht herunterladen“, jeweils mit den Karten, Ereignissen und Protokolltexten des Tages.

Menüpfad: Systemeinstellungen → Betriebszustand



Die Tagesansicht im Verlauf mit den Verursacher-Protokollen dieses Tages.
(© 2026 Comidio GmbH)

Die Tagesfarbe folgt den Karten des Tages. Rot ist dabei den Fällen vorbehalten, in denen die Box ungeschützt ist oder sich selbst gefährdet; der Ausfall einer Zusatzfunktion färbt Tag und Ampel höchstens orange, damit sich Rot nicht abnutzt. Greift der Speicher-Wächter ein, zeigt seine Kachel den Eingriff mit Zeitpunkt, freiem Speicher und den am stärksten gewachsenen Prozessen.

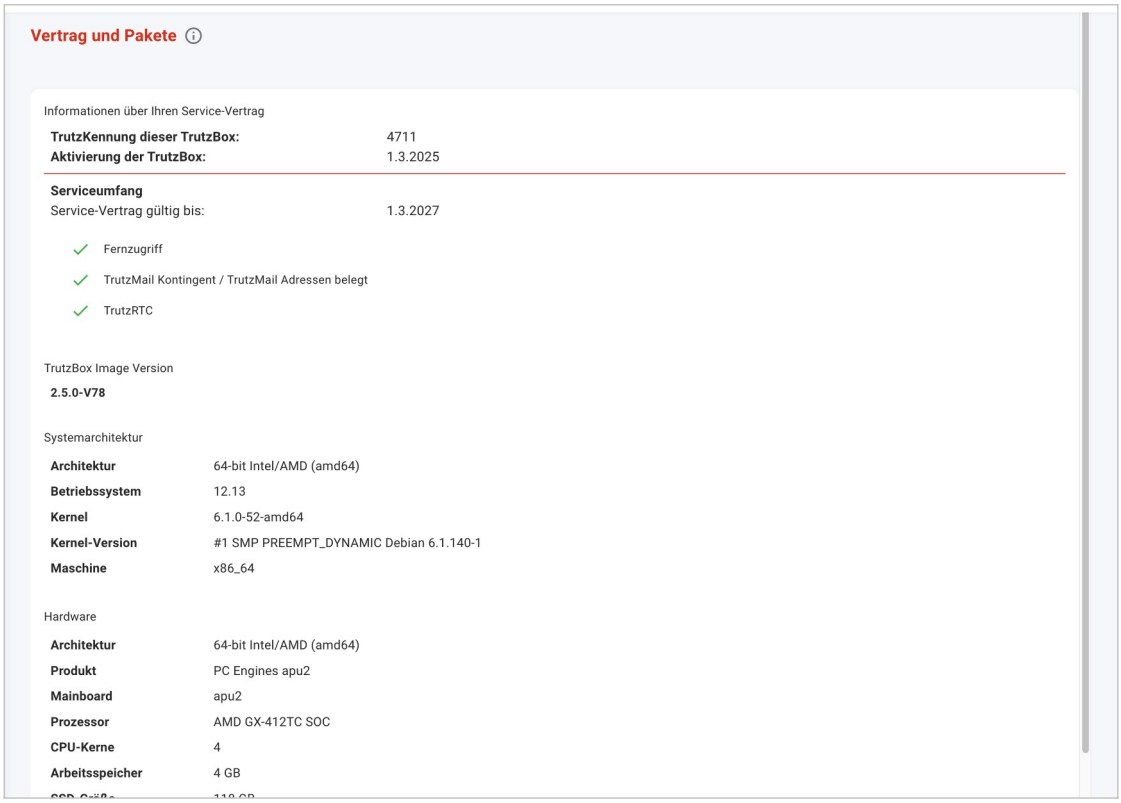
Ereignis-Protokoll

Das „Ereignis-Protokoll“ filtert aus den System-Logs nur die für die Gesundheit der Box relevanten Ereignisse heraus und übersetzt sie in Klartext. Die Liste lässt sich durchsuchen und nach Kategorie und Wichtigkeit filtern. Auch die Warnungen der Systemgrenzen-Überwachung und erkannte doppelte IP-Adressen erscheinen hier.
Anders als ein klassischer Überwachungsdienst läuft die Gesundheitsprüfung nicht dauerhaft mit: Der Zustand wird bei jedem Aufruf der Seite frisch ermittelt (aus Arbeitsspeicher-, Dienst-, SSD- und Log-Daten), und die Ampel in der App-Leiste aktualisiert sich etwa minütlich. Lediglich zwei kleine Hintergrund-Dienste laufen dauerhaft: Einer schreibt alle 15 Minuten einen Messpunkt für den 30-Tage-Verlauf, ein zweiter prüft alle fünf Minuten mit niedrigster Priorität die Systemgrenzen-Zähler. So bleibt die Funktion ressourcenschonend und belegt praktisch keinen Arbeitsspeicher.

17.2 Vertrag und Pakete

Das Menü „Vertrag und Pakete“ zeigt den vollständigen Status des Service-Vertrags, der installierten Software und der Hardware-Architektur der TrutzBox auf einen Blick.

Menüpfad: Systemeinstellungen → Vertrag und Pakete



Das Menü „Vertrag und Pakete“ mit Vertragsstatus, Kanal und Hardware-Angaben.
(© 2026 Comidio GmbH)

Die Ansicht gliedert sich in vier Bereiche:

- **Informationen über Ihren Service-Vertrag:** Zeigt TrutzKennung und Aktivierungszeitpunkt der TrutzBox, die Laufzeit des Service-Vertrags (gültig bis) sowie den gebuchten Serviceumfang: freigeschalteter Fernzugriff, TrutzMail-Kontingent (z. B. 2 von 5 TrutzMail-Adressen belegt) und TrutzRTC.
- **Image-Version:** Zeigt die aktuell installierte Software-Version der TrutzBox (z. B. 2.10.0, Build V75). Daran ist erkennbar, auf welchem Softwarestand die TrutzBox basiert.
- **Systemarchitektur:** Die Hardware-Architektur der TrutzBox (z. B. 64-bit Intel/AMD, amd64).
- **Pakete:** Tabelle aller installierten TrutzBox-Software-Pakete mit der jeweils installierten Version und der neuesten verfügbaren Version auf dem Update-Server. Ein Häkchen in der Spalte „Version im Kanal“ zeigt an, dass das Paket aktuell ist. Die Tabelle führt zusätzlich mitgelieferte Debian-Pakete auf, und zwar genau dann, wenn für sie eine Aktualisierung aussteht oder der eingestellte Aktualisierungskanal sie nicht führt. Ist alles auf dem Stand, bleibt die Liste kurz. Ein Knopf lädt die Übersicht neu, ohne die Seite zu wechseln.
- Ein Schalter „Nur relevante Pakete“ blendet Debian-Pakete aus, deren Versionsvergleich nicht aussagekräftig ist, weil der Update-Server sie für eine andere Debian-Fassung führt als die, mit der die Box läuft; ausgeschaltet erscheinen alle Pakete, die betroffenen grau und ohne Vergleichssymbol. Eine ältere, noch installierte Kernel-Version zählt nicht als ausstehende Aktualisierung; maßgeblich ist der neueste installierte Kernel.

Neben der Überschrift „Pakete“ steht der Paketkanal, aus dem die TrutzBox ihre Updates bezieht. Auf Kundengeräten ist das immer der Kanal „Stabil“, und die Anzeige ist reine Information. Ein Umschalten des Kanals gibt es dort nicht; Test-Aktualisierungen erhalten ausschließlich Boxen, die Comidio ausdrücklich dafür vorgesehen hat.
Die beiden Kanäle unterscheiden sich nicht nur in der Version der TrutzBox-Pakete, sondern auch in den Paketquellen. Testing nutzt das TrutzBox-Test-Repository und zusätzlich alle Debian-Quellen sowie die Quellen von Drittanbietern (etwa Node.js, Tor und Webmin). Hier werden neue Pakete gesehen, installiert und geprüft. Stable nutzt ausschließlich das von Comidio betreute TrutzBox-Repository; alles, was eine Box im Betrieb braucht, wird dorthin übernommen, andere Quellen sind bewusst abgeschaltet. Beim Umschalten tauscht die Box den kompletten Satz ihrer Paketquellen aus und liest die Paketlisten neu ein. Die nächtliche automatische Aktualisierung läuft nur im Kanal Stable. Eine Box im Kanal Testing aktualisiert sich ausschließlich von Hand; das automatische Update wird dort übersprungen und hinterlässt nur eine Zeile im Protokoll. Der gewünschte Kanal wird in der Konfiguration gespeichert und bei jedem Start mit den tatsächlichen Paketquellen abgeglichen, auch nach einer Wiederherstellung. Dieselbe Umschaltung steht im Setup-Assistenten im Willkommen-Schritt zur Verfügung.

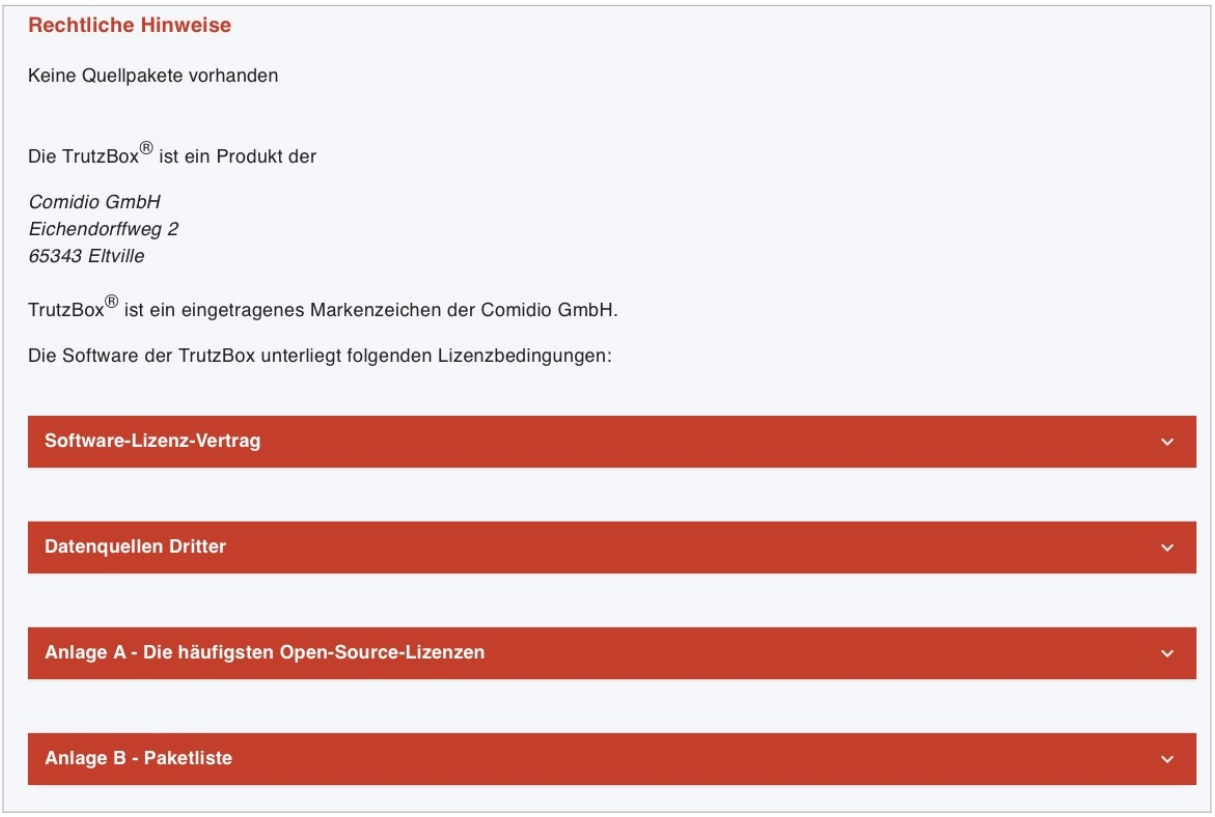
© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

17.3 Rechtliche Hinweise

Die Seite „Rechtliche Hinweise“ (Menü „Systemeinstellungen → Rechtliche Hinweise“) bündelt die rechtlichen Angaben zur TrutzBox sowie die Lizenz- und Quellcode-Informationen der eingesetzten Open-Source-Software. Sie nennt den Hersteller (Comidio GmbH, Eichendorffweg 2, 65343 Eltville) und weist darauf hin, dass „TrutzBox“ ein eingetragenes Markenzeichen der Comidio GmbH ist.
Markenhinweis: TrutzBox ist eine eingetragene Marke der Comidio GmbH. Alle weiteren in diesem Dokument genannten Produkt- und Firmennamen sowie Marken (etwa FRITZ!Box, WhatsApp, Signal, Telegram, Google, Apple, Microsoft, Amazon, Akamai, Sony, Samba TV, Pi-hole, Chrome, Edge, Firefox, Thunderbird, Adium, Monal, Siskin, Tunnelblick, Jitsi, Webmin, Debian, PC Engines, Cloudflare, Quad9, t-online, GMX) sind Eigentum der jeweiligen Rechteinhaber und werden ausschließlich zur Beschreibung genannt.
Über die Schaltfläche „Quellpakete löschen“ (mit Angabe der Größe) lassen sich die zur Erfüllung der Open-Source-Lizenzbedingungen vorgehaltenen Quellcode-Pakete entfernen; sind keine vorhanden, erscheint der Hinweis „Keine Quellpakete vorhanden“.
Die eigentlichen Lizenztexte sind in vier aufklappbare Bereiche gegliedert:

- **Software-Lizenz-Vertrag:** der Lizenzvertrag, dem die TrutzBox-Software unterliegt.
- **Datenquellen Dritter:** Herkunft und Lizenzen der von der TrutzBox genutzten Datenbestände (etwa Geo-IP-Daten und Filter-/Sperrlisten) mit Quellenangaben und Lizenzlinks.
- **Anlage A „Die häufigsten Open-Source-Lizenzen“:** eine Liste der gängigen Lizenzen (z. B. GPL, LGPL, BSD, Apache); ein Klick öffnet den jeweiligen Lizenztext.
- **Anlage B „Paketliste“:** die vollständige, seitenweise dargestellte Liste aller installierten Software-Pakete; ein Klick auf ein Paket zeigt dessen Copyright- und Lizenzangaben.

Menüpfad: Systemeinstellungen → Rechtliche Hinweise

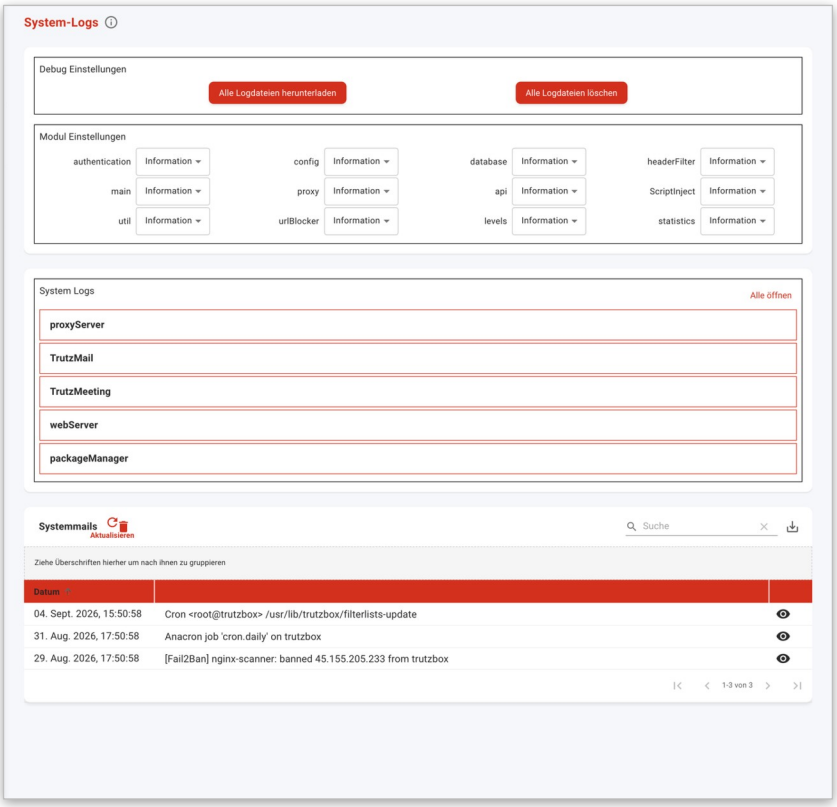


Die Seite „Rechtliche Hinweise“ mit den vier aufklappbaren Bereichen.
(© 2026 Comidio GmbH)

17.4 System-Logs

Unter System-Logs werden die Protokolle der TrutzBox angezeigt und die Debug-Einstellungen vorgenommen. Hier ist es zum einen möglich, den Proxy im Detail zu debuggen, zum anderen werden hier Inhalte von Mails angezeigt, die das Betriebssystem selbständig sendet. Zusätzlich lassen sich die laufenden Protokolle der wichtigsten Dienste live mitlesen und herunterladen.
Im Bereich „Debug-Einstellungen“ stehen außerdem folgende Funktionen bereit: „Alle Logdateien herunterladen“ (lädt sämtliche Logdateien als ZIP-Archiv für die Analyse herunter), „Alle Logdateien löschen“ sowie eine Option, bei Fehlern ein akustisches Signal auszugeben. Die laufenden Protokolle werden als Live-Ansicht für fünf Quellen angeboten: Proxy-Server, TrutzMail, TrutzMeeting (Videokonferenz), Web-Server und Paketmanager.

Menüpfad: Systemeinstellungen → System-Logs



Die Seite „System-Logs“ mit Protokollanzeige und Debug-Einstellungen.
(© 2026 Comidio GmbH)

Proxy debuggen

Die Protokollierung wird unter „System → Protokolle“ eingestellt:

- **Kategorien und Stufen:** Dort steht für jede der 13 Protokoll-Kategorien des Backends (etwa proxy, api, database, urlBlocker, statistics oder authentication) ein Auswahlfeld mit den Stufen debug, verbose, info, warn und error.
- **Vorgabe:** Die Stufe „info“ ist die Vorgabe und schreibt nur grundlegende Meldungen. Auf „debug“ liefert eine Kategorie meist genug Informationen, um ein Problem einzugrenzen.
- **Sofort wirksam:** Eine Änderung wirkt sofort, ein Neustart der Box ist nicht nötig.
- **Dateien:** Geschrieben wird in zwei Dateien unter /var/log/comidio: webServer.log für den Web- und API-Server und proxyServer.log für den Proxy.
- **Kategorie „api“:** Sie ist zugleich die Auffangkategorie für alle Dienste ohne eigenen Eintrag. Wer sie auf „debug“ stellt, sieht deshalb auch die Startmeldungen des Servers, das sind einige hundert Zeilen je Start.

- **Kategorie „authentication“:** Sie hält abgewiesene Zugriffe auf die Bedienoberfläche fest, mit Methode, aufgerufener Adresse und Absender; gleichartige Abweisungen innerhalb einer Minute werden gezählt und nur einmal ausgegeben. So lässt sich nachvollziehen, welcher Aufruf einen Benutzer aus der Oberfläche geworfen hat.

Da die TrutzBox mit diesen Funktionen evtl. sehr viele Daten ins Logdatei schreibt, sollte diese Debug-Funktion nur mit Bedacht und nur für kurze Zeit aktiviert werden, um einen Überlauf der SSD-Platte zu vermeiden.
Alle Logdateis werden nach voreingestellten Zeiten komprimiert und später dann gelöscht.

Systemmails

Das TrutzBox Betriebssystem sendet regelmäßig interne E-Mails um bestimmte Vorgänge mitzuteilen. Diese internen E-Mails können hier abgerufen werden. Diese E-Mails werden nur kurze Zeit gehalten und danach automatisch gelöscht.

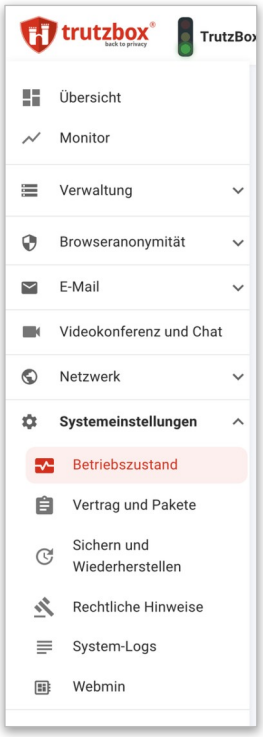
17.5 Webmin

Einige sehr betriebssystemnahe Funktionen, können mit dem Werkzeug „Webmin“ bedient werden. Webmin wird standardmäßig auf der TrutzBox ausgeliefert und mit dem Menüpunkt „Systemeinstellungen“ → „Webmin“ aufgerufen.

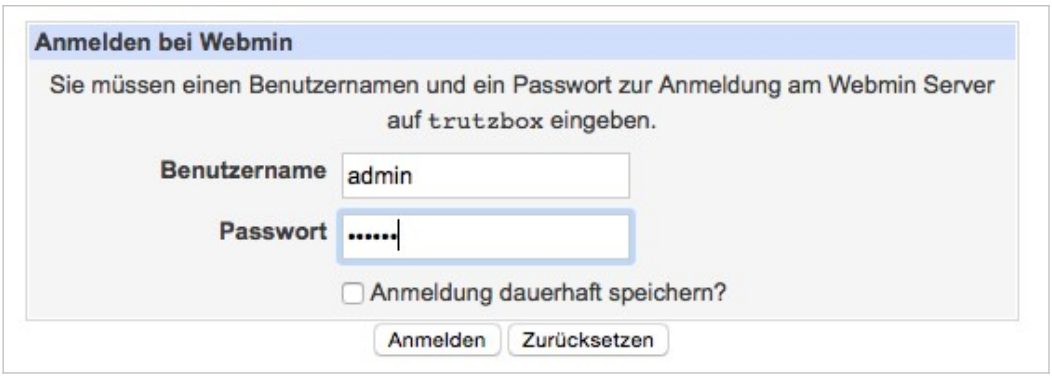
Wichtig: Webmin sollte nur von erfahrenen Linux Administratoren benutzt werden, da es mit diesem Werkzeug möglich ist, die Konfiguration der TrutzBox derart zu verstellen, dass diese nicht mehr nutzbar ist!

In einem solchen Fall kann es passieren, dass die TrutzBox nur noch durch Zurücksetzen auf Werkseinstellung wieder funktionsbereit gemacht werden kann. Dadurch gehen allerdings alle TrutzBox Daten (z. B. E-Mails) und Einstellungen verloren!

Menüpfad: Systemeinstellungen (aufgeklapptes Menü)

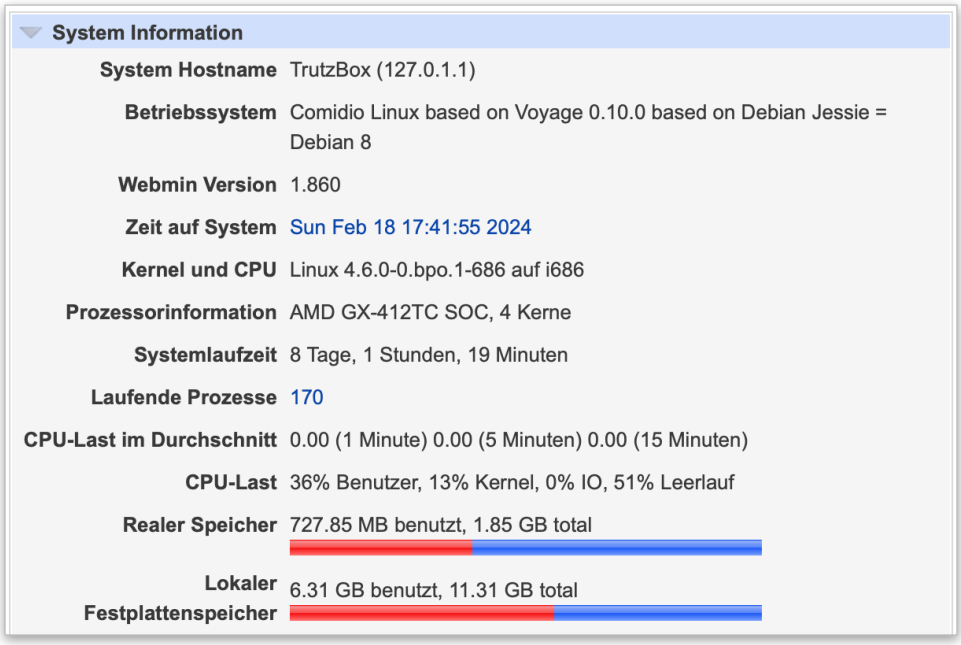


Da es sich bei Webmin[34] um ein eigenständiges Programm handelt, ist es notwendig, sich zunächst neu einzuloggen. Dazu bitte als Benutzernamen „admin“ und das TrutzBox Administrator-Passwort eingeben.



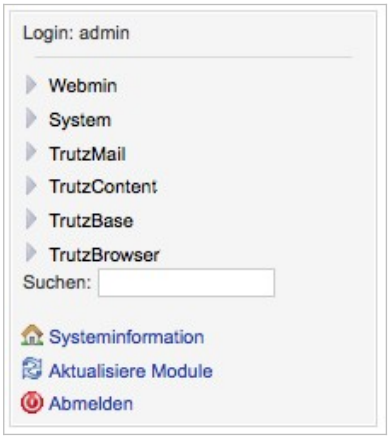
Nach dem Anmelden zeigt Webmin eine zusammengefasste Übersicht der Systeminformationen an:

[34] http://doxfer.webmin.com/Webmin/Main_Page



Evtl. ausstehende Updates der TrutzBox können direkt mit dem Link nach „Paket-Updates“ verwaltet werden. Das manuelle Einspielen von Updates sollte nur nach Rücksprache mit dem TrutzBox-Support durchgeführt werden, da Updates normalerweise immer automatisch eingespielt werden.

Über das Webmin Menü



Für die TrutzBox sind nur zwei Funktionen von Webmin vorgesehen: das Herunterladen des Systemstatus auf den eigenen Rechner und das Zurücksetzen auf Werkseinstellung; beide sind in den folgenden Abschnitten beschrieben. Die übrigen Menüpunkte von Webmin (etwa Paketverwaltung, Dienste oder Netzwerk) sind für den Betrieb der TrutzBox nicht erforderlich. Die Firewall der TrutzBox arbeitet mit nftables, dem Paketfilter des Linux-Kerns, und wird vollständig über die TrutzBox-Oberfläche verwaltet („Netzwerk → Firewall“ und „Netzwerk → Angriffsschutz“). Ein Webmin-Modul dafür gibt es nicht.

Warnung: Ohne laufende Firewall sind die TrutzBox und alle angeschlossenen Geräte ungeschützt. Die Firewall darf über Webmin oder die Kommandozeile nicht angehalten oder geleert werden. Das Zurücksetzen auf Werkseinstellung löscht alle Daten der TrutzBox, einschließlich E-Mails, Chat-Verläufe und Einstellungen; eine vorherige Sicherung unter „Systemeinstellungen → Sichern und Wiederherstellen“ ist deshalb dringend zu empfehlen.

Über Webmin den Systemstatus der TrutzBox auf den eigenen PC laden

1. **Solange man in Webmin eingeloggt ist, wird durch Eingabe des Links:** *https://trutzbox:10000/sysinfo.cgi* eine Datei, die den Systemstatus der TrutzBox enthält auf den eigenen PC geladen. Dieser kann dann, evtl. zusammen mit Logdateis, zur Analyse an Comidio geschickt werden.

TrutzBox mit Hilfe von Webmin auf Werkseinstellung zurücksetzen

Da Webmin unabhängig von der restlichen TrutzBox Software läuft und einen eigenen Web-Server hat, ist die Wahrscheinlichkeit groß, dass im Fall einer Störung der TrutzBox, Webmin noch funktioniert. Somit ist Webmin ein nützliches Werkzeug, das im Fall einer Fehlfunktion des TrutzBox Admin-Bedienoberfläche zur Analyse und Reparatur der TrutzBox verwendet werden kann.
Dazu zunächst in Webmin mit dem Link https://trutzbox:10000 aufrufen und einloggen. Unter dem Menüpunkt „System“ → „Kommandozeile“ ist es möglich, ein Systemkommando auf der TrutzBox (Shell) abzusetzen.
Dort bitte rechts neben dem Knopf „Führe Befehl aus:“ das Kommando

/usr/lib/comidio/trutzbox/system-update/system-update.sh reset

eintragen und dann den Knopf „Führe Befehl aus:“ drücken. Damit wird das Zurücksetzen der TrutzBox, wie im Handbuch beschrieben, angestoßen. Warnung: Dabei werden alle Einstellungen und Daten auf der TrutzBox gelöscht, auch gespeicherte E-Mails und die TrutzMail-Schlüssel. Zuvor eine Benutzerdaten-Sicherung anlegen (siehe Kapitel „TrutzBox zurücksetzen“). Warnung: Dabei werden alle Einstellungen und Daten auf der TrutzBox gelöscht, auch gespeicherte E-Mails und die TrutzMail-Schlüssel. Zuvor eine Benutzerdaten-Sicherung anlegen (siehe Kapitel „TrutzBox zurücksetzen“).

17.6 Die Kommandozeile: Terminal und SSH

Zwei Wege führen auf die Kommandozeile der TrutzBox, beide mit dem Passwort von admin und unabhängig von Webmin: SSH und das Terminal im Browser.

Anmeldung an der Kommandozeile (SSH)

Der erste Weg ist SSH (Port 22). Wie Webmin richtet sie sich an erfahrene Linux-Administratoren; für den normalen Betrieb wird sie nie gebraucht.

- **Anmeldung mit Passwort:** Mit einem Passwort meldet sich nur der Benutzer admin an, und zwar mit dem Administrator-Passwort aus dem Setup, zum Beispiel mit „ssh admin@trutzbox“. Root-

Rechte gibt danach das Kommando „sudo -i“, das dasselbe Passwort noch einmal verlangt. Vor dem Setup gibt es keine Anmeldung an der Kommandozeile, denn admin erhält sein Passwort erst dort.

- **Das Konto root:** Für root nimmt die TrutzBox per SSH kein Passwort an („PermitRootLogin prohibit-password“ in /etc/ssh/sshd_config.d/05-trutzbox-root-login.conf). Ab Werk hat root kein Passwort. Ein Passwort, das jemand selbst für root setzt, gilt nur direkt am Gerät und nicht per SSH.
- **Anmeldung mit Schlüssel:** Wer für root einen SSH-Schlüssel hinterlegt hat (/root/.ssh/authorized_keys), meldet sich damit direkt als root an.
- **Schutz vor dem Durchprobieren:** Der Angriffsschutz bewacht die Anmeldung. Nach fünf Fehlversuchen innerhalb von 30 Minuten sperrt er die Absenderadresse für eine Stunde, bei jeder Wiederholung doppelt so lang, höchstens eine Woche (Kapitel „Angriffsschutz“, Wächter „sshd“). Geräte im Netz der TrutzBox, im Netz vor der TrutzBox mit privaten Adressen und im VPN sperrt er nie. Eine Sperre steht wie jede andere im Reiter „Sperrlisten“ und lässt sich dort vorzeitig aufheben.
- **Von außen:** Die Firewall der TrutzBox nimmt Port 22 auch auf der Seite zum Internet-Router an. Aus dem Internet erreichbar ist er aber nur, wenn der Router ihn weiterleitet oder die TrutzBox ohne Router direkt am Modem hängt. Eine Freigabe für Port 22 ist nicht nötig und nicht zu empfehlen; von unterwegs führt der Weg zur Kommandozeile über TrutzVPN. In jedem Fall gilt: Das Administrator-Passwort schützt auch diesen Zugang und sollte entsprechend gut gewählt sein.

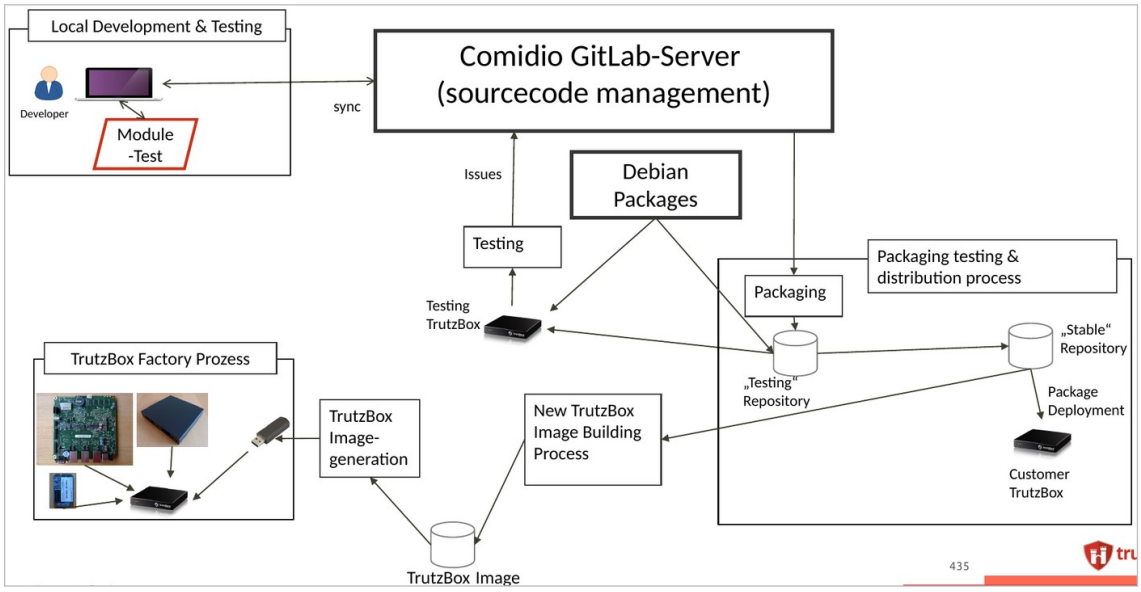
Terminal im Browser

Der zweite Weg ist das Terminal unter „Systemeinstellungen“ → „Terminal“: eine Kommandozeile mit vollen Rechten in einem eigenen Browser-Fenster, gedacht für den Notfall und für Befehle, die der Support nennt.

- **Eigener Dienst:** Das Terminal läuft als eigener Dienst (trutz-terminal), getrennt von der Verwaltungsoberfläche, und öffnet sich auch, wenn diese nicht läuft. systemd startet ihn erst mit der ersten Verbindung (Socket /run/trutz-terminal.sock); nach dem letzten Terminal beendet er sich wieder.
- **Aufruf:** Direkt unter „https://trutzbox/terminal/“; nginx reicht „/terminal-ws/“ an den Socket weiter. Erreichbar ist das Terminal wie die Verwaltungsoberfläche, also nicht aus dem Internet.
- **Anmeldung:** Jedes Öffnen fragt das Passwort des Benutzers admin ab, danach startet bash als root (xterm-256color). Fehlversuche bremst der Dienst selbst: ab dem sechsten 30 Sekunden Wartezeit, ab dem elften fünf Minuten, ab dem 21. 30 Minuten, je Absenderadresse und für das Konto insgesamt.
- **Ende:** Bis zu vier Terminals laufen gleichzeitig. Ein Terminal endet mit dem Fenster, mit „exit“ oder nach zwei Stunden ohne Eingabe und ohne neue Ausgabe.
- **Protokoll:** Beginn, Ende und falsche Passwörter stehen mit der Absenderadresse im Protokoll des Dienstes, die eingegebenen Befehle und das Passwort nicht.

18 Aktualität und Pflege der TrutzBox

Die TrutzBox hält sich selbstständig auf dem aktuellen Stand. Jede Nacht prüft sie automatisch, ob neue Updates bereitstehen, lädt diese und spielt sie ein, ohne dass der Anwender oder Administrator eingreifen muss. So bleibt die Software laufend gegen neu bekannt gewordene Bedrohungen geschützt, und neue Funktionen erreichen die Box ohne manuelle Pflege.



Weg eines Updates: Pakete aus der Entwicklung landen im Testing-Kanal, werden auf Testing-Boxen geprüft und erst dann in den Stable-Kanal übernommen, den die Kunden-Boxen nachts abfragen. (© 2026 Comidio GmbH)

18.1 Drei Arten von Updates im Überblick

Auf der TrutzBox werden drei Arten von Updates unterschieden:

- **Software-Paket-Updates**: einzelne Software-Pakete der TrutzBox werden gegen neue Versionen ausgetauscht. Das umfasst sowohl von Comidio entwickelte Komponenten als auch Pakete der zugrundeliegenden Linux-Distribution.
- **Filter- und Sperrlisten-Updates**: die Listen, mit denen die TrutzBox Tracker, Werbung, kompromittierte E-Mail-Adressen oder bösartige IP-Adressen blockiert, werden täglich aktualisiert.
- **Komplette TrutzBox-Image-Updates**: das gesamte Betriebssystem der TrutzBox wird neu aufgespielt. Diese Variante ist die Ausnahme und kommt nur in besonderen Fällen zum Einsatz, etwa bei einem Hardware-Tausch oder einer schweren Betriebsstörung.

18.2 Voraussetzung: gültiger TrutzServices-Vertrag

Die hier beschriebenen Update-Arten sind Leistungen des TrutzServices-Vertrags. Solange der Vertrag gültig ist, erhält die TrutzBox kontinuierlich Sicherheits- und Funktions-Updates, ohne zusätzliche Kosten und ohne Eingriff des Anwenders. Läuft der Vertrag aus, werden über die TrutzServices keine neuen Pakete und Listen mehr ausgeliefert; gesetzliche Aktualisierungsansprüche von Verbrauchern (§ 475b BGB) bleiben davon unberührt. Die TrutzBox bleibt als Filter grundsätzlich funktionsfähig, ihre Schutzwirkung gegen neue Bedrohungen lässt jedoch mit der Zeit nach; Dienste, die einen gültigen Vertrag voraussetzen (z. B. TrutzMail und TrutzRTC), stehen ohne Verlängerung nicht mehr zur Verfügung. Comidio empfiehlt deshalb, den Service-Vertrag durchgehend zu verlängern.

18.3 Software-Paket-Updates

Comidio-eigene Pakete

Diese Pakete werden von Comidio selbst entwickelt und enthalten Bug-Fixes oder Funktions-Erweiterungen für die TrutzBox-spezifische Software (zum Beispiel den Proxy, die Mail-Komponenten oder die Bedienoberfläche). Vor der Auslieferung werden sie intern getestet. Was in einem Update enthalten ist und welche Verbesserungen es bringt, wird im TrutzBox-Forum unter https://forum.trutzbox.de im Bereich „TrutzBox-Updates“ angekündigt und beschrieben. Wer die Entwicklung mitverfolgen möchte, kann dort regelmäßig vorbeischauen.

Debian-System-Pakete

Das TrutzBox-Betriebssystem basiert auf der Linux-Distribution Debian. Für diese Basis gibt es laufend Sicherheits- und Stabilitäts-Updates der Debian-Community. Comidio übernimmt diese Pakete nicht ungeprüft, sondern testet sie zunächst in einer eigenen Umgebung gegen die TrutzBox-Software. Erst nach diesem Test werden sie an die Boxen der Kunden ausgerollt. Das verringert das Risiko unerwarteter Störungen durch externe Änderungen. Schlägt das Abholen der Paketlisten fehl, etwa wegen einer falsch gehenden Uhr oder einer nicht erreichbaren Quelle, bricht der Aktualisierungslauf nicht komplett ab. Er arbeitet mit den vorhandenen Listen weiter und setzt beim nächsten erfolgreichen Abruf normal fort.

Updates beim TrutzBox-Setup

Schon während der erstmaligen Inbetriebnahme einer TrutzBox finden zwei Update-Prüfungen statt:

- Zu Beginn prüft die TrutzBox, ob es für das Setup-Programm selbst eine neuere Version gibt. Falls ja, wird das Setup zunächst aktualisiert, bevor die Inbetriebnahme weiterläuft.
- Am Ende des Setups prüft die TrutzBox, ob für die übrigen Software-Pakete neuere Versionen vorliegen, und spielt diese ein.

Damit ist eine TrutzBox unmittelbar nach der Erstinstallation auf demselben Stand wie eine seit langem in Betrieb befindliche Box.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

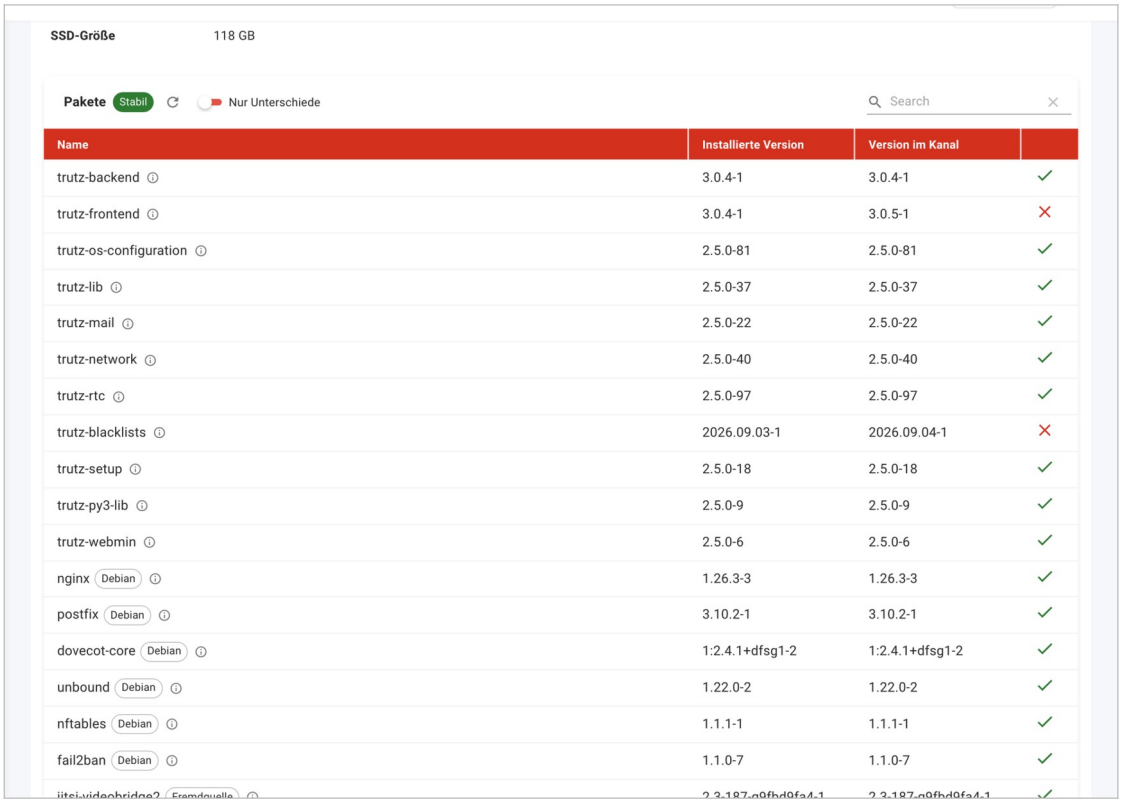
Automatische tägliche Auslieferung im Betrieb

Im laufenden Betrieb prüft die TrutzBox jede Nacht selbstständig, ob neue Pakete bereitstehen. Falls ja, werden sie heruntergeladen und installiert. Die Authentizität jedes Pakets wird durch eine kryptografische Signatur abgesichert; die Übertragung erfolgt über einen verschlüsselten und gegenseitig authentifizierten Kanal zum Comidio-Repository. Manipulierte oder gefälschte Pakete werden auf diese Weise erkannt und nicht eingespielt. Für den Anwender bedeutet das: nichts zu tun und nichts zu beachten; die Box bleibt aktuell.

Aktuelle Paketübersicht für den Administrator

Wer wissen möchte, welche Comidio-Software in welcher Version aktuell auf der eigenen TrutzBox installiert ist, findet diese Informationen im Menü „Systemeinstellungen → Vertrag und Pakete“. Dort werden für jedes von Comidio gepflegte Paket die installierte Version und die aktuell verfügbare Version nebeneinander angezeigt.

Menüpfad: Systemeinstellungen → Vertrag und Pakete



Die Paketübersicht nennt zu jedem Comidio-Paket die installierte und die verfügbare Version. (© 2026 Comidio GmbH)

Eine vollständige Liste aller Software-Bestandteile der TrutzBox, einschließlich der zugrundeliegenden Debian-Pakete, findet sich unter „Systemeinstellungen → Rechtliche Hinweise → Anlage B, Paketliste“. Diese Liste dokumentiert lückenlos, welche Komponenten in der Software enthalten sind, und macht die

Zusammensetzung der TrutzBox transparent, sowohl für den Anwender als auch für eine externe Prüfung.

18.4 Filter- und Sperrlisten-Updates

Neben der eigentlichen Software lebt die Schutzwirkung der TrutzBox von ihren Filter- und Sperrlisten. Diese werden ebenfalls automatisch aktualisiert, ohne dass der Anwender eingreifen muss. Nachvollziehen lässt sich das an drei Stellen: Die Kachel „Filterlisten“ auf der Seite „TrutzBox-Betriebszustand“ zeigt Stand und Installationszeitpunkt der Listen samt Zahl der veränderten Listen und warnt orange, wenn bereitstehende Listen länger als zwei Tage nicht installiert wurden. Über „Verlauf durchsuchen“ öffnet sich dort der Filterlisten-Verlauf, der je Liste jede Aktualisierung mit Eintragszahl und Veränderung auflistet, bei eigenen importierten Listen inklusive „Überschneidung anzeigen“. Und unter „Verwaltung → Filterlisten“ steht an jeder Liste das Datum der letzten Aktualisierung.

TrutzContent- und TrutzBrowse-Filterlisten

Die von Comidio gepflegten Filterlisten gegen Tracker- und Werbe-Server, Schadcode-Quellen und thematische Sperrkategorien werden täglich aktualisiert und an die TrutzBoxen verteilt. Einzelheiten im Kapitel „TrutzBox Filterlisten“.

TrutzMail-Adress-Blacklist

Wenn eine TrutzMail-Adresse kompromittiert wird (z. B. durch Diebstahl der TrutzBox), wird sie auf einer zentralen Blacklist beim Comidio-Server geführt. Jede TrutzBox gleicht täglich automatisch ab und entfernt gespeicherte Schlüssel solcher Adressen. So wird verhindert, dass kompromittierte Adressen weiter für vertrauenswürdige Kommunikation verwendet werden.

TrutzMail-Zertifikat-Updates

Auch die auf der TrutzBox gespeicherten Empfänger-Zertifikate werden täglich gegen den zentralen Comidio-CA-Server abgeglichen, damit ungültig gewordene Zertifikate zeitnah aussortiert werden. Aus Datenschutzgründen werden bei diesem Abgleich nur Hash-Werte der TrutzMail-Adressen übertragen. Eine ausführliche Beschreibung dieses Verfahrens findet sich im Kapitel „TrutzMail-Zertifikat Updates“. Dieser Abgleich dient dem Widerruf ungültiger Zertifikate. Wurde ein TrutzMail-Konto dagegen lediglich neu eingerichtet, tauschen die TrutzBoxen den neuen Schlüssel direkt untereinander aus (siehe Kapitel „Automatische Schlüssel-Aktualisierung zwischen TrutzBoxen“).

IP-Blocklisten

IP-Blocklisten werden nicht zentral verteilt, sondern vom Administrator lokal gepflegt (Menü „Netzwerk → Angriffsschutz“, Reiter „Sperrlisten“); zusätzlich trägt der Angriffsschutz erkannte Angreifer-Adressen automatisch ein. Einzelheiten in den Kapiteln „IP-Blocklisten-Verwaltung“ und „Angriffsschutz“.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

18.5 Komplette TrutzBox-Image-Updates

Ein Image-Update tauscht das gesamte Betriebssystem der TrutzBox aus. Dies ist die Ausnahme und kein Bestandteil des täglichen Update-Mechanismus. Ein vollständiges Image kommt nur zum Einsatz, wenn:

- ein Versions-Sprung über die normalen Paket-Updates nicht sauber durchgeführt werden kann,
- das interne Speichermedium der TrutzBox defekt war und ausgetauscht wurde,
- die TrutzBox aufgrund einer schweren Betriebsstörung anderweitig nicht mehr in einen funktionsfähigen Zustand gebracht werden kann.

Zwei Wege zum neuen Image

Der Administrator hat zwei Möglichkeiten, ein Image neu auf die TrutzBox aufzuspielen:

- **System zurücksetzen:** löscht alle Daten und installiert das Betriebssystem frisch; danach wird das TrutzBox-Setup mit der vorhandenen TrutzLegitimation erneut durchlaufen (Einzelheiten im Kapitel „TrutzBox zurücksetzen“).
- **Image per USB-Stick aufspielen**: kommt zum Einsatz, wenn das interne Speichermedium defekt ist oder die TrutzBox nicht mehr bootet. Der Anwender kann dies selbst vornehmen und benötigt dafür einen mindestens 32 GB großen USB-Speicherstick. Die ausführliche Schritt-für-Schritt-Anleitung findet sich im TrutzBox-Handbuch.

Beim Zurücksetzen über die Oberfläche holt die TrutzBox vor dem Einspielen eine kleine Beschreibungsdatei (Manifest) vom Update-Server. Sie enthält die Prüfsumme des Images (SHA-256). Während das Image direkt auf die Systempartition geschrieben wird, rechnet die Box die Prüfsumme mit und vergleicht sie mit dem Manifest. Vor dem ersten geschriebenen Byte prüft sie außerdem, ob die Daten ein gültiges Dateisystem mit der Kennung „TRUTZ-OS“ sind und ob das Ziel tatsächlich die Systempartition ist. Ein falsches Image, ein Abbild der ganzen Platte oder ein falsches Ziel werden so abgewiesen, auch wenn die Prüfsumme stimmen sollte. Eine Signaturdatei zum Manifest wird bereits mitgeladen; die Prüfung dieser Signatur auf der Box ist in Vorbereitung. Die Software-Pakete selbst sind davon unabhängig signiert und werden von der Paketverwaltung (apt) vor dem Einspielen geprüft.

18.6 Sichere Voreinstellungen

Die TrutzBox wird mit sicheren Standardeinstellungen ausgeliefert, die der Anwender nicht aktivieren oder anpassen muss:

- Automatische Updates sind ab Werk aktiviert.
- Die Prüfung auf neue Updates läuft jede Nacht zu fester Uhrzeit.
- Alle Update-Kanäle sind verschlüsselt und gegenseitig authentifiziert. Jedes Software-Paket ist kryptografisch signiert und wird von der Paketverwaltung (apt) vor dem Einspielen geprüft. Ein

Betriebssystem-Image wird über die Prüfsumme aus dem Manifest, die Kennung des Dateisystems und die Prüfung der Zielpartition abgesichert; die Signaturprüfung des Images ist in Vorbereitung.

- Die TrutzBox stellt nach außen nur die Dienste bereit, die für ihren Betrieb tatsächlich notwendig sind. Die Angriffsfläche bleibt klein.

Damit ist die TrutzBox unmittelbar nach dem Auspacken auf sichere Voreinstellungen nach Stand der Technik eingestellt. Eingriffe an diesen Voreinstellungen sind im Normalfall weder nötig noch ratsam.

18.7 Schwachstellen melden

Kunden, Sicherheitsforscher und aufmerksame Beobachter können vermutete Schwachstellen, ungewöhnliches Verhalten oder generelle Sicherheitsfragen jederzeit an Comidio melden, entweder per E-Mail an support@comidio.de oder über das TrutzBox-Forum unter https://forum.trutzbox.de. Comidio bewertet eingehende Meldungen und liefert eine Korrektur, soweit erforderlich, über den normalen nächtlichen Update-Mechanismus an alle TrutzBoxen aus. Bei besonders kritischen Schwachstellen können Updates auch außerhalb des Tagesrhythmus bereitgestellt werden. Wesentliche Änderungen werden im Forum-Bereich „TrutzBox-Updates“ angekündigt.

18.8 Was der Anwender tun (bzw. nicht tun) muss

Im Normalfall ist von Seiten des Anwenders nichts zu tun. Trotzdem hier kurz zusammengefasst, was man bei Bedarf machen kann:

- **Im Normalfall:** nichts. Die TrutzBox hält sich selbst aktuell.
- **Wer informiert bleiben möchte:** regelmäßig im TrutzBox-Forum im Bereich „TrutzBox-Updates“ nachschauen.
- **Wer den aktuellen Stand prüfen möchte:** „Systemeinstellungen → Vertrag und Pakete“ oder „Anlage B, Paketliste“ im TrutzBox-Menü aufrufen.
- **Bei Problemen oder Auffälligkeiten:** Meldung an Comidio, Kontaktwege im Kapitel „Schwachstellen melden“.
- **Auf einen gültigen Service-Vertrag achten:** über die TrutzServices werden Updates nur bei aktivem Vertrag ausgeliefert. Gesetzliche Aktualisierungsansprüche von Verbrauchern (§ 475b BGB) bleiben davon unberührt.

19 TrutzBox Betriebssystem

Comidio hält sich, soweit möglich, an die sieben Prinzipien des „Privacy by Design“ (PbD)[35]. Da Comidio ein kommerzielles Unternehmen ist, kann allerdings nicht garantiert werden, dass alle sieben Prinzipien vollständig eingehalten werden können.
Um bestmögliche Sicherheit zu bieten, muss es dem Markt möglich sein, die TrutzBox Software von neutralen Dritten zu verifizieren. Quelloffenheit ist ein wichtiges PbD Prinzip. Das TrutzBox-Betriebssystem basiert auf der Linux-Distribution Debian, die Comidio für den Einsatz als TrutzBox gehärtet hat. Die TrutzBox-Software baut überwiegend auf quelloffenen Komponenten auf; deren Quellcodes sind gemäß den jeweiligen Lizenzbedingungen verfügbar (siehe „Rechtliche Hinweise“).
Der Proxy und die Verwaltungsoberfläche sind Eigenentwicklungen von Comidio.
Auf dem Betriebssystem wurde eine webbasierte Management-Konsole implementiert (TrutzBox Bedienterface), die es einem TrutzBox Administrator unter anderem erlaubt, die Benutzer und die TrutzBox Funktionalitäten zu verwalten.
Um die TrutzBox Software und TrutzBrowse/TrutzContent Blacklists aktuell halten zu können, wurde der Standard-„Debian Package Manager“ (dpkg) verwendet.

35 http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

Als Debian-Version kommt bei der TrutzBox EVO (64 Bit, APU2) Debian GNU/Linux 12 (bookworm) zum Einsatz. Die 32-Bit-TrutzBox läuft mit Debian GNU/Linux 8 (jessie). Die Debian-Version bestimmt, wie lange die Basis mit Sicherheits-Updates versorgt wird; diese Updates erreichen die TrutzBox über den im Kapitel „Aktualität und Pflege der TrutzBox“ beschriebenen Weg, nachdem Comidio sie geprüft hat. Auf dem 64-Bit-System übernimmt der NetworkManager die Netzwerkkonfiguration, die Firewall arbeitet mit nftables (dem Paketfilter des Linux-Kerns), und die Dienste werden über systemd gestartet.

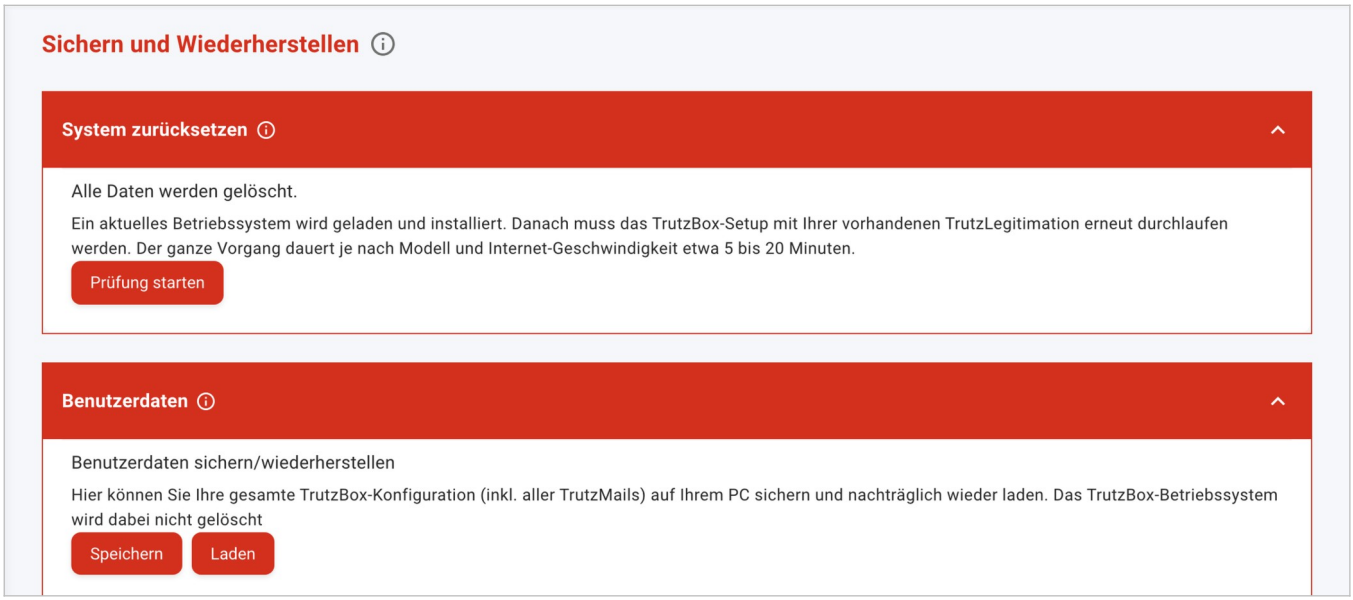
© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

20 TrutzBox zurücksetzen

Um bei Betriebsstörungen, die nicht mehr behebbar sind, die TrutzBox dennoch wieder in einen betriebsbereiten Zustand zu versetzen, hat der Administrator unter dem Menüpunkt „Systemeinstellungen“ → „Sichern und Wiederherstellen“ die Möglichkeit, die TrutzBox in einen definierten Zustand zu versetzen. Hier ist es auch möglich, alle Einstellungen der TrutzBox zu speichern (Sicherung aller Einstellungen) und eine vorherige Sicherung aufzuspielen.

Dazu gibt es drei Möglichkeiten.

Menüpfad: Systemeinstellungen → Sichern und Wiederherstellen



Die Seite „Sichern und Wiederherstellen“ mit Zurücksetzen und Benutzerdaten-Sicherung. (© 2026 Comidio GmbH)

System zurücksetzen

Alle Daten auf der TrutzBox werden gelöscht. Ein aktuelles Betriebssystem wird geladen und installiert. Danach muss das TrutzBox-Setup mit Ihrer vorhandenen TrutzLegitimation erneut durchlaufen werden. Der Vorgang wird über die Schaltfläche „Prüfung starten“ angestoßen; die TrutzBox prüft dabei zunächst die Voraussetzungen, bevor das eigentliche Zurücksetzen beginnt. Wie lange es dauert, hängt von der Internet-Geschwindigkeit ab und liegt bei rund fünf Minuten.

Bei dieser Prüfung geht die TrutzBox sieben Punkte durch: Internetverbindung, ein gültiges Betriebssystem-Abbild auf dem Update-Server, Vorhandensein des Wiederherstellungsbereichs, dessen Startfähigkeit, dessen Vollständigkeit, die Konfiguration des Bootloaders mit dem Eintrag für diesen Bereich und schließlich, ob das angebotene Abbild überhaupt auf die Systempartition passt. Zum Punkt für das Abbild zeigt die Oberfläche zusätzlich an, was der Update-Server für genau diese Box bereithält: Version und Bau-Nummer, die entpackte Größe und die enthaltenen Kernel, alles aus der

Beschreibungsdatei des Abbilds. Erst wenn alle Punkte erfüllt sind, lässt sich das Zurücksetzen auslösen; danach wird der Fortschritt laufend angezeigt, und am Ende meldet sich die TrutzBox automatisch wieder zurück.

Jedes Betriebssystem-Abbild trägt den Netzwerknamen trutzbox. Eine Box, die vorher anders hieß, meldet sich nach dem Zurücksetzen wieder unter diesem Namen; ein selbst vergebener Netzwerkname ist damit weg. Der Einrichtungsassistent ist dann unter http://trutzbox/setup/ erreichbar, an einer Fritzbox auch unter http://trutzbox.fritz.box/setup/.

Das Browserfenster bleibt während des Vorgangs offen und zeigt die vergangene Zeit. Es wartet zunächst, bis das alte System nicht mehr antwortet, und sucht die Box danach alle fünf Sekunden unter ihrem Namen und unter ihren bisherigen Adressen. Antwortet sie wieder, springt die Seite von selbst in den Einrichtungsassistenten. Nach 45 Minuten ohne Antwort nennt sie stattdessen die Adresse zum Eintippen und bietet eine erneute Suche an. Diese Suche setzt voraus, dass die Verwaltung über http geöffnet ist: Aus einer https-Seite heraus darf der Browser keine http-Adressen abfragen, dann bleibt nur der Sprung von Hand.

Die TrutzBox sollte vor einem Besitzerwechsel mit diesem Menüpunkt auf die Werkseinstellung zurückgesetzt werden. Was dabei sonst noch zu beachten ist, steht im Abschnitt „Was vor einem Besitzerwechsel zu tun ist“.

Bitte beachten Sie, dass dabei alle Einstellungen und Daten auf der TrutzBox gelöscht werden. Also auch evtl. noch gespeicherte E-Mails werden dabei gelöscht. Danach lädt die TrutzBox ein aktuelles Betriebssystem-Abbild und spielt es über die aktive Partition ein. Das kann je nach Internet-Geschwindigkeit längere Zeit dauern.
Dann kann die TrutzBox erneut mit der ursprünglich ausgelieferten TrutzLegitimation in Betrieb genommen werden. Weil dabei ein neues Stammzertifikat entsteht, muss es auf allen Geräten neu installiert und das alte entfernt werden (Einzelheiten im Kapitel „Allgemeine Einstellungen“).

> **Technischer Hintergrund:** Der Wiederherstellungsbereich steckt in jeder 64-Bit-TrutzBox, seit es das erste 64-Bit-Abbild gibt. Für ältere Auslieferungen ist deshalb kein neues Abbild auf dem Speichermedium nötig; die Rescue-Software kommt über den gewöhnlichen Update-Weg. Bei diesen Boxen war die Einhänge-Tabelle des Wartungssystems noch unvollständig, seit der Fassung 1.0.1~28 hängt der Updater die benötigten Partitionen selbst ein. Geprüft am 6. September 2026 an einem Stand vom August: Paket eingespielt, Vorprüfung durchweg grün, Zurücksetzen in sechs Minuten durch, danach meldete sich die Box mit dem aktuellen Abbild zurück.

Drei Wege, das Zurücksetzen auszulösen

Das Zurücksetzen lässt sich auf drei Wegen starten. Alle drei führen in dasselbe Wartungssystem und laufen von dort an gleich ab.

- Über die Bedienoberfläche: Menüpunkt „Sichern und Wiederherstellen“, Schaltfläche „Prüfung starten“. Erst nach bestandener Vorprüfung lässt sich der Vorgang auslösen. Das ist der empfohlene Weg.

- Über die Taste am Gehäuse: Die TrutzBox einschalten. Der Start wartet nicht auf die Taste. Innerhalb der ersten 2 Minuten nach dem Einschalten die Taste 3 Sekunden lang gedrückt halten. Solange sie gedrückt ist, blinken die drei grünen Leuchtdioden gemeinsam, zweimal je Sekunde. Nach 3 Sekunden leuchten sie dauerhaft, dann loslassen. Erst das Loslassen löst den Vorgang aus. Vom Loslassen bis zum Neustart in das Wartungssystem leuchten die drei Leuchtdioden weiter dauerhaft. Wer vor Ablauf der 3 Sekunden loslässt, löst nichts aus und kann es innerhalb der 2 Minuten noch einmal versuchen. Eine Taste, die nach dem dauerhaften Leuchten länger als 30 Sekunden gedrückt bleibt, gilt als klemmend und löst ebenfalls nichts aus. Nach den 2 Minuten bewirkt die Taste nichts. Wer die Taste schon beim Einschalten hält, sieht das Blinken erst, sobald das Betriebssystem die Taste liest: auf der APU2 etwa 40 Sekunden nach dem Einschalten, auf dem NanoPi R5C nach etwa 10 Sekunden. Die 2 Minuten zählt die TrutzBox ab dem Start des Betriebssystemkerns. Auf der APU2 ist es die Taste an der Gerätefront, auf dem NanoPi R5C die Taste „reset“ neben der Strombuchse; sie schaltet die TrutzBox nicht hart ab. Vor dem Auslösen wartet die TrutzBox bis zu drei Minuten auf ihre Internetverbindung, dann läuft dieselbe Vorprüfung wie in der Oberfläche. Schlägt sie fehl, blitzen die drei grünen Leuchtdioden fünfmal gemeinsam auf, und die TrutzBox arbeitet normal weiter. Die TrutzBox beobachtet die Taste nur in diesen 2 Minuten. Danach kostet sie keine Rechenzeit.
- Über das Startmenü der Box: Die APU2 zeigt beim Einschalten fünf Sekunden lang ein Menü, auf dem Bildschirm und auf der seriellen Konsole; dort den Eintrag für das Wartungssystem wählen. Dieser Weg ist für Wartung und Notfälle gedacht: Es gibt dort weder Rückfrage noch Vorprüfung, der Werksreset läuft sofort an.

Leuchtdioden bei der Taste. Auf der APU2 sind es die drei grünen Leuchtdioden an der Front, auf dem NanoPi R5C die drei grünen Leuchtdioden WAN, LAN und WLAN (von links nach rechts).

Die drei grünen Leuchtdioden	Bedeutung
blinken gemeinsam, 250 ms an, 250 ms aus	Die Taste ist gedrückt, noch keine 3 Sekunden. Loslassen jetzt löst nichts aus, danach zeigen die Leuchtdioden wieder ihre gewohnte Anzeige.
leuchten dauerhaft	Die Taste ist 3 Sekunden gehalten: jetzt loslassen. Nach dem Loslassen bleibt die Anzeige so, bis die TrutzBox in das Wartungssystem neu startet. Für Netz und Vorprüfung hat sie bis zu 3 Minuten, eine nicht bestandene Vorprüfung wiederholt sie nach 10 Sekunden.
blitzen fünfmal schnell auf, 150 ms an, 150 ms aus	Netz oder Vorprüfung nicht rechtzeitig bestanden. Es wird nichts zurückgesetzt, die TrutzBox arbeitet normal weiter. Der Grund steht in /home/trutzbox-update.log.
zeigen nach dem dauerhaften Leuchten wieder die gewohnte Anzeige	Die Taste blieb länger als 30 Sekunden gedrückt und gilt als klemmend. Es wird nichts zurückgesetzt.

Was die Leuchtdioden während des Zurücksetzens anzeigen

Im laufenden Betriebssystem zeigt der Vorgang selbst nichts an, die Box startet einfach neu. Sobald das Wartungssystem läuft, zeigen die drei grünen Leuchtdioden den Fortschritt: Erledigte Schritte leuchten dauerhaft, der laufende Schritt blinkt. In den folgenden Bildern steht ein grauer Kreis für eine dunkle Leuchtdiode, ein grüner für eine leuchtende und ein grüner mit gestricheltem Ring für eine blinkende.

Die drei Leuchtdioden	Was gerade passiert
	Die Box wartet auf Netzwerk und Namensauflösung und holt die Beschreibungsdatei vom Update-Server. Das dauert nur wenige Sekunden.
	Das Abbild wird geladen, auf die Systempartition geschrieben und die Prüfsumme kontrolliert. Das dauert rund vier Minuten.
	Nacharbeit: Der Startbereich wird erneuert und das Datenverzeichnis auf den Werkszustand gebracht. Das geht schnell.
	Alles ist geschrieben. Die Anzeige bleibt zehn Sekunden stehen, dann startet die Box neu.

Die Anzeige gibt es seit der Rescue-Fassung 1.0.1~29, die eigene Stufe für die Nacharbeit und die zehn Sekunden am Ende seit ~30. Ältere Boxen lassen die Leuchtdioden im Wartungssystem unverändert, weil das Wartungssystem den Treiber dafür noch nicht mitbekam; die Box arbeitet trotzdem.

Bleibt das Wartungssystem mit dauerhaftem Blinken stehen, ist ein Fehler aufgetreten, und die Box muss von Hand neu gestartet werden. Das Blinkmuster nennt die Ursache; dabei bedeutet „schnell“ ein Takt von 0,1 Sekunden und „mittel“ ein Takt von 0,25 Sekunden. Ein Protokoll des Vorgangs liegt anschließend als Datei /home/trutzbox-update.log auf der Datenpartition, sofern diese erreichbar war.

Die drei Leuchtdioden	Takt	Fehler	Mögliche Ursache
	schnell	Netzwerk	Kein Kabel, kein DHCP, keine Namensauflösung
	schnell	Beschreibungsdatei	Server erreichbar, aber Beschreibungsdatei fehlt oder unlesbar
	mittel	Server	Update-Server antwortet nicht
	schnell	Download	Abbild ließ sich nicht laden
	mittel	Prüfsumme	Abbild beschädigt oder unvollständig
	mittel	Schreiben	Schreiben auf die Systempartition fehlgeschlagen
	schnell	Werksreinigung	Datenverzeichnis ließ sich nicht bereinigen
	schnell	Gerät	Systempartition oder Datenpartition nicht gefunden
	mittel	Bootloader	Bootloader ließ sich nicht umstellen
	schnell	Sonstiges	Unbekannter Fehler, Protokoll prüfen

Nach dem Neustart in das frische System gilt wieder die gewohnte Anzeige: Die drei grünen Leuchtdioden gehen aus, kurz darauf leuchtet die linke dauerhaft, dann werden alle drei für einen Moment dunkel, weil der Kernel die Leuchtdioden übernimmt, danach leuchtet die linke wieder, bis das System läuft; es folgt

langsames Blinken und schließlich der Herzschlag, sobald die Bedienoberfläche antwortet. Das kurze Dunkel dazwischen ist kein Fehler.

Vom Einschalten bis zum Setup. Die beiden Tabellen zeigen die Anzeige nach jedem Einschalten, bis das Setup oder die Bedienoberfläche erreichbar ist. Die Zeiten sind ungefähre Werte. Beim allerersten Start und nach Updates der TrutzBox-Software dauern die letzten Stufen länger. Ist die Herzschlag-Leuchte abgeschaltet, bleibt die Betriebs-Leuchtdiode auch beim Start dunkel.

APU2: drei grüne Leuchtdioden an der Front, die linke zeigt den Start.

Nach dem Einschalten	Leuchtdioden	Bedeutung
sofort	links dauerhaft an	Die Hardware startet (BIOS).
nach einigen Sekunden	alle drei kurz dunkel	Der Kernel übernimmt die Leuchtdioden. Kein Fehler.
danach	links wieder dauerhaft an	Das Betriebssystem startet. Ab etwa 40 Sekunden nach dem Einschalten liest die TrutzBox die Taste. Bis 2 Minuten nach dem Start des Kernels löst sie dort das Zurücksetzen aus.
etwa 1 bis 2 Minuten	links langsam, gleichmäßig blinkend	Das Betriebssystem läuft, die Bedienoberfläche startet noch. Bleibt es dabei, konnte die Bedienoberfläche nicht starten.
etwa 2 bis 3 Minuten	links Herzschlag (Doppelpuls)	Die Bedienoberfläche antwortet. Das Setup unter http://trutzbox/setup/ oder die Bedienoberfläche ist erreichbar.

NanoPi R5C: eine rote Leuchtdiode für den Betrieb und drei grüne Leuchtdioden WAN, LAN und WLAN. Die rote zeigt den Start in denselben Stufen wie die linke Leuchtdiode der APU2. Jede grüne zeigt die Auslastung des Anschlusses, neben dem sie steht: aus ohne Verbindung, seltenes kurzes Aufblitzen in Ruhe, schnelleres Blinken bei mehr Verkehr, Dauerlicht bei voller Auslastung.

Nach dem Einschalten	Leuchtdioden	Bedeutung
sofort	rot an, kurz auch blinkend, grün aus	Startprogramm und Kernel laden. Das kurze Blinken ist das Lebenszeichen des Kernels.
nach wenigen Sekunden	rot dauerhaft an, grün aus	Das Betriebssystem startet. Ab etwa 10 Sekunden nach dem Einschalten liest die TrutzBox die Taste „reset“. Bis 2 Minuten nach dem Start des Kernels löst sie dort das Zurücksetzen aus.
etwa 1 bis 2 Minuten	rot langsam, gleichmäßig blinkend, grün je nach Anschluss	Das Betriebssystem läuft, die Bedienoberfläche startet noch. Die grünen Leuchtdioden zeigen ihre Anschlüsse.
etwa 2 bis 3 Minuten	rot Herzschlag, grün je nach Anschluss	Die Bedienoberfläche antwortet. Das Setup unter http://trutzbox/setup/ oder die Bedienoberfläche ist erreichbar.

> **Technischer Hintergrund:** Das Wartungssystem liegt auf einer eigenen Partition und enthält einen einzigen Dienst. Beim Auslösen stellt die TrutzBox den Bootloader auf diese Partition um, legt die Plattform-Konfiguration dorthin und startet neu. Der Dienst holt das Betriebssystem-Abbild vom Update-Server, schreibt es unmittelbar auf die Systempartition, rechnet dabei die Prüfsumme mit und

> vergleicht sie mit der Beschreibungsdatei, erneuert anschließend den Startbereich mit Kernel und Startdateien, setzt das Datenverzeichnis auf den Werkszustand und startet neu.
>
> Der Bootloader der APU2 kennt einen einmaligen Start: Der Eintrag gilt genau für den nächsten Start und fällt danach von selbst weg.

Benutzerdaten sichern/wiederherstellen

Hier können Sie Ihre gesamte TrutzBox-Konfiguration (inkl. aller TrutzMails) auf Ihrem PC sichern und nachträglich wieder laden. Das TrutzBox-Betriebssystem wird dabei nicht gelöscht und auch nicht erneuert.
Speichern: erzeugt eine vollständige Sicherungskopie der TrutzBox-Konfiguration und lädt sie als verschlüsselte Datei auf Ihren PC herunter. Enthalten sind unter anderem die allgemeinen Einstellungen, die Filter- und Sicherheitsstufen sowie die Sperrlisten und, besonders wichtig, sämtliche TrutzMail-Konten mit ihren persönlichen Schlüsseln und .onion-Adressen sowie die TrutzChat-Daten (Verläufe, Gruppen) und die Tor-Kennungen der Postfächer. Die Sicherungsdatei ist mit einer Passphrase verschlüsselt; sie sollte dennoch an einem geschützten Ort aufbewahrt werden, und die Passphrase darf nicht verloren gehen.
Laden: spielt eine zuvor gespeicherte Sicherungsdatei wieder ein. Die TrutzBox-Dienste werden dabei kurz neu gestartet, das Betriebssystem bleibt unangetastet. So lässt sich die TrutzBox auf einen früheren Stand zurücksetzen oder, mit derselben TrutzLegitimation, auf eine ausgetauschte TrutzBox-Hardware übertragen.
Eine regelmäßige Sicherung ist besonders ratsam, weil die je TrutzMail-Adresse erzeugten Schlüssel und die daran gebundenen .onion-Adressen bei Verlust nicht wiederhergestellt werden können. Empfehlenswert ist eine Sicherung vor größeren Änderungen sowie in regelmäßigen Abständen.

Sicherungskopie der Filter-Einstellungen

Unabhängig davon lässt sich eine reine Sicherungskopie der Filter-Konfiguration erstellen („Sicherungskopie erstellen“): Sie wird als Datei „TrutzBox-Konfiguration-Backup-[Datum].zip“ auf den PC heruntergeladen und enthält nur die Filtereinstellungen, keine TrutzMails und keine Schlüssel. Über „Sicherungskopie wiederherstellen“ wird eine solche Datei wieder eingespielt. Für eine vollständige Sicherung inklusive der TrutzMail-Konten ist die oben beschriebene Benutzerdaten-Sicherung zuständig.

20.1 TrutzMail-Adressen bleiben reserviert nach Zurücksetzen der TrutzBox

Beim Reset auf Werkseinstellungen werden alle Mail-Accounts auf der TrutzBox gelöscht. Die zuvor angelegten TrutzMail Adressen bleiben jedoch für die TrutzLegitimation reserviert, mit der sie eingerichtet wurden, und lassen sich nur mit ihr wieder anlegen; so kann niemand eine fremde Adresse übernehmen. Unter „Benutzer verwalten“ erscheinen sie als reaktivierbare Benutzer mit dem Knopf „Reaktivieren“. Einzelheiten im Kapitel „Die TrutzLegitimation aus Anwendungssicht“.

20.2 Was vor einem Besitzerwechsel zu tun ist

Wird die TrutzBox verkauft, verschenkt oder anderweitig weitergegeben, gehört sie danach jemand anderem, die darauf gespeicherten Postfächer, Schlüssel und Verläufe aber nicht. Die folgende Reihenfolge hat sich bewährt.

- Zuerst eine vollständige Sicherung anlegen und auf den eigenen Rechner laden. Sie enthält die TrutzMail-Konten mit ihren privaten Schlüsseln und den zugehörigen .onion-Adressen. Ohne sie sind diese Schlüssel nach dem Zurücksetzen unwiederbringlich verloren, auch Comidio hat keine Kopie davon.
- Danach die TrutzBox über „Systemeinstellungen“ → „Sichern und Wiederherstellen“ auf die Werkseinstellung zurücksetzen. Das löscht alle Einstellungen, Benutzer, E-Mails, Chatverläufe, Gerätenamen und das WLAN-Passwort. Ein Zurücksetzen der Filtergruppen allein genügt dafür nicht. Wer sich nicht mehr anmelden kann, löst denselben Vorgang aus, indem er in den ersten 2 Minuten nach dem Einschalten die Taste am Gehäuse 3 Sekunden lang gedrückt hält und loslässt, sobald die Leuchtdioden dauerhaft leuchten; dafür ist kein Passwort nötig.
- Die TrutzLegitimation behalten und keinesfalls mitgeben, weder das mitgelieferte Blatt noch eine Abschrift von TrutzKennung und TrutzSchlüssel. Wer sie besitzt, kann die damit registrierten TrutzMail-Adressen auf einer beliebigen TrutzBox neu anlegen und damit die Mail-Identität des Vorbesitzers annehmen. Der neue Besitzer braucht eine eigene TrutzLegitimation von Comidio; Einzelheiten im Kapitel „Die TrutzLegitimation aus Anwendungssicht“.
- Die Registrierung bei Comidio klären. Die Box hängt an der TrutzLegitimation und am Konto des bisherigen Besitzers; dort sind der Name unter mytrutzbox.de und die TrutzMail-Adressen hinterlegt. Ohne eigene Registrierung kommt der neue Besitzer im Einrichtungsassistenten nicht durch.
- Zeigt eine eigene Mail-Domain auf die Box, deren MX- und übrige DNS-Einträge umstellen oder entfernen.
- Auch die Sicherungsdatei und ihre Passphrase bleiben beim bisherigen Besitzer. Beides zusammen öffnet die Postfächer und Schlüssel unabhängig von der Hardware.
- Auf den eigenen Geräten das Root-Zertifikat dieser TrutzBox entfernen, in Firefox und Thunderbird zusätzlich im jeweils eigenen Zertifikatsspeicher. Ebenso die VPN-Profile und die Mail-Konten löschen, die auf diese Box zeigen. Sonst vertrauen diese Geräte weiterhin einem Zertifikat, dessen zugehörigen Schlüssel jemand anderes besitzt.
- Am Internet-Router die Freigaben zurücknehmen, die für diese TrutzBox eingerichtet wurden, insbesondere die Weiterleitung für TrutzVPN und die für die Videokonferenz, ebenso etwaige DynDNS-Einträge für diese Box. Sie zeigen sonst weiter auf ein Gerät, das nicht mehr zum eigenen Haushalt gehört.

- Den bisherigen TrutzDynDNS-Namen als erledigt betrachten. Die Box aktualisiert ihn nach dem Zurücksetzen nicht mehr; ausgegebene Konferenz-Einladungen und Chat-Adressen unter diesem Namen führen ins Leere.
- Die zurückgesetzte TrutzBox nicht noch einmal selbst einrichten, sondern ausgeschaltet weitergeben. Der Einrichtungsassistent gehört dem neuen Besitzer, der ihn mit seiner eigenen TrutzLegitimation durchläuft.

Die eigenen TrutzMail-Adressen gehen dabei nicht an den neuen Besitzer über. Sie bleiben für die TrutzLegitimation reserviert, mit der sie eingerichtet wurden, und lassen sich auf einer neuen TrutzBox mit derselben TrutzLegitimation wieder anlegen; der Abschnitt davor beschreibt das im Einzelnen. Geht die TrutzLegitimation dagegen verloren, stellt Comidio einen neuen TrutzSchlüssel für dieselbe TrutzKennung aus; die TrutzMail-Adressen bleiben nutzbar.

> **Technischer Hintergrund:** Der Werksreset überschreibt die Systempartition vollständig mit dem frischen Abbild, erneuert den Startbereich, leert das Datenverzeichnis und überschreibt anschließend dessen freien Platz. E-Mails, Schlüsselbunde, Chat-Konten, Sicherungen, eigene Filterlisten, VPN-Profile und WLAN-Kennwörter sind damit weg und mit Bordmitteln nicht wiederherstellbar. Beim ersten Start entstehen ein neues Root-Zertifikat des Proxys und neue Host-Schlüssel für den Fernzugang, die Box heißt wieder trutzbox, und das Administrator-Passwort wird im Einrichtungsassistenten neu vergeben. Der Wiederherstellungsbereich bleibt bestehen; er enthält nichts Persönliches.

Bei hohem Schutzbedarf ist eine Einschränkung zu bedenken: Das Überschreiben des freien Platzes ist kein zertifiziertes Löschverfahren. Ein Flash-Speicher verteilt Schreibzugriffe intern, Reste können auf ausgetauschten Blöcken liegen bleiben. Wer das ausschließen will, tauscht das Speichermedium oder löscht es mit dem eingebauten Löschbefehl des Laufwerks und spielt danach ein frisches Abbild auf. Vor einer Weitergabe ist deshalb zu prüfen, wie schutzbedürftig die zuletzt gespeicherten Daten waren; bei sensiblen Beständen sind ein gesondertes Löschverfahren oder der Austausch des Speichermediums vorzuziehen.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

21 TrutzBox Hardware

Schon bei der Erstellung der TrutzBox Software-Architektur war klar, dass ein Gerät, das Firewall, Proxy-Filterung, Mail-Server und Echtzeitkommunikation gleichzeitig bereitstellen soll, auch relativ hohe Anforderungen an die Hardware stellt. Vor allem TrutzBase und viele gleichzeitige TrutzMail und TrutzBrowse Nutzer benötigen hohe CPU-Leistung und viel Hauptspeicher; zumal speziell bei der Internet-Nutzung eine spürbare Verzögerung nicht akzeptierbar wäre.
Bei einer E-Mail stört es in der Regel wenig, wenn diese 2 Minuten später ankommt. Wenn aber gerade viele E-Mails gesendet werden, sollte die Internet-Nutzung trotzdem immer noch flüssig sein.
Die benötigte Hardware-Leistung für Echtzeit-Kommunikation hält sich in Grenzen. Dort wird i.d.R. der Zugang zum Internet zuerst zum Engpass, bevor die Leistungsgrenze der TrutzBox erreicht wird.
Folgende Hardware-Anforderungen waren für Comidio entscheidend:

- für den Dauerbetrieb ausgelegter Server,
- keine mechanischen Bauteile (keine drehende Festplatte sondern eine schnelle SSD),
- geringer Stromverbrauch,
- neben WLAN auch noch mindestens zwei LAN-Anschlüsse mit 1 Gbit/s,
- geringer Kühl- und Platzbedarf, mechanisch stabil, sodass weitere Geräte darauf gestapelt werden können und
- eine Home-Version mit für Privathaushalte geeigneten Anschaffungskosten.

Aus diesen Gründen hat Comidio als Hardware-Basis für die TrutzBox Embedded-Boards des Herstellers PC Engines gewählt; die jeweils aktuell ausgelieferte Hardware nennt die Produktbeschreibung auf www.trutzbox.de.

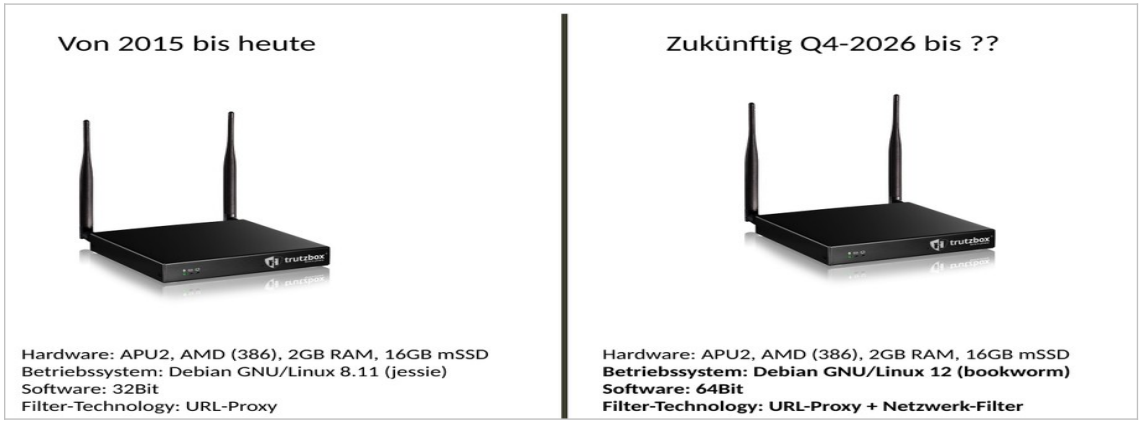
- Bis 8/2016 wurde die TrutzBox auf Basis des APU.1 System-Boards in der 2-GB-Version ausgeliefert.
- Ab 9/2016 kommt das APU2 System-Board des gleichen Herstellers zum Einsatz. Des Weiteren wird mit dieser Version als Speichermedium eine SSD, anstatt der zuvor eingesetzten SD-Karte verwendet.
- Ab 2020 wird die TrutzBox-Business mit 4 GB Hauptspeicher und größerer SSD alternativ angeboten.

Die Hauptplatine (Board) ermöglicht vier verschiedene Speichermedien: SD-Karte, USB-Stick, SATA HD/SSD und mSATA-SSD. Von allen vier Medien kann das System hochgefahren (gebootet) werden.



Das Board wird mit LAN-Kabel und Netzteil ausgeliefert. Optional kann ein WLAN-Adapter dazu oder nachträglich bestellt werden. Die TrutzBox erkennt, welches WLAN-Modul angeschlossen ist und, falls es ein von Comidio unterstütztes WLAN-Modul ist, lädt die entsprechende WLAN-Konfiguration automatisch.

Die TrutzBox läuft auf dem APU2-Board von PC Engines und gibt es in zwei Software-Generationen. Die erste ist die 32-Bit-TrutzBox. Die zweite, die TrutzBox EVO (auch TrutzBox 2 genannt), nutzt dieselbe Hardware, bringt aber ein 64-Bit-System und zusätzlich zum URL-Proxy einen Netzwerk-Filter mit. Die Tabelle stellt beide gegenüber:



Die zwei Software-Generationen der TrutzBox auf dem APU2-Board: 32 Bit und TrutzBox EVO mit 64 Bit.(© 2026 Comidio GmbH)

	TrutzBox (32 Bit)	TrutzBox EVO / TrutzBox 2
Hardware	APU2, AMD (x86), 2 GB RAM, 16 GB mSATA-SSD	APU2, AMD (x86), 2 GB RAM, 16 GB mSATA-SSD
Betriebssystem	Debian GNU/Linux 8 (jessie)	Debian GNU/Linux 12 (bookworm)
Software	32 Bit	64 Bit
Filter-Technik	URL-Proxy	URL-Proxy und Netzwerk-Filter
Stand	Bestandsgeräte bei Kunden	aktuelle Generation

Die TrutzBox EVO nutzt die vorhandene APU2-Hardware weiter. Der Umstieg von der 32-Bit-Software auf die TrutzBox EVO erfolgt über ein neues Image auf derselben Hardware (siehe Kapitel „Aktualität und Pflege der TrutzBox“).

21.1 LED-Anzeigen an der Gerätefront

Die TrutzBox hat drei grüne LEDs an der Gerätefront:
Die linke LED zeigt den Betriebszustand: beim Start erst Dauerleuchten (Box bootet), dann langsames Blinken (Betriebssystem läuft, Bedienoberfläche startet), im Betrieb dauerhaft das schnelle Herzschlag-Blinken (Bedienoberfläche antwortet); die Abfolge ist im Kapitel „TrutzBox Setup“ beschrieben. Auf dem NanoPi R5C übernimmt die rote Leuchtdiode diese Rolle, die drei grünen Leuchtdioden WAN, LAN und WLAN zeigen dort die Auslastung ihres Anschlusses. Beim Zurücksetzen über die Taste und im Wartungssystem zeigen auf beiden Geräten die drei grünen Leuchtdioden den Fortschritt.
Die mittlere LED leuchtet auf, während TrutzMail E-Mails verarbeitet.
Die rechte LED kann auf Wunsch jede geblockte Verbindung durch kurzes Aufblinken anzeigen. Die Schalter für alle drei Leuchtdioden und den Lautsprecher der Box beschreibt das Kapitel „Allgemeine Einstellungen“.

21.2 Austausch der Hardware

Im Falle einer defekten Hardware, kann diese recht einfach ausgetauscht werden. Da alle Authentisierungsschlüssel nur in Form von Software auf dem Boot-Medium gespeichert sind, ist es möglich, das Boot-Medium in eine andere TrutzBox Hardware zu stecken und diese unverändert in Betrieb zu nehmen.
Weil die TrutzMail-Identität an die TrutzLegitimation gebunden ist und nicht an die Hardware, kann auch das interne Speichermedium (SSD) bei Defekt ausgetauscht werden; der Nutzer stellt seine Identität gegenüber seinen E-Mail-Partnern wieder her, ohne seine Anonymität gegenüber Comidio aufzugeben. Einzelheiten im Kapitel „Die TrutzLegitimation aus Anwendungssicht“.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

22 Anhang: Zertifikate und Schlüssel

Um den Betrieb der TrutzBox und die Kommunikation zwischen TrutzBoxen abzusichern, generiert die TrutzBox mehrere digitale Zertifikate und kryptographische Schlüssel. Dies geschieht ohne Eingriff des Benutzers.
Hier die wichtigsten Zertifikate und Schlüssel:

- 1. Ein TrutzMail OpenPGP-Schlüsselpaar pro TrutzMail-Adresse. Es bestätigt die Echtheit der TrutzMail-Adressen und dient dazu, E-Mails Ende-zu-Ende zu verschlüsseln und digital zu signieren. Es wird von Comidio zertifiziert. Falls beim Senden einer TrutzMail das Zertifikat des Empfängers noch nicht bekannt ist, wird es vom zentralen Comidio Keyring-Server geholt. Das Schlüsselpaar enthält:
  - Den öffentlichen 2048-Bit-RSA-Schlüssel des Empfängers, mit dem der Sender die E-Mail automatisch verschlüsselt.
  - Die Tor-Hidden-Service-Adresse (.onion-Adresse), um Mails anonym an die Empfänger-TrutzBox ausliefern zu können.
  - Das Schlüsselpaar wird auch für die XMPP-Server-to-Server-Kommunikation zwischen TrutzBoxen verwendet.
  - **Ablage:** /var/lib/comidio/trutzmail/openpgp/pubring.gpg und secring.gpg
  - Kein Ablaufdatum; tägliche CRL-Prüfung um 04:00 Uhr. Eine CRL (Certificate Revocation List) ist die Sperrliste, über die eine Zertifizierungsstelle vorzeitig zurückgezogene Zertifikate bekannt macht.
- 2. Ein TrutzBox-Identitätszertifikat (Box-Cert) pro TrutzBox, das zur mTLS-Authentifizierung gegenüber Comidio-Diensten dient (APT-Repository, DynDNS, Let's Encrypt-Proxy, Keyring-Server). Es wird beim Setup der TrutzBox einmalig generiert. Laufzeit ca. 27 Jahre; keine automatische Erneuerung. mTLS (gegenseitiges TLS) bedeutet, dass sich bei der verschlüsselten Verbindung beide Seiten per Zertifikat ausweisen, nicht nur der Server, sondern auch die TrutzBox als Client.
  - /etc/comidio/boxCert.pem: TrutzBox-Zertifikat (X.509, sha256WithRSAEncryption, RSA 4096 Bit)
  - /etc/comidio/boxKey.pem: TrutzBox Private Key (RSA 4096 Bit)
- 3. Ein Web-Server TLS-Zertifikat pro TrutzBox (für https://trutzbox/, SMTP/IMAP/POP3, XMPP). Signiert durch das Proxy-CA-Zertifikat (Nr. 4). Dient dazu, die TrutzBox gegenüber Nutzern (Web-Browser, Mail-Client, XMPP-Client) zu authentisieren. Wird automatisch erneuert durch certs.sh::removeIfExpired() bei Package-Updates.

- /etc/comidio/webCert.pem, /etc/comidio/webKey.pem

- 4. Ein Proxy-CA-Zertifikat (das „TrutzBox-Stammzertifikat“, das auf den Geräten installiert wird) pro TrutzBox. Dieses Self-Signed Root-CA-Zertifikat dient dazu, die von TrutzBrowse pro aufgerufener HTTPS-Verbindung dynamisch generierten Host-Zertifikate zu signieren. Es sollte im Web-Browser und Betriebssystem der Client-Geräte importiert werden, damit diese die Authentizität des Web-, XMPP- und Mail-Servers auf der TrutzBox überprüfen können. RSA 4096 Bit; Gültigkeit ab 1970 für rund 30 Jahre. Bleibt bei Neustart, Updates und Wiederherstellung mit Sicherung erhalten; wird nur bei Neuinstallation des Images, Werksreset oder Wiederherstellung ohne Zertifikat neu erzeugt (dann Neuimport auf allen Geräten).
  - /etc/comidio/proxyCA.crt (PEM), /etc/comidio/proxyCA.crt.der (DER), /etc/comidio/proxyCA.key
- 5. Ein Zertifikat für die Authentisierung des Jitsi-Servers (TrutzRTC Videokonferenz-Server). Dies ist ein Symlink auf das webCert.pem und muss auf einem anderen Hostnamen als „trutzbox“ ausgestellt sein, damit externe Teilnehmer keine Zertifikatsfehler erhalten. Andernfalls würden Browser anderer TrutzBox-Besitzer, die ihr eigenes Stammzertifikat importiert haben, das Zertifikat ablehnen.
  - /etc/comidio/trutzrtc/webCert.pem → webCert.pem, /etc/comidio/trutzrtc/webKey.pem → webKey.pem (Symlinks)
- 6. Ein OpenVPN CA-Zertifikat und Server-Zertifikat für den Fernzugriff (VPN-Server auf der TrutzBox). Diese werden erst generiert, wenn der Fernzugriff aktiviert wird. Laufzeit 10 Jahre; bei Ablauf muss das VPN komplett neu initialisiert werden (openvpn.sh -i [domain]).
  - /etc/openvpn/ca.crt, /etc/openvpn/ca.key (CA)
  - /etc/openvpn/server.crt, /etc/openvpn/server.key (Server)
- 7. Ein OpenVPN Client-Zertifikat pro TrutzBox-Account, für den der Fernzugriff aktiviert wurde. Cipher: AES-256-GCM. Das Zertifikat befindet sich in der .ovpn-Datei (OpenVPN-Konfigurationsdatei), die der Nutzer unter „Verwaltung → Benutzer“ herunterlädt. Laufzeit 10 Jahre; Erneuerung manuell (openvpn.sh -a [client]).
  - /etc/openvpn/easy-rsa/keys/[CLIENT].crt, /etc/openvpn/[CLIENT].ovpn
- 8. Ein offizielles, öffentlich vertrauenswürdiges Let’s Encrypt-Zertifikat (ACME). Dieses kann im Menü „Fernzugriff“ oder „Videokonferenz“ für den vom Internet aus erreichbaren Domainnamen (TrutzDynDNS) der TrutzBox generiert werden. Notwendig wenn die TrutzBox vom Internet erreichbar sein soll, z. B. für den Videokonferenz-Server. Laufzeit 90 Tage; automatische Erneuerung 30 Tage vor Ablauf via Cron (/etc/cron.daily/acme-sh-cron-daily). Signiert durch eine Zwischenzertifizierungsstelle von Let’s Encrypt (Wurzelzertifikat ISRG Root X1).
  - /etc/comidio/acme/[DOMAIN]/[DOMAIN].cer, /etc/comidio/extern.trutzbox/fullchain.pem

- 9. Die Comidio Root CA Chain enthält 5 X.509 CA-Zertifikate (Root CA und Intermediate CAs), die zur Server-Verifikation aller Comidio-Verbindungen dienen. Wird via trutz-lib Package-Update aktuell gehalten.
  - /usr/lib/trutz-lib/certificate/comidio-root.pem (64-Bit)
  - /usr/lib/comidio/certs/comidio-root.pem (32-Bit)
- 10. Tor-Hidden-Service Keys (Ed25519-Schlüsselpaar) pro TrutzMail-Adresse. Ermöglichen die anonyme Zustellung von TrutzMails über das Tor-Netzwerk (.onion-Adresse) ohne Preisgabe der IP-Adresse. Kein Ablaufdatum. Das Backup der Keys ist kritisch, da bei Verlust die .onion-Adresse unwiederbringlich verloren ist.
  - 64-Bit: /var/lib/tor/[USER]/hs_ed25519_secret_key
  - 32-Bit: /home/[USER]/.torhs/hs_ed25519_secret_key
- 11. Dynamische TrutzBrowse Proxy-Zertifikate (X.509 Zertifikate, on-the-fly). Werden vom TrutzBrowse-Proxy für jede aufgerufene HTTPS-Verbindung dynamisch generiert, um die Inhaltsfilterung verschlüsselter Verbindungen zu ermöglichen (HTTPS-Interception). Signiert durch die Proxy-CA (proxyCA.crt). Die Zertifikate werden im Cache vorgehalten (TTL 10 Minuten) und bei Bedarf automatisch neu generiert.
  - /tmp/trutzbox-ca/certs/[HOSTNAME].crt
- 12. TrutzMail XMPP-Zertifikat (Prosody) (X.509 Zertifikat + Private Key). Dient der TLS-Absicherung der Server-to-Server (S2S) XMPP-Kommunikation zwischen TrutzBoxen für verschlüsselte Chat-Verbindungen. Signiert durch die Comidio Root CA. Erneuerung via Comidio Package-Update.
  - /etc/prosody/certs/auth.comidio.email.crt, /etc/prosody/certs/auth.comidio.email.key
- 13. Comidio Public Keys (Signatur-Verifikation) (OpenPGP Public Keys). Dienen als Trust Anchor zur Verifikation von Comidio-signierten Inhalten. Aktualisierung via trutzmail Package-Update. Kein Ablaufdatum.
  - /etc/comidio/comidio_email-pgp_D0340448_[...]_public.key
- 14. Jitsi Prosody XMPP-Zertifikat (X.509 Zertifikat + Private Key). Wird für die interne XMPP-Kommunikation zwischen den Jitsi-Komponenten (Videobridge, Jicofo, Prosody) verwendet. Erneuerung wie webCert (automatisch).
  - /usr/share/comidio/trutzrtc/comidio/prosody/certs/comidio.email.crt
- 15. APT Package Signatures (GPG-Signaturen + Package-Hashes). Sichern die Integrität der Debian-Softwarepakete bei Updates ab und schützen vor Manipulation. Signiert durch den Comidio APT Repository GPG Key. Automatische Aktualisierung bei apt-get update (täglich).

- /var/lib/apt/lists/update*.comidio.com_*_Release.gpg

- 16. Filterlisten-Download (Prüfsummen via mTLS). Dienen der Integritätsprüfung der heruntergeladenen Comidio-Filterlisten. Die Authentifizierung erfolgt über mTLS mit dem Box-Zertifikat. Die Listen werden täglich automatisch aktualisiert.
  - /usr/lib/blacklists/
- 17. Parameter für den Schlüsselaustausch im TLS-Handshake der OpenVPN-Verbindung (elliptische Kurve P-256, TLS 1.3). Die Sitzungsschlüssel werden je Verbindung neu ausgehandelt (Perfect Forward Secrecy). Kein Ablaufdatum.
  - /etc/openvpn/dh2048.pem
- 18. Let's Encrypt Account-Key (ACME Account Private Key, EC/RSA). Identifiziert die TrutzBox gegenüber dem Let's Encrypt ACME-Dienst. Wird einmalig angelegt und muss nicht erneuert werden. Kein Ablaufdatum.
  - /etc/comidio/acme/ca/acme-v02.api.letsencrypt.org/account.key
- 19. DynDNS API-Authentifizierung (mTLS Client-Auth). Für die DynDNS-Updates der Adresse [name].mytrutzbox.de wird das TrutzBox-Identitätszertifikat (Box-Cert, Nr. 2) zur mTLS-Authentifizierung gegenüber dem Comidio DynDNS-Server verwendet.
  - **Verwendet:** /etc/comidio/boxCert.pem + boxKey.pem
- 20. SSH Host Keys (RSA, ECDSA, Ed25519). Identifizieren die TrutzBox als SSH-Server und ermöglichen die Host-Authentifizierung bei Wartungszugängen. Selbst-generiert, kein Ablaufdatum. Bei Image-Deployment müssen die Keys neu generiert werden.
  - /etc/ssh/ssh_host_ed25519_key, /etc/ssh/ssh_host_ecdsa_key, /etc/ssh/ssh_host_rsa_key
- 21. Webmin Server-Zertifikat (X.509 Self-Signed, Combined PEM). Dient der TLS-Absicherung des Webmin-Interface (Port 10000) für die Systemadministration. Self-Signed; Erneuerung manuell über die Webmin-UI oder openssl.
  - /etc/webmin/miniserv.pem

Falls die TrutzBox von Comidio ausgetauscht oder vom Anwender auf Werksauslieferungsstand zurückgesetzt wird, werden alle Daten auf der TrutzBox gelöscht. Somit werden auch alle Zertifikate auf der TrutzBox gelöscht und beim erneuten Setup der TrutzBox neu generiert. Die TrutzMail OpenPGP-Schlüssel können mit der gleichen TrutzLegitimation auf neuer Hardware wiederhergestellt werden.

23 Anhang: Comidio BSS/OSS und TrutzLegitimation

Comidio unterhält zum Verwalten seiner Kunden und der TrutzBoxen ein BSS (Business Support System) und ein OSS (Operational Support System). Das BSS beinhaltet die trutzbox.de Webseite inkl. Content-Management-System, den Shop, CRM und Payment System. BSS und OSS dienen Comidio dazu, dem Kunden nach dem Kauf die Comidio TrutzServices liefern zu können.

23.1 TrutzServices

Ein Kunde kann eine, oder falls eine Firma gleich mehrere Remote-Mitarbeiter damit ausstatten möchte, auch mehrere TrutzBoxen kaufen. Er kauft gleichzeitig ein Servicepaket dazu (TrutzServices). Der TrutzServices-Vertrag stellt den Comidio-Support und die TrutzBox Updates sicher. Der TrutzServices-Vertrag steuert auch die Laufzeit der TrutzMail-Zertifikate und damit die Nutzbarkeit von TrutzMail und TrutzChat (für TrutzMeeting muss nur der Einladende eine TrutzMail-Adresse besitzen, die anderen Teilnehmer nicht).
Das Servicepaket beinhaltet:

- je nach Servicepaket (TrutzBox-Home oder TrutzBox-Business) ein Kontingent von TrutzMail-Accounts pro TrutzBox für die vereinbarte Laufzeit.
- Support im Umfang der jeweils gültigen Leistungsbeschreibung.
- Regelmäßige Updates für
- **Updates der Empfänger-Zertifikate:** damit werden abgelaufene oder kompromittierte Zertifikate anderer TrutzMail Accounts Ihrer TrutzBox bekannt gemacht.
- TrutzBox Software-Fehlerbeseitigungen,
- Sicherheits-Updates und
- kleinere funktionelle Erweiterungen
- **TrutzContent:** Updates für Filterlisten
- **TrutzBrowse:** Updates für Header-Ergänzungen, Standard-Slider-Einstellungen und TrutzBrowse-Blacklists
    -

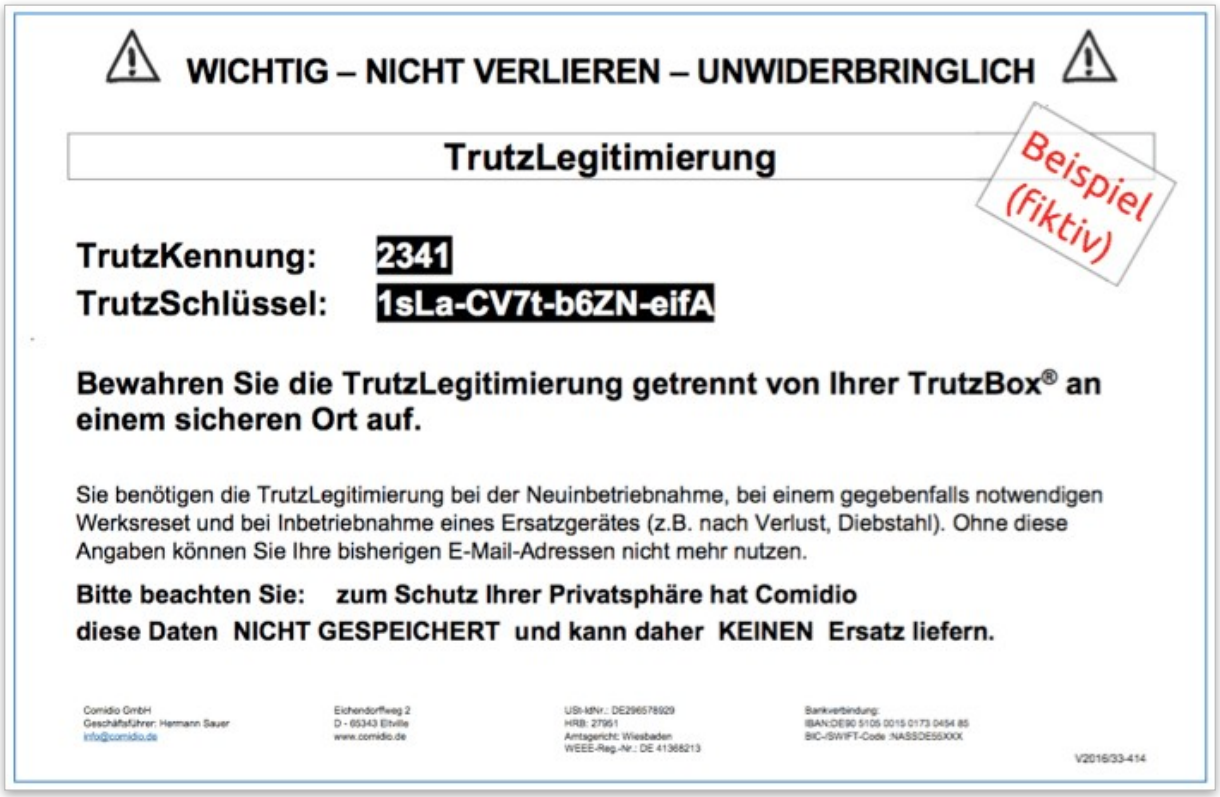
Der Kunde kann dieses Servicepaket nach Ablauf verlängern; vor Ablauf erhält er eine Erinnerung an die im trutzbox.de-Account hinterlegte E-Mail-Adresse. Ist der Service-Vertrag abgelaufen, weist eine Meldung im TrutzBox-UserInterface darauf hin, dass die TrutzBox keine Sicherheits- und Funktionsupdates mehr erhält. Maßgeblich sind die jeweils gültigen AGB und die Leistungsbeschreibung.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

Das Servicepaket ist an den Kauf einer TrutzBox gebunden. Der Kunde kann somit für jede gekaufte TrutzBox individuell entscheiden, ob er weitere TrutzMail-Accounts erwerben und ob er diese Services verlängern möchte.
Ohne Vertragsverlängerung bleibt die TrutzBox als Filter grundsätzlich nutzbar; TrutzMail und die daran gebundenen Dienste wie TrutzRTC setzen einen gültigen Service-Vertrag voraus. Maßgeblich sind die jeweils gültigen AGB und die Leistungsbeschreibung.
Auf der Serverseite von Comidio (dem OSS) entstehen die Pakete und Listen, die die TrutzBoxen beziehen. Die Paketverwaltung übernimmt Trutz-PackageMgmt, ein eigener Dienst mit Web-Oberfläche, der im Betrieb ist. Er verwaltet die Repositories für die Kanäle Testing und Stable und prüft vor jeder Veröffentlichung in einem festen Prüfschritt (Gate), ob der Paketsatz in sich stimmig ist. Die Bedienung der Repositories über einzelne, von Hand gestartete Skripte entfällt damit.
Darüber liegt als Konzept das Portal Trutz-OSS-Management. Es soll die vorhandenen Werkzeuge der Serverseite unter einer Oberfläche bündeln und die Bereiche ergänzen, die noch keine eigene Oberfläche haben. Vorgesehen sind die Bereiche Übersicht (Status aller Teilsysteme, offene Alarme, letzte Auslieferungen), Paketverwaltung (das eingebettete Trutz-PackageMgmt), Konten und Legitimationen (Verwaltung der TrutzKennungen und Verträge), Zertifikate (Bestand, Ablaufdaten und Abläufe für den Austausch, ohne Schlüsselmaterial), DynDNS (die Zone mytrutzbox.de und die Einträge je Box), Mail-Gateway (Zustellung und Warteschlangen), Monitor (die bestehende Überwachung der Server) und Plattform (die Server, auf denen die Dienste laufen). Die Verwaltung einzelner Kunden-TrutzBoxen ist ausdrücklich nicht Gegenstand des Portals; eine Fernwartung der Boxen ist nicht vorgesehen. Wenn die TrutzBox ihre Erreichbarkeit von außen prüft, bittet sie einen Server von Comidio um Testpakete an ihre eigene Adresse. Ein Zugang ist das nicht: Der Server wird nur auf Bitte der TrutzBox tätig, meldet sich nirgends an und liest nichts (Abschnitt „Erreichbarkeit von außen“ im Kapitel „Status (Netzwerk)“). Das Konzept liegt mit einer klickbaren Demo vor.

23.2 Die TrutzLegitimation aus Anwendungssicht

Beim Kauf einer TrutzBox registriert sich der Kunde im Comidio Shop mit seiner schon vorhandenen, normalen (nicht sicheren) E-Mail Adresse. Nach Bezahlung erhält er die TrutzBox, inkl. einer TrutzBox Kennung (TrutzKennung) und eines Passworts (TrutzSchlüssel). Die Kombination aus TrutzKennung und TrutzSchlüssel bildet die TrutzLegitimation. Der TrutzSchlüssel liegt bei Comidio nach dem Anlegen und nach jedem Zurücksetzen vier Wochen lang verschlüsselt vor; so lange kann Comidio das Blatt erneut ausstellen. Danach wird er bei Comidio gelöscht und ist nur noch auf dem mitgelieferten Blatt vorhanden.



Die TrutzLegitimation aus Anwendersicht (fiktives Beispiel): TrutzKennung und TrutzSchlüssel gehören zusammen.(© 2026 Comidio GmbH)

Wenn ein TrutzBox-Besitzer seine TrutzBox-Hardware verkauft, darf die TrutzLegitimation nicht weitergegeben werden, da der neue Eigentümer mit dieser TrutzLegitimation die E-Mail Identität des Verkäufers annehmen könnte.
Durch Bindung der TrutzMail Identitäten an die TrutzLegitimation (und nicht an die TrutzBox Hardware) kann Comidio folgende Anwendungsfälle (Use-Cases) mit der erforderlichen Sicherheit abdecken:

- TrutzBox verkaufen,
- TrutzBox verlieren,
- Austausch defekter TrutzBoxen; und das mit oder ohne das TrutzBox-Speichermedium (z. B. SD-Karte oder SSD-Platte),
- mehrere TrutzBoxen kaufen und Dritten zur Verfügung stellen,
- Wiedereinrichtung bereits vergebener TrutzMail Accounts auf der gleichen TrutzBox,
- TrutzBox auf Auslieferungszustand zurücksetzen,
- TrutzBox Nutzerdaten sichern und wieder zurückspeichern.

Die TrutzLegitimation ist vergleichbar mit einem Fahrzeugbrief, der den Eigentümer eines Fahrzeugs ausweist.
Bei Verlust stellt Comidio auf Anfrage einen neuen TrutzSchlüssel für dieselbe TrutzKennung aus. Der bisherige Schlüssel wird damit ungültig; eine bereits eingerichtete TrutzBox läuft weiter, weil sie sich mit ihrem Zertifikat ausweist, und die TrutzMail-Adressen bleiben der TrutzKennung zugeordnet.
Trotzdem gehört die TrutzLegitimation sicher verwahrt: Sie weist den Inhaber des Service-Vertrags aus, und wer sie in die Hände bekommt, kann die TrutzBox neu einrichten, solange der Schlüssel gilt.
Wer die TrutzLegitimation hat, kann bei Diebstahl die damit bereits registrierten TrutzMail Accounts aufsetzen und die TrutzMail Identität z. B. des Bestohlenen übernehmen. Der Verlust der TrutzLegitimation sollte Comidio sofort gemeldet werden, damit Comidio alle damit ausgestellten TrutzMail Accounts für „ungültig“ erklären kann. Durch den TrutzMail Blacklist-Update werden dann allen TrutzBoxen, die dieses Zertifikat haben, die Kompromittierung mitgeteilt.
Somit hat Comidio dafür gesorgt, dass die TrutzBox die komplette Zertifikats- und Key-Verwaltung für den Anwender übernimmt. Weitere Details dazu sind im Kapitel TrutzMail beschrieben.
Loggt sich ein Kunde in seinem Account bei trutzbox.de ein, wird ihm eine Übersicht seines Comidio Accounts angezeigt. Er kann sehen, inwieweit sein TrutzMail Kontingent ausgeschöpft ist, kann weitere TrutzMail-Account-Kontingente kaufen oder die Laufzeit seiner Kontingente und seines Servicepakets verlängern.

23.3 Die TrutzLegitimation aus System-Sicht

Die TrutzLegitimation bekommt jeder Kunde pro TrutzBox einmal ausgedruckt und in dem TrutzBox Paket mitgeliefert. Sie wird zentral von Comidio kurz vor Auslieferung einer bestellten und bezahlten TrutzBox generiert. Sie beinhaltet die TrutzKennung und den zugehörigen TrutzSchlüssel.
Beides gibt der Kunde bei der erstmaligen Inbetriebnahme und nach jedem Reset auf Werkseinstellung ein; damit weist er sich als Inhaber des TrutzBox Service-Abos aus. Bei der Auslieferung ist die TrutzLegitimation der TrutzBox Hardware noch nicht zugeordnet.
Erst bei der Inbetriebnahme der TrutzBox durch den Kunden wird die TrutzLegitimation mit der TrutzBox Hardware verknüpft (genauer gesagt mit der SSD-Platte, auf der alle Daten gespeichert sind). Während des Betriebs der TrutzBox wird dann überprüft, welche TrutzServices der Kunde nach aktueller Abo-Situation bekommt. Die Laufzeit des Abos steuert das Ablaufdatum (Expire-Date) der TrutzMail-Zertifikate und der Updates. Die TrutzServices (Mail und Updates) sind somit immer mit der TrutzLegitimation verknüpft.
Private Schlüssel und Passwörter liegen ausschließlich auf der TrutzBox; nach einem Verlust legt die Box mit derselben TrutzLegitimation die TrutzMail Adressen auf beliebiger TrutzBox Hardware neu an und erzeugt dabei neue Schlüssel. Was die Bindung an die TrutzLegitimation für Verkauf, Verlust und Hardware-Tausch bedeutet, steht im Kapitel „Die TrutzLegitimation aus Anwendungssicht“; eine Ersatz-Legitimation gibt es nur nach Rücksprache mit Comidio im Shop.

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2

24 Index

5-GHz-Kanäle 186

Absenderadresse (SMTP) 114

Abstreitbarkeit 105

Alias (Absenderadresse) 115

Alle Empfänger-Zertifikate löschen 120

Angriffsschutz (fail2ban) 8, 170

Anmeldename (SMTP) 114

Apache-Traffic-Server 61

Audio- und Video-Konferenz-Server 134

Authentizität 104

Autoconfig (Thunderbird) 125

Betriebszustand 204

Blacklist 60

Blockierte IP-Adressen 169

Bonjour 161

Bot-Netz 104

Browser SSL-Verbindungen 88

Brückenverkehr (br_netfilter) 27

CGNAT 129

Chat 134

Chat-Räume 145

Client-basierter Fingerprint 74

Cookies 60

Debian Package Manager 229

Details (Erreichbarkeit von außen) 163

DHT 108

Dienst-Symbole (Monitor) 28

Digitalen Selbstverteidigung 8

distributed hash tables 108

DNS-Auflösung, verschlüsseltes DNS (DoT) 8, 179

Dovecot 107

Dpkg 229

DS-Lite-Tunnel 129, 130, 131, 198

Edge-Computing 106

EFF (Electronic Frontier Foundation) 134

Eigener Name (TrutzDynDNS) 131

Eigenhosting 106

E-Mail-Programm 104, 125

E-Mail-Provider 103, 104

E-Mail-Verschlüsselung 103

Ereignis-Protokoll 213

Erreichbar, nur über IPv4 163

Erreichbarkeit von außen 155, 163

Extensible Messaging and Presence Protocol 139

Externe Verbindungen zu TrutzRTC 145

Externe Verbindungen zum TrutzRTC-Konferenz-Server 151

Fernzugriff 187

Filtergruppe 96

Filterlisten 66

Filterlisten importieren 67, 68

Firewall 8, 9, 164, 166

Firewall-Ausnahmen 169

Firewall-Monitor 155, 176

FRITZ!Box, IPv6-Freigabe 199

Geführte Touren (Monitor) 22

Gehärtetes Betriebssystem 229

Geräte an der TrutzBox anschließen 15

Gerätetyp festlegen 51, 52

http-header 85

HTTP-Header-Daten 60, 74

http-Query Parameter 85

Image-Update 223, 227

Intelligenter Security-Slider 77

Interface-ID (IPv6) 128

Interner Datenverkehr (Monitor) 27

Internetfähige Geräte 10

IP-Blocklisten 42, 167

IPv6 198

IPv6 Unterstützung 197

IPv6-Interface-ID 199

Jabber 139

Jitsi-Meet 150

Kommandozeile (SSH) 221

Kommunikation über öffentliche Netze 104

Kompromittiert 119

Kompromittierung 250

LAN-Anschlüsse 239

LAN-Ext-Anschluss 158

Last-Seen 145

Lavabit 107

Let's Encrypt (DNS-01) 131

Mail-Programm einrichten 125

MailCert 118

Mail-Server 106

mDNS 100, 161, 202

Messaging 134

Mobilfunk-Router 129

ModSecurity 61

Monitor 8, 21

Monitor, Sperren und Freischalten 44

mytrutzbox.de 127

Netzwerk-Bridge 159

Netzwerkname (Mail-Programm) 125

Node.js 61

Öffentliche IPv4-Adresse ermitteln 128

öffentliche Schlüssel 112, 113

Online-Status 145

Open-Source Proxys 61

OpenVPN 189

Outlook 126

Paketkanal Testing/Stable 213

Passwortregel 56

Perfect Forward Secrecy 105

PGP 103

Port von außen für VPN 132

Präfix-Delegation (DHCPv6-PD) 129

Privacy by Design (PbD) 229

Privater Schlüssel 118

Privoxy 61

Raum-Name 149

root (Konto) 222

Root-Zertifikat 90

Root-Zertifikate 89

RoundCube 107

Schwachstellen melden 228

Security-Anforderungen 104, 105

Security-Slider 77, 96

Sicherheits- und Anonymisierungsvorteile 9

Sicherheits-Schieberegler 77

Sicherung aller Einstellungen 231

Sicherungskopien (TrutzDynDNS) 133

SIP-Gateway 150

Skype 134

Slider-Definition 78

SSH (Kommandozeile) 175, 221

SSL/TLS 88

Stamm-Zertifikat 90

Standardposition Slider 52

Stateful Packet Inspection Firewall (SPI) 166

Systemgrenzen 210

Telefon- oder Video-Konferenzen 147

Terminal (im Browser) 222

Testpakete (Erreichbarkeit) 129

Third-Party-Cookies 80

Thunderbird 125

Tor-hidden-services 108

Tor-Netzwerk 52

Tor-Netzwerk verwenden 52

TrutzBase 8, 9, 154

TrutzBox Betriebssystem 218, 229

TrutzBox Hardware 239

TrutzBox Setup 13

TrutzBox User-Interface 229

TrutzBox zurücksetzen 231

TrutzBox-Proxy 95

TrutzBox-VPN Portfreigabe 190

trutzbox.local 13, 100, 161

TrutzBrowse 9, 60, 73, 96

TrutzBrowse-Blacklists 82

TrutzBurg 53

TrutzBurg Symbol 82

TrutzChat (Web-Client) 140

TrutzContent 9, 60, 96

TrutzDynDNS 127

TrutzDynDNS nur mit IPv6 130, 131

TrutzLegitimation 120, 242, 248, 250

TrutzMail Adresse 109

TrutzMail-Adress-Blacklist 119

TrutzRTC 8, 9

TrutzRTC Architektur 152

TrutzRTC Portfreigabe 151

TrutzServices 224, 247

Verkehr ohne Domain-Namen (QUIC, ECH, DoH) 176

Vertraulichkeit 104

Video-Konferenz 134, 147

Voice-over-IP-Verschlüsselung 147

VPN - Virtual Private Network 187

VPN-Server 189

VPN-Zugriff 196

Web-Mailer 107

WebRTC 134, 147

Werbe- oder Statistik-Server 60

WhatsApp 134

Whitelist 51

WireGuard 190, 193, 202

WLAN 8, 185

WLAN-Adapter 240

XMPP-Server 134

Zeitserver (NTP) 8, 183

Zone mytrutzbox.de 128, 129

zrtp 147

© 2026 Comidio GmbH · Alle Rechte vorbehalten · Rechtliche Hinweise Seite 2