

TrutzBox Handbuch

Privatsphäre und Sicherheit, zuhause, unterwegs und in der Firma

Gilt für die TrutzBox EVO (64 Bit) ab Betriebssystem 2.5.0, Image V80

Ausgabe November 2026

Comidio GmbH · Eichendorffweg 2 · 65343 Eltville

Inhaltsverzeichnis

Über dieses Handbuch 7

Teil A: Die TrutzBox kennenlernen 8

1 Was die TrutzBox für Sie tut 8
1.1 Privatsphäre und Sicherheit: für jeden Einzelnen, zuhause, unterwegs und in der Firma 8
1.2 Das Geschäft mit Ihren Daten 9
1.3 Angriffe: was aus den Daten gemacht wird 9
1.4 Warum Einzelmaßnahmen nicht reichen 10
1.5 Warum eine Firewall allein nicht genügt 11
1.6 Wovor die TrutzBox schützt 11
1.7 Die Funktionen im Überblick 13
1.8 Ihr Weg durch dieses Handbuch 14
2 Auspacken und Anschlüsse 16
2.1 Lieferumfang 16
2.2 Die Anschlüsse 17
2.3 Die LEDs an der TrutzBox 19
2.4 Aufstellort, Belüftung und Dauerbetrieb 20
2.5 Mehr Geräte anschließen: der Switch 21

Teil B: Inbetriebnahme 22

3 TrutzBox einrichten (Setup) 22
3.1 Die TrutzBox anschließen 22
3.2 Das Setup im Browser öffnen 23
3.3 Schritt „Willkommen" 25
3.4 Schritt „Netzwerkeinstellungen" 25
3.5 Software-Updates während der Einrichtung 26
3.6 Schritt „TrutzBox registrieren" und Sicherung einspielen 27
3.7 Schritt „Admin-Passwort setzen" 29
3.8 Schritt „TrutzMail einrichten" 30
3.9 Schritt „Einrichtung abgeschlossen" 32
3.10 Wie es jetzt weitergeht: Geräte anschließen 32
3.11 Der Ablauf auf einen Blick 33
Häufige Fragen zur Einrichtung 33
4 Ein Gerät mit der TrutzBox absichern 35
4.1 Drei Wege zur TrutzBox 35
4.2 Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen 36
4.3 Weg 2: Gerät im Proxy-Mode betreiben 37
4.4 Weg 3: TrutzVPN für mobile Geräte 38
4.5 Welcher Weg für welches Gerät? 39
Häufige Fragen zum Anschließen 39

Teil C: Die Funktionen im Alltag 41

5 Startseite und Betriebszustand 41
5.1 Die Startseite lesen 42
5.2 Betriebszustand: die Ampel lesen 48
5.3 Betriebszustand: die Karten im Einzelnen 50
5.4 Betriebszustand: Verlauf und Ereignis-Protokoll 55
5.5 Betriebszustand: Meldungen verstehen 56
6 Geräte verwalten 58
6.1 Neue Geräte erscheinen automatisch 58
6.2 Geräte benennen 59
6.3 Filtergruppen zuordnen 60
6.4 Die Spalten der Geräteliste 60

6.5 Unbekannte Geräte erkennen....61
6.6 Gäste und gemeinsam genutzte Geräte....62
6.7 Weitere Einstellungen je Gerät....62
6.8 Aufräumen: alte Einträge entfernen....64
Häufige Fragen zu Geräten....65
7 Benutzer, Postfächer, Passwörter....67
7.1 Drei Arten von Konten....67
7.2 Benutzer anlegen und verwalten....68
7.3 Passwörter ändern....69
7.4 Die Detail-Einstellungen eines Benutzers....70
7.5 Löschen, Reaktivieren und das Kontingent....71
7.6 Anmelden an der Oberfläche....72
Häufige Fragen zu Benutzern....73
8 Webfilter und Jugendschutz (TrutzContent)....74
8.1 So greift alles ineinander: Geräte, Filtergruppen, Filterlisten....74
8.2 Filtergruppen einrichten....76
8.3 Wie die Altersgruppen eingeteilt sind....77
8.4 Filterlisten verwalten....78
8.5 Filterlisten aus dem Internet laden und automatisch aktualisieren....80
8.6 Ausnahmen je Gerät....82
8.7 Die Sperrseite verstehen....82
8.8 Ein Vorschlag für den Anfang....83
8.9 Eigene Sperren und Ausnahmen....83
Häufige Fragen zum Webfilter....86
9 Monitor und Statistiken....87
9.1 Die eingebauten Führungen: Hilfe direkt in der Seite....87
9.2 Der Aufbau: Geräte, TrutzBox, Internet....89
9.3 Die drei Darstellungen....92
9.4 Zeitraum und Speicherdauer....96
9.5 Untersuchen und eingreifen....96
9.6 Drei Fragen, die der Monitor beantwortet....98
9.7 Statistiken: Blockierungen über lange Zeiträume....98
9.8 Eine Seite zeigt eine Sperrseite: die Seitenanalyse....99
Häufige Fragen zum Monitor....101
10 TrutzMail: sichere E-Mail....103
10.1 Drei Wege des Mail-Austauschs....103
10.2 Webmail benutzen....105
10.3 Ein Mail-Programm einrichten....105
10.4 Die Kennzeichnung im Betreff: [SE], [UE], [UU]....107
10.5 Weg B einrichten: Postfach beim Anbieter verbinden....108
10.6 Schlüssel und Zertifikate....110
10.7 Wenn eine Mail nicht ankommt....112
10.8 Adressen anlegen, löschen und reaktivieren....113
10.9 Was Comidio sieht und was nicht....114
Häufige Fragen zu TrutzMail....114
11 TrutzDynDNS: Ihre TrutzBox aus dem Internet erreichbar machen....116
11.1 Wozu Ihre TrutzBox von außen erreichbar sein muss....116
11.2 TrutzDynDNS einschalten....116
11.3 Welcher Anschluss ist von außen erreichbar?....117
11.4 TrutzDynDNS nur mit IPv6....119
11.5 Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden....120
12 TrutzChat und Videokonferenz....122
12.1 Die Seite Videokonferenz und Chat....122
12.2 Reiter Videokonferenz: einmalig einrichten....124
12.3 Konferenzen im Alltag....126
12.4 Reiter TrutzChat: Selbsttest, Aufbewahrung, Gruppen....127
12.5 TrutzChat benutzen: im Browser und mit einer Chat-App....129

12.6 Kontakte und Gruppen ... 132
12.7 Was im Hintergrund für Sicherheit sorgt ... 133
Häufige Fragen zu Chat und Videokonferenz ... 133
13 TrutzBox unterwegs nutzen (TrutzVPN) ... 135
13.1 So funktioniert TrutzVPN ... 135
13.2 Schritt 1: Domain-Name festlegen (TrutzDynDNS) ... 139
13.3 Schritt 2: Portweiterleitung am Internet-Router ... 139
13.4 Schritt 3: Tunnel wählen ... 140
13.5 Schritt 4: Erreichbarkeit von WireGuard prüfen ... 141
13.6 Schritt 5: Zugänge für die WireGuard-App anlegen ... 143
13.7 Ihre Geräte einrichten ... 145
13.8 Unterwegs verbinden ... 145
13.9 Wenn es nicht klappt ... 146
13.10 Was der Fernzugriff sonst noch ermöglicht ... 148
13.11 VPN auch über IPv6 anbieten ... 148
13.12 OpenVPN statt WireGuard verwenden ... 150
Häufige Fragen zu TrutzVPN ... 153
14 TrutzBrowse: zusätzlicher Schutz für Browser und Apps ... 155
14.1 Was TrutzBrowse leistet ... 155
14.2 Woraus ein Fingerabdruck entsteht ... 156
14.3 Webfilter und TrutzBrowse: zwei Stufen, ein Ziel ... 157
14.4 Was der Security-Slider praktisch bewirkt ... 158
14.5 Das TrutzBurg-Menü im Browser ... 160
14.6 TrutzBrowse je Gerät einschalten ... 161
14.7 Wenn eine Seite nicht richtig funktioniert ... 161
14.8 Den Nutzen im Monitor sehen ... 162
Häufige Fragen zu TrutzBrowse ... 162

Teil D: Die TrutzBox verwalten 164
15 TrutzBox-Netzwerk: Schutz und Verwaltung ... 164
15.1 Netzwerk-Übersicht: außen und innen ... 164
15.2 Das WLAN der TrutzBox ... 168
15.3 DNS-Schutz und verschlüsselte Namensauflösung ... 171
15.4 Angriffsschutz: Firewall und Wächter ... 173
15.5 Netzwerk-Einstellungen ändern ... 177
Häufige Fragen zum Netzwerk ... 177
16 Updates ... 179
16.1 Die drei Arten von Updates ... 179
16.2 Software-Paket-Updates ... 180
16.3 Filter- und Sperrlisten-Updates ... 181
16.4 Warum diese Updates sicher sind ... 181
16.5 Voraussetzung: ein gültiger Service-Vertrag ... 182
16.6 Stand und Verlauf einsehen ... 182
16.7 Der Ausnahmefall: ein komplettes Image ... 183
16.8 Ankündigungen, Fragen und Meldungen ... 186
Häufige Fragen zu Software-Updates ... 186
17 Sichern, Wiederherstellen und Zurücksetzen ... 188
17.1 Was in der Sicherung steckt ... 188
17.2 Eine Sicherung anlegen ... 189
17.3 Wiederherstellen: im Betrieb oder im Setup ... 190
17.4 System zurücksetzen (Werksreset) ... 190
17.5 Checkliste vor und nach dem Zurücksetzen ... 196
17.6 Die TrutzBox weitergeben ... 197
Häufige Fragen zum Sichern ... 198
18 Experten-Zugänge: Webmin, Terminal und SSH ... 200
18.1 Webmin: der Experten-Zugang ... 200
18.2 Die Kommandozeile: Terminal und SSH ... 200

Teil E: Wenn etwas nicht klappt 202
19 Was tun, wenn …? 202
19.1 Die Übersicht: welches Symptom, welcher Abschnitt 202
19.2 … kein Internet da ist 203
19.3 … eine Seite blockiert wird oder eine App nicht startet 203
19.4 … eine Seite sehr langsam lädt 204
19.5 … der Browser eine Zertifikatswarnung zeigt 205
19.6 … eine E-Mail nicht ankommt 206
19.7 … ein Gerät nicht auftaucht 206
19.8 … ein Gerät sich nicht mit dem TrutzBox-WLAN verbindet 207
19.9 … Gäste in der Videokonferenz eine Zertifikatswarnung sehen 207
19.10 … ein Chat-Kontakt dauerhaft als nicht erreichbar erscheint 208
19.11 … die Verwaltungsoberfläche nicht erreichbar ist 209
19.12 … die TrutzBox überhaupt nicht mehr reagiert 210
19.13 … nach einem Software-Update etwas nicht mehr funktioniert 211
19.14 … der Speicherplatz knapp wird 211
19.15 … die TrutzBox neu gestartet oder zurückgesetzt werden soll 212
19.16 … das Passwort für das Admin-Panel nicht mehr bekannt ist 213
19.17 … Sie umziehen oder einen neuen Internet-Router bekommen 213
20 Support kontaktieren 215
20.1 Zuerst: die Selbstdiagnose der TrutzBox 215
20.2 Was in den Support-Bericht gehört 216
20.3 Protokolldateien herunterladen 217
20.4 Wege zum Support 218
20.5 Das Forum sinnvoll nutzen 218
20.6 Was Comidio nicht kann und nicht tut 219
20.7 Hardware-Defekt und Tausch des Boot-Mediums 219
20.8 Das Speichermedium tauschen 220

Teil F: Anhang 222
21 Das Root-Zertifikat installieren 222
21.1 Wann Sie das Root-Zertifikat brauchen 222
21.2 Das Root-Zertifikat herunterladen 223
21.3 Installieren auf den gängigen Systemen 223
21.4 Programme mit eigenem Zertifikatsspeicher 224
21.5 Wenn sich kein Zertifikat installieren lässt 224
21.6 Nach einem Zurücksetzen der TrutzBox 225
Häufige Fragen zum Root-Zertifikat 225
22 Mail-Programme für TrutzMail einrichten 226
22.1 Die Angaben für jedes Mail-Programm 226
22.2 Thunderbird einrichten 227
22.3 Apple Mail auf dem Mac einrichten 227
22.4 Mail auf iPhone und iPad einrichten 227
22.5 Mail-App auf Android einrichten 228
22.6 Outlook einrichten 228
22.7 Wenn das Mail-Programm keine Verbindung bekommt 228
23 Chat-Programme für TrutzChat einrichten 230
23.1 Die Angaben für jedes Chat-Programm 230
23.2 Empfohlene Chat-Programme 230
23.3 Ein Chat-Programm einrichten 231
23.4 Wenn das Chat-Programm keine Verbindung bekommt 231
24 VPN-Apps für TrutzVPN einrichten 232
24.1 WireGuard unter Windows 232
24.2 WireGuard unter macOS 232
24.3 WireGuard auf iPhone und iPad 232
24.4 WireGuard auf Android 233
24.5 WireGuard unter Linux 233

24.6 Geräte mit OpenVPN einrichten....233
24.7 Wenn die VPN-App keine Verbindung bekommt....234
25 Den Proxy-Mode am Gerät einrichten....235
25.1 Die Angaben für jedes Gerät....235
25.2 Proxy unter Windows....235
25.3 Proxy unter macOS....235
25.4 Proxy auf iPhone und iPad....236
25.5 Proxy auf Android....236
25.6 Proxy unter Linux....236
25.7 Firefox....236
25.8 Prüfen, ob der Proxy-Mode wirkt....236
26 Ports und Freigaben am Internet-Router....237
26.1 Welche Ports die TrutzBox braucht....237
26.2 Beispiel: die Freigaben in einer FRITZ!Box....238
26.3 Die IPv6-Freigabe in einer FRITZ!Box....240
26.4 Anleitungen der Router-Hersteller....241
27 Sicherheit, Entsorgung und Kontakt....242
27.1 Sicherheitshinweise....242
27.2 Entsorgung....242
27.3 Gewährleistung und Ersatzteile....243
27.4 Datenschutz in eigener Sache....243
27.5 Hersteller und Kontakt....243
Glossar: wichtige Begriffe erklärt....245
Stichwortverzeichnis....251

Über dieses Handbuch

Dieses Handbuch begleitet Sie durch alle Funktionen Ihrer TrutzBox, von der ersten Inbetriebnahme bis zur täglichen Nutzung. Es richtet sich an Anwender ohne besondere Technik-Vorkenntnisse: Jeder Fachbegriff wird bei seinem ersten Auftreten kurz erklärt, und hinten im Buch fasst das Glossar die wichtigsten Begriffe noch einmal zusammen.

Sie müssen das Buch nicht von vorne bis hinten lesen. Jedes Kapitel steht für sich; wo Wissen aus anderen Kapiteln nützlich ist, finden Sie einen Verweis mit dem Titel des Kapitels oder Abschnitts. Wenn Sie Ihre TrutzBox gerade erst ausgepackt haben, beginnen Sie mit Teil B: Kapitel „TrutzBox einrichten (Setup)“ führt durch die Einrichtung, Kapitel „Ein Gerät mit der TrutzBox absichern“ bringt Ihre Geräte unter den Schutz der TrutzBox.

So finden Sie sich zurecht:

- **Nummerierte Schritte** zeigen Handgriffe in fester Reihenfolge. Führen Sie sie von oben nach unten aus.
- **Fettdruck** bezeichnet Dinge, die Sie so auf dem Bildschirm sehen: Menüpunkte, Schaltflächen, Feldnamen.
- Farbige Kästen ergänzen den Text: **Wichtig** (rot) warnt vor Stolpersteinen, **Tipp** (grün) gibt praktische Ratschläge, **Für Neugierige** (grau) erklärt die Technik dahinter. Alles in grauen Kästen können Sie überspringen, ohne etwas für die Bedienung zu verpassen.
- Verweise wie „Benutzer, Postfächer, Passwörter“ nennen den Titel eines Kapitels oder Abschnitts. Im PDF springen Sie mit einem Klick dorthin, auf Papier hilft die Inhaltsübersicht vorn im Buch. Das Stichwortverzeichnis am Ende hilft bei der Suche nach einzelnen Begriffen.

Zu sechs Themen gibt es das Wichtigste außerdem als **Anleitung zum Anklicken**: Ersteinrichtung, Monitor, Webfilter, Angriffsschutz, TrutzVPN und TrutzMail. Jede Anleitung zeigt echte Bildschirmansichten, markiert die Stelle, auf die es ankommt, und erklärt sie in Text und Ton, Station für Station. Sie läuft im Browser ohne Installation und passt gut als erster Überblick, bevor Sie das Kapitel lesen. Alle sechs finden Sie unter trutzbox.de/videodokumentation; die betreffenden Kapitel verweisen am Anfang darauf.

Die Bildschirmfotos zeigen die deutsche Oberfläche in der zum Redaktionsschluss aktuellen Version. Einzelne Ansichten können sich mit Software-Updates leicht ändern; die beschriebenen Wege bleiben davon in aller Regel unberührt.

Ihre TrutzBox schützt Sie an zwei Fronten zugleich: Sie wahrt Ihre Privatsphäre gegenüber Datensammlern und Werbenetzwerken, und sie sichert Ihr Netzwerk gegen Angriffe aus dem Internet ab. Beides gilt für jeden Einzelnen, ob die TrutzBox nun zuhause die Familie schützt oder in der Firma die Mitarbeiter.

1 Was die TrutzBox für Sie tut

Die TrutzBox ist ein kleines Gerät, das zwischen Ihrem Internet-Router und Ihren Geräten sitzt und dort zwei Aufgaben zugleich erledigt: Sie schützt Ihre **Privatsphäre** vor Datensammlern und Werbenetzwerken, und sie schützt Ihr Netzwerk vor **Angriffen** aus dem Internet. Dieses Kapitel erklärt, warum beides nötig ist und mit welchen Funktionen die TrutzBox es leistet. Wer gleich loslegen möchte, kann direkt zu Kapitel „TrutzBox einrichten (Setup)“ springen und später hierher zurückkehren.

Das Kapitel ist bewusst ausführlich. Sie müssen es nicht gelesen haben, um die TrutzBox zu benutzen. Wer aber verstehen möchte, warum die TrutzBox so arbeitet, wie sie arbeitet, und warum sie ausgerechnet an dieser Stelle im Netzwerk sitzt, findet hier die Begründung. Die genannten Zahlen stammen aus veröffentlichten Studien und Berichten, die das Comidio-Team im TrutzBox-Kompendium zusammengetragen hat.

1.1 Privatsphäre und Sicherheit: für jeden Einzelnen, zuhause, unterwegs und in der Firma

Stellen Sie sich vor, ein unsichtbarer Beobachter notiert genau, was Sie im Internet anschauen, wie lange, von welchem Gerät und was Sie als Nächstes tun. Genau das passiert bei fast jedem Seitenaufruf. Allein ein Baustein von Google, der aufzeichnet, was Besucher auf einer Seite tun, steckt nach aktuellen Messungen in 61 Prozent aller Webseiten. Dazu kommen die Werbeauktionen, die bei jedem Seitenaufruf im Hintergrund ablaufen: Angaben über jeden Menschen in Europa werden dabei im Schnitt 376-mal am Tag an Werbefirmen weitergereicht, ohne dass der Betroffene etwas davon sieht.

Diese Übermittlung ist kein Angriff und kein Einbruch. Für jedes Schutzprogramm sieht sie aus wie ganz normaler Web-Verkehr, und genau darin liegt das Problem: Was legal und unauffällig aussieht, wird von klassischen Schutzmaßnahmen nicht angehalten.

Die zweite Front sind Angriffe: automatische Scanner, die rund um die Uhr jeden Internet-Anschluss abklopfen, Schadsoftware, Erpressungstrojaner, Phishing. Ein einziger unbedachter Klick eines Kindes oder Gastes kann genügen, um das gesamte Netz zu kompromittieren. Und die Zahl der Geräte, die dabei zum Einfallstor werden können, wächst ständig: Fernseher, sprachgesteuerte Lautsprecher, Thermostate, Kameras. Viele dieser Geräte senden, was und wohin der Hersteller will, und lassen sich selbst weder absichern noch kontrollieren.

Einzelmaßnahmen greifen hier zu kurz. Ein Browser-Zusatz schützt den Browser, aber nicht das Smartphone. Ein Werbeblocker hilft am PC, aber nicht dem Fernseher. Schutz, der davon abhängt, dass jedes Gerät einzeln richtig eingestellt ist und bleibt, funktioniert im Alltag nicht. Die TrutzBox setzt deshalb an der einen Stelle an, an der alle Geräte vorbeimüssen: am Übergang zwischen Ihrem Netzwerk und dem Internet. Was durch die TrutzBox läuft, wird geprüft, gefiltert und protokolliert, vollautomatisch und für alle Geräte gleichzeitig, vom PC bis zum Thermostat.

Das gilt zuhause wie in der Firma. In der Familie schützt die TrutzBox Kinder vor ungeeigneten Inhalten und alle vor Schadsoftware und unerwünschtem Datenverkehr: Werbung, dem Aufzeichnen dessen, was man im Internet tut, und Verbindungen zu gefährlichen Servern. Im Unternehmen schützt sie Mitarbeiter vor Ausspähung und senkt damit ganz direkt das Risiko von

Phishing und Betrugsmaschen, die auf gesammelten persönlichen Daten aufbauen. Die TrutzBox wird in Deutschland entwickelt; alle Comidio-Dienste laufen auf eigener Infrastruktur in Deutschland nach deutschem und europäischem Datenschutzrecht.

> **Zwei Ziele, ein Gerät**
>
> Privatsphäre und Sicherheit werden oft als getrennte Themen behandelt. Sie hängen aber eng zusammen: Je mehr ein Angreifer über eine Person weiß, desto überzeugender kann er sie täuschen. Persönliche Daten, die heute ganz legal gehandelt werden, sind das Rohmaterial für den Betrug von morgen. Deshalb behandelt die TrutzBox beides als eine einzige Aufgabe.

1.2 Das Geschäft mit Ihren Daten

Hinter der Beobachtung steht kein Zufall, sondern ein Markt. Der weltweite Handel mit persönlichen Daten wird für 2025 je nach Schätzung auf 300 bis 430 Milliarden US-Dollar beziffert. Zum Vergleich: Für IT-Sicherheit wurden im selben Jahr weltweit rund 218 Milliarden US-Dollar ausgegeben. Mit dem Sammeln und Verkaufen von Daten lässt sich also mehr verdienen als mit dem Schutz davor.

Ein einzelner großer Datenhändler wirbt mit Daten zu 2,6 Milliarden Menschen und mehr als 10.000 Merkmalen je Person. Bei rund sechs Milliarden Internetnutzern weltweit ist damit ein Großteil der Online-Bevölkerung in kommerziellen Datenbanken verzeichnet. Diese Menschen wissen davon nichts, haben es nie aktiv erlaubt und können die Daten praktisch nicht löschen lassen.

Wie fein diese Daten sortiert werden, zeigte 2023 eine Recherche zu einem großen Werbe-Datenmarktplatz: Dort wurden über 650.000 Kategorien angeboten, in die sich Nutzer einsortieren lassen, und 93 Datenhändler stellten ihre Datensätze zum Verkauf. Der Erwerb solcher Daten ist kein Hackerangriff, sondern ein gewöhnlicher Geschäftsvorgang auf einem offiziellen Marktplatz.

Für Sie als Einzelnen bedeutet das: Ihre Interessen, Ihr Tagesablauf, Ihr Gesundheitszustand, Ihr Wohnort und Ihre beruflichen Kontakte liegen in fremden Datenbanken, verknüpft zu einem Profil, das Sie selbst nie zu Gesicht bekommen. Sichtbar wird es nur indirekt, in Preisen, in Angeboten, in Bewertungen der Kreditwürdigkeit oder in einer auffallend gut informierten Betrugsmail.

> **Für Neugierige: Warum das Sammeln so schwer zu bemerken ist**
>
> Das Aufzeichnen nutzt keine Sicherheitslücke, sondern den ganz normalen Aufbau moderner Webseiten. Eine Seite besteht aus Bausteinen, die von vielen verschiedenen Servern kommen: Bilder, Schriften, Skripte, Werbeflächen. Jeder dieser Aufrufe ist eine eigene Verbindung, und jede Verbindung verrät dem Empfänger Ihre Adresse, Ihr Gerät und die Seite, auf der Sie gerade sind. Was Sie als eine Seite wahrnehmen, sind technisch oft dutzende Gespräche mit dutzenden Fremden.

1.3 Angriffe: was aus den Daten gemacht wird

Gesammelte Daten bleiben nicht in der Werbewirtschaft. Sie sind auch die Grundlage für gezielte Angriffe. Beim sogenannten CEO-Betrug geben sich Täter als Vorgesetzte aus und bringen

Mitarbeiter dazu, Geld zu überweisen oder vertrauliche Unterlagen herauszugeben. Zwischen 2013 und 2023 wurden dem FBI über 305.000 solcher Vorfälle mit einem Gesamtschaden von mehr als 55 Milliarden US-Dollar gemeldet.

Wirksam macht diese Angriffe nicht Technik, sondern Wissen. Ein Angreifer kauft Angaben über eine Zielperson zusammen: vollständiger Name, genauer Titel, Arbeitgeber, Telefonnummer, ungefährer Wohnort, berufliche Aktivitäten der letzten Monate, Name des Vorgesetzten. Mit diesem Material schreibt er eine E-Mail, die ein laufendes Projekt beim Namen nennt und deshalb echt wirkt. Ohne den Datenmarkt wäre dieser Brief nicht zu schreiben.

Für Unternehmen kommen die unmittelbaren Folgen von Schadsoftware hinzu. Der Digitalverband Bitkom beziffert die Schäden der deutschen Wirtschaft für 2026 auf 211 bis 271 Milliarden Euro, durch Diebstahl von Ausrüstung und Daten, Spionage und Sabotage; rund drei Viertel davon gehen auf Cyberangriffe zurück. Weltweit wird der jährliche Schaden durch Cyberkriminalität auf rund 10,5 Billionen US-Dollar geschätzt, eine Zahl, auf die sich auch das Weltwirtschaftsforum stützt.

Die dritte Quelle sind die eigenen Geräte. Ende 2025 waren weltweit rund 21 Milliarden vernetzte Geräte in Betrieb, Smartphones und Computer nicht mitgezählt; bis 2030 werden rund 39 Milliarden erwartet: Glühbirnen, Steckdosen, Waschmaschinen, Kühlschränke, Heizkessel, Türklingeln, Sicherheitskameras, Babyfone, Spielzeug. Viele davon übermitteln regelmäßig Nutzungszeiten, Einstellungen, Standort- und Verhaltensdaten an die Server ihrer Hersteller. Sprachgesteuerte Lautsprecher lauschen dauerhaft auf ihr Aktivierungswort.

Diese Geräte sind der Punkt, an dem persönliche Ratschläge endgültig nicht mehr helfen. Ein Fernseher nimmt keine Schutzsoftware an, ein Heizungsregler kennt keine Zwei-Faktor-Anmeldung, eine Türklingel lässt sich nicht härten. Sie senden, was der Hersteller vorgesehen hat. Nur eine vorgeschaltete Instanz im Netz kann diesen Verkehr überhaupt sichtbar und damit kontrollierbar machen.

1.4 Warum Einzelmaßnahmen nicht reichen

Gegen all das gibt es viele einzelne Werkzeuge, und jedes davon ist für sich sinnvoll. Das Problem ist nicht ihre Qualität, sondern ihre Zersplitterung: Jedes Werkzeug deckt genau einen Ausschnitt ab, und die Lücken dazwischen bleiben offen.

- **Browser-Erweiterungen** blockieren bekannte Werbeserver und Server, die das Surfverhalten aufzeichnen, und machen das Surfen spürbar ruhiger. Sie schützen aber ausschließlich den Browser, in dem sie installiert sind. E-Mail-Programm, Office-Software und Apps bleiben ungeschützt, ebenso jedes andere Gerät im Netzwerk. Sie sind auf Listen bekannter Server angewiesen, sodass neue Server dieser Art so lange ungehindert arbeiten, bis sie erkannt und in eine Liste aufgenommen sind, was Wochen dauern kann. Gegen das Wiedererkennen am Geräte-Fingerabdruck helfen sie in der Regel nicht, auf Mobilgeräten wirken sie nur in bestimmten Browsern und in Apps gar nicht.
- **Ein VPN-Dienst** verbirgt Ihre Internet-Adresse, aber nicht die Merkmale, an denen Ihr Browser wiedererkannt wird. Die Bausteine auf der Seite, die Ihr Verhalten aufzeichnen, arbeiten unverändert weiter.
- **Eine sichere E-Mail-Anwendung** schützt die E-Mail, aber weder das Surfen noch die übrigen Geräte im Netzwerk.

- **Einstellungen am einzelnen Gerät** wirken nur, solange sie gepflegt werden. Wer zehn verschiedene Werkzeuge einrichten und aktuell halten muss, vergisst irgendwann eines oder übersieht ein Gerät. Datenschutz, der von dauerhafter persönlicher Aufmerksamkeit abhängt, hält im Alltag nicht durch.

Dazu kommt der Faktor Mensch. Alle guten Verhaltensregeln, sichere Passwörter, keine unbedachten Klicks, regelmäßige Software-Updates, setzen voraus, dass jeder Nutzer jederzeit aufmerksam bleibt. In einem Haushalt oder Betrieb mit mehreren Personen, mehreren Geräten und mehreren Herstellern ist das nicht durchzuhalten. Die Regeln bleiben die unverzichtbare Grundlage, aber sie brauchen eine technische Ergänzung, die unabhängig von der Disziplin des Einzelnen wirkt.

Genau dort setzt die TrutzBox an: eine zentrale Kontrolle des Datenverkehrs für alle Geräte, die im Hintergrund arbeitet und keine ständige Aufmerksamkeit verlangt.

1.5 Warum eine Firewall allein nicht genügt

> **Für Neugierige: Das Bild vom Wachmann**
>
> Eine Firewall ist wie ein Wachmann am Eingang eines Gebäudes. Er prüft, wer hereinkommt, und hält Ungebetene fern. Aber er schaut nicht, was die Mitarbeiter in ihrer Tasche nach draußen tragen, wenn sie das Gebäude verlassen. Genau das ist das Problem: Klassische Sicherheitssysteme sind auf Eindringlinge von außen ausgerichtet. Den stillen, täglichen Abfluss von Daten über ganz normale Internetverbindungen bemerken sie nicht.

Eine Firewall ist unverzichtbar und bildet die erste Verteidigungslinie gegen Angriffe von außen. Sie hat aber zwei strukturelle Grenzen. Erstens arbeitet sie überwiegend gegen bekannte Bedrohungen; bei täglich über 450.000 neuen Schadprogrammen entstehen dabei zwangsläufig Lücken. Zweitens kontrolliert sie vor allem den eingehenden Verkehr. Eine Regel, die ausgehenden Web-Verkehr erlaubt, erlaubt damit auch die Übermittlung von Daten über Ihr Verhalten an hunderte fremde Server, denn dieser Verkehr sieht für sie aus wie jeder andere Seitenaufruf.

Systeme zur Angriffserkennung ergänzen die Firewall, greifen aber erst, wenn ein Eindringling schon im System ist. Sie sind wie ein Rauchmelder, der vor einem Brand warnt, ihn aber nicht verhindert. Nach der aktuellen Studie von IBM dauert es im Durchschnitt rund 180 Tage, bis eine Datenpanne überhaupt entdeckt wird, und weitere zwei Monate, bis sie eingedämmt ist.

Die TrutzBox schließt diese Lücke von der anderen Seite: Sie betrachtet auch den ausgehenden Verkehr. Sie prüft nicht nur, wer hereinkommt, sondern ebenso, wohin Ihre Geräte etwas senden, und sie macht dieses Geschehen im Monitor sichtbar (Kapitel „Monitor und Statistiken“). Erst beide Richtungen zusammen ergeben einen vollständigen Schutz. Deshalb bringt die TrutzBox beides mit: eine Firewall mit Angriffsschutz für die eine Richtung und einen filternden Proxy für die andere.

1.6 Wovor die TrutzBox schützt

Comidio unterscheidet sechs Gruppen, die es auf Ihre Daten oder Ihr Netzwerk abgesehen haben. Diese Einteilung ist bewusst breiter als die übliche Sicherheitsliteratur, die sich meist auf die Abwehr von Angriffen von außen beschränkt. Sie schließt ausdrücklich auch das Ausspähen durch

an sich legale Unternehmen und den Datenabfluss durch schlecht gesicherte Geräte im eigenen Netz ein. Jede Funktion der TrutzBox richtet sich gegen mindestens eine davon:

Wer	Was sie tun	Was dagegen hilft
Werbeplattformen und Analysedienste	Zeichnen Ihr Surfverhalten über viele Seiten hinweg auf	TrutzBrowse und die Filterlisten (Kapitel „Webfilter und Jugendschutz (TrutzContent)“ und „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“)
Datenhändler	Kaufen, verknüpfen und verkaufen Profile aus vielen Quellen	TrutzBrowse, Filterlisten (Kapitel „Webfilter und Jugendschutz (TrutzContent)“ und „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“)
Geheimdienste und staatliche Autoritäten	Lesen unverschlüsselte Kommunikation mit	TrutzMail, TrutzChat und Videokonferenz mit durchgehender Verschlüsselung, alles auf Ihrer eigenen TrutzBox (Kapitel „TrutzMail: sichere E-Mail“ und „TrutzChat und Videokonferenz“)
Internet-Kriminelle	Erpressungstrojaner, Phishing, Kontenübernahme	Firewall, Angriffsschutz und Webfilter (Kapitel „Webfilter und Jugendschutz (TrutzContent)“ und „TrutzBox-Netzwerk: Schutz und Verwaltung“)
Staatlich unterstützte Angreifer	Gezielte, lang laufende Angriffe auf Netzwerke	Firewall und Angriffsschutz mit Protokollierung (Kapitel „TrutzBox-Netzwerk: Schutz und Verwaltung“)
Geräte mit zweifelhafter Datenpolitik	Fernseher, sprachgesteuerte Lautsprecher und andere Geräte senden ungefragt Daten an Hersteller	Filtergruppen je Gerät und der Monitor, der alles sichtbar macht (Kapitel „Geräte verwalten“ und „Monitor und Statistiken“)

Etwas ausführlicher gesagt:

Werbeplattformen und Analysedienste zeichnen das Verhalten von Nutzern auf Webseiten und in Apps auf, um daraus Werbeprofile zu bilden. Sie sitzen nicht auf einer Seite, sondern auf vielen tausend Seiten gleichzeitig und erkennen Sie dadurch über Seitengrenzen hinweg wieder.

Datenhändler kaufen solche Datensätze aus den verschiedensten Quellen zusammen, reichern sie an und verkaufen sie weiter. Sie treten Ihnen nie gegenüber und haben mit Ihnen keinerlei Vertragsbeziehung. Genau das macht sie so schwer greifbar.

Geheimdienste und staatliche Autoritäten überwachen Internet-Kommunikation. Gegen mitgelesene Inhalte hilft nur Verschlüsselung, und zwar durchgehend vom Absender bis zum Empfänger, nicht nur auf dem Weg zum Anbieter.

Internet-Kriminelle setzen Erpressungssoftware, Phishing und Täuschung ein. Ihr Werkzeug ist selten der geniale Einbruch, sondern die gut vorbereitete Nachricht an einen Menschen.

Professionelle, staatlich unterstützte Angreifer betreiben Wirtschaftsspionage und Sabotage. Sie arbeiten langfristig und unauffällig, weshalb Protokollierung und Sichtbarkeit hier ebenso wichtig sind wie das Blockieren selbst.

Gerätehersteller mit zweifelhafter Datenpolitik bauen Sammelfunktionen in ihre Produkte ein, die weit über das hinausgehen, was das Gerät zum Funktionieren braucht. Betroffen sind vor allem Fernseher, sprachgesteuerte Lautsprecher und Apps, die besonders gründlich aufzeichnen, was ihre Nutzer tun.

1.7 Die Funktionen im Überblick

Alle Funktionen stecken in einer TrutzBox und arbeiten zusammen. Die wichtigsten im Kurzporträt, jeweils mit dem Kapitel, das sie ausführlich beschreibt:

TrutzContent, der Webfilter (Kapitel „Webfilter und Jugendschutz (TrutzContent)“): prüft bei jedem Seitenaufruf, ob das Gerät den angefragten Server überhaupt kontaktieren darf. Grundlage sind Filtergruppen, die Sie jedem Gerät zuweisen: streng fürs Kinder-Tablet, locker für den Arbeits-PC, eng begrenzt für den Fernseher. Die Filterlisten dahinter hält Comidio automatisch aktuell. Ändern kann die Einstellungen nur der Administrator, nicht der einzelne Anwender.

TrutzBrowse, der Anonymisierer (Kapitel „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“): entfernt beim Surfen identifizierende Merkmale aus dem Datenverkehr, damit Werbe- und Analysedienste aus Browser und Gerät keinen wiedererkennbaren „Fingerabdruck" bilden können. Wie stark, bestimmen Sie mit dem Security-Slider: zehn Stufen von L1 bis L10, auf Wunsch je Gerät und je Webseite.

TrutzMail, die sichere E-Mail (Kapitel „TrutzMail: sichere E-Mail“): verschlüsselt E-Mails automatisch von Ende zu Ende, samt der sonst überall anfallenden Metadaten (wer schreibt wem wann). Die Schlüsselverwaltung übernimmt die TrutzBox; Sie schreiben einfach E-Mails wie bisher.

TrutzChat und TrutzMeeting (Kapitel „TrutzChat und Videokonferenz“): Nachrichten und Videokonferenzen, die vollständig auf Ihrer eigenen TrutzBox laufen statt auf fremden Servern. Für Videokonferenz-Gäste genügt ein moderner Browser und ein Link, ganz ohne App und Konto. Beides gehört zu TrutzRTC und steht nur in der Business-Ausstattung der TrutzBox zur Verfügung.

Ob Ihre TrutzBox diese Ausstattung mitbringt, sehen Sie am schnellsten unter **Systemeinstellungen → Vertrag und Pakete**. Dort steht, was Ihr Service-Vertrag umfasst, wie viele TrutzMail-Adressen dazugehören und bis wann er läuft. Ein zweites Indiz ist die Betriebszustand-Seite: Erscheint dort eine Karte **TrutzRTC**, sind Chat und Videokonferenz an Bord (Kapitel „Betriebszustand: die Karten im Einzelnen“).

TrutzBase, Firewall und Angriffsschutz (Kapitel „TrutzBox-Netzwerk: Schutz und Verwaltung“): überwacht ein- und ausgehenden Verkehr, wehrt Angriffe aus dem Internet ab und

sperrt auffällige Absender automatisch. Der Angriffsschutz blockiert dabei auf Netzwerkebene und wirkt so auch für Geräte, die kein Zertifikat tragen können, etwa Fernseher und andere Smart-Geräte.

Der VPN-Fernzugriff (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“): nimmt den Schutz mit auf Reisen. Ein verschlüsselter Tunnel, wahlweise über WireGuard oder OpenVPN, verbindet Smartphone oder Laptop unterwegs mit Ihrer TrutzBox, als wären Sie vor Ort.

Der Monitor (Kapitel „Monitor und Statistiken“): macht sichtbar, was sonst verborgen bleibt: welches Gerät wann mit welchem Server spricht, was durchgelassen und was blockiert wurde. Alle Aufzeichnungen bleiben dabei auf Ihrer TrutzBox.

> **Für Neugierige: Warum kein einfacher DNS-Filter?**
>
> Viele Werbeblocker fürs ganze Netzwerk filtern nur die Namensauflösung (DNS): Eine gesperrte Adresse wird dann gar nicht erst gefunden. Das ist grob, denn ein Name ist immer nur ganz oder gar nicht gesperrt, und ein Gerät, das an der Namensauflösung vorbei direkt eine Adresse anspricht, bleibt unbehelligt. Die TrutzBox arbeitet zusätzlich als Proxy mitten im Datenstrom: Sie entscheidet über jede einzelne Verbindung, sperrt also etwa die Bausteine einer sonst erlaubten Seite, die Ihr Verhalten aufzeichnen, und mit TrutzBrowse sogar einzelne Unterseiten. Fremde DNS-Server und das Ausweichen auf QUIC unterbindet sie.

Der Anspruch dahinter lässt sich in einem Satz zusammenfassen: Privatheit bei möglichst allen Tätigkeiten im Internet, beim Mailen, beim Surfen, beim Chatten und bei Video- und Audiokonferenzen, ohne tiefgehende Fachkenntnisse und für alle Geräte im Netzwerk gleichzeitig. Die Rechenleistung der TrutzBox ist für den Alltag eines Haushalts oder kleinen Büros bemessen; im normalen Betrieb bremst sie das Surfen kaum merklich. Am meisten Rechenzeit kosten TrutzBrowse und viele gleichzeitige Nutzer.

Drei Wege gibt es, ein Gerät an die TrutzBox anzuschließen. Beim ersten hängt das Gerät im **internen TrutzBox-Netzwerk**, per Kabel oder über das TrutzBox-WLAN; dann ist es automatisch komplett geschützt, und einzustellen ist am Gerät nichts. Das ist der empfohlene Weg. Beim zweiten, dem **Proxy-Mode**, bleibt das Gerät am Router und wird gezielt auf die TrutzBox eingestellt, ideal zum Ausprobieren und für Sonderfälle. Der dritte ist **TrutzVPN**, der Weg für Geräte, die auch unterwegs geschützt sein sollen. Alle drei erklärt Kapitel „Ein Gerät mit der TrutzBox absichern“.

> **Was Sie sich merken sollten**
>
> Die TrutzBox nimmt Ihnen die Entscheidung nicht ab, sie nimmt Ihnen die Arbeit ab. Einmal eingerichtet, wirkt sie für jedes Gerät, das über sie ins Internet geht, ohne dass jemand auf dem Gerät etwas einstellen, installieren oder pflegen müsste. Das ist der eigentliche Unterschied zu jeder Einzellösung.

1.8 Ihr Weg durch dieses Handbuch

Je nachdem, was Sie vorhaben, führen unterschiedliche Wege durch dieses Buch:

Ihr Vorhaben	Lesen Sie
Die TrutzBox zum ersten Mal in Betrieb nehmen	Kapitel „TrutzBox einrichten (Setup)“ (Einrichtung), dann Kapitel „Ein Gerät mit der TrutzBox absichern“ (Geräte anschließen). Damit läuft der Grundschutz.
Kinder oder Jugendliche schützen	Kapitel „Geräte verwalten“ (Geräte zuordnen) und Kapitel „Webfilter und Jugendschutz (TrutzContent)“ (Filtergruppen und Jugendschutz).
Wissen, was die Geräte im Netzwerk eigentlich tun	Kapitel „Monitor und Statistiken“ (Monitor). Besonders aufschlussreich bei Fernsehern und Haustechnik.
Sicher E-Mails schreiben	Kapitel „TrutzMail: sichere E-Mail“ (TrutzMail), dazu Kapitel „Benutzer, Postfächer, Passwörter“ für weitere Postfächer.
Unterwegs geschützt sein	Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“ (TrutzVPN).
Etwas funktioniert nicht	Kapitel „Was tun, wenn …?“ (Was tun, wenn) und bei Bedarf Kapitel „Support kontaktieren“ (Support).

Und wenn Sie einfach nur wissen möchten, was ein Begriff bedeutet: Das Glossar am Ende des Buches erklärt alle Fachwörter in einem Satz.

2 Auspacken und Anschlüsse

Die TrutzBox ist ein kompakter Rechner im Format eines kleinen Routers. Sie findet neben dem Internet-Router Platz und braucht außer Strom und Netzwerkkabeln nichts weiter.

Im Inneren steckt bewusst keine gewöhnliche Bastel-Hardware, sondern ein für den Dauerbetrieb ausgelegter kleiner Server: mit einer SSD statt einer drehenden Festplatte, mit geringem Kühl- und Platzbedarf und mit Netzwerkanschlüssen für 1 Gbit/s. Das Gehäuse ist mechanisch stabil, sodass sich andere Geräte darauf abstellen lassen. Dieses Kapitel führt einmal um das Gerät herum und beantwortet die Fragen, die sich beim Auspacken stellen.

2.1 Lieferumfang

In der Verpackung finden Sie:

- Die TrutzBox
- Steckernetzteil
- Ein Netzwerkkabel
- Beileger mit Ihrer **TrutzKennung** und Ihrem **TrutzSchlüssel**. Beides brauchen Sie bei der Einrichtung (Kapitel „TrutzBox einrichten (Setup)“); bewahren Sie den Beileger danach gut auf.

Das mitgelieferte Netzwerkkabel ist für die Verbindung von der TrutzBox zum Internet-Router gedacht. Mehr braucht es für die Einrichtung nicht. Für jedes Gerät, das Sie später per Kabel an die TrutzBox anschließen, brauchen Sie ein weiteres Netzwerkkabel; jedes handelsübliche Netzwerkkabel ist geeignet, sofern es für 1 Gbit/s taugt, was auf praktisch alle heute verkauften Kabel zutrifft. Ein zu langes Kabel schadet nicht, ein sehr altes oder beschädigtes dagegen kann die Verbindung unbemerkt ausbremsen. Wenn Sie ohnehin neu kaufen, nehmen Sie lieber ein Kabel zu viel als eines zu wenig.

Ebenfalls nicht enthalten, aber je nach Aufbau nötig oder nützlich:

- **Ein Netzwerk-Verteiler (Switch),** falls Sie mehr als zwei Geräte per Kabel anschließen möchten. Mehr dazu in Abschnitt „Mehr Geräte anschließen: der Switch“.
- **Das WLAN-Modul,** sofern Sie es nicht mitbestellt haben. Es lässt sich auch nachträglich bestellen; die TrutzBox erkennt ein unterstütztes Modul selbst und lädt die passende Konfiguration automatisch.
- **Weitere Netzwerkkabel** für jedes zusätzliche Gerät, das per Kabel an die TrutzBox soll.



Abbildung 2-1: Die TrutzBox von vorn. Links die drei LEDs für Betrieb, TrutzMail und geblockte Verbindungen. (© 2026 Comidio GmbH)

Nicht nötig sind Bildschirm, Tastatur und Maus. Die TrutzBox wird ausschließlich über den Browser eines anderen Geräts bedient. Ebenso wenig brauchen Sie Software, die auf einem PC installiert werden müsste.

TrutzKennung und TrutzSchlüssel gut aufheben

Der Beileger ist das einzige Papier, das Sie aufbewahren müssen. **TrutzKennung** und **TrutzSchlüssel** brauchen Sie bei der Erstinbetriebnahme und erneut, falls die TrutzBox später einmal neu eingerichtet werden muss. Beide zusammen heißen Ihre **TrutzLegitimation**: der Nachweis, dass diese TrutzBox Ihnen gehört. Fotografieren Sie den Beileger nicht mit dem Smartphone ab, sondern legen Sie ihn zu Ihren wichtigen Unterlagen.

2.2 Die Anschlüsse

Auf der Rückseite finden Sie drei beschriftete Netzwerkbuchsen und den Stromanschluss:



Abbildung 2-2: Die Rückseite mit ihren beschrifteten Anschlüssen. LAN-Ext zeigt zum Internet-Router, LAN-Int1 und LAN-Int2 zu Ihren eigenen Geräten. (© 2026 Comidio GmbH)

- **LAN-Ext:** der Anschluss nach außen, zum Internet-Router. Hier kommt genau ein Kabel hinein, das zur „unsicheren" Seite Richtung Internet führt.
- **LAN-Int1 und LAN-Int2:** die Anschlüsse für Ihr geschütztes Netzwerk. Hier schließen Sie PC, Drucker oder einen Netzwerk-Verteiler (Switch) an, über den weitere Geräte Platz finden. Beide Buchsen sind gleichwertig.
- **Strom:** die Buchse **12V DC** für das mitgelieferte Netzteil. Die TrutzBox startet, sobald sie Strom bekommt, und ist für den Dauerbetrieb gebaut.

Die beiden **USB**-Buchsen und der Anschluss **COM-1** bleiben im Normalbetrieb frei. Eine USB-Buchse brauchen Sie nur, wenn Sie ein neues System mit dem Tank-Stick aufspielen (Kapitel „Der Ausnahmefall: ein komplettes Image“); den Anschluss COM-1 nutzt allenfalls der Support.

Der Unterschied zwischen außen und innen ist der Kern des ganzen Aufbaus. Über **LAN-Ext** holt sich die TrutzBox beim Start selbst eine Adresse vom Internet-Router und meldet sich dort unter dem Namen `trutzbox` an. Alles, was an **LAN-Int1**, **LAN-Int2** oder am TrutzBox-WLAN hängt, liegt dagegen in einem eigenen, vom Router getrennten internen Netz. Die TrutzBox verteilt dort selbst die Adressen und vermittelt zwischen innen und außen. Damit ist sichergestellt, dass wirklich jede Verbindung dieser Geräte durch die TrutzBox läuft.

Die drei internen Anschlüsse (WLAN, LAN-Int1 und LAN-Int2) sind intern zu einem einzigen Netz zusammengeschaltet. Geräte an unterschiedlichen Buchsen können deshalb ungehindert miteinander sprechen, etwa ein Notebook mit einem Netzwerkdrucker. Eine später eingerichtete VPN-Verbindung von unterwegs gehört dagegen nicht zu dieser internen Zusammenschaltung: Sie liegt in einem eigenen Netz, aus dem die TrutzBox in Ihr internes Netz weiterleitet (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

Optional kann die TrutzBox ein **WLAN-Modul** enthalten. Sie stellt dann ein eigenes, geschütztes Funknetz bereit, das sich wie ein weiterer interner Anschluss verhält (Kapitel „Das WLAN der TrutzBox“).

> **Die wichtigste Regel im ganzen Buch**
>
> Das Kabel zum Internet-Router gehört immer und ausschließlich in **LAN-Ext**. Alle Ihre eigenen Geräte gehören an LAN-Int1, LAN-Int2 oder ins TrutzBox-WLAN. Wer beides vertauscht, hebelt den Schutz aus.

Die Buchsen sind beschriftet. Falls Sie die TrutzBox in einer dunklen Ecke stehen haben, lohnt es sich, vor dem Einbau einmal mit einer Lampe hinzusehen und sich einzuprägen, welche Buchse welche ist. Ein vertauschtes Kabel ist der mit Abstand häufigste Fehler bei der Erstinbetriebnahme, und er ist auch der am schnellsten behobene.

2.3 Die LEDs an der TrutzBox

Die Netzwerkbuchsen haben kleine Leuchtdioden, die bei bestehender Verbindung leuchten und bei Datenverkehr flackern. Daran erkennen Sie auf einen Blick, ob ein Kabel Kontakt hat. Ob alle Dienste der TrutzBox gesund sind, sehen Sie nicht an den LEDs, sondern auf der Seite **Betriebszustand** der Verwaltungsoberfläche (Kapitel „Betriebszustand: die Ampel lesen“).

An der Gerätefront sitzen zusätzlich drei grüne LEDs mit fester Bedeutung:

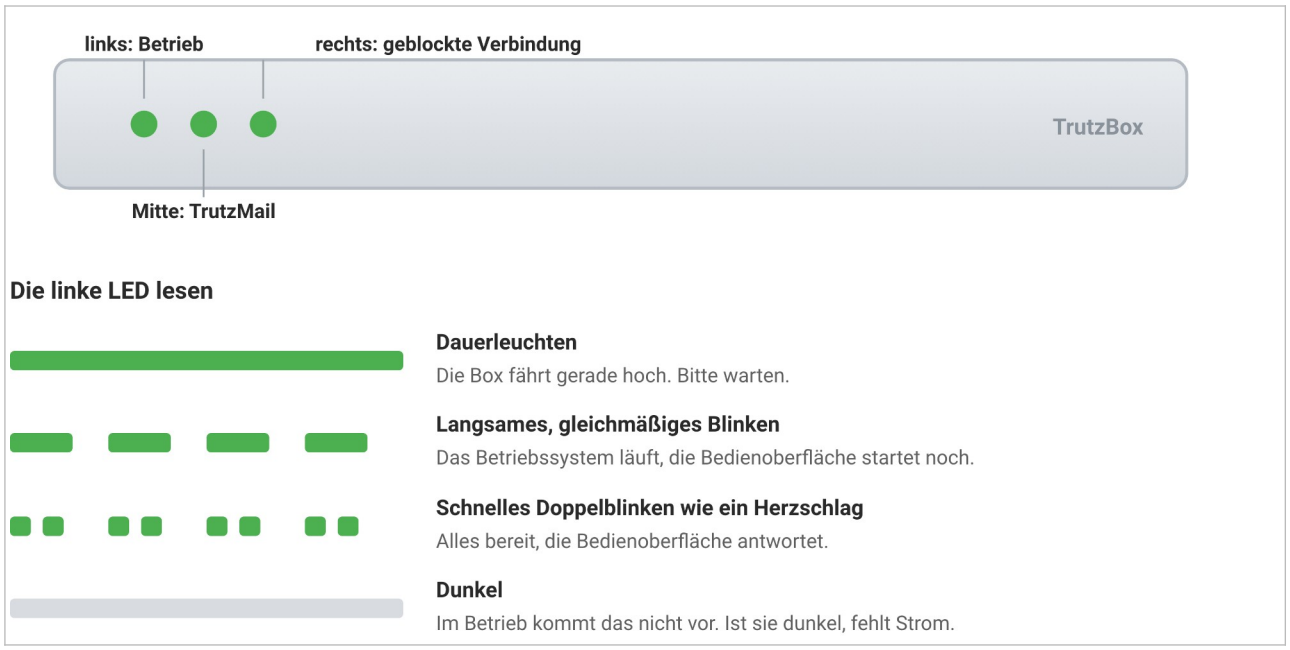


Abbildung 2-3: Die drei LEDs an der Gerätefront und die Blinkmuster der linken LED. (© 2026 Comidio GmbH)

- **Die linke LED** zeigt den Betriebszustand. Beim Start leuchtet sie zunächst dauerhaft (die TrutzBox fährt hoch), danach blinkt sie langsam (das Betriebssystem läuft, die Bedienoberfläche startet gerade), und im normalen Betrieb blinkt sie schnell wie ein Herzschlag (die Bedienoberfläche antwortet).
- **Die mittlere LED** leuchtet auf, während TrutzMail E-Mails verarbeitet.

- **Die rechte LED** zeigt jede geblockte Verbindung durch kurzes Aufblinken an. Ab Werk ist das eingeschaltet; der Schalter **Blockungen anzeigen** findet sich unter **Verwaltung → Allgemeine Einstellungen** in der Karte **LED-Anzeige an der TrutzBox**. Dort lassen sich auch die Herzschlag-Leuchte und die Aktivitäts-Leuchten ganz abschalten; sie bleiben dann auch nach einem Neustart aus.

Die dritte LED ist ein hübscher Nebeneffekt der Filterung: Sie macht ohne jedes Nachsehen sichtbar, wie viel im Hintergrund tatsächlich blockiert wird. Wer ein paar Minuten hinschaut, während an den Geräten normal gearbeitet wird, hat den besten Eindruck davon, was die TrutzBox leistet.

Die TrutzBox ARM zeigt den Betriebszustand mit einer roten LED in denselben drei Stufen; ihre drei grünen LEDs zeigen die Auslastung der Anschlüsse WAN, LAN und WLAN. Was die LEDs vom Einschalten bis zum Setup der Reihe nach anzeigen, steht für beide Modelle in Kapitel „System zurücksetzen (Werksreset)“.

Direkt nach dem Einstecken braucht die TrutzBox einen Moment zum Starten. Beim allerersten Start und nach Software-Updates kann diese Phase mehrere Minuten dauern. Danach folgt die Einrichtung im nächsten Kapitel.

2.4 Aufstellort, Belüftung und Dauerbetrieb

Die TrutzBox ist dafür gebaut, ununterbrochen zu laufen. Sobald sie Strom bekommt, startet sie, und sie bleibt an. Nur so kann sie den Verkehr aller Geräte lückenlos prüfen, nachts Filterlisten und Software-Updates einspielen und einen VPN-Zugang von unterwegs annehmen. Ein Gerät, das jemand abends ausschaltet, schützt nur halb.

Für den Platz gelten deshalb die üblichen Regeln für Dauerläufer:

- Stellen Sie die TrutzBox auf eine feste, ebene Fläche, am besten direkt neben den Internet-Router. Kurze Wege sparen Kabel und Fehlerquellen.
- Lassen Sie ringsum etwas Luft. Die TrutzBox gibt ihre Wärme zu einem guten Teil über das Gehäuse ab. Sie darf deshalb nicht in einen geschlossenen Schrank ohne Belüftung, nicht unter eine Decke und nicht in die pralle Sonne.
- Legen Sie nichts direkt auf das Gehäuse, was die Wärmeabgabe behindert, etwa Papierstapel. Andere Geräte darauf zu stellen ist mechanisch unproblematisch, sofern sie selbst nicht heiß werden und Luft an das Gehäuse kommt.
- Vermeiden Sie feuchte Räume und Orte, an denen die TrutzBox angestoßen werden kann.
- Sorgen Sie für eine dauerhaft belegte Steckdose. Wer die TrutzBox an eine schaltbare Steckdosenleiste hängt, schaltet sie versehentlich mit ab.

Die Betriebstemperatur beobachtet die TrutzBox selbst und zeigt sie im **Betriebszustand** an. Steigt der Wert dauerhaft an, ist fast immer der Aufstellort die Ursache und nicht das Gerät.

> **Strom und Neustart**
>
> Ein Neustart der TrutzBox erfolgt normalerweise über die Verwaltungsoberfläche, nicht durch Ziehen des Netzteils. Wenn Sie den Stecker doch einmal ziehen müssen, ist das nicht schlimm, die TrutzBox startet danach von selbst wieder. Geben Sie ihr anschließend einen Moment, bevor Sie

die Oberfläche aufrufen. Weil die TrutzBox bei jedem Start nach Software-Updates sieht, zeigt die Oberfläche danach unter Umständen einige Minuten lang die Seite „Software-Updates werden installiert".

2.5 Mehr Geräte anschließen: der Switch

Die TrutzBox hat zwei interne Netzwerkbuchsen. Wer mehr als zwei Geräte per Kabel anschließen möchte, erweitert sie mit einem **Switch**, einem kleinen Netzwerk-Verteiler. Er ist nicht im Lieferumfang enthalten und im Fachhandel ohne besondere Anforderungen erhältlich.

Ein Switch ist unkompliziert: Sie stecken ein Kabel von LAN-Int1 oder LAN-Int2 in eine beliebige Buchse des Switch, und jedes weitere Gerät bekommt eine der übrigen Buchsen. Der Switch braucht keine Einrichtung und keine Zugangsdaten; er verteilt nur die Daten weiter. Für die TrutzBox ändert sich dadurch nichts: Alle Geräte hinter dem Switch liegen im internen Netz und werden genauso geschützt und in der Geräteliste geführt, als hingen sie direkt an der TrutzBox.

1. Switch an eine Steckdose anschließen.
2. Ein Netzwerkkabel von **LAN-Int1** oder **LAN-Int2** der TrutzBox in eine freie Buchse des Switch stecken.
3. Die weiteren Geräte jeweils mit einem eigenen Kabel an die übrigen Buchsen des Switch anschließen.
4. Nach kurzer Zeit erscheinen die neuen Geräte von selbst in der Geräteliste der TrutzBox (Kapitel „Geräte verwalten“).

Statt eines Switch lässt sich auch ein weiterer Router oder ein WLAN-Zugangspunkt anschließen, um zusätzliche Buchsen oder Funkabdeckung zu bekommen. Achten Sie dann darauf, dass dieses Gerät nur weiterverteilt und nicht selbst noch einmal ein eigenes, abgeschottetes Netz aufspannt, weil sonst die Geräte dahinter für die TrutzBox nicht mehr einzeln unterscheidbar sind.

Was ist eigentlich der Unterschied zu einem Router?

Ein **Switch** verteilt Daten innerhalb eines Netzes weiter, mehr nicht. Ein Router verbindet zwei verschiedene Netze miteinander und vergibt eigene Adressen. Für die Erweiterung hinter der TrutzBox ist der Switch die einfachere und die richtige Wahl: Er bleibt unsichtbar und lässt die TrutzBox ihre Arbeit machen.

Wenn alle Geräte an der TrutzBox hängen, kann das WLAN des Internet-Routers grundsätzlich sogar abgeschaltet werden. Das ist keine Pflicht, verhindert aber zuverlässig, dass sich ein Smartphone unbemerkt wieder im alten, ungeschützten Funknetz anmeldet. Kapitel „… ein Gerät nicht auftaucht“ greift genau diesen Fall noch einmal auf.

3 TrutzBox einrichten (Setup)

Ihre TrutzBox ist ausgepackt und liegt vor Ihnen? Dann kann es losgehen. In diesem Kapitel schließen Sie die TrutzBox an Ihren Internet-Router an und durchlaufen anschließend das Einrichtungsprogramm, das Setup. Es führt Sie in sechs Schritten von der ersten Verbindung bis zur fertig eingerichteten TrutzBox. Sie müssen dafür kein Technik-Profi sein: Das Setup fragt alles der Reihe nach ab, und dieses Kapitel erklärt zu jedem Schritt, was gemeint ist und worauf es ankommt.

Das brauchen Sie

- Ihre TrutzBox mit Netzteil
- Das beiliegende Netzwerkkabel
- Die **TrutzKennung** und den **TrutzSchlüssel**; beides finden Sie auf dem Beileger im TrutzBox-Paket
- Einen PC oder Laptop mit Browser, der bereits über Ihren Internet-Router im Netz ist, per Kabel oder WLAN
- Etwa 15 bis 20 Minuten Zeit. Einen Teil davon arbeitet die TrutzBox allein; Sie können nebenher etwas anderes tun. Muss sie viele Software-Updates nachholen, kann es bis zu einer Stunde länger dauern (Abschnitt „Software-Updates während der Einrichtung“).

Anleitung zum Anklicken

Wer die Einrichtung lieber erst einmal zuschaut, statt zu lesen: Die Anleitung „Ersteinrichtung" zeigt die Stationen dieses Kapitels mit Bild, Text und Ton im Browser: trutzbox.de/videodokumentation.

3.1 Die TrutzBox anschließen

Die TrutzBox hat drei Netzwerkanschlüsse, und die Beschriftung verrät ihre Aufgabe: **LAN-Ext** ist der Anschluss nach „außen" zu Ihrem Internet-Router. **LAN-Int1** und **LAN-Int2** sind die Anschlüsse für Ihr „inneres", von der TrutzBox geschütztes Netzwerk.

Für die Einrichtung genügt ein einziges Kabel, das zum Router. Eingerichtet wird die TrutzBox von einem PC oder Laptop, der ohnehin schon in Ihrem lokalen Netz am Router hängt; ob per Kabel oder WLAN, spielt keine Rolle. Ihre Geräte schließen Sie erst nach dem Setup an die Innenseite der TrutzBox an.

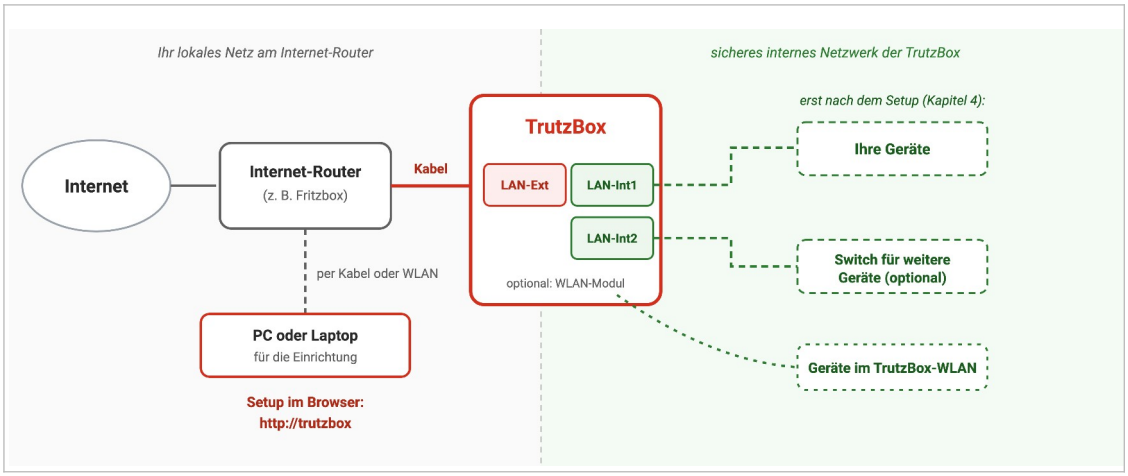


Abbildung 3-1: So wird die TrutzBox angeschlossen: ein Kabel vom Router zu LAN-Ext. Eingerichtet wird sie von einem PC in Ihrem lokalen Netz; Ihre Geräte kommen erst danach an LAN-Int1, LAN-Int2 oder ins TrutzBox-WLAN. (© 2026 Comidio GmbH)

1. Verbinden Sie das beiliegende Netzwerkkabel mit einem freien LAN-Anschluss Ihres Internet-Routers und mit dem Anschluss **LAN-Ext** der TrutzBox.
2. Stecken Sie das Netzteil ein. Die TrutzBox startet von selbst; beim allerersten Start kann das mehrere Minuten dauern.

Wichtig: Das Router-Kabel gehört in LAN-Ext

Vertauschen Sie die Anschlüsse nicht. Steckt das Kabel zum Router in einem der internen Anschlüsse, findet die TrutzBox den Weg ins Internet nicht, und der Verbindungstest im Schritt „Netzwerkeinstellungen" schlägt fehl.

Für Neugierige: Warum zwei Seiten?

Die TrutzBox stellt sich bewusst zwischen Ihren Router und Ihre Geräte. Auf der Außenseite (LAN-Ext) liegt das „unsichere" Netz Richtung Internet, auf der Innenseite Ihr geschütztes Netzwerk. Alles, was Ihre Geräte senden und empfangen, muss durch die TrutzBox hindurch. Nur so kann sie Filter durchsetzen, Angriffe abwehren und unerwünschten Datenverkehr anhalten: Werbung, das Aufzeichnen dessen, was Sie im Internet tun, und Verbindungen zu gefährlichen Servern. Die beiden internen Anschlüsse sind übrigens zusammengeschaltet: Es ist egal, welchen Sie benutzen, und über einen kleinen Netzwerk-Verteiler (Switch) können Sie weitere Geräte anschließen.

3.2 Das Setup im Browser öffnen

Öffnen Sie auf Ihrem PC oder Laptop im lokalen Netz einen Browser und geben Sie in die Adresszeile ein:

```
http://trutzbox
```

Die TrutzBox meldet sich mit dem Setup. Deutet der Browser den Namen als Suchbegriff oder findet er die TrutzBox nicht, versuchen Sie es als Zweites mit dieser Adresse:

```
http://trutzbox.local
```

Unter diesem Namen antwortet die TrutzBox selbst, auch wenn Ihr Router ihren Namen nicht kennt. Klappt auch das nicht, schauen Sie in der Geräteübersicht Ihres Routers nach, welche Adresse er der TrutzBox gegeben hat, und geben Sie diese ein, etwa `http://192.168.178.25`. Bei einer FRITZ!Box steht die Liste unter **Heimnetz → Netzwerk**.

> **Für Neugierige: Wie der Browser die TrutzBox findet**
>
> Den Namen `trutzbox` teilt die TrutzBox Ihrem Router mit, wenn sie sich bei ihm eine Adresse holt. Eine FRITZ!Box merkt sich solche Namen und gibt sie an Ihre Geräte weiter. Nicht jeder Router kann das, und mancher hält noch eine alte Adresse fest, etwa nachdem die TrutzBox zurückgesetzt wurde.
>
> Für diesen Fall kündigt sich die TrutzBox zusätzlich selbst im Netz an. Das Verfahren heißt **mDNS**, ist ein offener Standard und bei Apple unter dem Namen „Bonjour" bekannt. Ein Gerät, das nach `trutzbox.local` sucht, fragt dabei nicht den Router, sondern stellt die Frage einfach in die Runde, und die TrutzBox antwortet selbst. Das verstehen iPhone und iPad, Mac, Windows 10 und 11 sowie Linux, wo das dafür zuständige Programm avahi auf den gängigen Desktops schon mitkommt. Manche Browser unter Android kennen solche Namen nicht; dort bleibt die Adresse aus der Geräteübersicht des Routers.
>
> Die Ankündigung reicht so weit wie das eigene Netz, also ins interne Netz der TrutzBox und ins Netz des Routers, aber nicht durch den VPN-Tunnel. Haben Sie der TrutzBox einen anderen Netzwerknamen gegeben, lautet die Adresse entsprechend `http://<Netzwerkname>.local`. Stehen zwei TrutzBoxen mit demselben Namen im selben Netz, weicht eine davon auf `trutzbox-2.local` aus.

> **Falls zuerst ein Wartebildschirm erscheint**
>
> Gleich nach dem Einschalten sieht die TrutzBox beim Update-Server von Comidio nach, ob es neuere Software-Pakete gibt, und spielt sie ein. Läuft das noch, wenn Sie das Setup öffnen, sehen Sie zuerst die Seite *„Software-Updates werden installiert"* (Abschnitt „Software-Updates während der Einrichtung"). Lassen Sie das Fenster einfach geöffnet. Ist die TrutzBox fertig, lädt die Seite einmal neu, und das Setup beginnt.

Links im Setup sehen Sie die sechs Schritte der Einrichtung. Der Schritt, an dem Sie gerade stehen, trägt eine rote Nummer, erledigte Schritte ein rotes Häkchen. Darunter stehen die Setup-Version und die Image-Version der TrutzBox. Mit **Weiter** und **Zurück** bewegen Sie sich zwischen den Schritten.

3.3 Schritt „Willkommen"

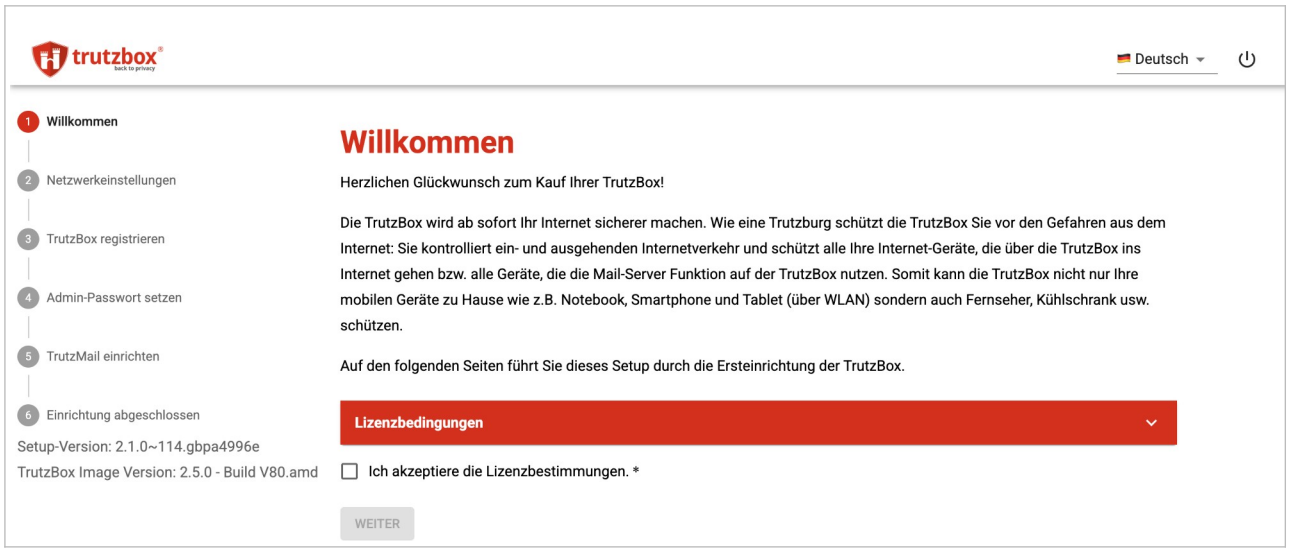


Abbildung 3-2: Der erste der sechs Schritte: Lizenzbedingungen lesen und akzeptieren. Links unten stehen die Setup-Version und die Image-Version, hier V80. (© 2026 Comidio GmbH)

Der erste Schritt begrüßt Sie und zeigt die Lizenzbedingungen. Klicken Sie auf **Lizenzbedingungen**, wenn Sie den Vertragstext lesen möchten, und setzen Sie dann das Häkchen bei *„Ich akzeptiere die Lizenzbestimmungen."* Erst damit wird die Schaltfläche **Weiter** aktiv.

3.4 Schritt „Netzwerkeinstellungen"

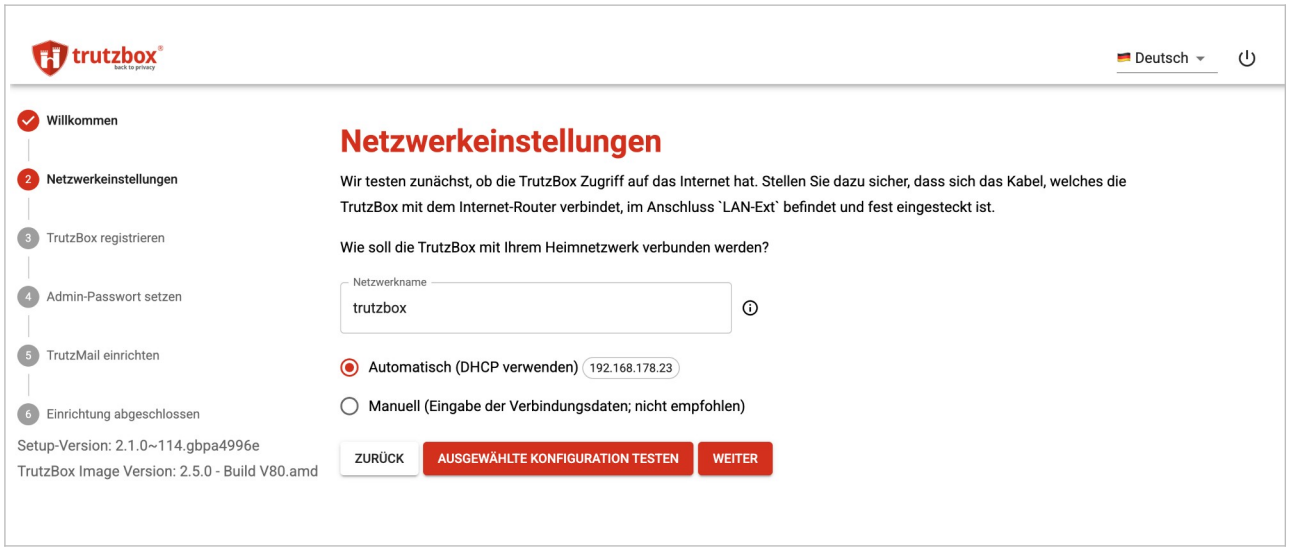


Abbildung 3-3: Der Schritt „Netzwerkeinstellungen": oben der Netzwerkname, darunter die Verbindungsart. Neben „Automatisch (DHCP verwenden)" steht die Adresse, die der Router der TrutzBox gegeben hat. (© 2026 Comidio GmbH)

Beim Öffnen dieses Schritts prüft die TrutzBox, ob sie über Ihren Router ins Internet kommt. Belassen Sie die Auswahl auf **Automatisch (DHCP verwenden)**. Das ist für praktisch alle Netzwerke richtig. Daneben steht die Adresse, die der Router der TrutzBox gegeben hat. Hat die TrutzBox Internet, ist **Weiter** sofort anklickbar.

Mit **Ausgewählte Konfiguration Testen** wendet die TrutzBox die gewählte Einstellung an und prüft die Verbindung noch einmal. Gelingt das, meldet sie *„Die Verbindung wurde erfolgreich hergestellt."* Danach klicken Sie auf **Weiter**.

Netzwerkname: Ab Werk steht hier `trutzbox`. Unter diesem Namen rufen Sie die TrutzBox im Browser auf. Ändern Sie ihn nur, wenn Sie einen anderen Namen möchten; erlaubt sind Kleinbuchstaben, Ziffern und Bindestriche. Ein neuer Name gilt mit **Weiter**, und das Setup wechselt dann von selbst auf die Adresse mit dem neuen Namen. Später ändern Sie den Namen unter **Verwaltung → Allgemeine Einstellungen** in der Karte **Netzwerkname**.

Feste IP-Adresse (Manuell): Über die Auswahl *„Manuell (Eingabe der Verbindungsdaten; nicht empfohlen)"* können Sie der TrutzBox eine feste IP-Adresse, DNS-Server, Gateway und Netzwerkmaske vorgeben. Das ist nur nötig, wenn Ihr Netzwerk ohne automatische Adressvergabe arbeitet, etwa in manchen Firmennetzen, und sollte erfahrenen Benutzern vorbehalten bleiben. Ein Tippfehler führt hier schnell dazu, dass die TrutzBox nicht mehr erreichbar ist. Die TrutzBox testet die neue Konfiguration deshalb erst und stellt bei einem Fehlschlag die vorherige Einstellung automatisch wieder her.

> **Wenn der Test fehlschlägt**
> Meldet die TrutzBox *„Der Verbindungsaufbau ist fehlgeschlagen. Bitte prüfen Sie die Netzwerkeinstellungen."*, bleibt **Weiter** grau. Prüfen Sie drei Dinge: Steckt das Router-Kabel wirklich in **LAN-Ext**? Sitzt es an beiden Enden fest? Ist der Router eingeschaltet und hat selbst Internet? Danach klicken Sie erneut auf **Ausgewählte Konfiguration Testen**.

3.5 Software-Updates während der Einrichtung

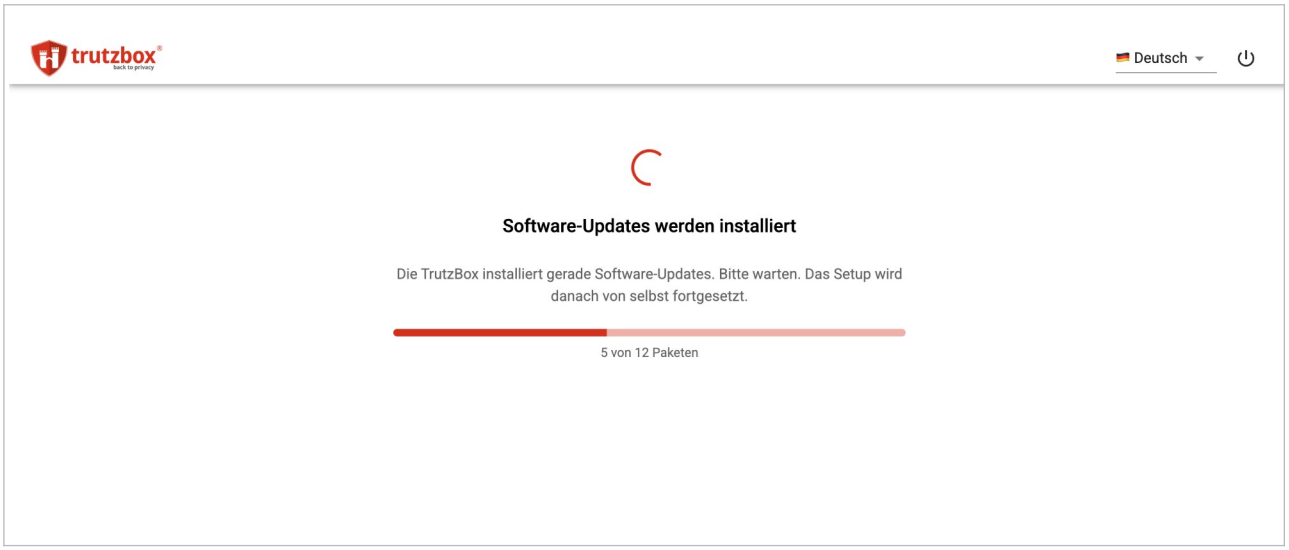


Abbildung 3-4: Die Warteseite „Software-Updates werden installiert": Der Balken zählt die eingespielten Pakete mit. Danach wird das Setup von selbst fortgesetzt. (© 2026 Comidio GmbH)

Die TrutzBox holt neuere Software-Pakete selbst vom Update-Server von Comidio und spielt sie ein, und zwar jede Nacht und bei jedem Start. Beim ersten Einschalten geschieht das, sobald sie über den Router Internet hat. Meist ist dieser erste Lauf deshalb schon fertig, wenn Sie im Setup beim Schritt Netzwerkeinstellungen ankommen.

Nach **Weiter** im Schritt Netzwerkeinstellungen sieht das Setup noch einmal nach. Hat die TrutzBox den Update-Server seit dem Einschalten schon erreicht und ist ihr Lauf beendet, folgt sofort der Schritt „TrutzBox registrieren". Die Seite *„Software-Updates werden installiert"* erscheint hier nur in zwei Fällen:

- Der Lauf vom Einschalten arbeitet noch. Dann wartet das Setup, bis er fertig ist.
- Die TrutzBox hatte beim Einschalten noch kein Internet, etwa weil sie erst mit der festen Adresse aus dem Schritt Netzwerkeinstellungen ins Internet kommt. Dann startet das Setup den Lauf jetzt einmal selbst. Solange es dafür den Update-Server sucht, steht dort *„Die Verbindung zum Server für Software-Updates wird geprüft."*

Auf der Warteseite steht, wie weit die TrutzBox ist: erst *„Pakete werden geholt"*, dann etwa *„5 von 12 Paketen"*. Anklicken müssen Sie nichts. Ist die TrutzBox fertig, lädt die Seite einmal neu, und das Setup wird von selbst fortgesetzt. Lassen Sie das Browserfenster offen und schalten Sie die TrutzBox in dieser Zeit nicht aus.

Wie lange das dauert, hängt davon ab, wie viele Pakete neu sind und wie schnell Ihr Internet-Anschluss ist. Meist sind es wenige Minuten. Liegt das Image der TrutzBox weit hinter dem aktuellen Stand zurück, kann es auch eine halbe Stunde und länger dauern. Länger als rund eine Stunde wartet das Setup aber nicht.

> **Wenn die Software-Updates scheitern**
>
> Findet das Setup den Update-Server nach dem Schritt Netzwerkeinstellungen innerhalb von zwei Minuten nicht, oder lässt sich ein Paket nicht einspielen, hält das die Einrichtung nicht auf: Das Setup wird trotzdem fortgesetzt. Die TrutzBox holt die Software-Updates in der nächsten Nacht oder beim nächsten Start nach. Ob das gelungen ist, zeigt später im Betriebszustand die Karte **Software-Updates** (Kapitel „Betriebszustand: die Karten im Einzelnen“).

3.6 Schritt „TrutzBox registrieren" und Sicherung einspielen

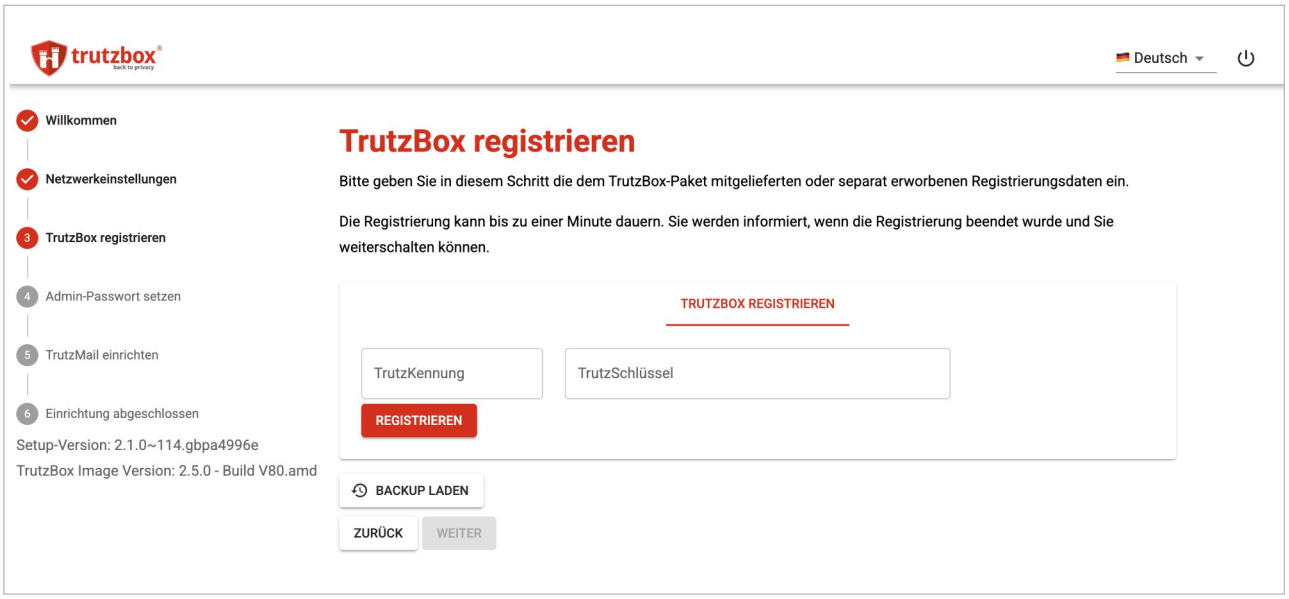


Abbildung 3-5: Registrierung mit TrutzKennung und TrutzSchlüssel vom Beileger. Darunter liegt „Backup laden" für eine Sicherung. (© 2026 Comidio GmbH)

Mit der Registrierung wird Ihre TrutzBox bei Comidio freigeschaltet. Dabei entstehen auch die Zertifikate, mit denen sich Ihre TrutzBox später ausweist. Nehmen Sie den Beileger aus dem TrutzBox-Paket zur Hand und tragen Sie ein:

1. **TrutzKennung**: Ihre Kundennummer bei Comidio. Sie besteht nur aus Ziffern.
2. **TrutzSchlüssel**: der 16-stellige Schlüssel im Format XXXX-XXXX-XXXX-XXXX. Geben Sie ihn mit den Bindestrichen ein.
3. Klicken Sie auf **Registrieren** und haben Sie einen Moment Geduld. Die Oberfläche weist darauf hin: *„Die Registrierung kann bis zu einer Minute dauern."*

Nach der Meldung *„Die TrutzBox wurde erfolgreich registriert."* führt **Weiter** zum nächsten Schritt.

Sicherung einspielen (Backup laden): Ersetzen Sie eine bestehende TrutzBox oder richten Sie Ihre TrutzBox nach einem Zurücksetzen neu ein? Dann spielen Sie Ihre Sicherung in diesem Schritt über die Schaltfläche **Backup laden** ein, und zwar bevor Sie auf **Registrieren** klicken: Die Sicherung bringt die Registrierung Ihrer TrutzBox mit. Die TrutzBox übernimmt daraus den kompletten gesicherten Zustand, also Benutzer, Postfächer und Einstellungen. Ist die Wiederherstellung gelungen, führt **Zur Administration** direkt ins Admin-Panel: Das Setup ist damit beendet, die übrigen Schritte durchlaufen Sie nicht mehr, weil die Sicherung sie bereits mitbringt. Wie Sie im laufenden Betrieb eine Sicherung anlegen, beschreibt Kapitel „Sichern, Wiederherstellen und Zurücksetzen“.

> **Fehlermeldung bei der Registrierung?**
>
> Schon beim Eintippen prüft die TrutzBox das Format: *„Die TrutzKennung besteht nur aus Ziffern"*, *„Der Schlüssel muss im Format XXXX-XXXX-XXXX-XXXX sein"* oder *„Quersumme des Schlüssels ist falsch"* bedeuten fast immer einen Tippfehler. Verwechseln Sie nicht 0 (Null) und O oder 1 und I; am sichersten tippen Sie beides noch einmal ab.
>
> Erscheint nach dem Klick auf **Registrieren** die Meldung *„Registrierung fehlgeschlagen"*, nennt die TrutzBox darunter den Grund: Hat der Registrierungsserver die Anmeldung abgelehnt, stimmen TrutzKennung und TrutzSchlüssel nicht zusammen; ist er nicht erreichbar, fehlt der TrutzBox der Internet-Zugang (zurück zum Schritt Netzwerkeinstellungen). Bleibt der Fehler bestehen, hilft der Comidio-Support (Kapitel „Support kontaktieren“) weiter.

3.7 Schritt „Admin-Passwort setzen"

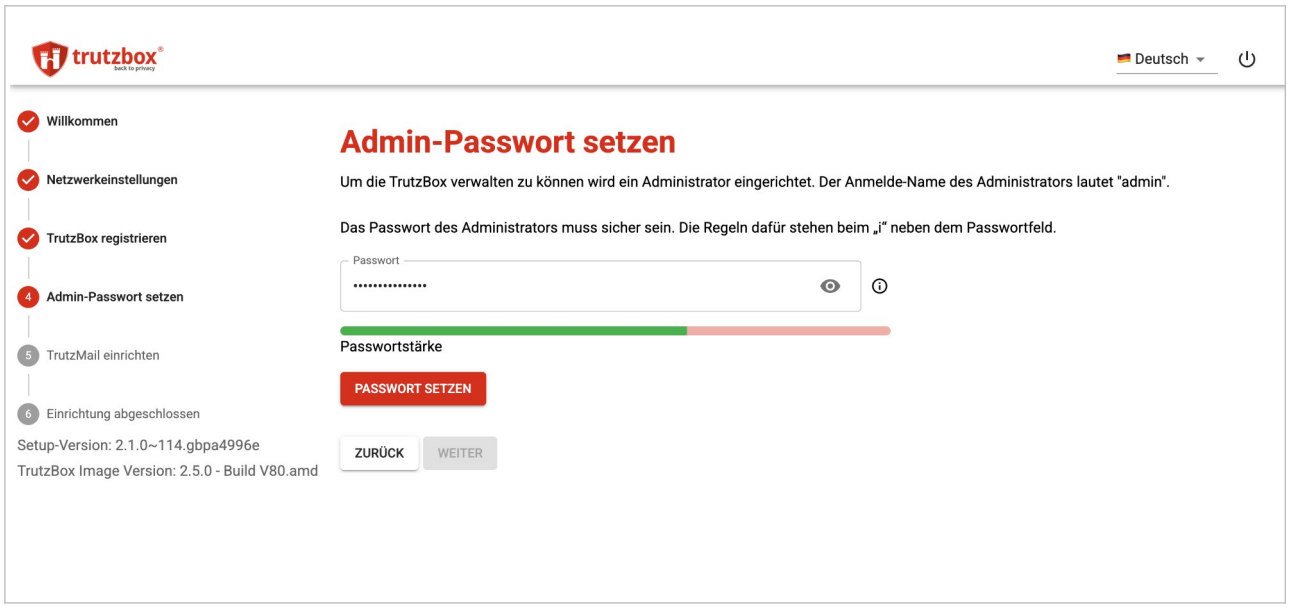


Abbildung 3-6: Das Passwort für den Verwalter-Zugang „admin" festlegen. Die Regeln stehen beim „i" neben dem Passwortfeld. (© 2026 Comidio GmbH)

Zum Verwalten der TrutzBox gibt es ein festes Benutzerkonto mit dem Anmelde-Namen **admin**. In diesem Schritt legen Sie sein Passwort fest. Es muss mindestens 8 und darf höchstens 128 Zeichen lang sein und mindestens drei der vier Zeichenarten Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen mischen; ab 16 Zeichen genügen zwei. Es darf weder „admin" noch „trutzbox" noch „comidio" enthalten, keine einfachen Folgen wie 1234, abcd, qwertz oder aaaa und kein bekanntes Allerweltspasswort wie Sommer2024!. Die vollständige Regel steht beim „i" neben dem Passwortfeld und in Kapitel „Passwörter ändern“. Der Balken *Passwortstärke* zeigt Ihnen zusätzlich, wie gut Ihre Wahl ist.

Klicken Sie anschließend auf **Passwort setzen** und dann auf **Weiter**.

> **So merken Sie sich ein starkes Passwort**
>
> Denken Sie sich einen kurzen Satz aus und nehmen Sie die Anfangsbuchstaben samt Zahlen und Zeichen, etwa: „Unser Hund Balu bellt seit 2019 jeden Postboten an!" ergibt `UHBbs2019jPa!`. Das ist lang, einprägsam und steht in keinem Wörterbuch. Bewahren Sie das Passwort gut auf, zum Beispiel in einem Passwort-Manager. Sie brauchen es künftig für alle Verwaltungsaufgaben.

3.8 Schritt „TrutzMail einrichten"

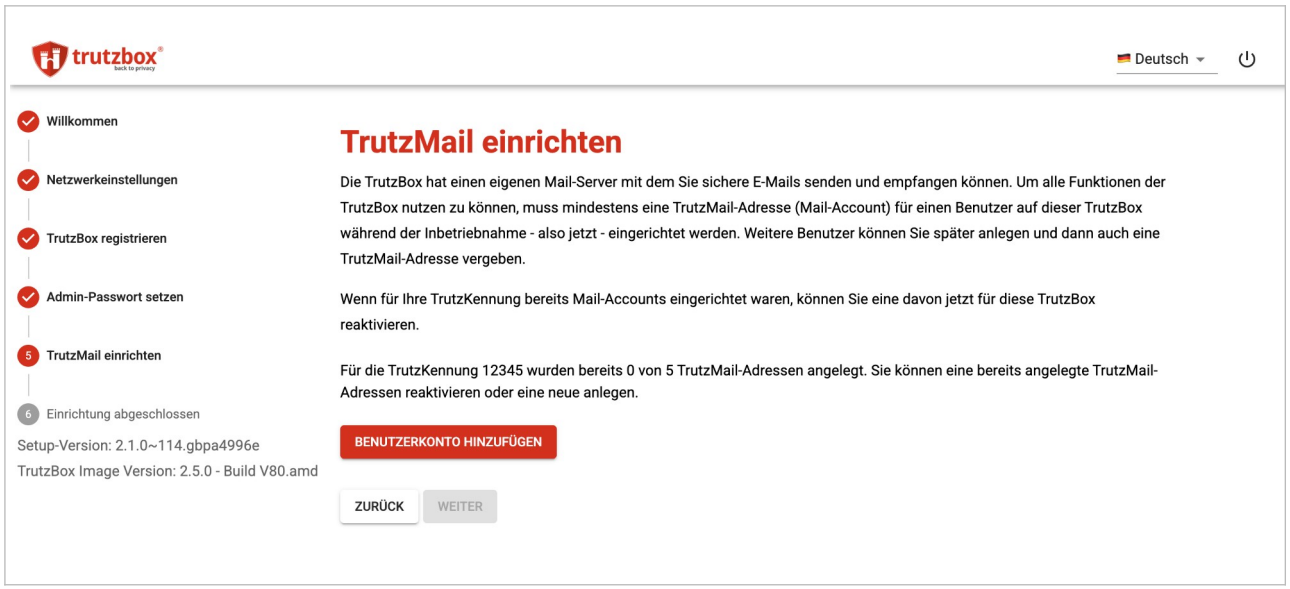


Abbildung 3-7: Der Schritt „TrutzMail einrichten": Er nennt, wie viele TrutzMail-Adressen Ihrer TrutzKennung schon angelegt sind. „Weiter" bleibt grau, bis eine Adresse eingerichtet ist. (© 2026 Comidio GmbH)

Die TrutzBox bringt einen eigenen Mail-Server mit, über den Sie später verschlüsselte E-Mails senden und empfangen. Damit alle Funktionen der TrutzBox nutzbar sind, muss jetzt mindestens eine **TrutzMail-Adresse** angelegt werden. Vorher lässt sich dieser Schritt nicht verlassen: **Weiter** bleibt grau, und einen Weg, den Schritt zu überspringen, hat das Setup nicht.

Oben nennt der Schritt, wie viele TrutzMail-Adressen für Ihre TrutzKennung schon angelegt sind, etwa *„Für die TrutzKennung 12345 wurden bereits 0 von 5 TrutzMail-Adressen angelegt."*

1. Klicken Sie auf **Benutzerkonto hinzufügen**. Es öffnet sich das Fenster *„Neuen Benutzer + TrutzMail hinzufügen"*.
2. Tragen Sie unter **Richtiger Name** den Namen ein, der bei Empfängern angezeigt wird, zum Beispiel „Anna Beispiel".
3. Wählen Sie den **Anmelde-Namen**. Er wird zugleich der vordere Teil der Mail-Adresse; die Endung `@comidio.email` ergänzt die TrutzBox automatisch.
4. Vergeben Sie ein Passwort für dieses Postfach und klicken Sie auf **Hinzufügen**.

Für das Postfach-Passwort gilt dieselbe Regel wie für das Admin-Passwort in Abschnitt „Schritt „Admin-Passwort setzen"“, und zusätzlich darf es den Anmelde-Namen nicht enthalten. Dieselbe Regel verlangt später auch das Admin-Panel, wenn Sie weitere Postfächer anlegen oder ein Passwort ändern (Kapitel „Passwörter ändern“). Das Passwort ist wichtig: Mit ihm melden Sie sich an Mail, Chat und Videokonferenz an.

Danach zeigt der Schritt *„Soeben wurde folgende TrutzMail-Adresse eingerichtet:"* mit der neuen Adresse, und **Weiter** wird anklickbar. Weitere Postfächer für Familie oder Kollegen legen Sie später bequem im Admin-Panel an (Kapitel „Benutzer, Postfächer, Passwörter“).

Hatten Sie schon einmal eine TrutzBox mit dieser TrutzKennung im Einsatz, zeigt der Schritt zusätzlich *Reaktivierbare Benutzer*. Eine vorhandene Adresse übernehmen Sie mit **Aktivieren**: Es öffnet sich dasselbe Fenster, der Anmelde-Name ist schon eingetragen, und Sie vergeben ein

Passwort und klicken auf **Hinzufügen**. Die Adresse bekommt dabei einen neuen Schlüssel (Kapitel „Adressen anlegen, löschen und reaktivieren“). Sind alle Adressen Ihres Kontingents schon vergeben, fehlt der Knopf **Benutzerkonto hinzufügen**, und Sie übernehmen eine der reaktivierbaren Adressen.

Wenn das Anlegen scheitert

Scheitert das Anlegen oder Aktivieren, nennt das Fenster den Grund oben rechts in einer roten Meldung:

„Die Service-Laufzeit dieser TrutzKennung ist abgelaufen. TrutzMail-Adressen lassen sich erst nach der Verlängerung wieder anlegen oder reaktivieren." Ihr Service-Vertrag ist abgelaufen. Dann kommt das Setup hier nicht weiter, auch nicht mit **Aktivieren**. Verlängern Sie den Vertrag über www.trutzbox.de oder schreiben Sie an support@trutzbox.de. Ist die Verlängerung bei Comidio eingetragen, klicken Sie erneut auf **Hinzufügen**. Bis dahin können Sie das Browserfenster schließen: Das Setup merkt sich den Schritt und macht beim nächsten Aufruf hier weiter.

„Das Kontingent an TrutzMail-Adressen dieser TrutzKennung ist erschöpft." Alle Adressen Ihres Vertrags sind vergeben. Übernehmen Sie eine Adresse aus *Reaktivierbare Benutzer* oder erweitern Sie das Kontingent über www.trutzbox.de.

„Diese TrutzMail-Adresse ist bereits vergeben. Bitte wählen Sie einen anderen Anmelde-Namen." TrutzMail-Adressen sind weltweit eindeutig. Wählen Sie einen anderen Anmelde-Namen.

„Verbindung zu den Comidio-Servern nicht möglich. Bitte überprüfen Sie Ihre Internetverbindung." Die TrutzBox erreicht Comidio gerade nicht. Prüfen Sie Kabel und Router und versuchen Sie es noch einmal.

Bei jedem anderen Grund lautet die Meldung *„Fehler beim Hinzufügen von neuem Benutzer"*. Versuchen Sie es noch einmal; bleibt der Fehler, hilft der Comidio-Support (Kapitel „Support kontaktieren“).

Nennt der Schritt die TrutzKennung 0 und „0 von 0" Adressen, konnte die TrutzBox beim Laden der Seite Comidio nicht fragen. Laden Sie die Seite neu, sobald die Internetverbindung steht.

3.9 Schritt „Einrichtung abgeschlossen"

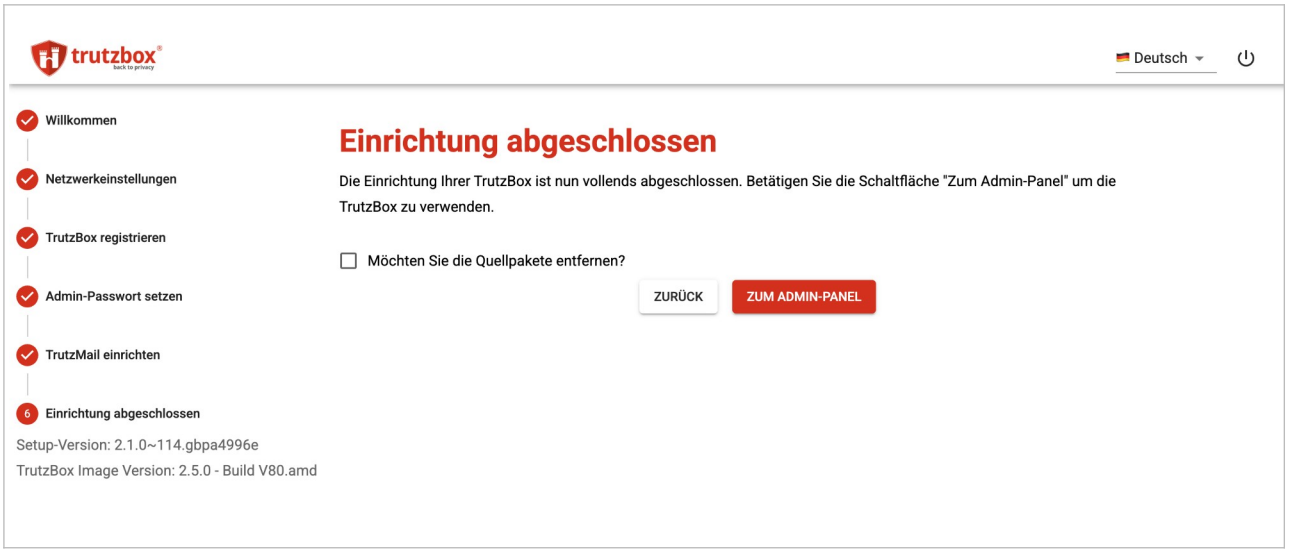


Abbildung 3-8: Der sechste und letzte Schritt: „Zum Admin-Panel" beendet das Setup und öffnet die Verwaltungsoberfläche. (© 2026 Comidio GmbH)

Die TrutzBox selbst ist damit fertig eingerichtet. Ein Klick auf **Zum Admin-Panel** beendet das Setup und bringt Sie zur Verwaltungsoberfläche. Ein Neustart ist nicht nötig. Die TrutzBox räumt im Hintergrund selbst auf und schaltet dabei unter anderem die verschlüsselte Namensauflösung (DNS) ein, die Ihre Internet-Anfragen vor neugierigen Blicken schützt. Der kurze Ladebildschirm dabei ist normal.

Das Häkchen *„Möchten Sie die Quellpakete entfernen?"* ist zunächst nicht gesetzt, und Sie können es so lassen. Setzen Sie es, löscht die TrutzBox beim Klick auf **Zum Admin-Panel** die mitgelieferten Quelltexte der Software-Pakete. Für den Betrieb braucht sie diese nicht; das Löschen schafft etwas Platz.

3.10 Wie es jetzt weitergeht: Geräte anschließen

Wichtig zu wissen: Fertig eingerichtet heißt noch nicht fertig geschützt. Geschützt sind nur die Geräte, die über die TrutzBox ins Internet gehen. Deshalb ist der nächste Schritt, einzelne oder alle Ihre Geräte an die TrutzBox anzuschließen. Wie Sie dabei vorgehen, ob per Kabel, über das TrutzBox-WLAN oder im Proxy-Mode, zeigt ausführlich das folgende Kapitel „Ein Gerät mit der TrutzBox absichern“ „Ein Gerät mit der TrutzBox absichern".

Drei Dinge im Überblick:

- **Anmelden:** Im Admin-Panel melden Sie sich mit dem Benutzernamen `admin` und Ihrem Passwort aus Abschnitt „Schritt „Admin-Passwort setzen"“ an.
- **Geräte anschließen:** Verbinden Sie Ihre Geräte nach und nach mit der TrutzBox (Kapitel „Ein Gerät mit der TrutzBox absichern“).
- **Geräte benennen und einordnen:** Geben Sie den Geräten anschließend sprechende Namen und ordnen Sie sie Filtergruppen zu (Kapitel „Geräte verwalten“).

Was Sie im Admin-Panel nach der Anmeldung erwartet, also die Startseite mit ihren Karten und die Ampel für den Betriebszustand, erklärt Kapitel „Startseite und Betriebszustand“. Es lohnt sich, dort einmal in Ruhe hineinzusehen, bevor Sie mit dem Einordnen der Geräte beginnen.

3.11 Der Ablauf auf einen Blick

Schritt	Was passiert	Dauer
Anschließen	Kabel vom Router in LAN-Ext, Netzteil einstecken; eingerichtet wird vom PC im lokalen Netz	wenige Minuten
Willkommen	Lizenzbedingungen bestätigen	kurz
Netzwerkeinstellungen	Verbindungstest zum Internet	kurz
Software-Updates	Meist schon beim Einschalten erledigt. Sonst spielt die TrutzBox jetzt neuere Software-Pakete ein, und das Setup wird danach von selbst fortgesetzt	meist keine Wartezeit, sonst wenige Minuten, höchstens rund eine Stunde
TrutzBox registrieren	TrutzKennung und TrutzSchlüssel eingeben; wahlweise vorher eine Sicherung einspielen	laut Oberfläche bis zu einer Minute
Admin-Passwort setzen	Passwort für den Verwalterzugang festlegen	kurz
TrutzMail einrichten	Erste TrutzMail-Adresse anlegen oder reaktivieren; ohne laufende Service-Laufzeit nicht möglich	kurz
Einrichtung abgeschlossen	Weiter ins Admin-Panel; danach die Geräte anschließen (Kapitel „Ein Gerät mit der TrutzBox absichern“)	kurz

Häufige Fragen zur Einrichtung

Muss ich die TrutzBox nach dem Setup neu starten?

Nein. Nach dem Klick auf „Zum Admin-Panel" ist die TrutzBox sofort einsatzbereit.

Kann ich das Setup abbrechen und später fortsetzen?

Ja. Die TrutzBox merkt sich den erreichten Schritt. Rufen Sie einfach wieder `http://trutzbox` auf, und das Setup macht dort weiter, wo Sie aufgehört haben. Über das Ein-Aus-Symbol rechts oben lässt sich die TrutzBox auch jederzeit neu starten oder sauber ausschalten.

Ich möchte die Einrichtung komplett neu beginnen. Ist das möglich?

Das ist erst möglich, wenn die TrutzBox einmal vollständig eingerichtet ist: Dann steht im Admin-Panel das Zurücksetzen auf den Werkszustand zur Verfügung, und Sie durchlaufen das Setup anschließend erneut mit Ihrer TrutzLegitimation, also TrutzKennung und TrutzSchlüssel vom Beileger. Der Vorgang dauert je nach Modell und Internet-Geschwindigkeit etwa 5 bis 25 Minuten, auf einer größeren SSD deutlich länger, bei einer großen auch Stunden (Kapitel „System

zurücksetzen (Werksreset)“). Mitten im Setup gilt stattdessen: Mit **Zurück** können Sie jeden Schritt noch einmal aufrufen und Eingaben korrigieren.

4 Ein Gerät mit der TrutzBox absichern

Die TrutzBox schützt genau die Geräte, deren Internet-Verkehr durch sie hindurchläuft. Nach der Einrichtung aus Kapitel „TrutzBox einrichten (Setup)“ ist das noch keines: Auch der PC, mit dem Sie das Setup erledigt haben, hängt weiter am Internet-Router. In diesem Kapitel holen Sie nach und nach Ihre Geräte unter den Schutz der TrutzBox: Computer, Smartphones, Tablets, Fernseher und Haustechnik, zuhause genauso wie in der Firma.

> **Gute Nachricht vorweg**
> Für den Grundschutz müssen Sie an den Geräten selbst nichts einstellen und nichts installieren. Der Webfilter TrutzContent arbeitet ohne jede Vorbereitung am Gerät, auch bei verschlüsselten Seiten. Erst für die Zusatzfunktion TrutzBrowse und für Programme, die sich direkt mit der TrutzBox verbinden, wird das Root-Zertifikat gebraucht; das beschreibt Kapitel „Das Root-Zertifikat installieren“.

4.1 Drei Wege zur TrutzBox

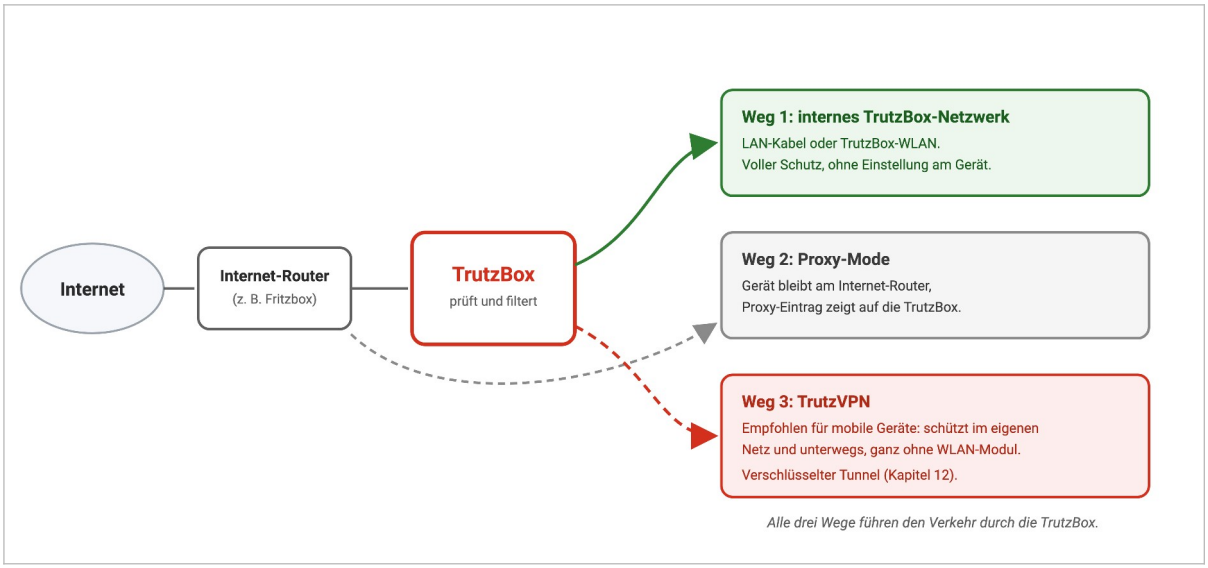


Abbildung 4-1: Drei Wege, ein Gerät mit der TrutzBox zu verbinden: internes Netzwerk, Proxy-Mode und TrutzVPN. (© 2026 Comidio GmbH)

Es gibt drei Wege, wie ein Gerät seinen Verkehr durch die TrutzBox leiten kann:

- **Weg 1, das interne TrutzBox-Netzwerk (empfohlen für alles, was an seinem Platz bleibt):** Das Gerät wird per Kabel an LAN-Int1 oder LAN-Int2 angeschlossen oder ins TrutzBox-WLAN eingebucht. Es bekommt seine Adresse automatisch von der TrutzBox, und der komplette Verkehr läuft ohne jede Einstellung am Gerät durch alle Schutzfunktionen. Nur dieser Weg lässt sich am Gerät selbst nicht abschalten; für Geräte von Kindern ist er deshalb der richtige.
- **Weg 2, der Proxy-Mode:** Das Gerät bleibt im Netz des Internet-Routers und bekommt lediglich die TrutzBox als Proxy eingetragen. Praktisch zum Ausprobieren und für Geräte, die nicht umgezogen werden können. Der Schutz gilt dann für den Web-Verkehr des Geräts. Die

Einstellung ließe sich am Gerät aber auch wieder abschalten, für den Jugendschutz ist dieser Weg deshalb ungeeignet.

- **Weg 3, TrutzVPN (empfohlen für mobile Geräte):** Smartphones und Tablets haben meist gar keinen Kabelanschluss. Für sie ist der VPN-Tunnel die beste Lösung, denn er schützt das Gerät im eigenen Netz und unterwegs gleichermaßen, und die TrutzBox braucht dafür kein eingebautes WLAN-Modul. Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“ beschreibt die Einrichtung.

4.2 Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen

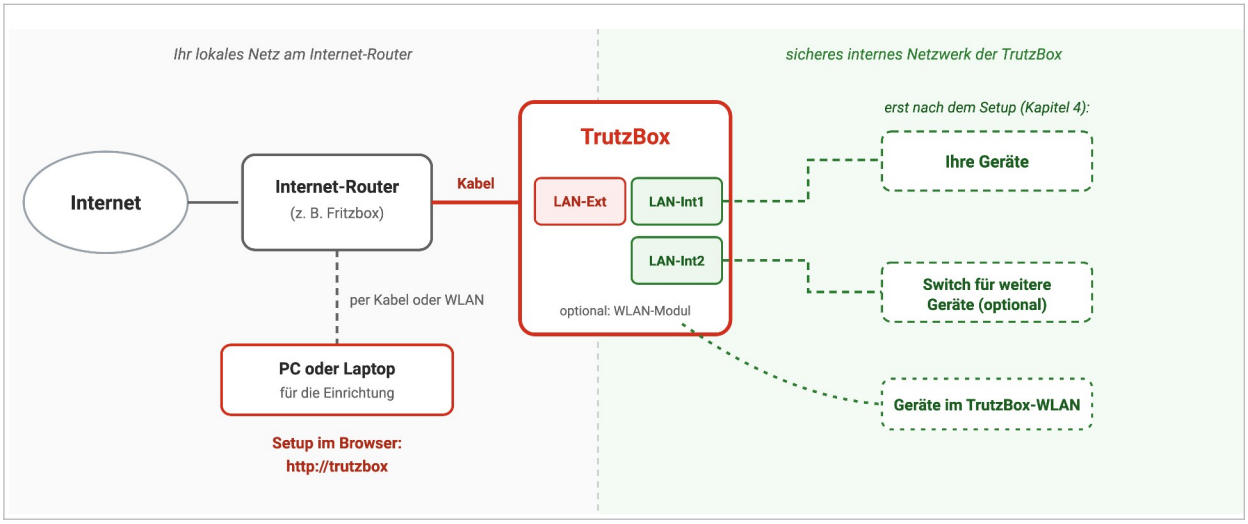


Abbildung 4-2: Das interne Netzwerk der TrutzBox: alles rechts der TrutzBox ist geschützt. (© 2026 Comidio GmbH)

1. **Per Kabel:** Verbinden Sie das Gerät mit **LAN-Int1** oder **LAN-Int2**. Reichen die beiden Buchsen nicht aus, hängen Sie einen gewöhnlichen Netzwerk-Verteiler (Switch) an eine davon; alle Geräte daran gehören dann ebenfalls zum geschützten Netz.
2. **Per WLAN:** Buchen Sie das Gerät in das WLAN der TrutzBox ein. Name und Passwort legen Sie unter **Netzwerk → WLAN** fest (Kapitel „Das WLAN der TrutzBox“). Das TrutzBox-WLAN ist Teil des internen Netzes.
3. **Gerät neu starten:** Manche Geräte merken den Netzwerkwechsel nicht von selbst und halten an ihrer alten Adresse fest. Starten Sie das Gerät nach dem Umstecken oder dem WLAN-Wechsel einmal neu, dann holt es sich eine neue Adresse von der TrutzBox.
4. **Erfolg prüfen:** Das Gerät erscheint nach dem ersten Datenverkehr unter **Verwaltung → Geräte**, zunächst in der Filtergruppe „Standard" und in der Spalte **Verbindung** mit „Transparent", dahinter in Klammern das Netz, etwa „Transparent (intern)". Geben Sie ihm dort gleich einen sprechenden Namen (Kapitel „Geräte verwalten“).

Das Gerät bezieht seine Adresse automatisch aus dem internen Bereich der TrutzBox. Prüfen Sie zur Sicherheit, dass es nicht mehr im alten WLAN des Internet-Routers angemeldet ist, sonst rutscht sein Verkehr am Schutz vorbei.

Am Gerät ist nichts einzustellen

Das ist der eigentliche Vorzug dieses Wegs: Sie tragen am Gerät keinen Proxy ein, weder von Hand noch über eine Konfigurationsadresse. Die TrutzBox holt sich den Web-Verkehr selbst. Alles, was

ein Gerät im internen Netz an die üblichen Web-Anschlüsse schickt, lenkt die TrutzBox im Vorbeigehen auf ihren eigenen Filter um; nur was an die TrutzBox selbst gerichtet ist, bleibt unberührt. Fachleute nennen das den **Transparent-Mode**: Für das Gerät sieht es aus, als spräche es direkt mit dem Zielserver.

Ein zusätzlicher Proxy-Eintrag bringt hier nichts und schadet eher. Er ist eine zweite Stelle, die falsch stehen kann, er verschwindet gerne bei Systemwechseln, und er lässt sich am Gerät abschalten, was bei Kindergeräten den Schutz aushebelt. Proxy-Einträge gehören ausschließlich zu Weg 2 im nächsten Abschnitt.

Einem Gerät eine feste Adresse geben

Manche Geräte, etwa ein Netzwerkdrucker oder ein Netzwerkspeicher, sollen immer unter derselben Adresse erreichbar sein. Das stellen Sie am Gerät selbst ein, nicht auf der TrutzBox. Die Adresse muss aus dem Bereich stammen, den die TrutzBox für ihr internes Netz nutzt, sonst gehört das Gerät nicht mehr dazu und ist weder erreichbar noch geschützt.

Angabe am Gerät	Wert
IP-Adresse	Aus 192.168.195.2 bis 192.168.195.49 oder 192.168.195.201 bis 192.168.195.254, eine noch nicht benutzte Adresse
Subnetzmaske	255.255.255.0
Standard-Gateway (Router)	192.168.195.200 (die TrutzBox)
DNS-Server	192.168.195.200 (die TrutzBox)
Such-Domain (falls gefragt)	sec

Nicht aus dem Bereich der automatischen Adressen

Die Adressen 192.168.195.50 bis 199 vergibt die TrutzBox selbst automatisch an Ihre Geräte. Eine feste Adresse aus diesem Bereich kann deshalb früher oder später doppelt vergeben werden, und dann streiten sich zwei Geräte um dieselbe Adresse. Nehmen Sie deshalb eine Adresse aus den freien Bereichen darunter oder darüber und notieren Sie sich, welche Sie vergeben haben. Die 192.168.195.200 ist die TrutzBox selbst.

Tragen Sie als DNS-Server unbedingt die TrutzBox ein. Ein fremder DNS-Server würde die Filterung und den Schutz vor DNS-Umgehung aushebeln.

4.3 Weg 2: Gerät im Proxy-Mode betreiben

Im Proxy-Mode bleibt das Gerät im Netz des Internet-Routers und schickt seinen Web-Verkehr zur TrutzBox. Anders als bei Weg 1 muss die TrutzBox hier am Gerät eingetragen werden, denn sie liegt ja nicht im Weg und kann sich den Verkehr nicht selbst holen.

Wo Sie eintragen, entscheidet über die Reichweite. Tragen Sie den Proxy in den **Netzwerkeinstellungen des Betriebssystems** ein, gilt er für alle Programme des Geräts. Das ist der empfohlene Weg. Nur der Browser **Firefox** bringt eine eigene Proxy-Einstellung mit und benutzt vorrangig diese; wer dort einträgt, schützt allein den Firefox und lässt alle übrigen Programme

direkt ins Internet. Wo die Einstellung je Betriebssystem steht, zeigt Kapitel „Den Proxy-Mode am Gerät einrichten“.

Möglichkeit A: die automatische Proxy-Konfiguration (empfohlen)

Statt Adresse und Port von Hand einzutragen, hinterlegen Sie eine einzige Adresse, unter der die TrutzBox die passende Konfiguration selbst ausliefert:

```
http://trutzbox/api/proxy/pac
```

Diesen Eintrag nehmen Sie in den Netzwerkeinstellungen des Geräts unter einer Bezeichnung wie *„Automatische Proxy-Konfiguration"* oder *„Konfigurationsadresse für automatischen Proxy"* vor. Der Vorteil: Sie müssen keinen Port kennen, Zugriffe auf die TrutzBox selbst laufen automatisch am Proxy vorbei, und sollte die TrutzBox einmal nicht erreichbar sein, nimmt das Gerät den direkten Weg ins Internet, statt ganz ohne Internet dazustehen.

Möglichkeit B: Proxy von Hand eintragen

1. Öffnen Sie die Netzwerkeinstellungen des Geräts und dort den Bereich für den Proxy.
2. Tragen Sie als Proxy-Server `trutzbox` ein und als Port `8081`. Dieser Port ist fest und ändert sich nicht.
3. Übernehmen Sie die Einstellung für HTTP und für HTTPS.

Unter **Verwaltung → Geräte** steht das Gerät in der Spalte **Verbindung** zunächst als „Nicht verbunden (extern)". „Proxy (extern)" erscheint erst, wenn wirklich Web-Verkehr des Geräts über den Proxy gelaufen ist, also nach dem ersten Seitenaufruf. Das Abholen der automatischen Konfiguration allein zählt dabei nicht. Im Monitor erscheint das Gerät in der Gruppe **Ext. Netz**. Beides ist richtig so: Das Gerät steht ja weiterhin im vorgelagerten Netz und nutzt die TrutzBox nur als Vermittler.

> **Was der Proxy-Mode nicht leistet**
>
> Der Eintrag lässt sich am Gerät jederzeit wieder entfernen. Für alles, was verlässlich geschützt sein muss, insbesondere Jugendschutz, ist Weg 1 die richtige Wahl.
>
> Gefiltert wird der Web-Verkehr über HTTP und HTTPS. Andere Protokolle laufen an der TrutzBox vorbei, ebenso Programme, die einen eingetragenen Proxy bewusst ignorieren.

4.4 Weg 3: TrutzVPN für mobile Geräte

Smartphones und Tablets wechseln ständig das Netz: das eigene WLAN, unterwegs Mobilfunk, im Hotel ein fremdes WLAN. Für sie ist der VPN-Tunnel die beste Lösung. Einmal eingerichtet, schützt er das Gerät überall gleich, ganz gleich wo es sich einbucht, und die TrutzBox braucht dafür kein eingebautes WLAN-Modul. Die Einrichtung, vom Domain-Namen über die Portfreigabe am Router bis zur App auf dem Gerät, beschreibt Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“ Schritt für Schritt.

4.5 Welcher Weg für welches Gerät?

Gerät	Empfohlener Weg
PC, Laptop am festen Platz	Weg 1, per Kabel oder TrutzBox-WLAN
Smartphone, Tablet	Weg 3 (TrutzVPN), dann ist das Gerät im eigenen Netz und unterwegs geschützt
Geräte von Kindern	Weg 1, weil sich nur dieser Weg am Gerät nicht abschalten lässt
Fernseher, Streaming-Gerät, Spielkonsole	Weg 1
Haustechnik, Kameras, Thermostate	Weg 1, dazu eine enge Filtergruppe (Kapitel „Webfilter und Jugendschutz (TrutzContent)“)
Gastgeräte	Weg 1 über das TrutzBox-WLAN
Arbeitsrechner, der am Router bleiben muss	Weg 2, Proxy-Mode

Für keinen dieser Wege ist am Gerät ein Zertifikat nötig. Erst wenn Sie zusätzlich TrutzBrowse einschalten möchten (Kapitel „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“) oder wenn ein Mail- oder Chat-Programm auf dem Gerät sich mit der TrutzBox verbinden soll (Kapitel „TrutzMail: sichere E-Mail“ und „TrutzChat und Videokonferenz“), kommt das Root-Zertifikat ins Spiel, und dafür gibt es Kapitel „Das Root-Zertifikat installieren“.

Häufige Fragen zum Anschließen

Muss wirklich jedes Gerät einzeln umgestellt werden?

Einzurichten ist am Gerät nichts. Es ändert sich nur der Anschluss: Kabel in die TrutzBox statt in den Router, WLAN der TrutzBox statt des Router-WLANs. Jedes Gerät muss sich danach allerdings einmal neu im Netzwerk anmelden, und das merken nicht alle von selbst. Starten Sie deshalb jedes umgezogene Gerät einmal neu.

Das gilt auch, wenn mehrere Geräte an einem Switch hängen: Das eine Kabel umzustecken bringt sie zwar alle auf einen Schlag ins neue Netz, aber jedes einzelne Gerät daran braucht trotzdem seinen Neustart, ebenso der Switch selbst, sofern er sich eine eigene Adresse holt. Sonst versuchen die Geräte weiter, über den alten Weg ins Internet zu kommen, und melden schlicht „kein Internet".

Was passiert mit Geräten, die am Router bleiben?

Sie funktionieren normal weiter, aber ungeschützt und für die TrutzBox unsichtbar, sofern sie nicht im Proxy-Mode angebunden sind. Der Monitor zeigt Ihnen jederzeit, welche Geräte über die TrutzBox laufen (Kapitel „Monitor und Statistiken“).

Ein Gerät hat nach dem Umstecken kein Internet. Was tun?

Starten Sie es neu. Meist hält es noch an der Adresse fest, die es vom alten Netz bekommen hat. Hilft das nicht, führt Kapitel „… ein Gerät nicht auftaucht“ durch die weitere Suche.

Funktioniert das auch mit IPv6?

Das interne TrutzBox-Netz arbeitet bewusst nur mit IPv4; den Geräten darin entsteht dadurch kein Nachteil. Nach außen zum Internet kann die TrutzBox zusätzlich IPv6 verwenden.

5 Startseite und Betriebszustand

Die Verwaltungsoberfläche der TrutzBox, das Admin-Panel, erreichen Sie von jedem Gerät im internen Netz unter `https://trutzbox`, ebenso von einem PC im lokalen Netz am Internet-Router. Findet der Browser den Namen nicht, hilft `http://trutzbox.local` weiter (Kapitel „Das Setup im Browser öffnen“). Melden Sie sich mit dem Benutzernamen `admin` und dem Passwort aus der Einrichtung an. Dieses Kapitel zeigt die beiden Seiten, die Sie am häufigsten sehen werden: die Startseite mit dem Überblick und den Betriebszustand mit der Ampel.

Beide Seiten sind reine Anzeigeseiten. Sie können dort nichts kaputt machen, und Sie müssen dort auch nichts regelmäßig tun. Wer sie einmal in Ruhe gelesen hat, erkennt später auf einen Blick, ob alles normal läuft.

5.1 Die Startseite lesen

Menüpfad: Übersicht



Abbildung 5-1: Die Übersicht: oben die Blockierungen, darunter Geräte, Netzwerk, Services, Festplatten Belegung, Arbeitsspeicher, Temperatur und Prozessor. (© 2026 Comidio GmbH)

Nach der Anmeldung begrüßt Sie eine Seite aus Karten; im Menü links heißt sie **Übersicht**. Sie beantwortet die Alltagsfragen auf einen Blick: Läuft alles? Wie viele Geräte sind gerade online? Wie viel hat die TrutzBox heute blockiert? Ein Klick auf die Überschrift **Statistiken**, **Geräte** oder **Netzwerk** führt zur ausführlichen Seite.

Die einzelnen Karten im Überblick:

- **Statistiken:** oben links die Karte **Blockierungen** mit der Anzahl der geblockten Verbindungen, getrennt nach Proxy-Filter und Firewall, in den Zeilen *Letzte 60 Minuten*, *Heute*, *Diesen Monat* und *Insgesamt*. „Letzte 60 Minuten" zählt gleitend die Stunde bis jetzt;

kurz nach Mitternacht kann dort deshalb mehr stehen als bei „Heute". Daneben zeigt **Blockierungen pro Tag** ein Zeitdiagramm, und neben der Überschrift steht, seit wann aufgezeichnet wird. Diese Zahlen sind der schnellste Beleg dafür, dass die TrutzBox tatsächlich arbeitet. Gezählt wird, solange unter **Verwaltung → Statistiken** der Schalter **Statistiken speichern** an ist; ab Werk ist er eingeschaltet (Kapitel „Statistiken: Blockierungen über lange Zeiträume“).

- **Geräte:** alle mit der TrutzBox verbundenen Geräte mit den Spalten Gerätename, Hersteller, Letzte Proxy-Verbindung und Filtergruppe. Ein Klick auf die Verbindungszeit öffnet das Verbindungsprotokoll genau dieses Geräts im Monitor. Die vollständige Liste mit allen Einstellmöglichkeiten finden Sie in Kapitel „Geräte verwalten“.
- **Netzwerk:** ein Live-Diagramm des aktuellen Netzwerkverkehrs. Die Anzeige für **LAN-Ext** steht für den äußeren Anschluss Richtung Internet-Router, also für alles, was tatsächlich ins Internet gesendet oder von dort empfangen wird.
- **Services:** drei Symbole für **Videokonferenz**, **TrutzMail** und **TrutzContent / TrutzBrowse**. Ein rotes Symbol bedeutet aktiv, ein graues inaktiv. Unter Videokonferenz und TrutzMail sitzt je ein Schalter, der den Dienst ein- oder ausschaltet. Unter TrutzContent / TrutzBrowse sitzt stattdessen ein runder Pfeil: Er startet den Webfilter neu, denn abschalten lässt sich der Webfilter hier nicht.
- **Festplatten Belegung:** vier Tortendiagramme zeigen den belegten und freien Speicherplatz der einzelnen Bereiche der SSD. Beschriftet sind sie mit der internen Bezeichnung des jeweiligen Bereichs. Ein Klick auf ein Diagramm öffnet eine Liste der größten Dateien des jeweiligen Bereichs, die sich zur Analyse auch als Datei herunterladen lässt.
- **Arbeitsspeicher (RAM und Swap):** ein Zeitdiagramm der letzten Stunde. Der Arbeitsspeicher besteht aus zwei Teilen: dem Hauptspeicher (RAM), also dem schnellen Speicher, mit dem die TrutzBox rechnet, und der Auslagerung (Swap). Die Auslagerung liegt nicht auf der SSD, sondern ist ein gepackter Bereich im Hauptspeicher selbst: Wird der Hauptspeicher knapp, legt die TrutzBox dort Daten zusammengedrückt ab, die sie gerade nicht braucht. So passt mehr hinein. Die Linie zeigt, wie viel von beiden zusammen belegt ist. Ein voller Hauptspeicher allein ist deshalb kein Engpass; eng wird es erst ab rund 90 Prozent. Das „i" neben der Überschrift nennt die Größen dieser TrutzBox. Ein Klick auf das Diagramm öffnet den Speicherverlauf (siehe unten).
- **Prozessor Temperatur:** ein Zeitdiagramm der aktuellen Temperatur, dazu der vom Sensor gemeldete Höchstwert. Bleibt der Wert dauerhaft hoch, liegt es fast immer am Aufstellort (Kapitel „Aufstellort, Belüftung und Dauerbetrieb“).
- **Prozessor:** je ein Diagramm pro Prozessorkern. Wie viele es sind, hängt von der verbauten Hardware ab.
- **Abmelden und TrutzBox steuern:** über das Symbol oben rechts melden Sie sich ab oder fahren die TrutzBox geordnet herunter beziehungsweise starten sie neu. Beim Neustart deckt die Warteseite *„Die TrutzBox wird neu gestartet"* die Oberfläche ab; das dauert rund drei Minuten, danach erscheint die Oberfläche von selbst wieder. Beim Herunterfahren erscheint *„Die TrutzBox wird ausgeschaltet"* mit dem Hinweis, dass Sie die Seite schließen können.

Der Speicherverlauf

Ein Klick auf das Diagramm **Arbeitsspeicher (RAM und Swap)** öffnet das Fenster **Speicherverlauf**; fährt man mit der Maus darüber, erscheint der Hinweis *„Speicherverlauf anzeigen"*. Dasselbe Fenster öffnet im Betriebszustand die Schaltfläche **Verlauf anzeigen** in der Karte Arbeitsspeicher (Abschnitt „Betriebszustand: die Karten im Einzelnen“). Es zeigt, wie voll der Speicher in den letzten 30 Tagen war, in drei Diagrammen mit derselben Zeitachse, jeweils in GB:

- **Hauptspeicher (RAM):** wie viel vom verbauten Hauptspeicher belegt ist.
- **Auslagerung (Swap):** wie viel der Auslagerung belegt ist, also des gepackten Bereichs im Hauptspeicher. Eng wird es erst, wenn Hauptspeicher und Auslagerung beide fast voll sind.
- **Webfilter:** wie viel Speicher der Webfilter belegt; die helle Fläche davon sind die Filterlisten. Die rote gestrichelte Linie ist seine Grenze, sie richtet sich nach dem verbauten Hauptspeicher. Erreicht der Webfilter sie, startet er neu, und für rund eine Minute erreichen die Geräte im Netz keine Webseiten. Bleibt der Abstand zur Grenze dauerhaft klein, hilft es, in den Filtergruppen Kategorien abzuwählen (Kapitel „Filtergruppen einrichten“).

Menüpfad: Übersicht → Diagramm Arbeitsspeicher

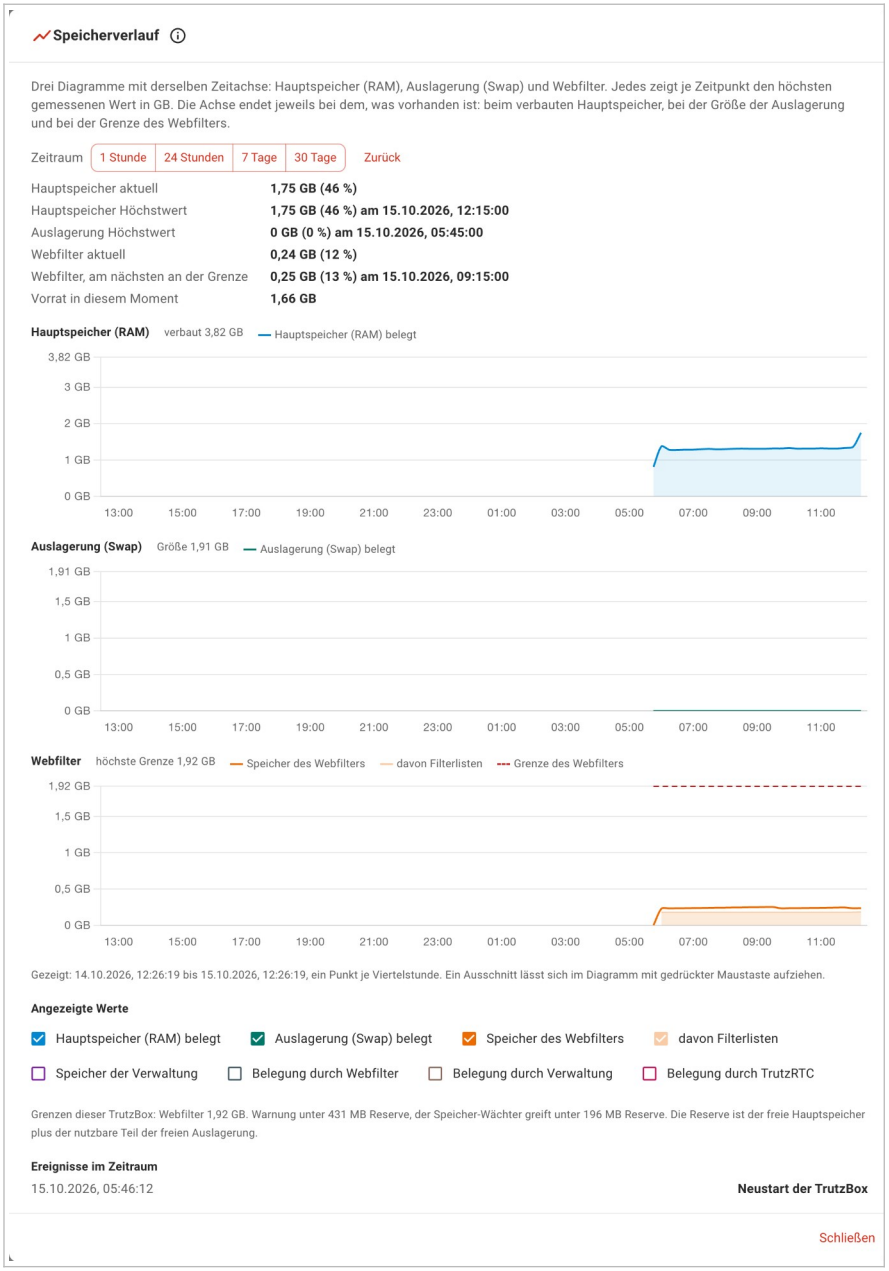


Abbildung 5-2: Der Speicherverlauf mit den drei Diagrammen Hauptspeicher, Auslagerung und Webfilter, hier über 24 Stunden auf einer TrutzBox mit rund 4 GB Hauptspeicher. (© 2026 Comidio GmbH)

Unter **Zeitraum** wählen Sie *1 Stunde*, *24 Stunden*, *7 Tage* oder *30 Tage*. Einen Ausschnitt ziehen Sie im Diagramm mit gedrückter Maustaste auf; **Zurück** stellt die vorige Ansicht wieder her. Jeder Punkt ist der höchste Wert seines Zeitabschnitts, nicht der Durchschnitt, damit kurze Spitzen sichtbar bleiben. Über den Diagrammen stehen die wichtigsten Zahlen, etwa *Hauptspeicher Höchstwert* und *Webfilter, am nächsten an der Grenze*. Unter **Angezeigte Werte** lassen sich weitere Linien zuschalten, etwa der Speicher der Verwaltung oder die Belegung durch TrutzRTC.

Abschnitte, in denen Hauptspeicher und Auslagerung beide fast voll waren, sind gelb hinterlegt, rot ab dem Punkt, an dem der Speicher-Wächter einen Dienst beendet hat. Unter den Diagrammen nennt das Fenster die Grenzen dieser TrutzBox, etwa *„Warnung unter 431 MB Reserve, der Speicher-Wächter greift unter 196 MB Reserve"*, und unter **Ereignisse im Zeitraum**

Vorkommnisse wie einen Neustart der TrutzBox. Was die Reserve ist, erklärt die Karte Arbeitsspeicher in Abschnitt „Betriebszustand: die Karten im Einzelnen“.

Links liegt das Menü, über das Sie alle Funktionen erreichen. Die Kapitel dieses Handbuchs nennen den jeweiligen Pfad immer in der Form **Verwaltung → Geräte**.

Die Landkarte: welcher Menüpunkt, welches Kapitel

Neben Übersicht und Monitor hat das Menü die aufklappbaren Bereiche Verwaltung, Browseranonymität, E-Mail, Netzwerk und Systemeinstellungen. E-Mail sowie Videokonferenz und Chat erscheinen nur, wenn TrutzMail beziehungsweise TrutzRTC auf Ihrer TrutzBox freigeschaltet sind. Die folgende Übersicht sagt Ihnen zu jedem Punkt, wo er in diesem Handbuch beschrieben ist. Sie ist zugleich der schnellste Weg, wenn Sie in der Oberfläche etwas gefunden haben und wissen möchten, was dahintersteckt.

Menüpunkt	Wozu er dient	Kapitel
Übersicht	Die Startseite mit allen Karten	5.1
Monitor	Live-Ansicht aller Verbindungen im Netz	9
Verwaltung → Geräte	Geräte benennen, einordnen und einschränken	6
Verwaltung → Benutzer	Konten, Postfächer, Passwörter, VPN-Freigabe	7
Verwaltung → Filtergruppen	Filterprofile anlegen und zuweisen	8.2
Verwaltung → Filterlisten	Sperr- und Ausnahmelisten pflegen und importieren	8.3, 8.4
Verwaltung → Eigene Sperren und Ausnahmen	Eigene Sperren und Freigaben für Webfilter und Firewall an einem Ort, mitgelieferte Ausnahmen ein- und ausschalten	8.8
Verwaltung → Statistiken	Blockierungen über lange Zeiträume	9.7
Verwaltung → Allgemeine Einstellungen	Admin-Passwort, Root-Zertifikat, Grundeinstellungen	7.3, 19.2
Browseranonymität	Alles rund um TrutzBrowse: Slider-Stufen, Zuordnung je Gerät und Seite, eigene Sperrlisten	13
E-Mail → Webmail	TrutzMail im Browser lesen und schreiben	10.2
E-Mail → Status	Warteschlange und Mailprotokoll	10.7
E-Mail → Schlüsselverwaltung	Schlüssel und Zertifikate für TrutzMail und PGP	10.6
Videokonferenz und Chat	TrutzMeeting und TrutzChat einrichten	11
Netzwerk → Status	Äußeres und inneres Netz, Datenraten, Geräte	14.1
Netzwerk → Angriffsschutz	Firewall, gesperrte Adressen, Sperrlisten	14.4

Menüpunkt	Wozu er dient	Kapitel
Netzwerk → Netzwerkdienste	Verschlüsselte Namensauflösung und Zeitserver	14.3
Netzwerk → WLAN	Eigenes Funknetz der TrutzBox	14.2
Netzwerk → Fernzugriff	TrutzVPN einrichten und prüfen	12
Systemeinstellungen → Betriebszustand	Ampel, Karten, Verlauf, Support-Bericht	5.2, 18
Systemeinstellungen → Vertrag und Pakete	Service-Vertrag, Kontingent, Hardware, Versionen	15, 7.5
Systemeinstellungen → Sichern und Wiederherstellen	Sicherung anlegen, einspielen, zurücksetzen	16
Systemeinstellungen → Rechtliche Hinweise	Hersteller, Lizenzbedingungen und vollständige Paketliste der Software	15.6, 20.5
Systemeinstellungen → System-Logs	Protokolle für den Support	18.3
Systemeinstellungen → Webmin	Technische Zweit-Oberfläche für den Notfall	14.6

Die drei Zahlen, auf die es im Alltag ankommt

Wenn Sie die Übersicht nur kurz überfliegen möchten: Die Ampel oben sagt, ob etwas zu tun ist. Die Blockierungszahl für heute sagt, ob die Filterung arbeitet. Die Karte **Geräte** sagt, ob ein Gerät auftaucht, das dort nicht hingehört. Alles Weitere ist Hintergrundinformation.

5.2 Betriebszustand: die Ampel lesen

Menüpfad: Systemeinstellungen → Betriebszustand

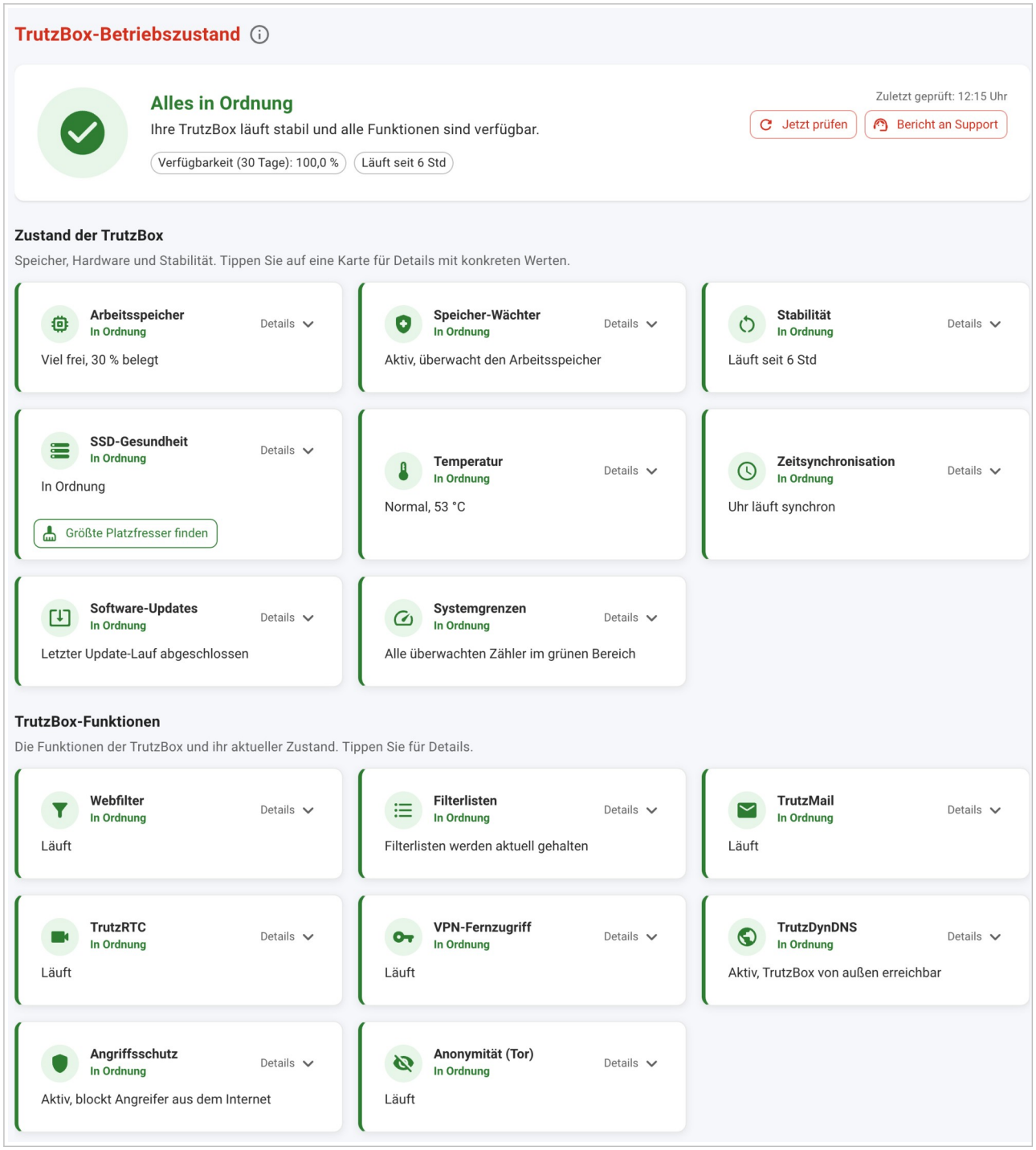


Abbildung 5-3: Der Betriebszustand: oben die Ampel mit „Alles in Ordnung", darunter die Karten unter „Zustand der TrutzBox" und „TrutzBox-Funktionen". (© 2026 Comidio GmbH)

Die Seite **Systemeinstellungen → Betriebszustand** ist die Gesundheitsanzeige Ihrer TrutzBox. Sie ist als schnelle Selbstdiagnose gedacht: Statt technische Protokolle zu durchsuchen, sehen Sie hier in Klartext, ob Hardware, Speicher und alle Dienste in Ordnung sind. Die TrutzBox prüft sich dafür alle 15 Minuten selbst. Ganz oben steht eine einzige Ampel für den Gesamtzustand. Die Karten darunter tragen dieselben Farben und benennen sie mit einem Wort:

- **Grün, „In Ordnung":** Oben steht *„Alles in Ordnung"*. Sie müssen nichts tun.
- **Gelb, „Auffällig":** Oben steht *„Kleinere Auffälligkeiten"*. Etwas verdient einen Blick, der Schutz läuft aber weiter, zum Beispiel wenn bereitstehende Filterlisten länger nicht installiert wurden.
- **Rot, „Kritisch":** Oben steht *„Aufmerksamkeit nötig"*. Ein Bereich braucht Ihre Aufmerksamkeit; die betroffene Karte darunter nennt Ursache und Abhilfe in Klartext.
- **Grau, „Ausgeschaltet":** Die Funktion wurde bewusst abgeschaltet. Eine abgeschaltete Funktion zieht die Ampel weder auf Gelb noch auf Rot. Wer den VPN-Fernzugriff gar nicht nutzt, bekommt deswegen also keine Warnung.

Auf Rot springt die Ampel oben nur bei Karten, die den Schutz oder den Bestand der TrutzBox betreffen: Webfilter, Filterlisten, Angriffsschutz, Arbeitsspeicher, SSD-Gesundheit, Software-Updates und DNS für Geräte. Steht eine andere Karte auf „Kritisch", etwa TrutzRTC oder TrutzMail, wenn der Dienst ausgefallen ist, zeigt die Ampel oben höchstens Gelb. So bleibt Rot den Fällen vorbehalten, in denen wirklich etwas zu tun ist.

Neben der Ampel stehen zwei Angaben, die den Zustand einordnen: die Verfügbarkeit der letzten 30 Tage und die Laufzeit seit dem letzten Neustart. Die Verfügbarkeit zählt dabei keine Ausfallminuten, sondern die Tage, an denen ein unerwarteter Neustart aufgetreten ist. Dieselbe Ampel erscheint übrigens auch in der Leiste jeder anderen Admin-Seite und führt von dort mit einem Klick hierher zurück, sodass Sie eine Störung auch dann bemerken, wenn Sie gerade an etwas anderem arbeiten.

Zur Ampel gehören zwei Schaltflächen und ein Schalter:

- **Jetzt prüfen:** stößt die Prüfung sofort neu an, ohne auf die nächste Viertelstunde zu warten.
- **Bericht an Support:** öffnet das Fenster *„Bericht an den Support senden"* mit allen für eine Anfrage wichtigen Angaben (siehe Kasten unten).
- **Ampel auf Grün stellen:** erscheint nur, wenn die Ampel nicht grün steht. Damit quittieren Sie die gemeldeten Punkte, etwa eine Störung, die Sie kennen und die Sie nicht stört. Die Ampel steht dann wieder auf Grün, oben steht *„Keine offenen Probleme"* mit dem Zusatz *„Quittiert"*, und sie meldet sich erst wieder, wenn ein neues Problem auftritt. Die Karten selbst zeigen weiter ihren tatsächlichen Zustand.

> **Der kürzeste Weg zum Support**
>
> Die Schaltfläche **Bericht an Support** öffnet das Fenster *„Bericht an den Support senden"*. Es zeigt den fertigen Bericht: oben Ihre Vertragsdaten, darunter Platz für Ihr Anliegen, dann die technischen Angaben. Mit **Bericht kopieren** übernehmen Sie ihn in die Zwischenablage, **E-Mail-Programm öffnen** bereitet eine Nachricht an support@trutzbox.de vor. Abgeschickt wird sie erst, wenn Sie es selbst tun; das Fenster weist eigens darauf hin. Öffnet sich das E-Mail-Programm nicht, bietet das Fenster **Als Datei speichern** an. Ist der Service-Vertrag abgelaufen, erstellt das Fenster keinen Bericht. Mehr dazu in Kapitel „Support kontaktieren“.

5.3 Betriebszustand: die Karten im Einzelnen

Die folgenden drei Abschnitte bleiben auf derselben Seite: Sie schlüsseln auf, was unterhalb der Ampel steht. Unter ihr liegen die einzelnen Karten, gruppiert in zwei Abschnitte. Jede Karte zeigt zunächst einen Kurzstatus; ein Klick oder Tipp darauf öffnet die Details mit konkreten Messwerten. Jede Karte erklärt ihren Zustand in ganzen Sätzen statt in Fehlercodes, bei Störungen samt Handlungsempfehlung, etwa dem Rat, TrutzRTC auf der Videokonferenz-Seite aus- und wieder einzuschalten.

Zustand der TrutzBox bündelt Speicher, Hardware und Stabilität. Zwei weitere Karten dieses Abschnitts, **Internet-Anschluss** und **DNS für Geräte**, erscheinen nur im Störungsfall; sie sind weiter unten beschrieben.

Karte	Was sie zeigt
Arbeitsspeicher	Wie voll der Arbeitsspeicher ist, also Hauptspeicher (RAM) und Auslagerung (Swap) zusammen, etwa „Viel frei, 30 % belegt". Beurteilt wird die Karte nach der Reserve: dem freien Hauptspeicher plus dem nutzbaren Teil der freien Auslagerung. Fällt die Reserve unter 11 % des Hauptspeichers, wird die Karte gelb („Wird knapp"), unter 5 % rot („Kritisch"); dann greift der Speicher-Wächter ein. Aufgeklappt nennt sie Belegung, Reserve, Warnschwelle und Auslagerung, den Speicher von Webfilter, Web-Server (Verwaltung) und TrutzRTC einzeln und darunter die Liste „Größte Speicherverbraucher" mit dem Anteil jedes Dienstes im Hauptspeicher und in der Auslagerung. Die Schaltfläche „Verlauf anzeigen" öffnet den Speicherverlauf (Abschnitt „Die Startseite lesen“).
Speicher-Wächter	Überwacht den Arbeitsspeicher nach derselben Reserve und hält bei Knappheit gezielt zuerst TrutzRTC und danach TrutzMail an, damit die TrutzBox nicht einfriert. Ist wieder genug Speicher frei, startet er den Dienst von selbst. Solange steht die Karte des Dienstes grau auf „Vom Speicher-Wächter angehalten"; das ist keine Störung.
Stabilität	Die Laufzeit seit dem letzten Neustart.
SSD-Gesundheit	Das Ergebnis des Selbsttests der SSD und wie voll sie ist: Ab 90 % belegt wird die Karte gelb, ab 96 % rot. Über „Größte Platzfresser finden" lassen sich die speicherintensivsten Daten aufspüren und alte Systemstände aufräumen; „SSD-Details anzeigen" nennt Modell, Kapazität, Firmware und die einzelnen Selbstdiagnose-Werte, jeweils mit eigener Ampelbewertung. Meldet die SSD es, steht dort auch „Unsaubere Abschaltungen": wie oft die TrutzBox ohne sauberes Herunterfahren ausging, etwa durch einen Stromausfall oder einen gezogenen Stecker. Einzelne sind unkritisch.
Temperatur	Die aktuelle Betriebstemperatur der Hardware.
Zeitsynchronisation	Ob die Uhr der TrutzBox mit vertrauenswürdigen Zeitservern abgeglichen ist. Eine falsche Uhrzeit stört verschlüsselte Verbindungen und Software-Updates. Direkt nach einem Neustart steht hier für einige Minuten „Synchronisierung läuft".
Software-Updates	Ob die TrutzBox ihre Software-Updates bekommt und einspielt: wann zuletzt Pakete eingespielt wurden, wie der letzte Update-Lauf endete, ob angebotene Pakete noch nicht eingespielt sind und wann der nächste Lauf ansteht. Gelb

Karte	Was sie zeigt
	und rot wird sie nach festen Regeln, siehe „Die Karte Software-Updates" weiter unten.
Systemgrenzen	Betriebsmittel, die knapp werden können, ohne dass Prozessor oder Arbeitsspeicher auffällig aussehen. Der Abschnitt „Die Karte Systemgrenzen" weiter unten erklärt sie im Einzelnen.

TrutzBox-Funktionen zeigt für jede zentrale Funktion, ob sie gerade läuft. Im Normalfall stehen alle auf *„In Ordnung"*:

- **Webfilter:** TrutzContent und TrutzBrowse, also der filternde und anonymisierende Proxy.
- **Filterlisten:** ob die Sperrlisten aktuell gehalten werden. Die Karte nennt zusätzlich, wann die Listen zuletzt aktualisiert wurden und welche Listen sich dabei verändert haben.
- **TrutzMail:** der verschlüsselte E-Mail-Dienst.
- **TrutzRTC:** Videokonferenz und Chat. Die Karte prüft zusätzlich die Videobrücke selbst.
- **VPN-Fernzugriff:** der sichere Zugang zur TrutzBox von unterwegs.
- **TrutzDynDNS:** sorgt dafür, dass die TrutzBox unter einem festen Namen von außen erreichbar ist.
- **Angriffsschutz:** überwacht die von außen erreichbaren Dienste und sperrt angreifende Internet-Adressen automatisch. Ein eigener Detail-Dialog zeigt die gesperrten Adressen mit Länderkennung und die betroffenen Angriffsziele.
- **Anonymität (Tor):** die Anbindung an das Tor-Netzwerk.
- **Eigener Name:** erscheint nur, wenn statt des TrutzDynDNS-Namens ein eigener Domain-Name eingerichtet ist (Kapitel „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden"). Sie zeigt, ob der Name auf den Anschluss der TrutzBox zeigt, wofür er verwendet wird und bis wann sein Zertifikat gilt. Gelb wird sie, wenn der Name länger auf eine andere Adresse zeigt oder sich nicht auflösen lässt. Dient der Name der Videokonferenz, wird sie außerdem gelb, kurz bevor das Zertifikat abläuft, und rot, sobald es abgelaufen ist.

Wie viel hinter einer einzelnen Karte stecken kann, zeigt das Beispiel **Filterlisten**: Aufgeklappt nennt sie den Speicherbedarf der Listen im Webfilter, Stand und Installationszeitpunkt der Listen, die Paketversion, die Zahl der blockierten Domains und der aktiven Filter, die Listen, die sich zuletzt geändert haben, und, falls vorhanden, die eigenen importierten Listen mit dem Ergebnis ihres letzten Abrufs. Über **Verlauf durchsuchen** lässt sich zu jeder Liste nachsehen, wann sie aktualisiert wurde, wie viele Einträge sie enthält und was sich gegenüber dem vorherigen Stand geändert hat.

Menüpfad: Systemeinstellungen → Betriebszustand



Abbildung 5-4: Die aufgeklappte Karte Filterlisten: Speicherbedarf im Webfilter, Stand, Paketversion und die Listen, die sich zuletzt geändert haben. (© 2026 Comidio GmbH)

Die Karte Software-Updates

Die TrutzBox sucht jede Nacht und bei jedem Start nach Software-Updates und spielt sie selbst ein (Kapitel „Updates“). Ob das klappt, zeigt die Karte **Software-Updates** unter Zustand der TrutzBox. Im Normalfall steht dort *„Letzter Update-Lauf abgeschlossen"*.

Menüpfad: Systemeinstellungen → Betriebszustand

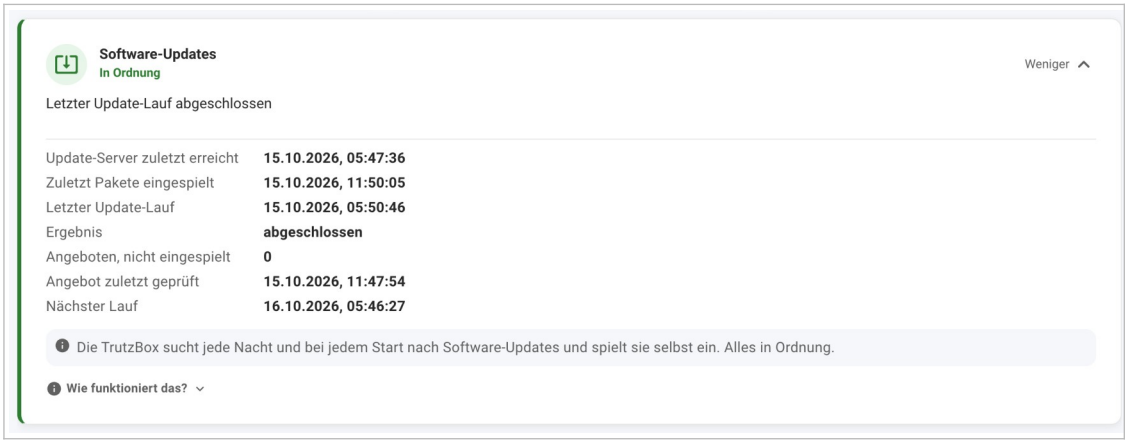


Abbildung 5-5: Die aufgeklappte Karte Software-Updates: letzter Lauf abgeschlossen, keine Pakete offen, der nächste Lauf am folgenden Morgen. (© 2026 Comidio GmbH)

Aufgeklappt nennt die Karte:

- **Update-Server zuletzt erreicht:** wann die TrutzBox zuletzt die Liste der angebotenen Pakete vom Update-Server geholt hat.
- **Zuletzt Pakete eingespielt:** wann die TrutzBox zuletzt Pakete installiert hat.
- **Letzter Update-Lauf** und **Ergebnis:** wann der letzte Lauf endete und wie, etwa „abgeschlossen" oder „mit Fehler beendet". Nach einem Fehler nennt die Karte darunter, soweit bekannt, den Grund und das Paket, bei dem der Lauf stehen blieb.

- **Angeboten, nicht eingespielt** und **Angebot zuletzt geprüft:** wie viele neuere Pakete der Update-Server anbietet, die noch nicht installiert sind, und wann die TrutzBox das zuletzt verglichen hat.
- **Nächster Lauf:** wann die TrutzBox das nächste Mal sucht.

Gelb und rot wird die Karte nur in diesen Fällen:

- **Gelb,** wenn ein Update-Lauf nicht fertig wurde (*„Letztes Software-Update nicht abgeschlossen"*) oder Pakete nur halb eingerichtet sind (*„Pakete nicht fertig eingerichtet"*).
- **Gelb nach 7 Tagen, rot nach 14 Tagen,** wenn der Update-Server neuere Pakete anbietet und die TrutzBox sie nicht eingespielt hat (*„Software-Updates seit … Tagen angeboten, nicht eingespielt"*), oder wenn sie den Update-Server so lange nicht erreicht hat (*„Update-Server seit … Tagen nicht erreicht"*). Gezählt wird nur die Zeit, in der die TrutzBox eingeschaltet ist.

Dass eine Woche lang kein Software-Update kommt, ist dagegen normal, solange der Update-Server keines anbietet; die Karte bleibt dann grün. Grün bleibt sie auch, während ein Lauf arbeitet (*„Software-Update läuft gerade"*) oder sich von selbst wiederholt (*„Software-Update wird wiederholt"*). Die Karte Software-Updates zählt zu den Karten, die die Ampel oben mitziehen: Wird sie rot, steht auch die Ampel auf Rot (Abschnitt „Betriebszustand: die Ampel lesen“). Was bei einer gelben oder roten Karte zu tun ist, steht in Abschnitt „Betriebszustand: Meldungen verstehen“.

Die Karte Systemgrenzen

Eine Karte fällt aus der Reihe, weil sie Dinge misst, die man sonst nirgends sieht. Manche Betriebsmittel einer TrutzBox sind begrenzt, ohne dass Prozessor oder Arbeitsspeicher etwas davon verraten: die Zahl gleichzeitig geöffneter Dateien, die Verbindungstabelle der Firewall, der Netzwerkspeicher des Systems, die Antwortzeit der SSD. Läuft eines davon langsam voll, wird die TrutzBox spürbar langsamer, während alle übrigen Anzeigen ruhig bleiben. Solche Fälle sind hinterher kaum aufzuklären, weil die Spuren beim nächsten Neustart verschwinden. Genau diese Lücke schließt die Karte **Systemgrenzen**.

Ein kleiner Hintergrund-Dienst misst alle fünf Minuten und immer nur dann, wenn die TrutzBox gerade nichts Wichtigeres zu tun hat; ausbremsen kann er sie deshalb nicht. Aufgeklappt zeigt die Karte jeden überwachten Wert samt seiner Warnschwelle, etwa *2 % (1443 von 65536), Warnung ab 80 %*. Überwacht werden unter anderem:

- **Dateien und Verbindungen:** wie viele Dateien die Dienste gleichzeitig geöffnet haben und wie voll die Verbindungstabelle der Firewall ist, also die Liste aller laufenden Verbindungen.
- **Netzwerk:** wie oft Daten ein zweites Mal gesendet werden müssen (Paket-Wiederholungen), ob der Zwischenspeicher für ankommende Daten überläuft (Empfangspuffer), Übertragungsfehler der Netzwerkanschlüsse und ein Anschluss, der nur noch langsam mit 10 Mbit/s arbeitet oder nicht mehr gleichzeitig senden und empfangen kann (Halbduplex).
- **SSD und Speicher:** die Antwortzeit der SSD und ob die TrutzBox ausgelagerte Daten laufend zurückholen muss.
- **Dienste:** wie schnell Webfilter und Web-Server reagieren und ob ein einzelner Prozessorkern dauerhaft voll ausgelastet ist.
- **Sonstiges:** zwei Geräte mit derselben IP-Adresse und Protokolldateien, die ungewöhnlich schnell wachsen.

Überschreitet ein Wert seine Schwelle, färbt sich die Karte gelb und benennt das Problem im Klartext, etwa *Zwei Geräte nutzen dieselbe IP-Adresse*; die auslösende Zeile ist farbig hervorgehoben, und der Vorgang erscheint zusätzlich im Ereignis-Protokoll. Damit ein einzelner Lastberg keinen Fehlalarm auslöst, muss der Wert zweimal nacheinander über der Schwelle liegen.

> **Was Sie mit einer gelben Systemgrenze tun**
>
> Im Alltag ist nichts zu tun: Die Karte meldet, sie schaltet nichts ab. Bleibt sie über Tage gelb oder wird die TrutzBox spürbar langsam, gehört ihr Text in den Support-Bericht (Kapitel „Was in den Support-Bericht gehört“). Bei einem Adress-Konflikt lohnt zuerst der Blick ins eigene Netz: Meist trägt ein Gerät eine feste Adresse, die der Router zusätzlich vergeben hat.

Die Karte Internet-Anschluss

Eine Karte sehen Sie im Normalfall überhaupt nicht: **Internet-Anschluss**. Sie taucht erst auf, wenn mit der Leitung zum Internet-Router etwas nicht stimmt, und bleibt ausgeblendet, solange alles läuft. So steht auf der Seite nicht dauernd eine Karte, die immer nur „in Ordnung" meldet.

Menüpfad: Systemeinstellungen → Betriebszustand

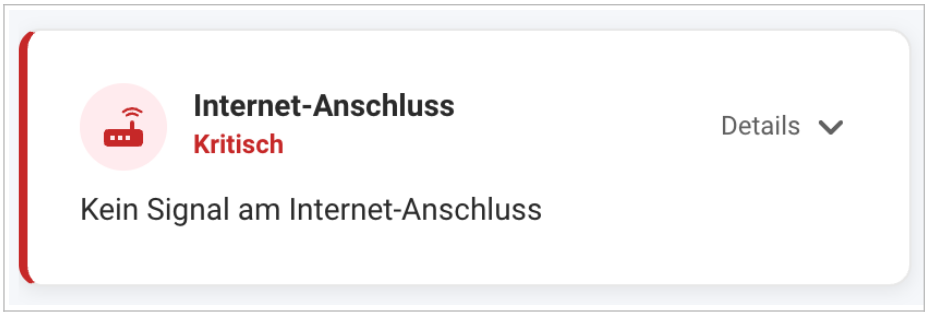


Abbildung 5-6: Die Karte erscheint erst im Störungsfall, hier mit gezogenem Netzwerkkabel. (© 2026 Comidio GmbH)

Aufgeklappt nennt sie den benutzten Anschluss der TrutzBox, die ausgehandelte Geschwindigkeit, die Adresse der TrutzBox und die des Routers, seit wann das Signal fehlt und wann das Internet zuletzt erreichbar war. Das genügt meist schon zur Einordnung: Fehlt das Signal, liegt es am Kabel oder am Router; ist die Adresse da, aber das Internet nicht erreichbar, liegt es hinter dem Router.

Nützlich ist außerdem, was die TrutzBox dabei mit den übrigen Karten macht. Ohne Internet melden auch Uhrzeit, TrutzDynDNS, Fernzugriff, Filterlisten, Mail und Videokonferenz Probleme. Damit Sie nicht sechs Fehlern nachlaufen, kennzeichnet die TrutzBox diese Karten als Folge des fehlenden Anschlusses. Zu tun ist dann nur eines: die Leitung zum Router prüfen (Kapitel „… kein Internet da ist“).

Die Karte DNS für Geräte

Die zweite Karte, die sich nur bei einer Störung zeigt, heißt **DNS für Geräte**. Sie prüft die Namensauflösung, also das Übersetzen eines Namens wie trutzbox.de in eine Internet-Adresse (Kapitel „DNS-Schutz und verschlüsselte Namensauflösung“). Die TrutzBox löst dazu einen Testnamen auf zwei Wegen auf: über ihre Adresse im internen Netz, so wie Ihre Geräte fragen, und über sich selbst, so wie sie für Software-Updates und Mail fragt. Solange beide Wege antworten und die Verschlüsselung zum DNS-Anbieter steht, bleibt die Karte ausgeblendet. Bei einer kurzen

Unterbrechung erscheint sie grün mit einem Hinweis (Abschnitt „Betriebszustand: Meldungen verstehen“).

Gebaut ist sie für einen Fall, der sonst kaum auffällt: Ihre Geräte kommen nicht mehr ins Internet, die Ampel steht aber auf Grün, weil die TrutzBox selbst weiter Namen auflöst. Typisch dafür ist, dass Webseiten nicht laden, während Programme, die direkt mit Internet-Adressen arbeiten, etwa manche Messenger oder ein VPN, weiterlaufen. Genau dann erscheint die Karte rot.

Meldung	Was sie bedeutet	Was Sie tun
Geräte im LAN bekommen keine Namensauflösung (rot)	Die Geräte hinter der TrutzBox bekommen keine Namen aufgelöst, die TrutzBox selbst schon. Für die Geräte ist das Internet damit weg.	Unter Netzwerk → Netzwerkdienste, Reiter DNS, die verschlüsselte Weiterleitung aus- und wieder einschalten. Bleibt es dabei, den Support-Bericht senden.
Die TrutzBox selbst löst keine Namen auf (gelb)	Die Geräte haben Internet, aber Software-Updates, TrutzDynDNS und der Mailversand der TrutzBox scheitern.	Wie oben: die verschlüsselte Weiterleitung aus- und wieder einschalten.
Keine Namensauflösung, weder für Geräte noch für die TrutzBox (rot)	Meist fehlt der Internet-Anschluss, oder der Router antwortet nicht.	Zuerst die Leitung zum Router prüfen (Kapitel „… kein Internet da ist“).
Verschlüsselung zum DNS-Anbieter nicht möglich, Auflösung unverschlüsselt (gelb)	Die TrutzBox erreicht ihren DNS-Anbieter seit über einer Stunde nicht verschlüsselt, oft weil der Router den dafür nötigen Port 853 sperrt. Damit alles weiterläuft, löst sie so lange unverschlüsselt auf und versucht es alle 30 Minuten erneut. Filter und Sperren arbeiten unverändert.	Port 853 im Router freigeben. Ist das nicht möglich, auf dem Reiter DNS die verschlüsselte Weiterleitung ausschalten oder einen anderen Anbieter wählen.

5.4 Betriebszustand: Verlauf und Ereignis-Protokoll

Unterhalb der Karten liegen zwei Ansichten, die nicht den Augenblick, sondern die Vergangenheit zeigen. Sie beantworten die Frage, die bei jeder Störung als Erstes aufkommt: Ist das neu, oder besteht das schon länger?

Der Verlauf der letzten 30 Tage ist eine Zeile mit einem Feld pro Tag. Die Farbe steht für den Tagesstatus: grün für *„In Ordnung"*, gelb für *„Auffällig"* und rot für *„Kritisch"*. Ein Klick auf einen Tag zeigt, was an diesem Tag passiert ist. Jede Tageskarte nennt unter **Aufgetreten** den Zeitraum der Störung, also die erste und die letzte Sichtung, und listet unter **Ereignisse an diesem Tag** die Vorkommnisse und Neustarts auf.

Das Ereignis-Protokoll filtert aus den technischen Systemprotokollen genau die Einträge heraus, die für die Gesundheit der TrutzBox wichtig sind, und übersetzt sie in verständliche Sprache. Die Liste lässt sich durchsuchen und nach Kategorie und Wichtigkeit filtern. Das ist der richtige Ort,

wenn Sie einer einmaligen Auffälligkeit nachgehen möchten, ohne sich mit Systemprotokollen zu befassen.

Die Prüfung selbst kostet die TrutzBox übrigens keine spürbare Leistung; Sie können die Seite so oft öffnen, wie Sie möchten.

Menüpfad: Systemeinstellungen → Betriebszustand → Verlauf

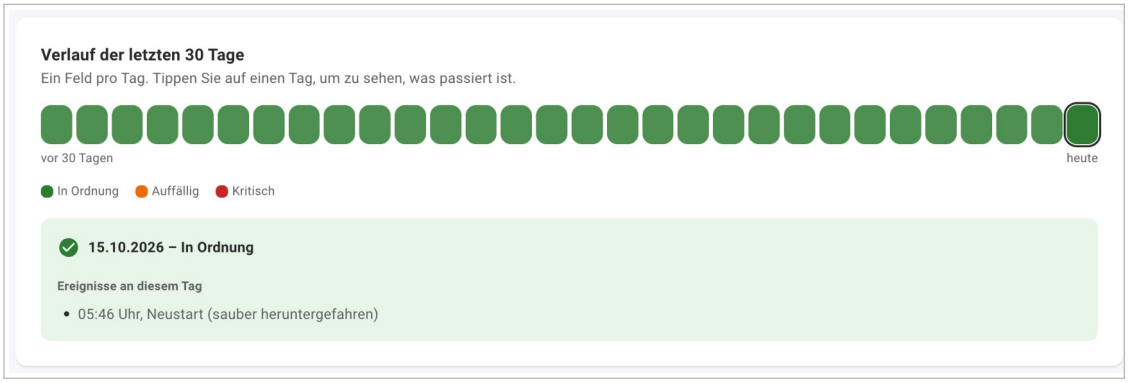


Abbildung 5-7: Der Verlauf der letzten 30 Tage: ein Feld pro Tag, die Farbe zeigt den Tageszustand. Aufgeklappt ist der heutige Tag mit einem Neustart unter „Ereignisse an diesem Tag". (© 2026 Comidio GmbH)

5.5 Betriebszustand: Meldungen verstehen

Ein paar Meldungen begegnen Ihnen früher oder später, ohne dass etwas kaputt ist:

- *„Neuere Filterlisten stehen bereit, sind aber nicht installiert"* (gelb): Die nächtliche Installation hat noch nicht stattgefunden oder wurde verpasst. Löst sich in der Regel in der folgenden Nacht von selbst.
- *„Software-Update läuft gerade"* bei der Karte Software-Updates (grün): Die TrutzBox spielt gerade Software-Updates ein. Bei einer neuen TrutzBox oder nach längerer Pause kann das eine halbe Stunde dauern.
- Karten mit dem Zustand *„Läuft, aber gestört"* nennen immer eine konkrete Empfehlung. Erst wenn die nicht hilft, ist der Support dran (Kapitel „Support kontaktieren“).

Die folgenden Fälle lohnen eine etwas genauere Erklärung, weil sie am häufigsten vorkommen:

Meldung	Was dahintersteckt	Was zu tun ist
Filterlisten veraltet (gelb)	Der Update-Server bietet neuere Filterlisten an, die die TrutzBox seit über zwei Tagen nicht übernommen hat. Die Karte nennt dazu die verfügbare Version und seit wann die TrutzBox zurückliegt. Gefiltert wird unverändert weiter, nur eben mit dem älteren Stand.	Abwarten. Die Übernahme läuft nächtlich. Bleibt die Meldung mehrere Tage stehen, prüfen Sie die Internet-Verbindung und wenden sich dann an den Support.
Verschlüsselung kurz unterbrochen, Auflösung solange unverschlüsselt (Karte DNS für Geräte, grün)	Die TrutzBox erreicht ihren DNS-Anbieter gerade nicht verschlüsselt, etwa weil er kurz nicht antwortet. Damit die Geräte Internet haben, löst sie so lange unverschlüsselt auf. Filter und Sperren arbeiten unverändert. Sie versucht es alle 5 Minuten erneut und schaltet	Nichts. Hält es länger als eine Stunde an, wird die Karte gelb. Dann Port 853 im Router freigeben oder einen anderen Anbieter wählen (Abschnitt

Meldung	Was dahintersteckt	Was zu tun ist
	von selbst zurück, meist nach wenigen Minuten.	„Betriebszustand: die Karten im Einzelnen“).
TrutzRTC gestört	Alle Dienste laufen, aber die Videobrücke antwortet nicht. Videokonferenzen kommen dann nicht zustande, obwohl äußerlich alles zu laufen scheint.	Der Empfehlung der Karte folgen und TrutzRTC einmal aus- und wieder einschalten.
Speicher-Wächter hat eingegriffen	Der Arbeitsspeicher wurde knapp. Um ein Einfrieren zu verhindern, hält die TrutzBox gezielt zuerst TrutzRTC und danach TrutzMail an. Der Webfilter und damit der Schutz bleiben davon unberührt.	Nichts. Ist wieder genug Speicher frei, startet der Wächter den Dienst von selbst neu, höchstens einmal am Tag. Tritt das wiederholt auf, nennt die Karte, was hilft; sonst ist der Support die richtige Adresse.
Software-Updates seit … Tagen angeboten, nicht eingespielt (gelb, nach 14 Tagen rot)	Der Update-Server bietet neuere Pakete an, die TrutzBox hat sie seit über einer Woche nicht eingespielt. Gezählt wird nur die Zeit, in der sie eingeschaltet ist. Sie versucht es jede Nacht und bei jedem Neustart von selbst erneut. Die aufgeklappte Karte nennt die betroffenen Pakete.	Abwarten. Bleibt die Karte gelb oder wird sie rot, den Support-Bericht senden (Kapitel „Was in den Support-Bericht gehört“).
Letztes Software-Update nicht abgeschlossen (gelb)	Der letzte Update-Lauf wurde nicht fertig. Den Grund nennt die aufgeklappte Karte, etwa „Update-Server nicht erreichbar" oder „kein Speicherplatz mehr frei". Dasselbe gilt für „Pakete nicht fertig eingerichtet": Ein Lauf wurde unterbrochen. Die TrutzBox holt das in der kommenden Nacht oder nach einem Neustart von selbst nach.	Abwarten. Bleibt die Karte länger als zwei Tage gelb, den Support-Bericht senden.
Update-Server seit … Tagen nicht erreicht (gelb, nach 14 Tagen rot)	Die TrutzBox hat den Update-Server seit über einer Woche nicht erreicht, gezählt in eingeschalteter Zeit. Sie bekommt dann auch keine Software-Updates.	Prüfen, ob die TrutzBox mit dem Internet verbunden ist und ob ihre Uhrzeit stimmt (Karte Zeitsynchronisation). Bleibt die Karte gelb oder wird sie rot, den Support-Bericht senden.

Grundsätzlich gilt: Die Ampel meldet nur echte Zustände. Sie wird nicht gelb, weil eine Funktion nicht genutzt wird, und nicht rot, weil etwas ungewöhnlich aussieht. Ein grünes Gesamtbild heißt, Sie können die Seite beruhigt wieder schließen; die TrutzBox ist für den unbeaufsichtigten Dauerbetrieb gebaut.

6 Geräte verwalten

Auf der Seite **Verwaltung → Geräte** führt die TrutzBox Buch über alle Geräte, die über sie ins Internet gehen. Hier geben Sie Geräten Namen, ordnen Filtergruppen zu und steuern je Gerät, was es darf.

Diese Seite ist die Schaltzentrale des Alltags. Alles, was die TrutzBox später filtert, anonymisiert oder sperrt, hängt daran, welchem Gerät welche Einstellung zugewiesen ist. Wer sich einmal eine halbe Stunde Zeit nimmt, allen Geräten verständliche Namen und die passende Filtergruppe zu geben, spart sich diese Arbeit dauerhaft und kann danach jede Auswertung im Monitor ohne Nachdenken lesen.

6.1 Neue Geräte erscheinen automatisch

Menüpfad: Verwaltung → Geräte

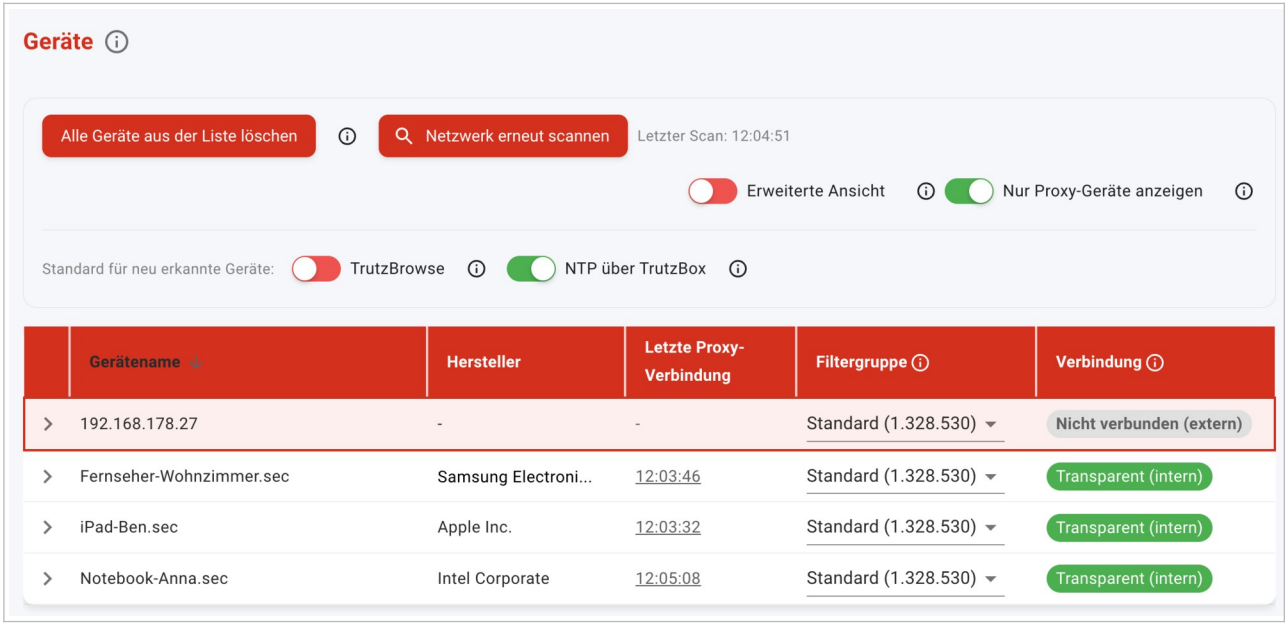


Abbildung 6-1: Die Geräte-Seite: oben Schaltflächen, Schalter und die Vorgaben für neu erkannte Geräte, darunter die Liste. Rot umrandet ist das Gerät, an dem man gerade sitzt, hier ein PC im lokalen Netz des Routers. (© 2026 Comidio GmbH)

Sobald ein Gerät zum ersten Mal Verkehr durch die TrutzBox schickt, taucht es in der Liste auf. Erkannt wird es an seiner Hardware-Adresse (MAC-Adresse), die jedes Netzwerkgerät eindeutig trägt; damit bleibt die Zuordnung auch bestehen, wenn sich die IP-Adresse einmal ändert. Lässt sich die Hardware-Adresse nicht ermitteln, greift die TrutzBox ersatzweise auf den Hostnamen oder die IP-Adresse zurück. Neue Geräte landen automatisch in der mitgelieferten Filtergruppe **Standard**.

Sie müssen also nichts anmelden und nichts eintragen. Beim Öffnen der Seite durchsucht die TrutzBox das Netz ohnehin automatisch; wann das zuletzt geschah, steht neben der Leiste. Mit **Netzwerk erneut scannen** stoßen Sie die Suche sofort an, ohne dass gespeicherte Einstellungen verloren gehen. Ein Gerät, das gerade ausgeschaltet ist, erscheint dabei als nicht verbunden, bleibt aber mit allen Einstellungen in der Liste.

In der Leiste über der Liste sitzen außerdem zwei Schalter. **Erweiterte Ansicht** blendet zu jedem Gerät zusätzlich die IP-Adresse und die Hardware-Adresse (MAC) ein. Das ist die schnellste Hilfe,

wenn ein Eintrag sich nicht zuordnen lässt: Die Hardware-Adresse steht bei vielen Geräten auf dem Typenschild oder in den Geräteeinstellungen, und ein Vergleich schafft sofort Gewissheit (Abschnitt „Unbekannte Geräte erkennen“). **Nur Proxy-Geräte anzeigen** ist in Abschnitt „Die Spalten der Geräteliste“ erklärt. Das Gerät, an dem Sie gerade sitzen, ist rot umrandet und steht ganz oben, bis Sie die Liste selbst nach einer Spalte sortieren. Die Schaltfläche **Alle Geräte aus der Liste löschen** löscht die gespeicherten Einstellungen aller Geräte: Namen, Filtergruppe, TrutzBrowse und Ausnahmen. Geräte, die die TrutzBox im Netz selbst erkennt, bleiben in der Liste sichtbar; beim nächsten Datenverkehr erhalten sie die Vorgaben für neu erkannte Geräte (Abschnitt „Aufräumen: alte Einträge entfernen“). Für einzelne Karteileichen ist das Löschen im jeweiligen Gerät der bessere Weg.

Über der Liste steht die Zeile **Standard für neu erkannte Geräte:** mit zwei Schaltern, die auf jedes künftig neu erkannte Gerät wirken. **TrutzBrowse** legt fest, ob die Anonymisierung für neue Geräte gleich eingeschaltet wird; ab Werk ist dieser Schalter aus. In öffentlich zugänglichen Umgebungen, in denen sich auf den Endgeräten kein Root-Zertifikat installieren lässt, sollte er auch ausgeschaltet bleiben. **NTP über TrutzBox** legt fest, ob neue Geräte ihre Uhrzeit von der TrutzBox statt von fremden Zeitservern beziehen; dieser Schalter ist ab Werk eingeschaltet. Beide wirken ausschließlich auf künftige Geräte; bereits eingerichtete bleiben unverändert.

> **Für Neugierige: Was eine Hardware-Adresse ist**
>
> Jede Netzwerkschnittstelle bekommt vom Hersteller eine weltweit einmalige Kennung, die MAC-Adresse. Sie ändert sich nicht, wenn ein Gerät eine neue IP-Adresse bekommt, und eignet sich deshalb gut zur Wiedererkennung. Neuere Smartphones erzeugen aus Datenschutzgründen für fremde Netze allerdings zufällige Adressen. Die TrutzBox weist in einem solchen Fall darauf hin, dass sich der Hersteller nicht eindeutig zuordnen lässt.

6.2 Geräte benennen

Frisch erkannte Geräte heißen oft kryptisch. Vergeben Sie deshalb gleich sprechende Namen wie „Annas MacBook" oder „Wohnzimmer-TV": Ein Klick auf den Namen genügt zum Umbenennen. Die Namen tauchen überall wieder auf, im Monitor, in den Statistiken und im Betriebszustand, und machen alle Auswertungen erst lesbar.

Der hier vergebene Name gilt nur innerhalb der TrutzBox. Der tatsächliche Netzwerkname des Geräts bleibt unverändert, Sie ändern also nichts am Gerät selbst. Solange kein eigener Name vergeben ist, zeigt die TrutzBox in dieser Reihenfolge an, was sie ermitteln konnte: zuerst den Hostnamen, dann den Hersteller, zuletzt die IP-Adresse. Genau deshalb stehen in einer frisch eingerichteten Liste oft Einträge, die aus einer Zeichenfolge oder einer bloßen Zahlenadresse bestehen.

Ein paar Empfehlungen aus der Praxis, wie Namen im Alltag am besten funktionieren:

- Nennen Sie Person und Gerät gemeinsam, etwa „Tim Tablet" statt nur „Tablet". In einer Familie gibt es selten nur ein Tablet.
- Nennen Sie bei fest installierten Geräten den Raum, etwa „Küche Radio" oder „Keller Kamera". So finden Sie das Gerät später auch körperlich wieder.

- Vermerken Sie bei Geräten, die per Kabel und per Funk erscheinen, die Anschlussart mit, etwa „Laptop (Kabel)" und „Laptop (WLAN)".
- Vergeben Sie den Namen sofort. Nach zwei Wochen weiß niemand mehr, welches der drei namenlosen Geräte das Thermostat war.

6.3 Filtergruppen zuordnen

In der Spalte **Filtergruppe** wählen Sie je Gerät die passende Gruppe aus, zum Beispiel eine Altersgruppe für die Geräte der Kinder oder eine eigene Gruppe „TV" für den Fernseher. Was die Gruppen bedeuten und wie Sie eigene anlegen, beschreibt Kapitel „Webfilter und Jugendschutz (TrutzContent)“. Dazu gibt es je Gerät die Felder **Diese Ausnahmen zulassen** (eine Whitelist, die trotz Filtergruppe immer erreichbar ist) und **Nur Ausnahmen erlauben** (das Gerät darf ausschließlich die Adressen einer Whitelist erreichen, die strengste Einstellung für Haustechnik).

Die Zuordnung lässt sich direkt in der Liste über das Auswahlfeld ändern und wirkt sofort. Sie brauchen das Gerät dafür nicht neu zu starten und müssen dort auch nichts einstellen. Das ist der eigentliche Vorzug dieser Lösung: Die Regel liegt in der TrutzBox, nicht auf dem Gerät, und lässt sich am Gerät nicht abschalten.

Eine bewährte Aufteilung für den Anfang:

Gerät	Sinnvolle Zuordnung
Arbeits-PC, Notebook der Erwachsenen	Die mitgelieferte Gruppe „Standard". Sie sperrt unerwünschten Datenverkehr wie Werbung, die Aufzeichnung dessen, was man im Netz tut, Spionage-Software und Kostenfallen, lässt aber sonst alles zu.
Tablet oder Smartphone eines Kindes	Eine eigene, strengere Gruppe passend zum Alter. Bei Bedarf ergänzt um eine Whitelist für Schulseiten.
Fernseher, Streaming-Gerät	Eine eigene Gruppe, die die Datensammelei des Herstellers eindämmt, ohne die eigentliche Nutzung zu stören.
Kamera, Thermostat, Haustechnik	Wenn möglich „Nur Ausnahmen erlauben" mit einer kurzen Liste der Adressen, die das Gerät zum Funktionieren wirklich braucht.
Gäste-Gerät	Die Gruppe „Standard" oder, wenn es strenger sein soll, „Konservativ", die zusätzlich etwa Glücksspiel, Gewalt und Pornografie sperrt. Details in Abschnitt „Gäste und gemeinsam genutzte Geräte“.

6.4 Die Spalten der Geräteliste

Die Liste zeigt je Gerät mehrere Spalten. Sie beantworten zusammen die Frage, wer da eigentlich mit welchen Rechten im Netz unterwegs ist:

Spalte	Bedeutung
Gerätename	Der von Ihnen vergebene Name. Ohne eigenen Namen zeigt die TrutzBox Hostname, Hersteller oder IP-Adresse, in dieser Reihenfolge.
Hersteller	Der aus der Hardware-Adresse ermittelte Gerätehersteller. Bei zufällig

Spalte	Bedeutung
	vergebenen Adressen weist die TrutzBox darauf hin, dass keine eindeutige Zuordnung möglich ist.
Letzte Proxy-Verbindung	Wann das Gerät zuletzt über die TrutzBox im Internet war. Sind Verbindungsdaten gespeichert, führt hier ein Link direkt in die Monitor-Liste dieses Geräts.
Filtergruppe	Die zugewiesene Filtergruppe. Über das Auswahlfeld direkt in der Liste änderbar.
Verbindung	Wie das Gerät angebunden ist. „Transparent": Das Gerät hängt per Kabel, WLAN oder VPN im Netz der TrutzBox, sein Verkehr wird ohne Einstellung am Gerät gefiltert. „Proxy": Das Gerät nutzt die TrutzBox ausdrücklich als Proxy, meist über den äußeren Anschluss LAN-Ext. In Klammern steht, über welches Netz das Gerät gerade verbunden ist: intern, WLAN, VPN oder extern, etwa „Transparent (intern)" oder „Proxy (extern)". „Nicht verbunden (extern)": Das Gerät ist am äußeren Anschluss sichtbar, hat aber noch keinen Verkehr über den Proxy geschickt; „Proxy" erscheint erst nach dem ersten Seitenaufruf über den Proxy. „Nicht verbunden" ohne Klammer: ein bekanntes Gerät, das gerade nicht im Netz ist.

Über der Liste sitzt außerdem der Schalter **Nur Proxy-Geräte anzeigen**. Er ist im Auslieferungszustand eingeschaltet und zeigt dann alle Geräte, deren Verkehr über den Proxy der TrutzBox läuft. Das sind sowohl die als Proxy-Client eingerichteten Geräte als auch die intern angeschlossenen Geräte an Kabel, WLAN und VPN, deren Verkehr transparent auf den Proxy umgeleitet wird. Heraus fallen dabei nur Geräte im äußeren Netz, die den Proxy nicht benutzen. Ein Gerät, das direkt an der TrutzBox hängt, verschwindet durch diesen Schalter also nicht; wer alle im Netz gesehenen Geräte sehen möchte, schaltet ihn aus.

6.5 Unbekannte Geräte erkennen

In fast jedem Netz taucht früher oder später ein Eintrag auf, den niemand zuordnen kann. Das ist normal und selten ein Grund zur Sorge: Viele Geräte melden sich mit einer Bezeichnung, die auf der Verpackung nirgends steht. Mit den folgenden Schritten lässt sich die Frage meist in wenigen Minuten klären.

1. Sehen Sie in der Spalte **Hersteller** nach. Sie ist der beste erste Hinweis, denn sie stammt aus der Hardware-Adresse. Ein bekannter Elektronikhersteller schränkt die Auswahl oft schon auf ein oder zwei Geräte im Haushalt ein.
2. Schalten Sie die **Erweiterte Ansicht** ein. Sie zeigt zu jedem Gerät IP- und Hardware-Adresse. Die Hardware-Adresse findet sich bei vielen Geräten auf dem Typenschild, in den Einstellungen des Geräts oder in der Geräteliste des Routers; stimmt sie überein, ist der Fall geklärt.
3. Öffnen Sie über die Spalte **Letzte Proxy-Verbindung** die Monitor-Liste dieses Geräts. Woran ein Gerät sich wendet, verrät fast immer, was es ist: ein Streaming-Dienst deutet auf

den Fernseher, ein Hersteller von Haustechnik auf ein Thermostat, ein Kartendienst auf ein Smartphone.

4. Achten Sie auf die Uhrzeiten. Ein Gerät, das nur abends aktiv wird, steht im Wohnzimmer. Ein Gerät, das im Minutentakt eine einzige Adresse kontaktiert, ist Haustechnik.
5. Wenn das nicht reicht: Trennen Sie das verdächtige Gerät kurz vom Strom oder schalten Sie das WLAN am Smartphone aus und sehen Sie nach, welcher Eintrag daraufhin als nicht verbunden erscheint. Das ist die zuverlässigste Methode.

Ist ein Gerät identifiziert, geben Sie ihm sofort einen Namen. Bleibt ein Eintrag auch nach diesen Schritten unerklärlich, können Sie ihm über die Detail-Einstellungen den **Internetzugang** entziehen und abwarten, wer sich beschwert. Die Sperre wirkt sofort und kappt auch laufende Verbindungen, lässt sich aber genauso schnell wieder aufheben. Bei einem Eintrag ohne Hardware-Adresse, der auch kein Proxy-Gerät ist, etwa einer bloßen IPv6-Adresse, fehlt dieser Schalter: Die TrutzBox sperrt nach Hardware-Adresse oder nach dem Namen eines Proxy-Geräts und kann einen solchen Eintrag nicht gezielt sperren.

> **Ein unbekanntes Gerät ist kein Alarm**
>
> Ein Eintrag, den Sie nicht zuordnen können, bedeutet nicht, dass jemand in Ihrem Netz ist. Weit häufiger handelt es sich um ein längst vergessenes eigenes Gerät oder um eine zweite Schnittstelle eines bekannten Geräts. Gehen Sie der Sache in Ruhe nach, bevor Sie Einstellungen ändern.

6.6 Gäste und gemeinsam genutzte Geräte

Besuch bringt eigene Geräte mit. Sobald ein Gast sich mit dem TrutzBox-WLAN verbindet oder ein Kabel einsteckt, erscheint sein Gerät in der Liste und landet in der mitgelieferten Filtergruppe **Standard**. Es ist damit vom ersten Augenblick an geschützt, ohne dass jemand etwas einstellen müsste. Das ist der übliche und in den meisten Fällen völlig ausreichende Weg.

Wenn Sie mehr Kontrolle möchten: Der Schalter **Internetzugang** in den Detail-Einstellungen bestimmt, ob dieses Gerät überhaupt ins Internet darf. Im Auslieferungszustand steht er auf „Erlaubt". Wird der Zugang entzogen, sperrt die TrutzBox das Gerät unmittelbar an der Firewall und trennt auch bereits laufende Verbindungen sofort. Die Sperre wirkt also nicht erst beim nächsten Verbindungsversuch und greift auch dann, wenn das Gerät den Proxy gar nicht benutzt. Den Schalter gibt es nur bei Einträgen mit Hardware-Adresse und bei Proxy-Geräten (Abschnitt „Unbekannte Geräte erkennen“).

Für längere Aufenthalte lohnt es sich, dem Gast-Gerät einen erkennbaren Namen zu geben, etwa „Besuch Laptop Mai". Danach ist beim Aufräumen sofort klar, welche Einträge weg können. Von allein verschwindet ein benanntes Gerät nämlich nicht: Automatisch entfernt die TrutzBox nur Einträge, zu denen weder eine Hardware-Adresse noch ein Hostname bekannt ist (Abschnitt „Aufräumen: alte Einträge entfernen“).

6.7 Weitere Einstellungen je Gerät

Ein Klick auf den Pfeil links vor dem Gerätenamen klappt die Detail-Einstellungen auf. Sie sind auf zwei Reiter verteilt: **Proxy** für Filterung und Anonymisierung, **Netzwerk** für Anschluss und

Zugang. Bei reinen Netzwerkgeräten, die den Proxy nicht nutzen, ist nur der Reiter Netzwerk gefüllt; die Oberfläche weist darauf hin.

Menüpfad: Verwaltung → Geräte → Gerät aufklappen → Proxy

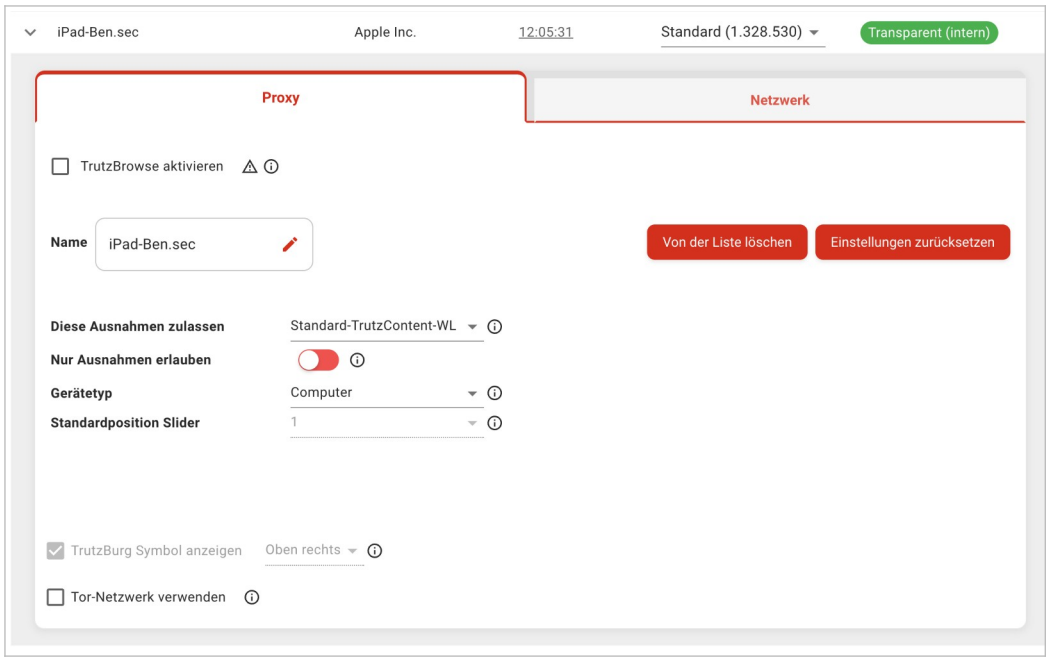


Abbildung 6-2: Der Reiter Proxy: TrutzBrowse, Ausnahmelisten, Gerätetyp und die TrutzBurg, dazu Löschen und Zurücksetzen. (© 2026 Comidio GmbH)

Auf dem Reiter **Proxy** finden Sie:

- **TrutzBrowse aktivieren:** schaltet die Anonymisierung für dieses Gerät ein; die **Standardposition Slider** daneben legt die Grundeinstellung des Security-Sliders fest (Kapitel „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“). Für Geräte ohne installierbares Zertifikat bleibt der Schalter aus.
- **Name:** der von Ihnen vergebene Gerätename (Abschnitt „Geräte benennen“).
- **Diese Ausnahmen zulassen** und **Nur Ausnahmen erlauben**: die beiden Whitelist-Einstellungen aus Abschnitt „Filtergruppen zuordnen“. Achten Sie bei **Nur Ausnahmen erlauben** vor allem auf eines: Ist der Schalter an, ohne dass eine Ausnahmeliste ausgewählt wurde, erreicht das Gerät gar nichts mehr. Wählen Sie deshalb immer zuerst die Whitelist aus und schalten Sie erst danach um.
- **Gerätetyp:** legt fest, ob es sich um ein Computer-, ein Android- oder ein iOS-Gerät handelt. Damit teilt die TrutzBox dem Server mit, für welche Geräteart eine Webseite aufbereitet werden soll, ohne mehr über das Gerät zu verraten als nötig.
- **TrutzBurg Symbol anzeigen:** blendet in aufgerufenen Seiten das TrutzBurg-Icon ein, über das sich der Security-Slider direkt im Browser verstellen lässt; daneben wählen Sie die Bildschirmecke (Kapitel „Das TrutzBurg-Menü im Browser“).
- **Tor-Netzwerk verwenden:** leitet den Verkehr dieses Geräts zusätzlich über das Tor-Netzwerk. Das verbirgt die Herkunft noch gründlicher, macht das Surfen aber deutlich langsamer; genau danach fragt Kapitel „… eine Seite sehr langsam lädt“, wenn eine Seite auffällig zäh lädt.

- **Von der Liste löschen** und **Einstellungen zurücksetzen**: entfernt den Eintrag beziehungsweise setzt alle Einstellungen genau dieses Geräts auf die Ausgangswerte zurück, ohne andere Geräte zu berühren.

Menüpfad: Verwaltung → Geräte → Gerät aufklappen → Netzwerk

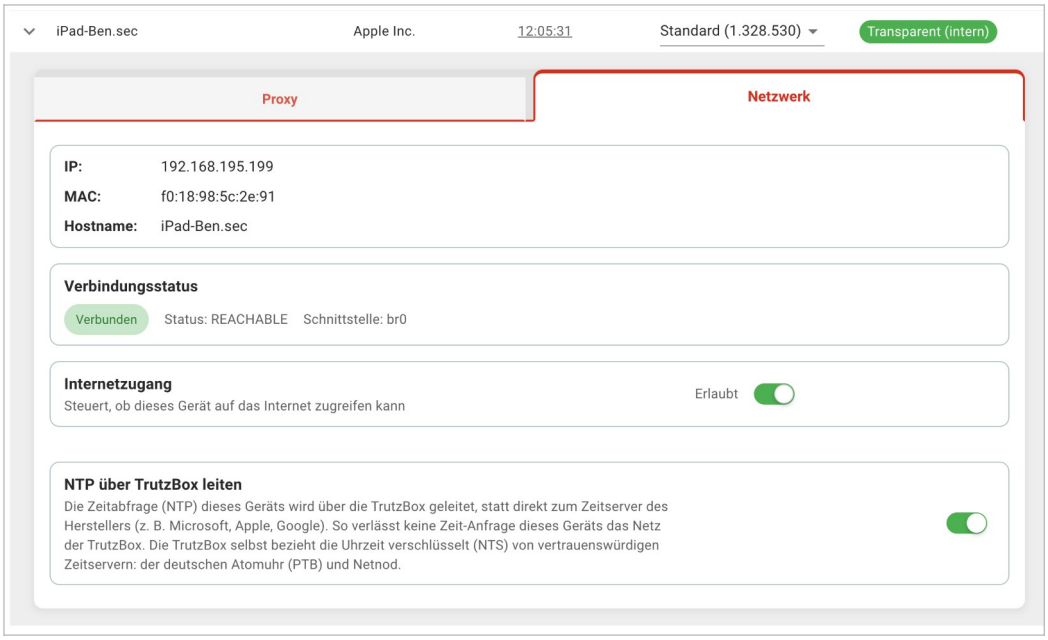


Abbildung 6-3: Der Reiter Netzwerk: Adressen, Verbindungsstatus, Internetzugang und die NTP-Umleitung. (© 2026 Comidio GmbH)

Auf dem Reiter **Netzwerk** stehen die technischen Kennungen des Geräts (IP- und Hardware-Adresse) und der aktuelle **Verbindungsstatus** mit der benutzten Schnittstelle. Dazu kommen zwei Schalter:

- **Internetzugang:** steuert, ob das Gerät überhaupt ins Internet darf (siehe Abschnitt „Gäste und gemeinsam genutzte Geräte“).
- **NTP über TrutzBox leiten:** lässt das Gerät seine Uhrzeit von der TrutzBox beziehen statt direkt vom Zeitserver seines Herstellers. So verlässt keine Zeitabfrage mit Gerätekennung mehr Ihr Netz. Die TrutzBox selbst holt sich die Uhrzeit verschlüsselt von vertrauenswürdigen Quellen, darunter die deutsche Atomuhr der Physikalisch-Technischen Bundesanstalt. Ab Werk ist der Schalter eingeschaltet.

Der Weg von der Geräteliste in den Monitor ist die am häufigsten gebrauchte Verbindung zwischen zwei Seiten der Oberfläche. Er beantwortet die Frage „Was macht dieses Gerät eigentlich?" ohne Umweg: Ein Klick auf die letzte Verbindungszeit öffnet die Liste aller Verbindungen genau dieses Geräts, mit Zielserver, Zeitpunkt und der Angabe, ob die Verbindung durchgelassen oder blockiert wurde. Besonders aufschlussreich ist dieser Blick bei Fernsehern, Lautsprechern und Haustechnik.

6.8 Aufräumen: alte Einträge entfernen

Nach einigen Monaten sammeln sich Einträge an, die niemand mehr braucht: das Gerät eines Besuchs, ein verkauftes Smartphone, ein zweiter Eintrag für dieselbe Person. Die Liste bleibt dadurch nicht falsch, aber unübersichtlich.

Zum Aufräumen gibt es drei Wege, vom schonendsten zum gründlichsten:

- **Von der Liste löschen:** entfernt genau ein Gerät aus der Liste. Meldet es sich später doch wieder, wird es beim nächsten Verbinden automatisch neu erkannt und landet wieder in der mitgelieferten Filtergruppe **Standard**.
- **Einstellungen zurücksetzen:** behält den Eintrag, setzt aber seine Proxy-Einstellungen auf die Ausgangswerte zurück. Sinnvoll, wenn an einem Gerät zu viel ausprobiert wurde.
- **Alle Geräte aus der Liste löschen:** löscht die gespeicherten Einstellungen aller Geräte: Namen, Filtergruppe, TrutzBrowse und Ausnahmen. Geräte, die die TrutzBox im Netz selbst erkennt, bleiben in der Liste sichtbar; die TrutzBox liest sie anschließend neu ein. Beim nächsten Datenverkehr erhalten sie die Vorgaben für neu erkannte Geräte.

Was „Alle Geräte löschen" wirklich entfernt

Der Dialog spricht von proxy-konfigurierten Geräten. Gemeint sind alle Geräte, zu denen die TrutzBox Einstellungen gespeichert hat, und das sind fast alle: jedes Gerät, das schon einmal über den Proxy der TrutzBox eine Webseite aufgerufen hat, und jedes, dem Sie einen Namen gegeben haben. Deren Namen, Filtergruppen-Zuordnungen und Proxy-Einstellungen sind danach weg und müssen neu vergeben werden. Aus der Liste verschwinden nur Geräte, die die TrutzBox im Netz gerade nicht sieht. Nutzen Sie die Schaltfläche deshalb nur, wenn Sie die Proxy-Einrichtung wirklich von vorn beginnen möchten, und löschen Sie im Zweifel lieber einzelne Einträge.

Karteileichen aufräumen

Geräte, die lange nicht mehr aufgetaucht sind, dürfen Sie gefahrlos löschen. Meldet sich ein Gerät doch wieder, erscheint es einfach neu in der Filtergruppe „Standard".

Ein wenig hilft die TrutzBox dabei von selbst, allerdings nur sehr zurückhaltend: Automatisch entfernt sie ausschließlich Einträge, zu denen weder eine Hardware-Adresse noch ein Hostname bekannt ist, also reine Zahlenadressen ohne jede weitere Angabe. Dieser Lauf findet beim Öffnen der Geräte-Seite statt, nicht als Dienst im Hintergrund. Alles andere, benannte Geräte eingeschlossen, bleibt so lange stehen, bis Sie es selbst löschen.

Häufige Fragen zu Geräten

Ein Gerät taucht nicht in der Liste auf. Warum?

Dann läuft sein Verkehr nicht durch die TrutzBox. Prüfen Sie, ob das Gerät wirklich am internen Netz hängt (Kabel in LAN-Int1/Int2 oder TrutzBox-WLAN) und nicht noch im alten WLAN des Routers angemeldet ist. Am Schalter **Nur Proxy-Geräte anzeigen** liegt es in aller Regel nicht: Intern angeschlossene Geräte werden transparent über den Proxy geführt und bleiben deshalb auch bei eingeschaltetem Schalter sichtbar. Ausblenden lässt er nur Geräte im äußeren Netz. Kapitel „Was tun, wenn …?“ führt durch die weitere Fehlersuche.

Zwei Einträge für dasselbe Gerät?

Das passiert, wenn ein Gerät mal per Kabel und mal per WLAN kommt, denn jede Schnittstelle hat ihre eigene Hardware-Adresse. Benennen Sie beide Einträge entsprechend, etwa „Laptop (Kabel)" und „Laptop (WLAN)", und geben Sie beiden dieselbe Filtergruppe.

Warum steht bei einem Gerät kein Hersteller?

Neuere Smartphones und Notebooks vergeben in fremden Netzen aus Datenschutzgründen eine zufällige Hardware-Adresse. Aus einer solchen Adresse lässt sich kein Hersteller ableiten, und die TrutzBox weist darauf hin. Das Gerät ist trotzdem vollständig geschützt; nur die automatische Erkennung ist eingeschränkt. Geben Sie ihm in diesem Fall besonders zeitnah einen eigenen Namen.

Ändert sich etwas am Gerät, wenn ich es hier umbenenne?

Nein. Der Name gilt nur innerhalb der TrutzBox und erscheint in ihren Anzeigen. Der Netzwerkname des Geräts selbst bleibt unverändert, und auf dem Gerät müssen Sie nichts nachtragen.

Ein Gerät soll vorübergehend gar nicht ins Internet. Ist das möglich?

Ja. Entziehen Sie ihm in den Detail-Einstellungen unter **Netzwerk** den **Internetzugang**. Die Sperre greift sofort, auch bei bereits laufenden Verbindungen, und lässt sich jederzeit mit demselben Schalter wieder aufheben.

7 Benutzer, Postfächer, Passwörter

Unter **Verwaltung → Benutzer** legen Sie fest, wer die TrutzBox mitbenutzt. Benutzerkonten sind die Grundlage für mehrere der folgenden Kapitel: für TrutzMail-Postfächer (Kapitel „TrutzMail: sichere E-Mail“), für TrutzChat und Videokonferenzen (Kapitel „TrutzChat und Videokonferenz“) und für den VPN-Fernzugriff (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Dieses Kapitel beschreibt alles, was für Konten übergreifend gilt: anlegen, Passwörter, Detail-Einstellungen, löschen und reaktivieren. Was ein Konto in der jeweiligen Funktion bewirkt, steht im zugehörigen Kapitel.

Ein Benutzerkonto ist dabei etwas anderes als ein Gerät. Geräte erkennt die TrutzBox von selbst und verwaltet sie auf der Geräte-Seite (Kapitel „Geräte verwalten“); dort bekommt jedes Gerät seine Filtergruppe (Kapitel „Webfilter und Jugendschutz (TrutzContent)“). Ein Benutzerkonto steht für eine Person. Es trägt ihren Namen und auf Wunsch eine TrutzMail-Adresse und einen VPN-Zugang für unterwegs. Was im Internet gesperrt wird, legt ein Benutzerkonto nicht fest: Das richtet sich immer nach dem Gerät.

7.1 Drei Arten von Konten

- **admin:** das eine Verwalterkonto, beim Setup angelegt. Es öffnet das Admin-Panel und Webmin und darf alles, bis hinunter auf die Ebene des Betriebssystems. Sein Passwort ist der Generalschlüssel Ihrer TrutzBox.
- **Benutzer ohne TrutzMail-Adresse:** beliebig viele. Ein solches Konto trägt den Namen der Person (Feld Richtiger Name) und kann einen VPN-Zugang bekommen (Abschnitt „Die Detail-Einstellungen eines Benutzers“). Es eignet sich für jemanden, der von unterwegs ins Netz der TrutzBox soll, aber kein Postfach braucht (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). In der Liste erkennen Sie solche Konten daran, dass keine E-Mail-Adresse angezeigt wird.
- **Benutzer mit TrutzMail-Adresse:** nötig für TrutzMail, Chat und das Eröffnen von Videokonferenzräumen. Einen VPN-Zugang können sie wie jedes Benutzerkonto bekommen. Die Zahl solcher Adressen begrenzt Ihr Service-Vertrag; jede Adresse ist weltweit eindeutig.

Am Admin-Panel meldet sich immer nur `admin` an; ein Benutzerkonto öffnet die Verwaltung der TrutzBox nicht. Chat und Videokonferenz gehören zu TrutzRTC und stehen nur in der Business-Ausstattung der TrutzBox zur Verfügung (Kapitel „TrutzChat und Videokonferenz“). Auf einer TrutzBox ohne diese Ausstattung dienen die Konten also TrutzMail und dem VPN-Fernzugriff.

Konten mit TrutzMail-Adresse können aktiv oder deaktiviert sein. Läuft Ihr Service-Vertrag ab, gibt das zentrale Comidio-Adressbuch die Schlüssel Ihrer Adressen nicht mehr heraus. Andere TrutzBoxen senden dann keine TrutzMails mehr an Ihre Adressen; ihre Absender erfahren, dass die Adresse derzeit nicht aktiv ist. Für eine Videokonferenz gilt eine Erleichterung: Nur wer den Raum eröffnet, braucht eine TrutzMail-Adresse. Alle übrigen Teilnehmer kommen ohne Konto aus.

7.2 Benutzer anlegen und verwalten

Menüpfad: Verwaltung → Benutzer

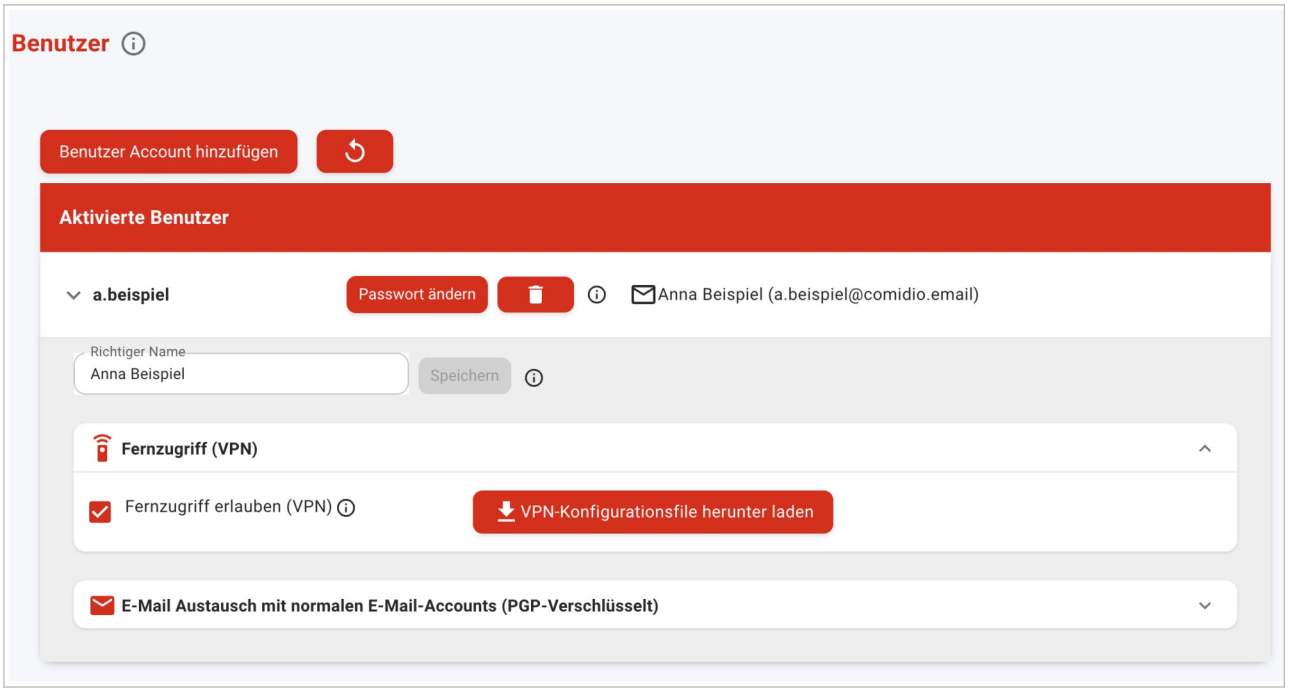


Abbildung 7-1: Die Benutzerliste mit aufgeklapptem Konto: oben das Feld Richtiger Name, darunter die einklappbaren Bereiche Fernzugriff (VPN) und E-Mail Austausch mit normalen E-Mail-Accounts. (© 2026 Comidio GmbH)

1. Klicken Sie auf **Benutzer Account hinzufügen**.
2. Tragen Sie **Richtiger Name** (der Anzeigename) und **Login Name** (der lokale Benutzername) ein. Soll ein Postfach entstehen, setzen Sie das Häkchen **Als TrutzMail-Adresse registrieren**; die Endung `@comidio.email` ergänzt die TrutzBox.
3. Vergeben Sie ein Passwort (mindestens 8 Zeichen, die vollständige Regel steht in Abschnitt „Passwörter ändern“) und speichern Sie.

Setzen Sie das Häkchen für die TrutzMail-Adresse, prüft die TrutzBox im selben Moment bei Comidio nach, ob der gewünschte Name noch frei ist, ob Ihr Vertrag noch eine freie Adresse hergibt und ob die Service-Laufzeit Ihrer TrutzKennung noch läuft. Erst danach entsteht das Konto samt Schlüsselpaar. Überlegen Sie sich den Login-Namen deshalb in Ruhe, denn er wird Teil einer weltweit eindeutigen Adresse, die Sie anschließend jahrelang verwenden.

Scheitert eine dieser Prüfungen, entsteht kein Konto, und die Oberfläche nennt den Grund. Dieselben Meldungen erscheinen beim Reaktivieren (Abschnitt „Löschen, Reaktivieren und das Kontingent“):

Meldung	Was zu tun ist
„Diese E-Mail-Adresse ist bereits registriert."	Einen anderen Login-Namen wählen.
„Adresskontingent erschöpft."	Eine Adresse freigeben, indem Sie einen nicht mehr gebrauchten Benutzer löschen, oder weitere Adressen bei Comidio buchen (Abschnitt „Löschen, Reaktivieren und

Meldung	Was zu tun ist
	das Kontingent“).
„Die Service-Laufzeit dieser TrutzKennung ist abgelaufen. TrutzMail-Adressen lassen sich erst nach der Verlängerung wieder anlegen oder reaktivieren."	Den Service-Vertrag verlängern (Abschnitt „Löschen, Reaktivieren und das Kontingent“). Ein Benutzer ohne TrutzMail-Adresse lässt sich weiterhin anlegen.
„Die Comidio-Server erkennen diese TrutzBox nicht. Bitte die Aktivierung der TrutzBox prüfen."	Die Comidio-Server nehmen die Anmeldung dieser TrutzBox nicht an. Ob sie beim Vertrags-Server angemeldet ist, steht unter Systemeinstellungen → Vertrag und Pakete. Fehlen dort die Vertragsdaten, hilft der Support (Kapitel „Support kontaktieren“).
„Verbindung zu Comidio-Servern nicht möglich. Bitte überprüfen Sie Ihre Internetverbindung."	Die Internet-Verbindung der TrutzBox prüfen (Kapitel „… kein Internet da ist“) und es danach noch einmal versuchen.

Die Übersicht ist zweigeteilt: **Aktivierte Benutzer** sind die aktiven Konten (Passwort ändern, löschen, über den Pfeil links die Detail-Einstellungen aufklappen), **Reaktivierbare Benutzer** sind früher angelegte Adressen, die nach einem Zurücksetzen oder Hardwaretausch mit einem Klick zurückkehren.

7.3 Passwörter ändern

Die Passwörter der Benutzerkonten ändern Sie in der Benutzerliste über die Aktion beim jeweiligen Konto. Für das Admin-Passwort gibt es einen eigenen Weg: Es liegt unter **Verwaltung → Allgemeine Einstellungen** hinter dem Punkt **Administrator Password ändern** und taucht in der Benutzerliste nicht auf. Für jedes neu vergebene oder geänderte Passwort gilt dieselbe Regel, beim Admin-Konto ebenso wie bei Benutzern und Postfächern und schon im Setup. Ein Passwort, das sie nicht erfüllt, wird nicht angenommen, und die Meldung nennt den Grund.

Die Passwortregel

- **Länge:** 8 bis 128 Zeichen. Leerzeichen und Umlaute sind erlaubt.
- **Zeichenarten:** mindestens drei der vier Arten Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen. Ab 16 Zeichen genügen zwei; ein Leerzeichen zählt dabei als Sonderzeichen.
- **Nicht erlaubt:** die Wörter TrutzBox, Comidio und admin, der eigene Benutzername, einfache Folgen wie 1234, abcd, qwertz oder aaaa sowie bekannte Allerweltspasswörter wie Sommer2024! oder Passwort123.

Bereits vergebene Passwörter bleiben gültig. Beim Anmelden prüft die TrutzBox sie nicht, und niemand muss sein Passwort deswegen ändern. Das „i" neben jedem Passwortfeld fasst die Regel zusammen; der Stärkebalken dient nur noch zur Orientierung.

Die Regel ist bewusst streng, denn das TrutzMail-Passwort schützt mehr als das Postfach: Mit ihm meldet man sich auch am Chat an, und diese Anmeldung ist über die Portfreigabe der

Videokonferenz aus dem Internet erreichbar (Kapitel „Reiter Videokonferenz: einmalig einrichten“). Der Angriffsschutz bremst das Ausprobieren von Passwörtern (Kapitel „Angriffsschutz: Firewall und Wächter“), gegen ein leicht zu erratendes Passwort hilft er aber nur begrenzt.

1. Für einen Benutzer: Öffnen Sie **Verwaltung → Benutzer**, suchen Sie das Konto in der Liste **Aktivierte Benutzer** und wählen Sie dort **Passwort ändern**.
2. Für das Admin-Konto: Öffnen Sie **Verwaltung → Allgemeine Einstellungen** und dort **Administrator Password ändern**.
3. Geben Sie das neue Passwort zweimal ein und speichern Sie. Lehnt die TrutzBox es ab, nennt die Meldung den Grund, etwa eine fehlende Zeichenart.
4. Tragen Sie das neue Passwort anschließend überall dort nach, wo es hinterlegt ist, also im Mail-Programm, im Chat-Programm und im Browser.

Für das Admin-Passwort gilt besondere Sorgfalt: Es schützt die gesamte TrutzBox, und niemand kann es zurücksetzen, auch Comidio nicht (Kapitel „… das Passwort für das Admin-Panel nicht mehr bekannt ist“). Wählen Sie ein langes, einprägsames Passwort (die Merkhilfe aus Kapitel „Schritt „Admin-Passwort setzen"“ hilft) und bewahren Sie es sicher auf, etwa in einem Passwort-Manager.

> **Ein geändertes Passwort will überall nachgetragen werden**
>
> Ein Benutzerpasswort steckt an mehreren Stellen: im Mail-Programm, im Chat-Programm und beim Webmail. Ändern Sie es, tragen Sie es dort überall nach. Sonst scheitert ein vergessenes Gerät im Hintergrund immer wieder an der alten Anmeldung. Meldet es sich dabei von unterwegs ohne VPN am Chat oder am Postfach an, wertet der Angriffsschutz das nach fünf Fehlversuchen innerhalb von 30 Minuten als Angriff und sperrt die Internet-Adresse, von der es kommt, für sechs Stunden, bei Wiederholung länger (Kapitel „Angriffsschutz: Firewall und Wächter“). Geräte im eigenen Netz und über VPN sperrt er nie.

7.4 Die Detail-Einstellungen eines Benutzers

Der Pfeil links neben einem aktivierten Benutzer klappt dessen Detail-Einstellungen auf. Was dort steht, gilt jeweils nur für diesen einen Benutzer. Ganz oben steht das Feld **Richtiger Name**, darunter folgen Bereiche, die sich einzeln auf- und zuklappen lassen: **Fernzugriff (VPN)** ist zunächst offen, der Bereich für den Mailversand zugeklappt.

- **Richtiger Name:** der Name, unter dem der Benutzer angezeigt wird, etwa im Chat und in Auswahllisten neben der TrutzMail-Adresse. Ändern Sie ihn im Feld und übernehmen Sie ihn mit **Speichern** (höchstens 64 Zeichen, kein Doppelpunkt). Der Schlüssel der TrutzMail-Adresse behält dabei den Namen, mit dem er angelegt wurde.
- **Fernzugriff (VPN):** was hier steht, hängt vom Tunnel ab, den die TrutzBox für den Fernzugriff nutzt (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Bei OpenVPN schaltet **Fernzugriff erlauben (VPN)** den Zugang für diesen Benutzer frei. Danach lädt **VPN-Konfigurationsfile herunter laden** die persönliche Konfigurationsdatei (.ovpn) für das Gerät herunter (Kapitel „OpenVPN statt WireGuard verwenden“). Jeder Benutzer bekommt seine

eigene Datei; geben Sie sie nicht weiter. Läuft die TrutzBox mit WireGuard, stehen hier stattdessen die WireGuard-Zugänge dieses Kontos, je Gerät einer, und die Schaltfläche **WireGuard-Zugang anlegen**. Ein neuer Zugang erscheint gleich in einem Fenster mit Bildcode und Datei für die App WireGuard auf dem Gerät (Kapitel „Schritt 5: Zugänge für die WireGuard-App anlegen“). Das Gerät eines gelöschten Zugangs verbindet sich nicht mehr.

- **E-Mail-Austausch mit normalen Adressen:** nur bei Benutzern mit TrutzMail-Adresse. Hier verbindet der Benutzer die TrutzBox mit seinem Postfach bei einem Mail-Anbieter. Darüber sendet sie PGP-verschlüsselte Post an Partner ohne TrutzBox und holt Mail ab (Kapitel „Weg B einrichten: Postfach beim Anbieter verbinden“). Unter **Erweitert** steht auch **Selbstsignierte Zertifikate erlauben**: Es betrifft nur die verschlüsselte Verbindung zu den Servern dieses Postfachs. Schalten Sie es nur ein, wenn Sie sicher wissen, dass dieser Server, etwa ein firmeneigener, ein Zertifikat ohne offizielle Zertifizierungsstelle verwendet; sonst könnte ein Angreifer die Verbindung abhören. Mit der PGP-Verschlüsselung der Mails hat es nichts zu tun.

Diese Einstellungen sind der Grund, warum sich in Kapitel „TrutzMail: sichere E-Mail“ und Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“ mehrere Verweise auf die Benutzerverwaltung finden: Die eigentlichen Funktionen werden dort beschrieben, eingeschaltet werden sie hier, je Person.

7.5 Löschen, Reaktivieren und das Kontingent

Löschen Sie einen Benutzer, verschwindet sein Zugang zur TrutzBox. Hatte er eine TrutzMail-Adresse, wird diese automatisch deaktiviert und ihr Zertifikat zentral als ungültig markiert, damit niemand mehr an einen alten Schlüssel verschlüsselt. Der Platz im Kontingent wird dadurch wieder frei.

Verloren ist die Adresse damit aber nicht. Sie bleibt für Ihre TrutzLegitimation reserviert, und nur eine TrutzBox mit genau dieser TrutzLegitimation darf sie erneut einrichten. So kann niemand eine aufgegebene Adresse übernehmen und sich als jemand anderes ausgeben. In der Liste **Reaktivierbare Benutzer** steht sie farblich abgesetzt bereit und kehrt über **Reaktivieren** zurück. Dasselbe gilt nach einem Zurücksetzen der TrutzBox oder nach einem Hardwaretausch (Kapitel „Sichern, Wiederherstellen und Zurücksetzen“).

1. Öffnen Sie **Verwaltung → Benutzer** und suchen Sie den Abschnitt **Reaktivierbare Benutzer**.
2. Klicken Sie bei der gewünschten Adresse auf **Reaktivieren**. Die TrutzBox fragt bei Comidio nach, ob diese Adresse zu Ihrer TrutzLegitimation gehört, und richtet sie dann neu ein.
3. Vergeben Sie ein Passwort für das Konto und tragen Sie es im Mail-Programm nach.

Reaktivieren holt die Adresse zurück, nicht die alte Post

Ein reaktiviertes Konto bekommt einen neuen Schlüssel. Postfachinhalte und den bisherigen geheimen Schlüssel bringt nur eine Sicherung zurück. Ihre TrutzBox-Partner merken vom Schlüsselwechsel nichts, deren TrutzBoxen holen den neuen Schlüssel selbst. PGP-Partner ohne TrutzBox brauchen dagegen Ihren neuen öffentlichen Schlüssel (Kapitel „Schlüssel und Zertifikate“).

Wie viele TrutzMail-Adressen Ihr Vertrag zulässt, sehen Sie unter **Systemeinstellungen → Vertrag und Pakete**, etwa als „TrutzMail Kontingent 2 / 5 TrutzMail Adressen belegt". Dieselbe Seite nennt Ihre TrutzKennung, den Aktivierungszeitpunkt der TrutzBox, die Laufzeit des Service-Vertrags und den gebuchten Umfang, also ob Fernzugriff und Videokonferenz freigeschaltet sind. Das Kontingent hängt am Service-Vertrag und gilt jeweils für zwölf Monate.

Ist das Kontingent ausgeschöpft, meldet die Oberfläche beim Anlegen einer weiteren Adresse „Adresskontingent erschöpft". Zusätzliche Adressen und die Verlängerung des Service-Vertrags laufen nicht über die TrutzBox, sondern über Comidio: Wenden Sie sich dafür an www.trutzbox.de oder schreiben Sie an support@trutzbox.de.

Vor Ablauf erinnert Comidio per E-Mail an die Verlängerung, und zwar an die Adresse, die in Ihrem Konto auf trutzbox.de hinterlegt ist. Läuft der Vertrag dennoch aus, weist die Oberfläche darauf hin, und die an die Mail-Adresse gebundenen Dienste stehen nicht mehr zur Verfügung: TrutzMail, TrutzChat und die Videokonferenz. TrutzMail-Adressen lassen sich dann weder anlegen noch reaktivieren; die Oberfläche meldet *„Die Service-Laufzeit dieser TrutzKennung ist abgelaufen. TrutzMail-Adressen lassen sich erst nach der Verlängerung wieder anlegen oder reaktivieren."* Die TrutzBox selbst arbeitet weiter, sie erhält dann aber keine Software-Updates mehr, was auf Dauer nicht empfehlenswert ist.

7.6 Anmelden an der Oberfläche

Die Anmeldung am Admin-Panel bleibt bestehen, solange Sie die Oberfläche benutzen: Jede Aktion verlängert sie. Erst wenn sie 30 Tage lang nicht benutzt wurde, läuft sie ab. Einen Neustart der TrutzBox überdauert sie dagegen nicht, und auch nicht jedes Software-Update: Die Sitzungen liegen im Arbeitsspeicher und gehen dabei verloren. Danach melden Sie sich also erneut an, etwa wenn Sie nach einem Software-Update nachsehen wollen, ob alles wieder läuft. Die Sitzungskennung ist dabei zusätzlich abgesichert.

Um Software-Updates kümmert sich die Oberfläche selbst. Startet die Verwaltung der TrutzBox dabei neu, deckt sie eine offene Seite mit dem Hinweis *„Die TrutzBox startet gerade neu"* ab und lädt sie danach von selbst neu. Läuft das Software-Update beim Öffnen der Oberfläche noch, erscheint statt der Anmeldung die Warteseite *„Software-Updates werden installiert"* mit dem Fortschritt, etwa „5 von 12 Paketen"; danach öffnet sich die Oberfläche von selbst. Hat ein Software-Update die Oberfläche selbst erneuert, lädt sich eine offene Seite von selbst neu, sobald dabei nichts verloren geht: wenn Sie zu ihr zurückkehren, nach einer Minute ohne Eingabe oder beim nächsten Wechsel der Seite. Solange ein Fenster offen ist oder Sie etwas eingegeben haben, wartet sie und zeigt stattdessen den Hinweis *„Die Oberfläche der TrutzBox wurde aktualisiert. Diese Seite zeigt noch die alte Fassung. Bitte laden Sie die Seite neu."* mit der Schaltfläche **Neu laden**.

Dieselbe Sitzung gilt auch für die Live-Ansichten wie den Monitor: Auch deren Datenverbindung wird geprüft, sodass niemand ohne Anmeldung mitlesen kann. Und falls ein Hintergrunddienst der TrutzBox einmal hängt, bricht die Anmeldeprüfung nach 15 Sekunden ab und zeigt Ihnen die Anmeldemaske, statt Sie dauerhaft auf einem Ladezeichen sitzen zu lassen.

Melden Sie sich an einem fremden oder gemeinsam genutzten Gerät an, melden Sie sich hinterher bewusst wieder ab. Solange eine Sitzung läuft, steht die gesamte Verwaltung der TrutzBox offen, und sie überdauert auch das Schließen des Browserfensters.

Häufige Fragen zu Benutzern

Braucht jede Person im Haushalt ein eigenes Konto?

Nein. Der Schutz im Internet hängt am Gerät, nicht an der Person; dafür genügt es, die Geräte einzuordnen (Kapitel „Geräte verwalten“). Ein eigenes Konto braucht nur, wer ein TrutzMail-Postfach, den Chat oder den VPN-Zugang nutzt. Sollen alle Geräte einer Person gleich gefiltert werden, geben Sie ihnen auf der Geräte-Seite dieselbe Filtergruppe (Kapitel „Filtergruppen zuordnen“).

Kann ich einen Benutzernamen später umbenennen?

Den Anzeigenamen ja, im Feld Richtiger Name der Detail-Einstellungen (Abschnitt „Die Detail-Einstellungen eines Benutzers“). Den Login-Namen nicht. Bei einem Konto mit TrutzMail-Adresse steckt der Login-Name in der weltweit eindeutigen Mail-Adresse; die lässt sich nachträglich nicht mehr ändern. Wählen Sie ihn deshalb von Anfang an mit Bedacht.

Was passiert mit dem Postfach, wenn ich einen Benutzer lösche?

Der Zugang verschwindet sofort, die Adresse wird deaktiviert und der Platz im Kontingent wird frei. Die Adresse selbst bleibt für Ihre TrutzLegitimation reserviert und lässt sich später reaktivieren. Die Postfachinhalte kehren dabei allerdings nicht zurück; dafür bräuchten Sie eine Sicherung (Kapitel „Sichern, Wiederherstellen und Zurücksetzen“).

Ein Benutzer wird immer wieder ausgesperrt. Woran liegt das?

Fast immer an einem Gerät, das noch das alte Passwort versucht, etwa eine vergessene Chat-App auf einem Zweittelefon. Kommt es dabei von unterwegs ohne VPN, wertet der Angriffsschutz die wiederholten Fehlversuche als Angriff und sperrt die Internet-Adresse, von der die Versuche kommen, für sechs Stunden, bei Wiederholung immer länger bis höchstens eine Woche; gesperrt wird also die Adresse, nicht das Konto. Tragen Sie das neue Passwort auf allen Geräten nach; die Sperre lässt sich außerdem von Hand aufheben (Kapitel „Angriffsschutz: Firewall und Wächter“).

8 Webfilter und Jugendschutz (TrutzContent)

TrutzContent ist der Webfilter der TrutzBox. Er entscheidet bei jedem Zugriff, ob ein Gerät den angefragten Internet-Server kontaktieren darf. Er blockiert unerwünschten Datenverkehr: Werbung, Dienste, die aufzeichnen, was Sie im Internet tun, Verbindungen zu gefährlichen Servern und, je nach Einstellung, jugendgefährdende Inhalte. TrutzContent ist immer aktiv, sobald der Verkehr eines Geräts durch die TrutzBox läuft. Wie streng gefiltert wird, bestimmt allein die Filtergruppe, der Sie das Gerät zuordnen.

Voraussetzungen

• Ihre TrutzBox ist eingerichtet (Kapitel „TrutzBox einrichten (Setup)“) und die zu schützenden Geräte sind angeschlossen (Kapitel „Ein Gerät mit der TrutzBox absichern“).

• Für verlässlichen Jugendschutz gehören die Geräte ins interne TrutzBox-Netzwerk. Im Proxy-Mode könnte ein findiges Kind die Einstellung am Gerät einfach wieder entfernen.

Anleitung zum Anklicken

Filtergruppen, Filterlisten und Ausnahmen lassen sich am Bildschirm schneller begreifen als im Text. Die Anleitung „Webfilter und Filterlisten" zeigt die Stationen dieses Kapitels mit Bild, Text und Ton im Browser: trutzbox.de/videodokumentation.

8.1 So greift alles ineinander: Geräte, Filtergruppen, Filterlisten

Drei Ebenen spielen zusammen, und wer sie einmal verstanden hat, findet sich überall zurecht:

- **Filterlisten** sind die Grundbausteine: lange Verzeichnisse von Internet-Adressen zu je einem Thema, etwa „Werbung", „Gewalt" oder „Abzocke und Kostenfallen". Ausgeliefert wird die TrutzBox mit rund vierzig Filterlisten, gebündelt nach Themengebieten; wie viele es gerade sind, zeigt die Seite Filtergruppen. In den Filtergruppen wählen Sie deshalb Themengebiete aus und nicht einzelne Listen. Comidio hält alle mitgelieferten Listen mit den täglichen Updates der Filterlisten automatisch aktuell.
- **Filtergruppen** bündeln Filterlisten und Themen zu einem Profil, zum Beispiel „Kinder 8-10 Jahre" oder „IoT" für Fernseher und Haustechnik. Die Gruppe legt fest, was blockiert wird.
- **Geräte** bekommen je genau eine Filtergruppe zugewiesen. Ab da gilt: Dieses Gerät darf nur, was seine Gruppe erlaubt.

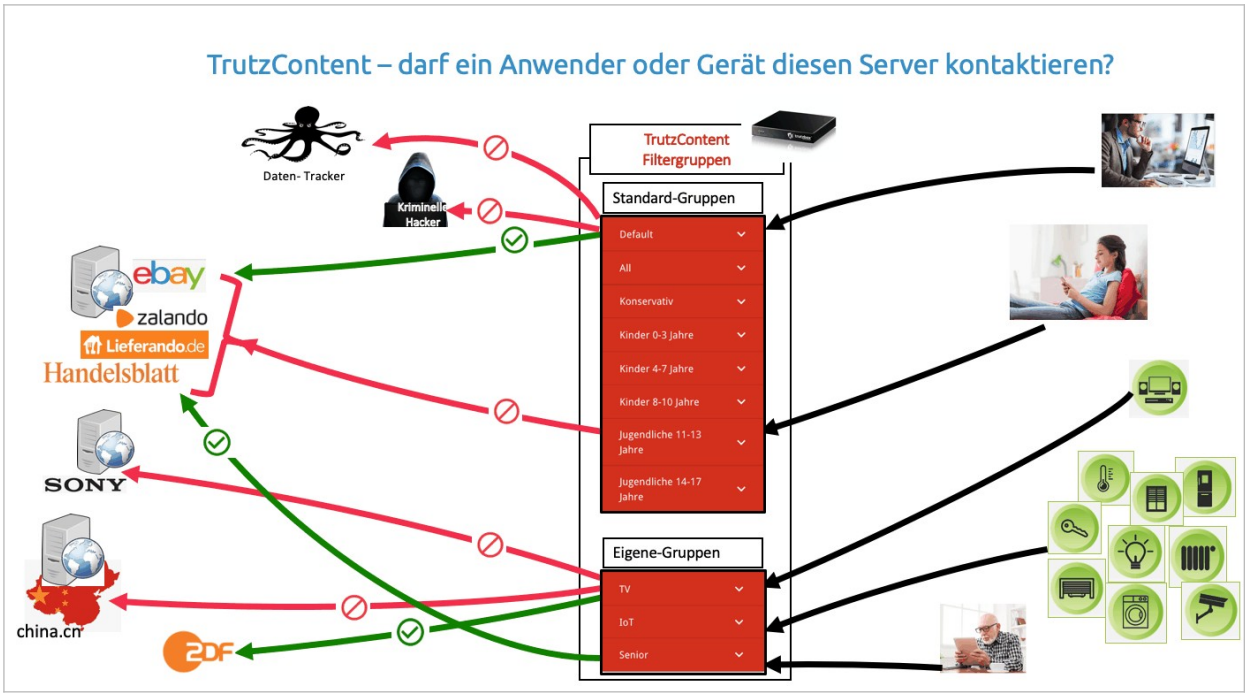


Abbildung 8-1: Das Prinzip: Jedes Gerät gehört zu einer Filtergruppe, und die Gruppe entscheidet, welche Server erreichbar sind. (© 2026 Comidio GmbH)

Ein neues Gerät landet automatisch in der mitgelieferten Gruppe **Standard**. Danach ordnen Sie es passend ein: den PC und das iPhone der zwölfjährigen Tochter etwa der Gruppe „Jugendliche 11-13 Jahre", den Fernseher einer selbst angelegten Gruppe „TV". Das Umstellen dauert nur einen Klick auf der Geräte-Seite (Kapitel „Filtergruppen zuordnen“).

Wichtig für den Jugendschutz: Die Einstellungen kann nur der Administrator ändern. Wer am Gerät sitzt, kann die Filterung an der TrutzBox nicht abschalten. Auch der bekannteste Schleichweg ist von vornherein zu: Das QUIC-Protokoll ist ab Werk im gesamten Netz gesperrt, nicht erst in einer bestimmten Filtergruppe.

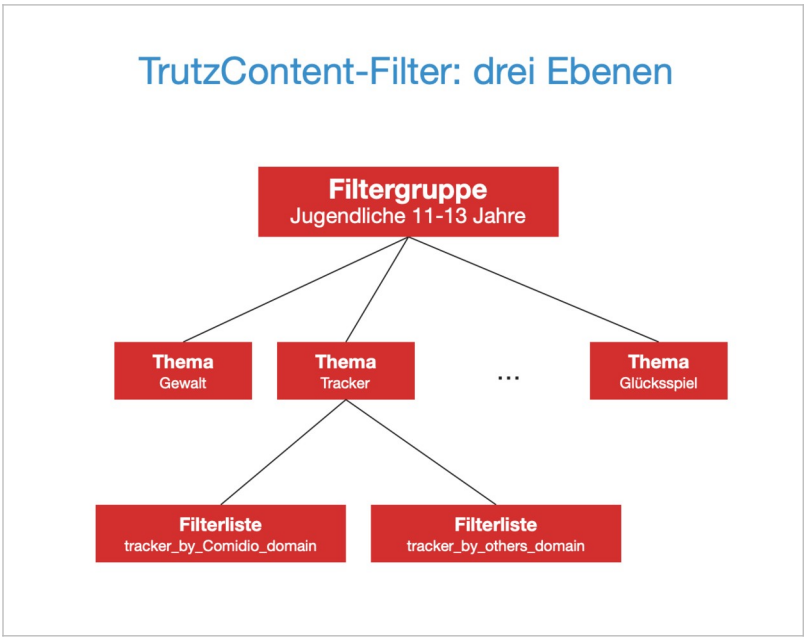


Abbildung 8-2: Die drei Ebenen im Detail: Eine Filtergruppe enthält Themen, ein Thema enthält einzelne Filterlisten. (© 2026 Comidio GmbH)

8.2 Filtergruppen einrichten

Die Filtergruppen verwalten Sie unter **Verwaltung → Filtergruppen**. Ausgeliefert werden neun fertige Gruppen: *Standard* für alle Geräte, *Trutz Browse*, *All*, *Konservativ* sowie die nach Alter gestaffelten Gruppen *Kinder 0-3 Jahre*, *Kinder 4-7 Jahre*, *Kinder 8-10 Jahre*, *Jugendliche 11-13 Jahre* und *Jugendliche 14-17 Jahre*. Für eigene Zwecke legen Sie mit **Filtergruppe hinzufügen** neue Gruppen an, etwa „TV", „IoT" oder eine Abteilungsgruppe in der Firma.

Menüpfad: Verwaltung → Filtergruppen

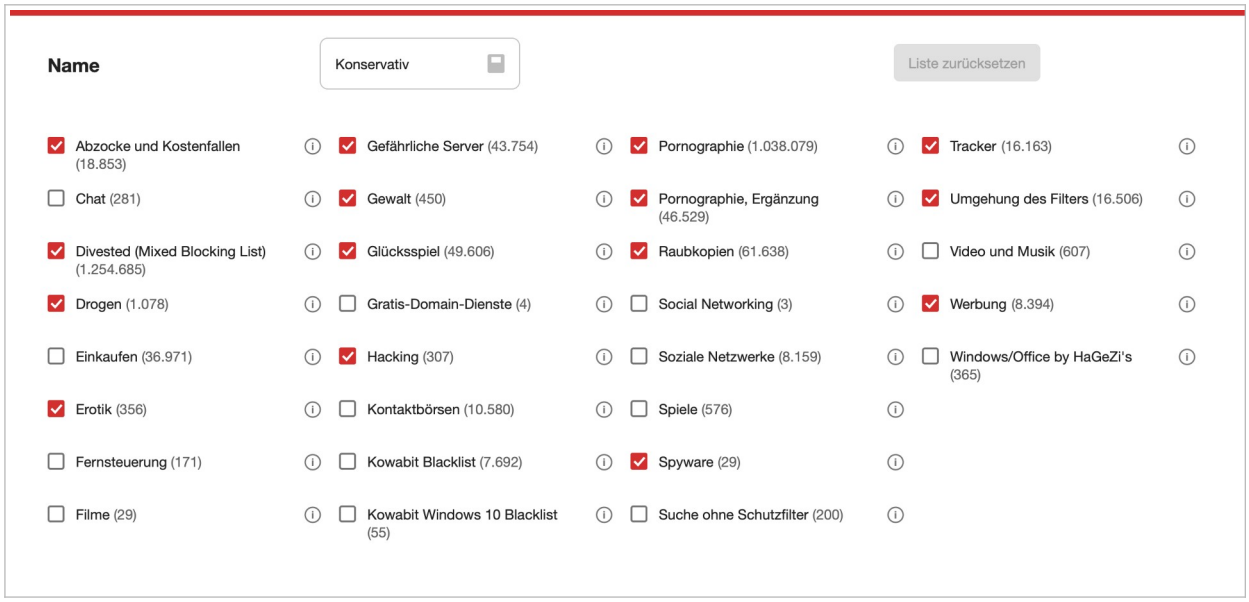


Abbildung 8-3: Die Filtergruppen-Seite: Pro Gruppe wird per Häkchen festgelegt, welche Themengebiete blockiert werden. Hinter jedem Thema steht die Zahl seiner Einträge. (© 2026 Comidio GmbH)

1. Öffnen Sie **Verwaltung → Filtergruppen** und klappen Sie eine Gruppe auf, oder klicken Sie auf **Filtergruppe hinzufügen**.

2. Setzen Sie Häkchen bei allen Themengebieten, die diese Gruppe blockieren soll, zum Beispiel „Werbung", „Tracker" (Dienste, die aufzeichnen, was man im Internet tut) und für Kindergruppen die altersgerechten Inhaltsthemen.
3. Speichern Sie mit **Liste speichern** und ordnen Sie anschließend auf der Geräte-Seite die passenden Geräte dieser Gruppe zu.

Weniger ist oft mehr

Starten Sie mit den mitgelieferten Gruppen und beobachten Sie eine Woche lang im Monitor, was blockiert wird. Nachjustieren ist einfacher, als von Anfang an alles perfekt einstellen zu wollen.

Haben Sie sich verrannt: **Liste zurücksetzen** holt eine veränderte mitgelieferte Gruppe in den Auslieferungszustand zurück, **Alle Gruppen zurücksetzen** in der Kopfzeile tut das für alle mitgelieferten Gruppen auf einmal. Selbst angelegte Gruppen bleiben dabei erhalten.

8.3 Wie die Altersgruppen eingeteilt sind

Die fünf Altersgruppen sperren, was für das jeweilige Alter nicht passt. Jede jüngere Gruppe sperrt alles, was die ältere sperrt, und mehr. Grundlage sind die Empfehlungen der Kinder- und Jugendärzte und der Nationalen Akademie der Wissenschaften Leopoldina, die Altersgrenzen der Anbieter und das Gesetz. In der Tabelle stehen die Themen so, wie sie auf der Seite Filtergruppen heißen.

Altersgruppe	Gesperrt	Warum
alle fünf	Pornographie, Erotik, Glücksspiel, Drogen, Gewalt, Kontaktbörsen, Raubkopien, Fernsteuerung, Abzocke und Kostenfallen, Gefährliche Server, Umgehung des Filters (VPN, Proxy)	Diese Inhalte sind Erwachsenen vorbehalten oder gefährden Kinder. Ohne Sperre der Umwege ließe sich der Filter umgehen.
11-13 Jahre	zusätzlich Soziale Netzwerke, Video und Musik (etwa YouTube, Netflix, Spotify), Filme, Hacking, Suche ohne Schutzfilter	Ein eigenes Konto in sozialen Netzwerken empfehlen Fachleute und Anbieter erst ab 13 Jahren.
8-10 Jahre	zusätzlich Chat	Kinderärzte empfehlen das Internet bis 16 Jahre nur unter Aufsicht. In Chats knüpfen Fremde Kontakt.
4-7 Jahre	zusätzlich Einkaufen und Spiele (etwa Roblox, Fortnite, Steam, Spielkonsolen)	Unter 7 Jahren kann ein Kind nach dem Gesetz nichts kaufen. Eine eigene Spielkonsole empfehlen Kinderärzte nicht vor 9 Jahren.
0-3 Jahre	wie 4-7 Jahre	Bis 3 Jahre empfehlen Kinderärzte keinen Bildschirm.

Ab 14 Jahren sind soziale Netzwerke, Video und Musik frei. Für 14- und 15-Jährige empfiehlt die Leopoldina die Zustimmung der Eltern. Die geben Sie, indem Sie das Gerät in die Gruppe „Jugendliche 14-17 Jahre" stellen.

Gut zu wissen

• Kinderärzte empfehlen, dass Kinder unter 9 Jahren das Internet gar nicht nutzen.

• Keine Sperrliste ist vollständig. Neue Seiten kommen täglich hinzu und landen erst nach und nach in den Listen.

• Für ein Gerät, das nur ausgewählte Seiten öffnen soll, schalten Sie „Nur Ausnahmen erlauben" ein (Abschnitt „Ausnahmen je Gerät“).

8.4 Filterlisten verwalten

Die einzelnen Filterlisten finden Sie unter **Verwaltung → Filterlisten**. Die von Comidio mitgelieferten Listen können Sie ansehen und durchsuchen, aber nicht verändern; sie kommen mit den täglichen Updates der Filterlisten automatisch auf den neuesten Stand. Eigene Listen legen Sie daneben an und pflegen sie selbst.

Menüpfad: Verwaltung → Filterlisten

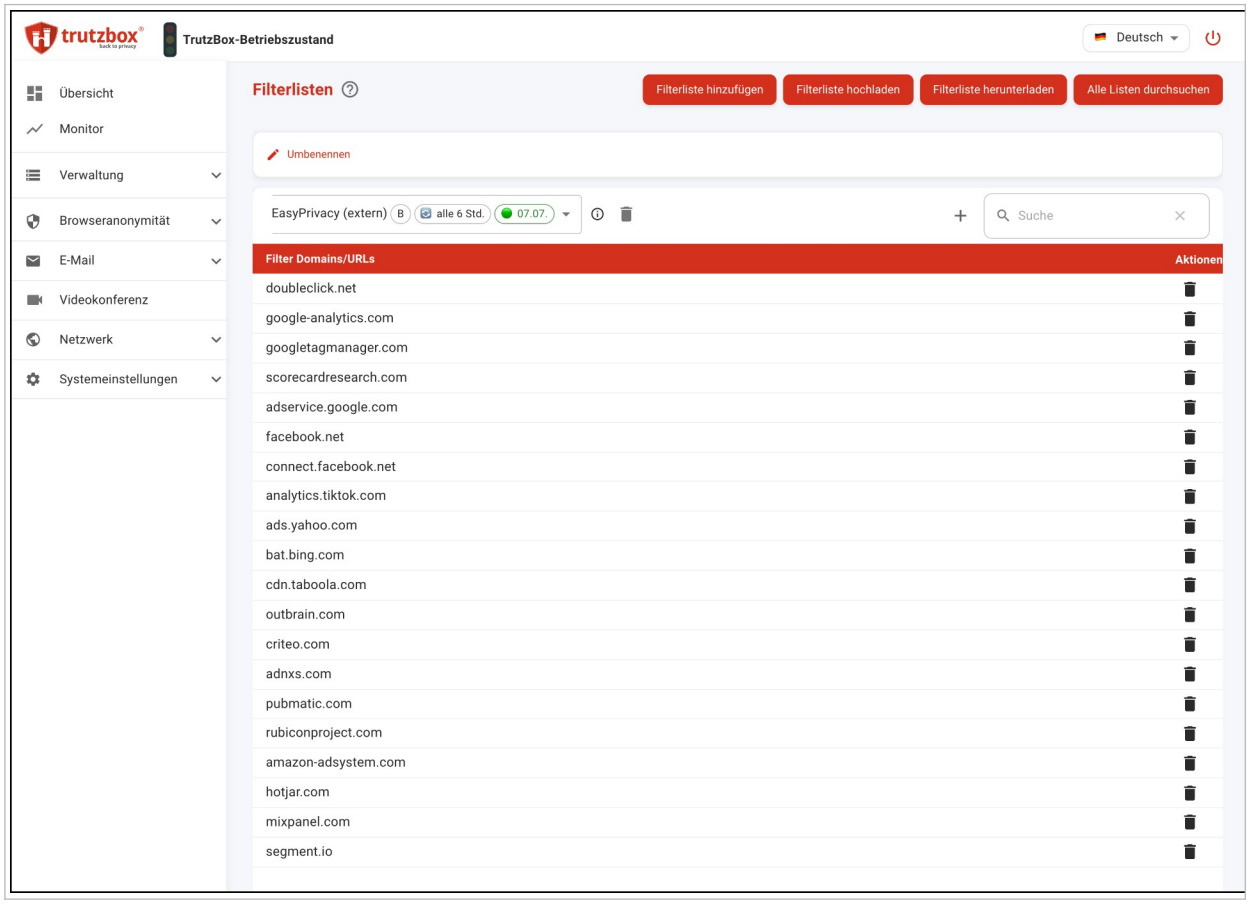


Abbildung 8-4: Die Filterlisten-Seite mit einer importierten Liste: Rhythmus, Status der letzten Aktualisierung und die enthaltenen Adressen. (© 2026 Comidio GmbH)

Beim Eintragen eigener Adressen gilt: nur den Domain-Namen eintragen, also zum Beispiel `facebook.com`, ohne „http" oder „www" davor. Die TrutzBox vergleicht dann jede aufgerufene Adresse mit diesem Eintrag.

Die drei Standard-Filterlisten

Drei besondere Listen liefert jede TrutzBox mit. Sie beginnen alle mit „Standard", lassen sich weder umbenennen noch löschen, und Sie können ihnen jederzeit eigene Einträge hinzufügen oder daraus entfernen. Ihr Zweck: Sperren und Freigeben mit einem einzigen Klick.

Liste	Wofür sie da ist
Standard-TrutzBrowse-BL	Sperrliste für TrutzBrowse, wirkt nur auf Geräten mit eingeschaltetem TrutzBrowse. Sie sperrt eine Adresse nur dann, wenn eine Seite sie im Hintergrund nachlädt, etwa die eines Dienstes, der mitschreibt, was Sie tun. Direkt aufgerufen bleibt die Adresse erreichbar. Zeigt die TrutzBox einen solchen Zugriff im Hintergrund, sperren Sie ihn mit einem Klick, und die Adresse landet in dieser Liste.
Standard-TrutzContent-BL	Sperrliste des Webfilters, gilt für alle Geräte, deren Verkehr über den Proxy läuft. Ein Klick auf einen angezeigten Zugriff übernimmt die Adresse hierher und sperrt sie.
Standard-TrutzContent-WL	Ausnahmeliste (Whitelist), bei allen Geräten aktiv. Blockiert die TrutzBox etwas zu Unrecht, geben Sie die Adresse mit einem Klick wieder frei; sie landet dann hier und hat fortan Vorrang vor allen Sperren.

Menüpfad: Verwaltung → Filterlisten

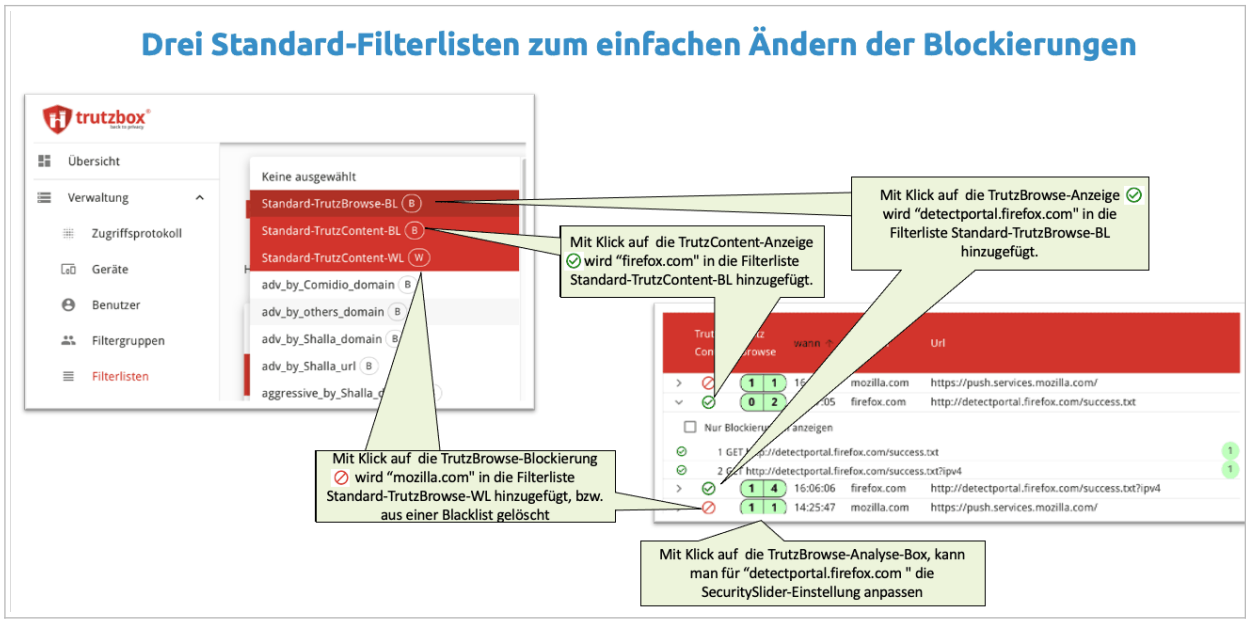


Abbildung 8-5: Sperren und Freigeben mit einem Klick: Aus der Monitor-Liste heraus wandern Adressen direkt in die passende Standard-Liste. (© 2026 Comidio GmbH)

Am bequemsten füllen sich diese Listen direkt aus dem **Monitor** (Kapitel „Monitor und Statistiken"): Dort öffnet das Schild-Symbol an einem Server das Menü **Sperren / Freischalten**; in der Liste genügt ein Klick auf den grünen Haken oder das rote Verbotsschild einer Zeile. Die Adresse wird gesperrt beziehungsweise freigegeben, ohne dass Sie die Filterlisten-Seite überhaupt öffnen müssen (Kapitel „Untersuchen und eingreifen"). Alle Einträge, die Sie selbst angelegt haben,

stehen zusammen auf der Seite Eigene Sperren und Ausnahmen (Abschnitt „Eigene Sperren und Ausnahmen“).

8.5 Filterlisten aus dem Internet laden und automatisch aktualisieren

Im Internet pflegen Freiwillige seit Jahren hervorragende öffentliche Sperrlisten gegen Werbung und anderen unerwünschten Datenverkehr. Solche Listen übernehmen Sie direkt in Ihre TrutzBox, samt automatischer Aktualisierung. Das Fenster „Neue Filterliste hinzufügen" führt in drei Schritten durch den Import:

Menüpfad: Verwaltung → Filterlisten → Filterliste hinzufügen

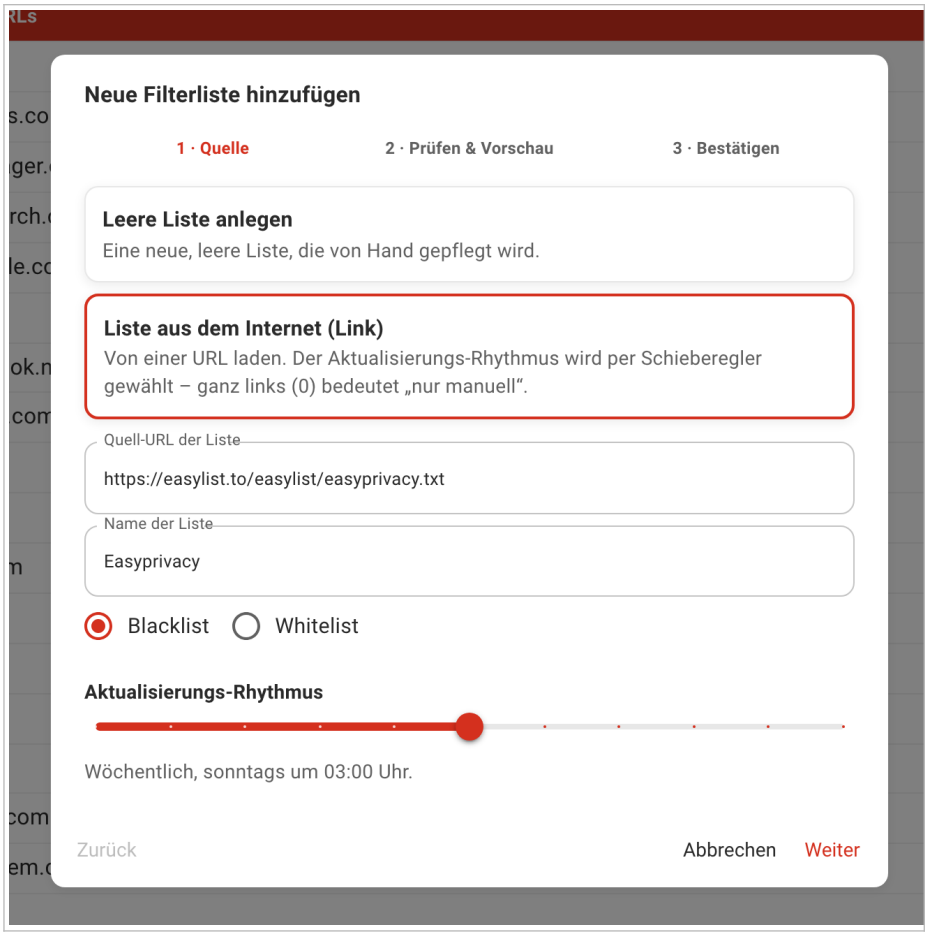


Abbildung 8-6: Das Fenster „Neue Filterliste hinzufügen", Schritt 1: Quell-Adresse, Name, Listenart und Aktualisierungs-Rhythmus. (© 2026 Comidio GmbH)

1. Klicken Sie unter **Verwaltung → Filterlisten** auf **Filterliste hinzufügen** und wählen Sie *„Liste aus dem Internet (Link)"*. Tragen Sie die **Quell-URL der Liste** ein, vergeben Sie einen Namen und wählen Sie mit dem Schieberegler den **Aktualisierungs-Rhythmus**: von „nur manuell" über monatlich, wöchentlich oder täglich bis „alle 6 Stunden".
2. Im Schritt **Prüfen & Vorschau** lädt die TrutzBox die Liste und zeigt, was erkannt wurde. Alle gängigen Listenformate erkennt die TrutzBox selbst und rechnet sie in ihr eigenes Format um. Zusätzlich sehen Sie, wie stark sich die Liste mit Ihren vorhandenen überschneidet, etwa „320 neu, 78 % schon abgedeckt".

3. Im Schritt **Bestätigen** übernehmen Sie die Liste. Danach aktivieren Sie sie wie jede andere Liste in den gewünschten Filtergruppen.

Importierte Listen zeigen auf der Filterlisten-Seite eine Quell-Karte mit dem erkannten Format, dem Zeitpunkt der letzten Aktualisierung und dem Status („aktuell" oder „veraltet, Update überfällig"). Über **Jetzt aktualisieren** laden Sie die Liste sofort neu, über **Rhythmus ändern** passen Sie das Intervall an. Die automatischen Aktualisierungen laufen zu festen Uhrzeiten, meist nachts um 3 Uhr; den nächsten Termin nennt die Quell-Karte. Schlägt eine Aktualisierung fehl, bleibt einfach der letzte funktionierende Stand der Liste aktiv.

Eigene Änderungen an importierten Listen

Die automatische Aktualisierung überschreibt Änderungen, die Sie von Hand an einer importierten Liste vornehmen. Dauerhafte eigene Ausnahmen gehören deshalb in eine Whitelist, am einfachsten in die Standard-TrutzContent-WL; sie hat im Filter Vorrang.

Streng ist die TrutzBox beim Prüfen: Enthält eine Liste auch nur einen nicht umwandelbaren Eintrag, wird sie komplett abgelehnt. So kann keine fehlerhafte Liste den Filter beschädigen. Akzeptiert werden nur Quellen mit http oder https.

Wie groß darf eine Liste sein?

Eine feste Grenze gibt es nicht. Sie richtet sich nach dem Hauptspeicher (RAM) der TrutzBox. Den Import erledigt die Verwaltung der TrutzBox, also der Dienst hinter dieser Oberfläche. Sie darf rund ein Viertel des Hauptspeichers belegen und braucht beim Prüfen für jedes Megabyte der Liste etwa 4,5 MB davon. Daraus ergibt sich die Grenze: mindestens 50 MB, mit mehr Hauptspeicher entsprechend mehr, etwa 140 MB bei 4 GB und 350 MB bei 8 GB. Wie viel gerade frei ist, schwankt. Ist eine Liste zu groß, nennt die Meldung die Grenze, die in diesem Moment gilt, etwa: „Der Arbeitsspeicher der Verwaltung reicht zurzeit für Listen bis 140 MB." Auch der freie Platz auf der SSD begrenzt den Import.

Eine zweite Grenze gilt für alle eingeschalteten Listen zusammen: Sie müssen in den Speicher des Webfilters passen. Der Webfilter bekommt mindestens gut ein Drittel des Hauptspeichers, auf TrutzBoxen mit mehr Hauptspeicher alles, was die übrigen Dienste nicht brauchen. Eine TrutzBox mit 4 GB Hauptspeicher nennt zum Beispiel 1,92 GB. Die Grenze Ihrer TrutzBox steht im Speicherverlauf in der Zeile „Grenzen dieser TrutzBox" (Kapitel „Die Startseite lesen“). Wird es eng, warnt die Seite Filtergruppen beim Speichern; eine Auswahl, die nicht mehr in den Speicher passt, speichert sie nicht.

Eigene Listen anlegen und pflegen

Neben den mitgelieferten und importierten Listen können Sie beliebig viele eigene führen, etwa eine Liste „Firma erlaubt" mit den Servern, die Ihre Arbeitsgeräte brauchen, oder eine Liste „Spielekonsole" für ein einzelnes Gerät. Über **Filterliste hinzufügen** und die Auswahl *„Leere Liste anlegen"* entsteht eine leere Liste, die Sie von Hand füllen. Jede Liste ist entweder eine **Blacklist** (was drinsteht, wird gesperrt) oder eine **Whitelist** (was drinsteht, ist erlaubt und schlägt alle Sperren).

Zum Sichern und Übertragen gibt es **Filterliste herunterladen** und **Filterliste hochladen**. Und wenn Sie einmal nicht wissen, in welcher der vielen Listen eine bestimmte Adresse steckt, hilft **Alle Listen durchsuchen**: Die TrutzBox zeigt jeden Treffer samt Liste, in der er steht. Das ist der schnellste Weg, wenn eine Seite blockiert wird und Sie den Grund suchen.

8.6 Ausnahmen je Gerät

Manchmal braucht ein einzelnes Gerät eine Sonderregel, ohne dass gleich die ganze Filtergruppe geändert werden soll. Dafür gibt es auf der Geräte-Seite zwei Einstellungen:

- **Diese Ausnahmen zulassen:** Sie wählen eine Whitelist, deren Adressen für dieses Gerät trotz Filtergruppe immer erreichbar sind. Praktisch, wenn der Webfilter eine Seite blockiert, die genau ein Familienmitglied braucht.
- **Nur Ausnahmen erlauben:** die strengste Betriebsart, gedacht für Fernseher, Kameras und andere Haustechnik. Das Gerät darf dann ausschließlich die Adressen der gewählten Whitelist erreichen, alles andere ist zu. Wählen Sie unbedingt zuerst die Whitelist aus: Ist der Schalter an, ohne dass eine Ausnahmeliste zugewiesen wurde, erreicht das Gerät überhaupt nichts mehr. Um Umgehungsversuche über moderne Übertragungsverfahren müssen Sie sich dabei nicht kümmern, die sperrt die TrutzBox ab Werk netzweit.

8.7 Die Sperrseite verstehen

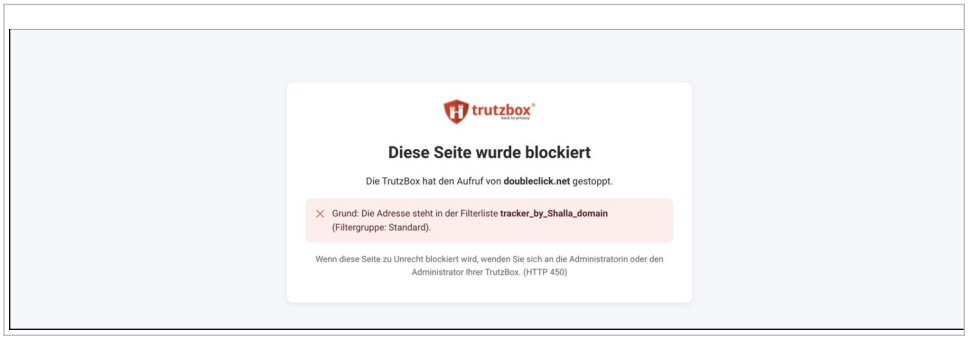


Abbildung 8-7: Die Sperrseite der TrutzBox nennt die blockierte Adresse, die Filterliste und die Filtergruppe. (© 2026 Comidio GmbH)

Blockiert der Webfilter einen Seitenaufruf, kann die TrutzBox eine eigene Sperrseite anzeigen, in der Sprache, die der Browser anfordert. Sie nennt die blockierte Adresse und den Grund, also Filterliste, Filtergruppe und die Regel, die zugeschlagen hat. Mit dem Grund in der Hand ist eine Ausnahme schnell eingerichtet.

Diese Seite erscheint allerdings nur dort, wo die TrutzBox in die Verbindung hineinsehen darf: bei unverschlüsselten Seiten und bei verschlüsselten Seiten mit eingeschaltetem TrutzBrowse. Der Normalfall ist heute eine verschlüsselte Seite ohne TrutzBrowse; dort weist die TrutzBox schon den Verbindungsaufbau ab, und für eine Hinweisseite gibt es keinen Kanal. Der Browser meldet dann nur einen allgemeinen Verbindungsfehler. Das ist keine Störung, sondern die Folge davon, dass die TrutzBox verschlüsselte Verbindungen ohne TrutzBrowse nicht aufbricht.

Apps außerhalb des Browsers zeigen ohnehin keine Sperrseite, sondern melden nur einen Fehler oder gar nichts. Ob hinter einem Verbindungsfehler eine TrutzBox-Sperre steckt, verrät in jedem Fall ein Blick in den Monitor (Kapitel „Monitor und Statistiken“).

8.8 Ein Vorschlag für den Anfang

Wer neu einsteigt, fährt mit dieser Aufteilung erfahrungsgemäß gut:

Gerätegruppe	Filtergruppe	Warum
Erwachsene: PC, Laptop, Telefon	Standard	Blockiert Werbung, Dienste, die aufzeichnen, was man tut, Spionage-Software und Kostenfallen, lässt aber alles Übrige durch. Guter Alltagsschutz ohne Nebenwirkungen und ohne Vorbereitung am Gerät.
Kinder und Jugendliche	Passende Altersgruppe	Zusätzlich altersgerechte Inhaltsfilter. Die Gruppe wächst einfach mit: Alle paar Jahre eine Stufe höher setzen.
Fernseher, Lautsprecher, Konsolen	Eigene Gruppe „TV"	Diese Geräte schicken besonders viele Daten an ihre Hersteller. Die Themen „Werbung" und „Tracker" konsequent sperren, den Rest beobachten.
Haustechnik: Thermostate, Kameras, Steckdosen	Eigene Gruppe „IoT", auf Wunsch „Nur Ausnahmen erlauben"	Solche Geräte brauchen meist nur eine Handvoll Server. Alles andere zu sperren senkt die Angriffsfläche erheblich.
Gastgeräte	Standard oder Konservativ	Schutz ohne Eingriff am fremden Gerät; ein Zertifikat wird dafür nicht benötigt. „Konservativ" sperrt zusätzlich etwa Glücksspiel, Gewalt und Pornografie.

Die Anonymisierung TrutzBrowse taucht in dieser Tabelle bewusst nicht auf. Sie ist ein Werkzeug für erfahrene Anwender, die bereit sind, dafür Ausnahmen zu pflegen: Sie verlangt das Root-Zertifikat auf jedem Gerät, und auf den strengen Stufen (L1 und nahe daran) funktionieren manche Seiten erst, wenn Sie den Slider für diese Seite weiter nach rechts schieben. Was sie leistet und für wen sie sich eignet, steht in Kapitel „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“.

Beobachten Sie danach eine Woche lang den Monitor. Was auffällig oft blockiert wird und trotzdem gebraucht wird, kommt in eine Whitelist; was durchgelassen wird und niemand braucht, kommt in eine Sperrliste. Nach zwei, drei solchen Runden passt die Einstellung.

8.9 Eigene Sperren und Ausnahmen

Was Sie im Monitor oder von Hand für alle Geräte gesperrt oder freigegeben haben, steht gesammelt unter **Verwaltung → Eigene Sperren und Ausnahmen**. Hier legen Sie auch neue Einträge an, ohne zu wissen, in welche Liste sie gehören: Die TrutzBox sortiert sie selbst ein. Eigene Listen, die Sie unter Filterlisten anlegen (Abschnitt „Filterlisten aus dem Internet laden und automatisch aktualisieren“), erscheinen hier nicht.

Menüpfad: Verwaltung → Eigene Sperren und Ausnahmen

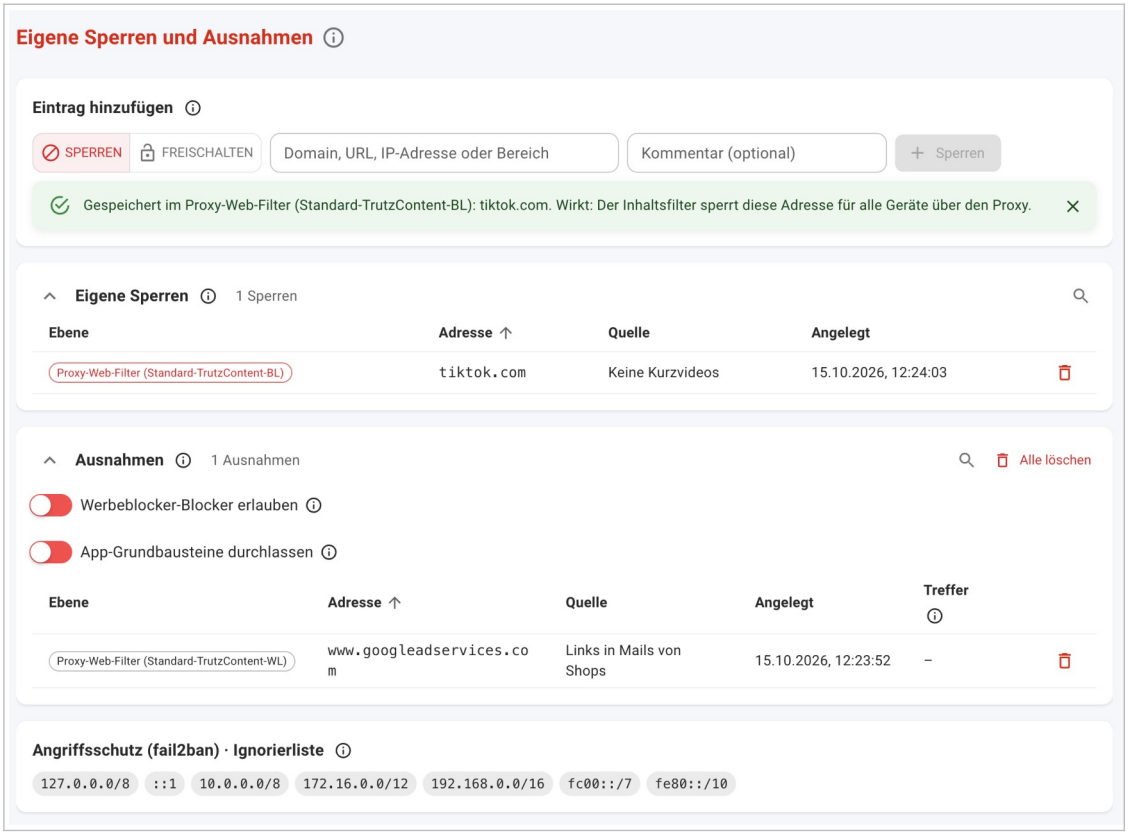


Abbildung 8-8: Die Seite „Eigene Sperren und Ausnahmen" mit einer eigenen Sperre im Webfilter (tiktok.com), einer Ausnahme und den beiden Schaltern für mitgelieferte Ausnahmen, beide aus. (© 2026 Comidio GmbH)

Die Seite hat vier Bereiche:

- **Eintrag hinzufügen:** Links wählen Sie **Sperren** oder **Freischalten**. Ins Feld „Domain, URL, IP-Adresse oder Bereich" tragen Sie die Adresse ein, etwa `tiktok.com`, oder einen ganzen Adressbereich wie `203.0.113.0/24`. Ein Kommentar ist freiwillig und erscheint später in der Spalte „Quelle". Die Eingabe entscheidet, wohin der Eintrag gehört: Ein Name oder eine Adresse mit Pfad kommt in den Webfilter (Standard-TrutzContent-BL zum Sperren, Standard-TrutzContent-WL zum Freischalten), eine IP-Adresse oder ein Bereich in die Firewall (IP-Blockliste oder Ausnahme dazu). Der Webfilter wirkt für alle Geräte, deren Verkehr über den Proxy läuft, die Firewall für alle Geräte auch ohne Proxy. Die Meldung nach dem Speichern nennt den Ort und was der Eintrag bewirkt.
- **Eigene Sperren:** alle Sperren, die Sie selbst angelegt haben, mit Ebene, Adresse, Quelle und Zeitpunkt. Mitgelieferte Filterlisten, importierte IP-Listen und Sperren des Angriffsschutzes stehen hier nicht. Der Papierkorb am Zeilenende hebt eine Sperre wieder auf.
- **Ausnahmen:** alle Freigaben, die trotz Sperrlisten durchgelassen werden, also die Einträge der Standard-TrutzContent-WL und die Ausnahmen der Firewall zur IP-Blockliste. Die Spalte „Treffer" zählt bei Firewall-Ausnahmen, wie viele Pakete die Ausnahme seit dem letzten Neuladen der Firewall durchgelassen hat. **Alle löschen** entfernt nach einer Rückfrage alle eigenen Ausnahmen auf einmal; Webfilter und Firewall sperren diese Adressen danach wieder. Die mitgelieferten Einträge der beiden Schalter (siehe unten) bleiben dabei stehen.

- **Angriffsschutz (fail2ban) · Ignorierliste:** Adressen, die der Angriffsschutz nie sperrt, etwa die privaten Adressbereiche lokaler Netze. Die Liste ist nur zum Lesen da; eigene Einträge legen Sie in den Einstellungen des Angriffsschutzes an (Kapitel „Angriffsschutz: Firewall und Wächter“).

Die Karten Eigene Sperren und Ausnahmen sind zunächst zugeklappt, weil sie lang werden können; der Pfeil links öffnet sie. Die Lupe rechts öffnet ein Suchfeld für die jeweilige Karte. Tippen Sie dort eine IP-Adresse ein, sagt die Seite zusätzlich, ob ein Bereich der IP-Blockliste sie sperrt oder eine Ausnahme sie freigibt, auch wenn die Adresse selbst in keiner Zeile steht. Hat ein Gerät eine eigene Ausnahmeliste (Abschnitt „Ausnahmen je Gerät“), erscheint außerdem die Karte „Geräte mit eigenen Ausnahmen" zum Nachlesen.

> **Freigabe im Webfilter, Sperre in der Firewall**
> Steht ein Dienst zusätzlich mit Server-Adressen auf der IP-Blockliste der Firewall, etwa weil Sie den Server im Monitor gesperrt oder eine Adressliste eingespielt haben, und geben Sie seinen Namen im Webfilter frei, warnt die Seite, dass die Firewall die Adressen dahinter weiter sperrt, und bietet je Adresse den Knopf **Firewall-Ausnahme anlegen** an.

Mitgelieferte Ausnahmen: zwei Schalter

In der Karte Ausnahmen sitzen zwei Schalter. Beide tragen eine kleine, von Comidio gepflegte Liste von Diensten als Ausnahmen in die Standard-TrutzContent-WL ein. Die Einträge stehen dann ganz normal in der Tabelle, mit eigener Herkunft in der Spalte „Quelle", und lassen sich einzeln löschen. Ausschalten nimmt nur diese mitgelieferten Einträge wieder heraus; was Sie selbst eingetragen haben, bleibt.

- **App-Grundbausteine durchlassen:** Viele Apps starten nicht oder bleiben auf einem weißen Bildschirm stehen, solange zwei Dienste gesperrt sind. Der eine ist die Firebase-Kennung von Google, ohne die eine App ihre Starteinstellungen nicht lädt. Der andere ist die Schnittstelle von RevenueCat, über die Apps Abos und Käufe abwickeln. Sperrlisten führen beide als Dienste, die aufzeichnen, was man tut, deshalb sperrt die TrutzBox sie. Eingeschaltet trägt sie genau diese zwei Adressen als Ausnahmen ein, mit der Herkunft „Mitgeliefert: App-Grundbausteine". Reine Messdienste, die nur auswerten, wie eine App benutzt wird, bleiben gesperrt. Ab Werk ist der Schalter aus.
- **Werbeblocker-Blocker erlauben:** Manche Nachrichtenseiten zeigen statt ihres Inhalts nur eine Sperrseite, sobald ihre Prüfdienste gegen Werbeblocker gesperrt sind. Eingeschaltet trägt die TrutzBox diese Dienste als Ausnahmen ein, mit der Herkunft „Mitgeliefert: Werbeblocker-Blocker". Auf den betroffenen Seiten erscheint dann wieder ein Teil der Werbung. Ab Werk ist der Schalter aus. Sparsamer ist die Seitenanalyse im Monitor: Sie gibt für eine einzelne Seite nur frei, was diese wirklich braucht (Abschnitt „Eine Seite zeigt eine Sperrseite: die Seitenanalyse“).

Löschen Sie einen mitgelieferten Eintrag, während sein Schalter an ist, warnt die Seite vorher: Der Schalter bleibt an, der Eintrag bleibt weg. Unter dem Schalter steht dann, wie viele mitgelieferte Einträge fehlen, und der Knopf **Wiederherstellen** holt sie zurück.

Häufige Fragen zum Webfilter

Eine Seite wird zu Unrecht blockiert. Was tun?

Am schnellsten über den Monitor: Eintrag suchen, auf das Schild-Symbol klicken, **Freischalten** wählen. Die Adresse landet in der Standard-TrutzContent-WL und ist sofort wieder erreichbar. Alternativ tragen Sie die Adresse unter Eigene Sperren und Ausnahmen mit **Freischalten** ein (Abschnitt „Eigene Sperren und Ausnahmen“).

Kann mein Kind die Filterung umgehen?

Nicht über die Einstellungen: Die liegen auf der TrutzBox, nicht auf dem Gerät, und nur der Administrator kann sie ändern. Auch die beliebten Schleichwege über das eigene Netz sind zu: Fremde DNS-Server fängt die TrutzBox ab, und das QUIC-Protokoll ist ab Werk im gesamten Netz gesperrt. Offen bleibt, was an der TrutzBox vorbeiführt, etwa die mobilen Daten eines Smartphones oder das WLAN des Routers. Deshalb gehört ein Kindergerät ins interne Netz der TrutzBox, und das Router-WLAN sollte für Kinder tabu sein (Kapitel „Ein Gerät mit der TrutzBox absichern“).

Verlangsamen die Filterlisten das Internet?

Im Alltag nicht merklich. Die Prüfung läuft in Echtzeit im Hauptspeicher der TrutzBox. Was zusätzliche Listen tatsächlich kosten, ist Speicher des Webfilters; deshalb nennt die Seite Filtergruppen beim Einschalten von Listen den Bedarf und warnt, bevor es knapp wird (Abschnitt „Filterlisten aus dem Internet laden und automatisch aktualisieren“).

Kann ich für ein einzelnes Gerät Internetzeiten festlegen, etwa „kein Netz nach 21 Uhr"?

Gerätebezogene Zeitfenster gibt es derzeit nicht. Der Webfilter entscheidet nach Inhalt, nicht nach Uhrzeit. Zwei Wege führen trotzdem zum Ziel: Ein Wochenplan im TrutzBox-WLAN schaltet das Funknetz zu festen Zeiten ab, allerdings für alle Geräte darin gleichzeitig (Kapitel „Das WLAN der TrutzBox“). Und der Internetzugang eines einzelnen Geräts lässt sich auf der Geräte-Seite jederzeit von Hand entziehen und später wieder freigeben (Kapitel „Gäste und gemeinsam genutzte Geräte“). Für Kindergeräte ist in der Praxis die Kombination üblich: eine altersgerechte Filtergruppe für den Inhalt und der Wochenplan für die Nacht.

9 Monitor und Statistiken

Der **Monitor** ist das Fenster in Ihr Netzwerk: Er zeigt in Echtzeit, welche Geräte mit welchen Internet-Servern kommunizieren, was der Webfilter erlaubt oder blockiert und welche Zugriffe die Firewall abwehrt. Was sonst unsichtbar im Hintergrund passiert, wird hier zum Bild. Sie finden ihn im Menü direkt unter der **Übersicht** als **Monitor**.

Alle Aufzeichnungen entstehen und bleiben ausschließlich auf Ihrer TrutzBox. Nichts davon wird an Comidio übertragen, und über die Speicherdauer bestimmen Sie selbst. Nur wenn Sie den Schalter IP-Infos aus dem Internet ergänzen einschalten (Abschnitt „Zeitraum und Speicherdauer“), fragt die TrutzBox zu den gerade angezeigten Server-Adressen die öffentlichen Registrierungsdienste ab; Angaben über Ihre Geräte verlassen die TrutzBox dabei nicht.

> **Anleitung zum Anklicken**
>
> Neben den Führungen in der Seite selbst gibt es einen Rundgang zum Anschauen. Die Anleitung „Bedienung des Monitors" zeigt die Stationen dieses Kapitels mit Bild, Text und Ton im Browser: trutzbox.de/videodokumentation.

9.1 Die eingebauten Führungen: Hilfe direkt in der Seite

Der Monitor bringt seine eigene Anleitung mit. Neben der Überschrift sitzt ein „i", der Knopf **Hilfe öffnen**; beim ersten Aufruf und wenn die Hilfe neue Inhalte bekommen hat, pulsiert ein blauer Ring darum. Ein Klick öffnet das Fenster **Hilfe & Führungen**. Oben steht, was man im Monitor machen kann, darunter folgen 28 Themen in sechs Abschnitten: „Typische Fälle", „Leicht zu übersehen", „Erste Schritte", „Geräte und Server untersuchen", „Sperren und freischalten" und „Blasendiagramm". Unter „Typische Fälle" stehen fertige Wege für häufige Fragen, etwa „Eine App oder Webseite funktioniert nicht" oder „Das Internet ist langsam: Wer überträgt viel?".

Jedes Thema läuft als Führung auf dem echten Bildschirminhalt: Die Seite wird abgedunkelt, das jeweilige Bedienelement bleibt hell, ein gezeichneter Mauszeiger fährt dorthin, und eine Sprechblase erklärt in ein bis zwei Sätzen, was passiert. Wer das markierte Element selbst anklickt, springt automatisch zum nächsten Schritt. Gehört ein Thema zu einer anderen Darstellung, fragt die Hilfe, ob sie dorthin wechseln soll. Beenden lässt sich eine Führung jederzeit mit dem Schließkreuz oder der Esc-Taste. Da die Führungen auf die tatsächlichen Bedienelemente zeigen, bleiben sie auch nach Software-Updates der Oberfläche aktuell. Dieses Kapitel gibt Ihnen das Grundverständnis; die Feinheiten zeigt Ihnen die TrutzBox am lebenden Objekt selbst.

Menüpfad: Monitor

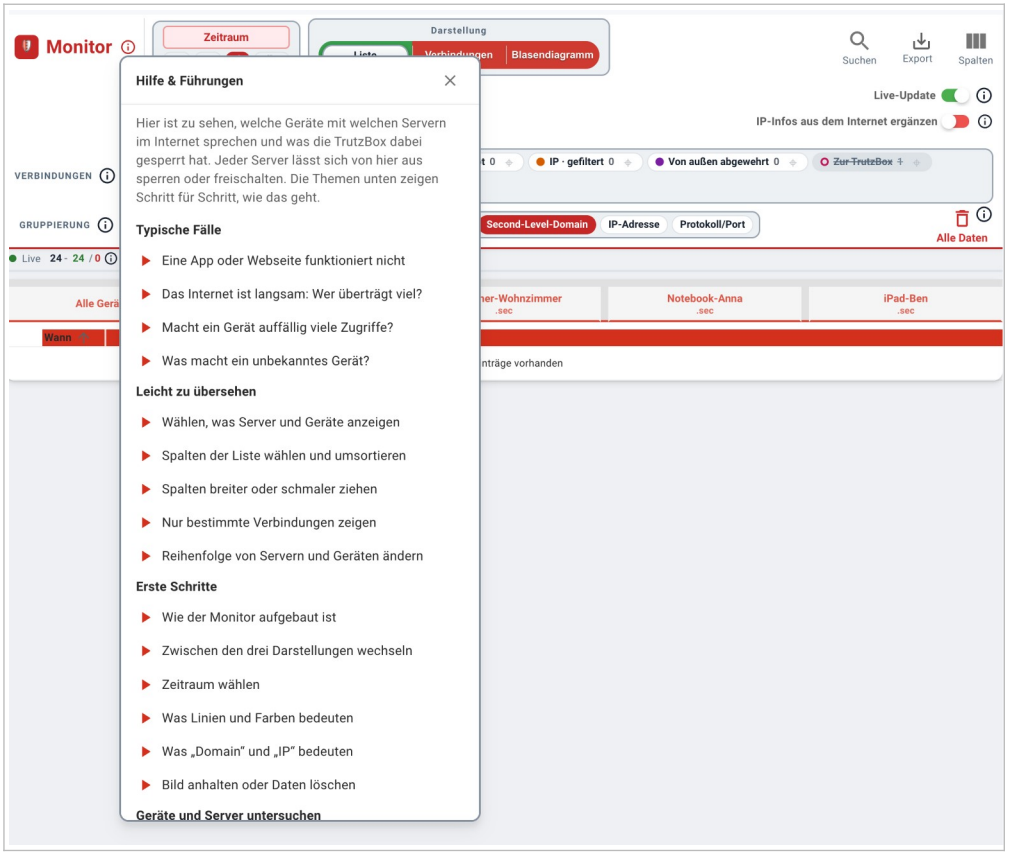


Abbildung 9-1: Das Fenster „Hilfe & Führungen": oben, was man im Monitor machen kann, darunter die Themen, nach Abschnitten geordnet. (© 2026 Comidio GmbH)

9.2 Der Aufbau: Geräte, TrutzBox, Internet

Menüpfad: Monitor → Verbindungen

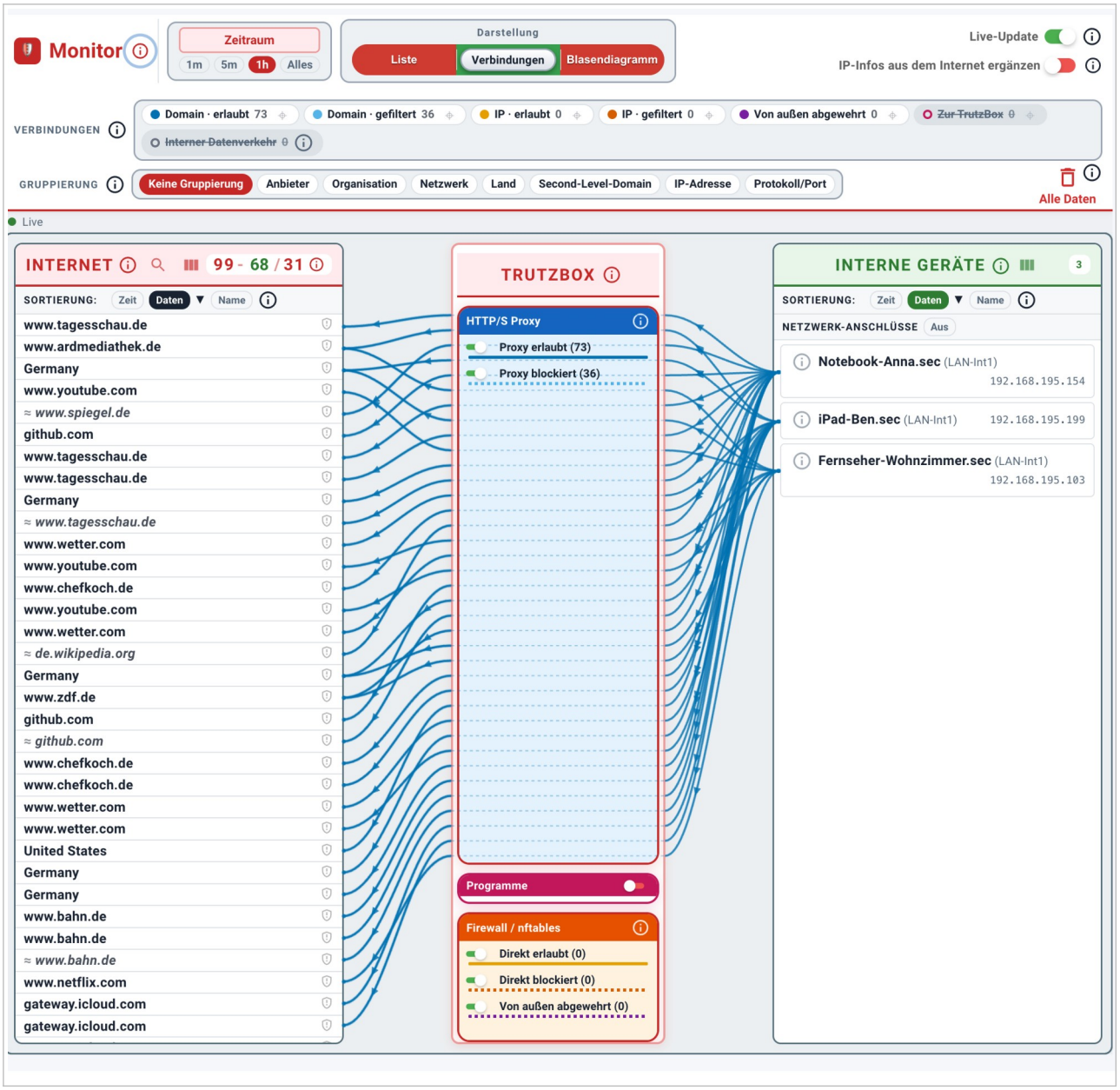


Abbildung 9-2: Die Darstellung „Verbindungen" mit drei Geräten: links die Server im Internet, in der Mitte die TrutzBox, rechts die eigenen Geräte, nach Datenmenge sortiert. (© 2026 Comidio GmbH)

Die Darstellung **Verbindungen** zeigt das Grundprinzip am deutlichsten, in drei Spalten:

- Rechts die **Geräte im eigenen Netz**. Die Zahl im Kopf der Spalte sagt, wie viele Geräte im gewählten Zeitraum aktiv waren. Hinter dem Namen steht in Klammern der Anschluss, etwa „LAN-Int1". Der Schalter **Netzwerk-Anschlüsse** im Kopf der Spalte ordnet die Geräte nach Anschluss: das LAN getrennt nach Anschlussbuchse („LAN-Int1", „LAN-Int2"), dazu WLAN und VPN-Tunnel. Zwei Gruppen fallen aus der Reihe: „Ext. Netz" für Geräte, die im vorgelagerten Netz am Router hängen und die TrutzBox als Proxy nutzen, und „Sonstige" für alles, was sich keiner Anschlussart zuordnen lässt.

- In der Mitte die **TrutzBox**: Gateway, Proxy und Firewall in einem. Jede Verbindung läuft hier durch und wird geprüft. Zwei Schalterbereiche stehen für die zwei Prüfstationen: oben der HTTP/S-Proxy, unten die Firewall. Dazwischen liegt die Karte **Programme** für den Verkehr der TrutzBox selbst.
- Links die **Gegenstellen im Internet**. Voreingestellt ist **Keine Gruppierung**, jede Gegenstelle steht also zunächst für sich. Über das Feld **Gruppierung** fassen Sie sie nach einem von sieben Merkmalen zusammen: Anbieter, Organisation, Netzwerk, Land, Second-Level-Domain (google.com), IP-Adresse oder Protokoll/Port. Die letzte Gruppierung zeigt auf einen Blick, welcher Verkehr am Webfilter vorbeiläuft. Die Zahl in Klammern nennt dann, wie viele Server hinter einem Eintrag stecken.

Geräte im VPN: Geräte, die über den VPN-Zugang verbunden sind, tragen im Monitor den Namen ihres Zugangs, zum Beispiel `iphone.vpn.sec (VPN)` statt einer bloßen Zahlenadresse. Bei WireGuard ist das der Gerätename, den Sie beim Anlegen des Zugangs eingetragen haben, bei OpenVPN der vordere Teil der TrutzMail-Adresse des Benutzers, dem der Zugang gehört (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

Private Adressen hinter dem Router: Manche Gegenstellen haben eine private Adresse, wie sie sonst nur in lokalen Netzen vorkommt, liegen aber nicht in Ihrem Netz. Ein Beispiel ist der Server, über den Ihr Anbieter die Telefonie abwickelt. Solche Ziele erreicht die TrutzBox nur über den Router, deshalb stehen sie links in der Internet-Spalte und nicht als Gerät unter „Ext. Netz". So bleibt auch der Kontakt zu diesen Servern im Monitor sichtbar.

Warum heißen manche Verbindungen „Domain" und andere „IP"? Über den Proxy laufen die Verbindungen, bei denen die TrutzBox den Namen der Gegenstelle kennt; nur dort kann nach Domain gefiltert werden. Alles andere, etwa verschlüsselte Apps und Spielkonsolen, läuft direkt durch die Firewall, und dort ist nur die IP-Adresse sichtbar. Die Zeile Verbindungen unterscheidet entsprechend sieben Arten, jede mit Farbpunkt und Zahl: „Domain · erlaubt", „Domain · gefiltert", „IP · erlaubt", „IP · gefiltert", „Von außen abgewehrt", also Zugriffe aus dem Internet, die die Firewall verworfen hat, dazu „Zur TrutzBox" für den Verkehr mit der TrutzBox selbst, etwa Namensauflösung oder Mail, und „Interner Datenverkehr" zwischen zwei eigenen Geräten. Ein Klick auf einen Eintrag blendet diese Art aus, ein zweiter wieder ein; der kleine Knopf rechts daneben zeigt nur diese eine Art. „Zur TrutzBox" ist ab Werk ausgeblendet. Was ein Browser mit der Oberfläche der TrutzBox austauscht, zeichnet der Monitor gar nicht auf und zählt es nicht mit. Ein Gerät, auf dem nur die Oberfläche offen ist, gilt deshalb nicht als aktiv.

Linien und Farben: Jede Linie ist eine Verbindung. Durchgezogen heißt durchgelassen, gestrichelt heißt blockiert. Die Farbe sagt, welchen Weg die Verbindung genommen hat: Blau steht für den Weg über den Proxy (gesperrte Zugriffe in hellerem Blau), Gelb für erlaubte und Orange für blockierte direkte Verbindungen, Violett für von außen Abgewehrtes und Magenta für den Verkehr, den die TrutzBox selbst erzeugt, etwa beim Abholen von Software-Updates. Alle Linien sind gleich dick; wie viele Daten fließen, zeigen die Felder „Datenmenge im Zeitraum" und „Verlaufskurve mit aktueller Rate" (siehe unten). Was die drei Zahlen im Kopf der Spalte Internet bedeuten, steht in Abschnitt „Untersuchen und eingreifen“.



Abbildung 9-3: Die Legende der Verbindungsansicht: Farbe und Linienart auf einen Blick. (© 2026 Comidio GmbH)

Interner Datenverkehr: Gemeint ist der Verkehr zwischen zwei Geräten im Netz der TrutzBox, auch zwischen WLAN und Kabel, etwa wenn ein Rechner auf den Netzspeicher zugreift oder ein Handy den Drucker anspricht. Anders als die Zugriffe über den Webfilter und die Sperren der Firewall zeichnet die TrutzBox ihn nur auf, solange der Monitor offen ist (Abschnitt „Zeitraum und Speicherdauer“). Der Punkt **Interner Datenverkehr** in der Zeile Verbindungen blendet diese Zeilen nur ein und aus. Wollen Sie ausschließlich den internen Verkehr sehen, schalten Sie die übrigen Punkte aus.

Felder anzeigen: Was an einem Server oder Gerät steht, wählen Sie selbst. Der Knopf mit den drei Balken neben der Lupe im Kopf der Spalte Internet öffnet das Menü **Felder anzeigen**. Zur Wahl stehen Name, Symbol für die Art des Dienstes, Land (Flagge), Dienst mit Namen, Organisation oder Anbieter, IP-Adresse, Protokoll und Port, Datenmenge im Zeitraum, Zuletzt gesehen und Verlaufskurve mit aktueller Rate. Derselbe Knopf im Kopf der Spalte Interne Geräte bietet für die Geräte Name, IP-Adresse, Hersteller, MAC-Adresse, Betriebssystem (vermutet), Datenmenge im Zeitraum, Zuletzt gesehen, Zahl der Internet-Server, Davon gefiltert und Verlaufskurve mit aktueller Rate. Ab Werk zeigt ein Server in „Verbindungen" nur seinen Namen, im Blasendiagramm Name, Symbol und Land; ein Gerät zeigt Name und IP-Adresse. **Alle anzeigen** hakt alles an, **Grundeinstellung** stellt den Anfangszustand wieder her. Die Auswahl gilt je Darstellung und bleibt in diesem Browser gespeichert.

Das Symbol für die Art des Dienstes, etwa Video und Streaming, Handel und Essen oder Werbung und Messung, stammt aus einem mitgelieferten Verzeichnis gebräuchlicher Dienste; das Feld „Dienst mit Namen" schreibt den Dienst aus. Eine Wolke statt einer Flagge heißt: Der Server gehört zu einem weltweiten Netz ohne festen Standort.

Menüpfad: Monitor → Verbindungen → Felder anzeigen

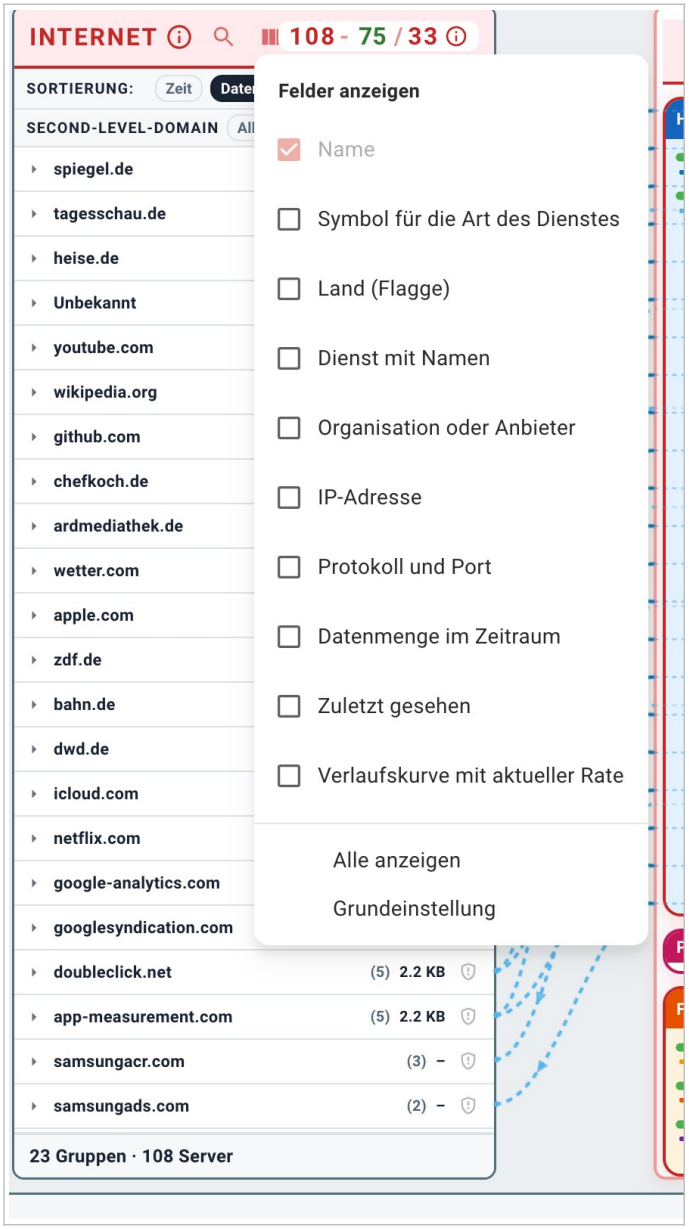


Abbildung 9-4: Das Menü „Felder anzeigen" an der Spalte Internet: Ab Werk ist nur der Name angehakt. (© 2026 Comidio GmbH)

9.3 Die drei Darstellungen

Derselbe Datenbestand lässt sich über den Umschalter **Darstellung** auf drei Arten ansehen: **Liste**, **Verbindungen** und **Blasendiagramm**. Der gewählte Zeitraum bleibt beim Wechsel erhalten. Jede Darstellung hat ihre eigene Stärke und ihre eigenen Handgriffe.

Liste: das Protokoll zum Nachschlagen

Menüpfad: Monitor → Liste

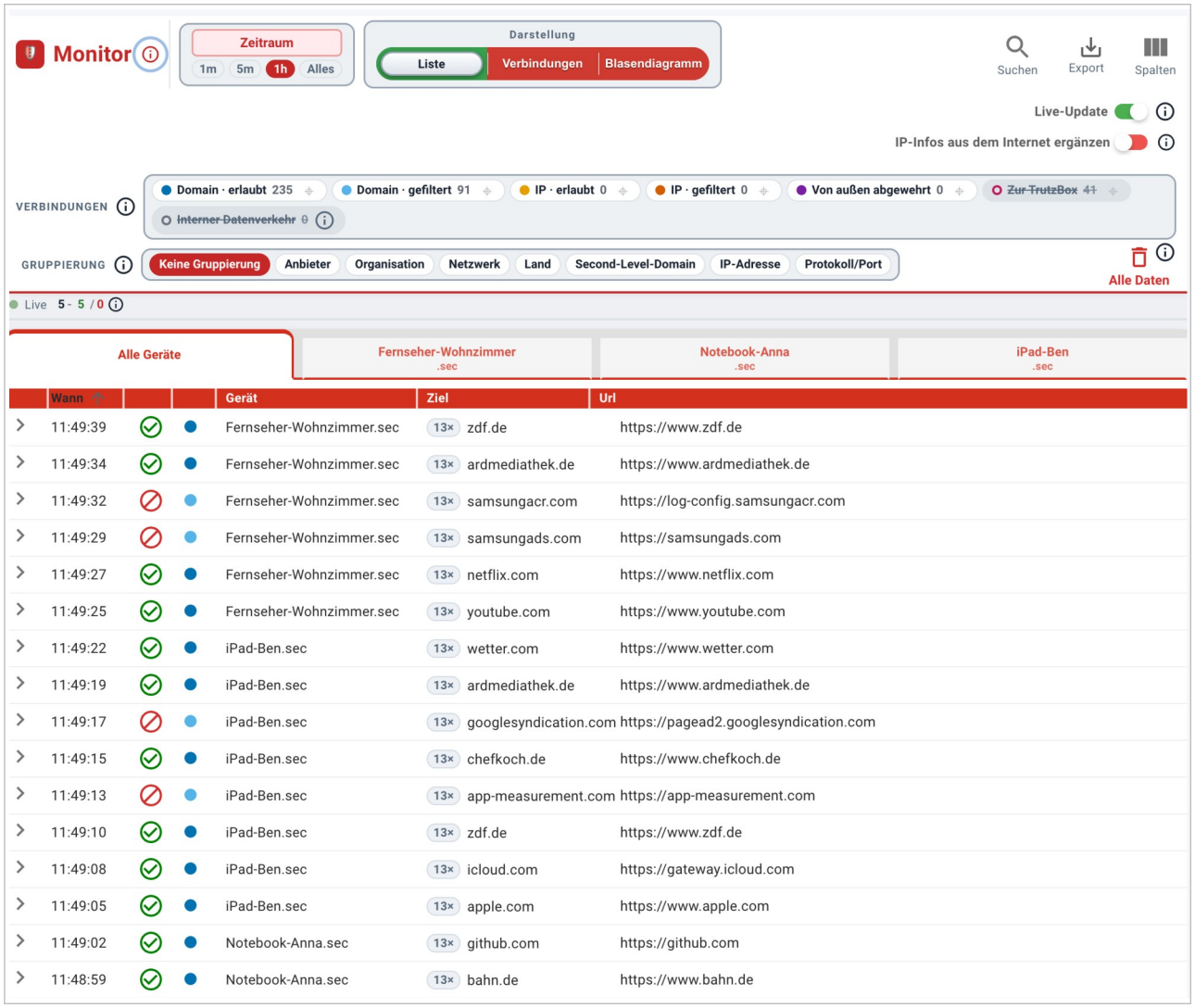


Abbildung 9-5: Die Darstellung „Liste": jeder Zugriff eine Zeile mit Zeit, Ergebnis, Art der Verbindung, Gerät, Ziel und Adresse; rechts oben die Knöpfe „Suchen", „Export" und „Spalten". (© 2026 Comidio GmbH)

Die Liste ist das tabellarische Protokoll aller Zugriffe und die richtige Wahl, wenn Sie etwas Bestimmtes suchen. Ihre Handgriffe:

- Rechts oben sitzen drei Knöpfe: **Suchen** durchsucht Gerät, Adresse und Ziel, **Export** lädt das Protokoll als CSV-Datei zur Auswertung herunter, und **Spalten** öffnet das Menü **Spalten anzeigen**.
- Im Menü **Spalten anzeigen** schalten Sie Spalten zu und ab: Zeit, Ergebnis, Art der Verbindung, Land, Anbieter, Organisation, Netzwerk, Protokoll und Port, IP-Adresse, Anzahl gleicher Zugriffe und die HTTP-Methode (GET, POST, CONNECT), die als Spalte „Methode" erscheint. Angeboten werden nur Spalten, für die die Liste gerade Werte hat. Die Auswahl gilt je Gruppierung und bleibt in diesem Browser gespeichert.

- Einen **Spaltenkopf** ziehen Sie mit der Maus nach links oder rechts, um die Reihenfolge zu ändern; auch sie bleibt gespeichert. Ein Klick auf einen Spaltenkopf sortiert; voreingestellt sind die neuesten Einträge oben.
- Je Gerät gibt es einen **Reiter**; „Alle Geräte" zeigt alles. Der Papierkorb im Reiter eines Geräts löscht nach Rückfrage, was zu diesem Gerät aufgezeichnet ist.
- Ein Klick auf den grünen Haken oder das rote Verbotsschild einer Zeile öffnet das Sperren oder Freischalten dieser Adresse, ein Klick auf den farbigen Punkt die Einzelheiten der Verbindung, ein Klick auf das **Ziel** die Einzelheiten des Servers.

Ohne TrutzBrowse zeigt jede Zeile das Ergebnis des Webfilters TrutzContent. Stehen in der Liste Zugriffe von Geräten mit eingeschaltetem TrutzBrowse, kommt eine Spalte für TrutzBrowse hinzu: Ihre Farbe zeigt die tatsächlich wirksame Slider-Stufe, und ein Zahlenpaar wie „3 | 17" sagt, dass drei von siebzehn Hintergrund-Zugriffen der Seite blockiert wurden. Ein Klick darauf verstellt die Stufe für genau diesen Server, und der Pfeil am Zeilenanfang klappt die einzelnen Hintergrund-Zugriffe auf (Kapitel „Den Nutzen im Monitor sehen“). Alle weiteren Einzelheiten der Listen-Darstellung beschreibt das TrutzBox-Kompendium.

Verbindungen: das Bild zum Verstehen und Eingreifen

Das Spaltenbild aus Abschnitt „Der Aufbau: Geräte, TrutzBox, Internet“ ist die Ansicht für gezielte Eingriffe:

- Die **Schalter in der TrutzBox-Säule** blenden die einzelnen Verbindungsarten ein und aus, getrennt nach erlaubt und blockiert für Proxy und Firewall. So reduzieren Sie das Bild auf genau die Frage, die Sie gerade haben, etwa nur auf das Blockierte.
- Ein Klick auf eine **Gerätekarte** rechts hebt nur dessen Linien hervor; ein zweiter Klick hebt das wieder auf. Dasselbe funktioniert mit den Einträgen der Karte **Programme** für den Verkehr der TrutzBox selbst.
- Ein Klick auf eine **Linie** heftet die Kurzinfo zu genau dieser Verbindung an.
- Die **grüne Zahl** im Kopf der Spalte Internet sperrt alle gerade angezeigten Server auf einmal, und zwar für alle Geräte (Abschnitt „Untersuchen und eingreifen“).
- Über die **Lupe** in der Internet-Spalte filtern Sie nach Namen. Die **Sortierung** wechselt in beiden Spalten zwischen Zeit, Daten und Name; ein zweiter Klick kehrt die Reihenfolge um.
- Mit dem Schalter **Netzwerk-Anschlüsse** bekommt jeder Anschluss (LAN, WLAN, externes Netz, VPN) eine eigene aufklappbare Karte, und die Geräte stehen darunter. Ist bei den Geräten zusätzlich das Feld „Verlaufskurve mit aktueller Rate" angehakt, zeigt jede Anschluss-Karte ihre eigene Kurve und Rate. Das beantwortet eine Frage, die sonst schwer zu greifen ist: Wie viel läuft eigentlich über das Funknetz, wie viel über Kabel?

Blasendiagramm: Ausreißer entdecken

Menüpfad: Monitor → Blasendiagramm

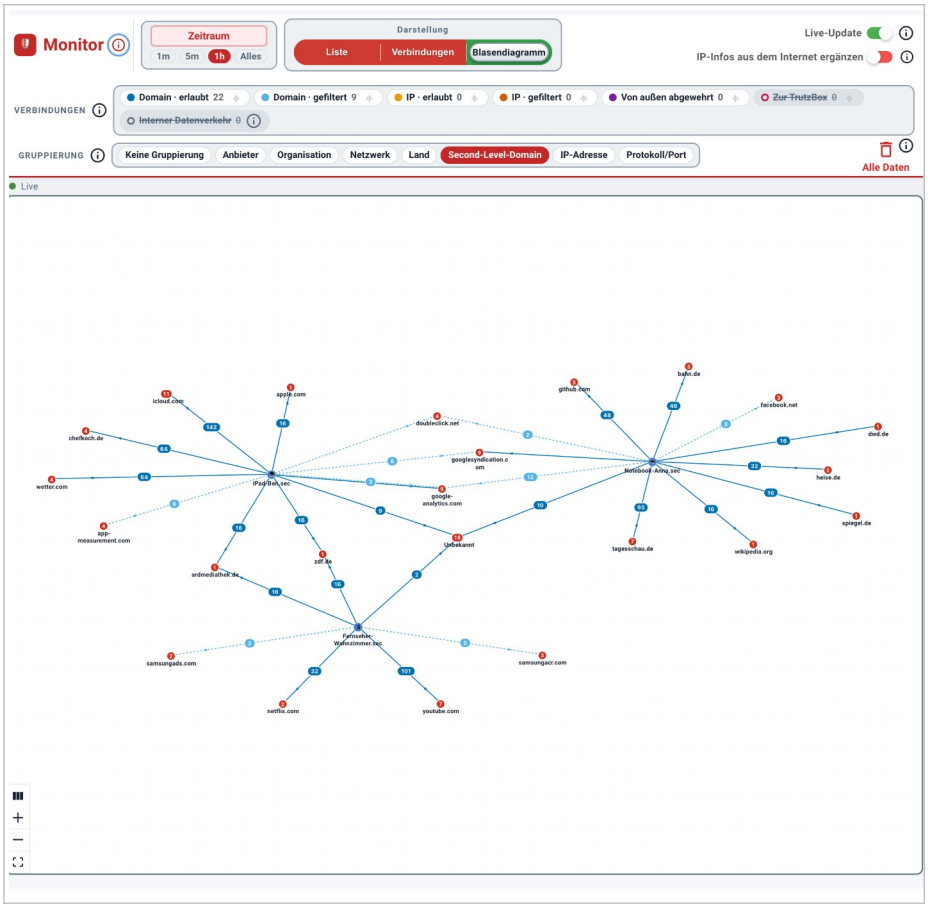


Abbildung 9-6: Das Blasendiagramm, nach Second-Level-Domain gruppiert: drei Geräte mit ihren Servern. Die rote Zahl an einem Server nennt die zusammengefassten Server, die Zahl auf einer Linie die Zugriffe. (© 2026 Comidio GmbH)

Geräte sind runde blaue Blasen, Server eckige orange Blasen mit abgerundeten Ecken. In einer Server-Blase steht das Symbol für die Art des Dienstes, an ihrer Ecke, soweit bekannt, die Flagge des Landes; welche Angaben eine Blase trägt, wählen Sie mit dem Knopf für Felder anzeigen. Ist „Zur TrutzBox" eingeblendet, erscheint auch die TrutzBox als Kasten mit rotem Rand, darin ihre Programme. Die Zahl auf einer Linie zählt die Zugriffe zwischen den beiden Blasen, ab zwei. Ist gruppiert, nennt die rote Zahl an einer Server-Blase, wie viele Server darin zusammengefasst sind. Nirgends fällt schneller auf, wenn ein Fernseher in zehn Länder telefoniert. Die Bedienung ist die einer Landkarte:

- Mit dem **Mausrad** zoomen Sie, mit gedrückter **linker Maustaste** verschieben Sie die Fläche oder eine einzelne Blase. Einmal verschobene Blasen bleiben liegen, auch wenn neue Daten eintreffen. Unten links sitzen Knöpfe zum Vergrößern, zum Verkleinern und zum Einpassen des ganzen Bildes, darüber der Knopf für Felder anzeigen.
- Mit der **rechten Maustaste** greifen Sie ein Gerät mitsamt allen verbundenen Blasen und ziehen die ganze Gruppe an eine freie Stelle. So entwirren Sie ein volles Bild in Sekunden.
- Ein **Klick auf eine Blase** blendet alles aus, was nicht mit ihr verbunden ist; ein Klick ins Leere holt das volle Bild zurück. Ein Klick auf eine **Verbindungslinie** öffnet die Einzelheiten.

- Bei sehr vielen Servern schlägt die Ansicht von selbst vor, nach Second-Level-Domain zu gruppieren; ein Klick auf den Vorschlag genügt.

9.4 Zeitraum und Speicherdauer

Zwei Einstellungen werden gern verwechselt: Der **Anzeigezeitraum** ist der Ausschnitt, den Sie gerade sehen; die Schnellwahl bietet 1 Minute, 5 Minuten, 1 Stunde oder alles Gespeicherte und steht voreingestellt auf 5 Minuten, und unter **Zeitraum** ziehen Sie den Ausschnitt frei durch die Vergangenheit. Die **Speicherdauer** dagegen bestimmt, wie lange die TrutzBox die Daten überhaupt aufhebt: Aus, 10 Minuten, 1 Stunde, 6 Stunden oder 24 Stunden, danach wird automatisch gelöscht. Weiter zurückzuschauen als die Speicherdauer ist naturgemäß nicht möglich.

Genau deshalb sind Schnellwahl-Knöpfe gesperrt, deren Ausschnitt länger ist als die eingestellte Speicherdauer. Wer trotzdem einen Zeitraum wählt, für den nichts vorliegt, bekommt die Meldung „Warte auf Daten…" zu sehen. Sie besagt nicht, dass etwas kaputt ist, sondern dass für diesen Ausschnitt noch keine Aufzeichnungen existieren.

Steht die Speicherdauer auf **Aus**, sammelt die TrutzBox nichts. Die Oberfläche schreibt es an dieser Stelle selbst hin: „Speicherung deaktiviert, nur Live-Ansicht (RAM, letzte 10 min)". Sie sehen dann also das laufende Geschehen, aber es bleibt nichts davon übrig, was sich später auswerten ließe.

Wer **Live-Update** ausschaltet, hält das Bild an; aufgezeichnet wird weiter. **IP-Infos aus dem Internet ergänzen** blendet Land, Anbieter und Organisation zu jeder Gegenstelle ein; dazu fragt die TrutzBox die öffentlichen Registrierungsdienste nach den angezeigten Server-Adressen, erst nach einer Rückfrage. **Alle Daten** löscht die Aufzeichnungen nach Rückfrage unwiderruflich; aufgezeichnet wird danach einfach weiter.

Was läuft, wenn niemand hinsieht? Die Übersicht der bestehenden Verbindungen und die Zähler der Anschlüsse erfasst die TrutzBox nur, solange die Monitor-Ansicht geöffnet ist. Unabhängig davon schreibt sie jedes Ereignis der Firewall mit und protokolliert jeden Zugriff über den Webfilter. Blockierte Zugriffe landen also auch dann in der Aufzeichnung, wenn gerade niemand zusieht; wer dagegen den laufenden Verkehr eines Geräts beobachten will, lässt den Monitor dabei offen.

9.5 Untersuchen und eingreifen

Der Monitor zeigt nicht nur, er lässt Sie auch handeln:

- **Ein Gerät analysieren:** Klick auf die Gerätekarte rechts, und nur noch dessen Linien bleiben stehen. So sehen Sie auf einen Blick, wohin genau dieses Gerät spricht. Zweiter Klick hebt die Auswahl auf.
- **Eine Verbindung verstehen:** Klick auf eine Linie öffnet die Erklärung: Gegenstelle, Anwendung, Datenmenge und bei blockierten Verbindungen die Regel oder Filterliste, die zugeschlagen hat, in Klartext unter „Was bedeutet das?". Darüber stehen gleich die Knöpfe zum Sperren und Freischalten, dieselben wie im Menü Sperren / Freischalten (siehe unten).
- **Auffälliges erkennen:** Manche Gegenstellen tragen zusätzlich das Abzeichen „Scan-Versuch erkannt". Es bedeutet schlicht, dass sämtliche Verbindungen zu dieser IP-Adresse blockiert wurden, und ist ein Hinweis zum Nachsehen. Einen Port-Scan erkennt es nicht. Bei einem Port-Scan klopft ein fremder Rechner der Reihe nach viele Ports ab, also die nummerierten

Zugänge, über die ein Rechner seine Dienste anbietet, und sucht so nach einem offenen Dienst. Die eigentliche Erkennung solcher Scanner sitzt beim Angriffsschutz (Kapitel „Angriffsschutz: Firewall und Wächter“) und speist dieses Abzeichen nicht.

Einen Server aus dem Monitor heraus sperren

Fällt Ihnen im Monitor eine Gegenstelle auf, die dort nichts zu suchen hat, brauchen Sie die Filterlisten gar nicht zu öffnen:

1. Klicken Sie in der Darstellung Verbindungen auf das Schild-Symbol an der betreffenden Gegenstelle. Ist gruppiert und kein Schild zu sehen, klappen Sie die Gruppe zuerst mit dem kleinen Dreieck auf. Es öffnet sich das Menü **Sperren / Freischalten**; es nennt auch, auf welcher Ihrer Listen die Adresse schon steht. In der Liste führt ein Klick auf den grünen Haken der Zeile zum selben Ziel.
2. Klicken Sie auf **Sperren** und bestätigen Sie die Rückfrage; sie nennt vorher, was geschieht. Gehört die Adresse zu einer größeren Domain, wählen Sie dort, ob die ganze Domain oder nur diese Adresse gesperrt wird. Den Namen trägt die TrutzBox in die Liste *Standard-TrutzContent-BL* ein; er ist ab sofort für alle Geräte gesperrt, deren Verkehr über den Proxy läuft (Kapitel „Filterlisten verwalten“). Kennt sie keinen Namen oder lief die Verbindung am Proxy vorbei, sperrt sie die IP-Adresse in der Firewall, für alle Geräte.
3. Umgekehrt funktioniert es genauso: Wurde etwas zu Unrecht blockiert, gibt **Freischalten** im selben Menü die Adresse wieder frei; sie landet dann in der Ausnahmeliste *Standard-TrutzContent-WL*.

Alle so angelegten Sperren und Freigaben stehen danach unter Eigene Sperren und Ausnahmen (Kapitel „Eigene Sperren und Ausnahmen“). Aufheben lassen sie sich dort oder im selben Menü mit **Sperre aufheben** beziehungsweise **Freigabe aufheben**. Lädt eine Seite nicht richtig, bietet das Menü außerdem **Analysieren** an, die Seitenanalyse (Abschnitt „Eine Seite zeigt eine Sperrseite: die Seitenanalyse“).

Die drei Zahlen neben Internet

In der Verbindungs-Darstellung stehen im Kopf der Spalte Internet, neben der Überschrift **Internet**, drei Zahlen: die Gesamtzahl der Gegenstellen im gewählten Zeitraum, davon in Grün die erreichten und in Rot die blockierten. Die grüne Zahl ist zugleich eine Schaltfläche: Ein Klick darauf öffnet das Fenster **Angezeigte IPs blockieren** mit allen gerade angezeigten, noch nicht gesperrten Servern. Einzelne Einträge nehmen Sie dort mit dem Kreuz aus der Liste; erst der Knopf zum Blockieren trägt die übrigen Adressen in die IP-Blockliste der Firewall ein. Diese Sperre gilt für alle Geräte, nicht nur für das gerade ausgewählte, und kann auch Dienste treffen, die andere Geräte brauchen, etwa von Google oder Apple. Grenzen Sie das Bild deshalb vorher mit den Schaltern, der Suche oder einem Klick auf das Gerät auf das Gewünschte ein. Dann ist das der schnellste Weg, eine ganze Gruppe unerwünschter Kontakte auf einmal zu sperren.

> **Der IoT-Check für neue Geräte**
>
> Neues Smart-Gerät im Haus? Schließen Sie es an, öffnen Sie den Monitor, wählen Sie das Gerät aus und schauen Sie ihm eine Viertelstunde zu: Mit welchen Servern in welchen Ländern spricht es? Was davon braucht es wirklich? Alles Überflüssige sperren Sie direkt aus der Ansicht heraus.

9.6 Drei Fragen, die der Monitor beantwortet

„Was macht dieses Gerät eigentlich den ganzen Tag?" In der Darstellung Verbindungen die Gerätekarte anklicken und den Zeitraum auf „1h" stellen. Links stehen dann nur noch die Server, die das Gerät kontaktiert hat; mit dem Feld „Datenmenge im Zeitraum" auch, wie viele Daten dabei flossen. Wie oft es einen Server aufgerufen hat, zeigt die Liste im Reiter des Geräts mit der Spalte „Anzahl gleicher Zugriffe". Bei einem Fernseher ist die Liste oft überraschend lang; jeder Eintrag, der nicht zum eigentlichen Zweck gehört, ist ein Kandidat für die Sperrliste.

„Warum wurde diese Seite blockiert?" In der Listen-Darstellung nach der Adresse suchen, auf die Zeile klicken. Die Erklärung nennt die Filterliste oder Regel, die zugeschlagen hat, und bietet gleich das Freigeben an. Das ist der schnellste Weg von einer Fehlermeldung zur Lösung.

„Wer verbraucht mein Datenvolumen?" Durch diese Frage führt auch die eingebaute Hilfe mit dem Thema „Das Internet ist langsam: Wer überträgt viel?" (Abschnitt „Die eingebauten Führungen: Hilfe direkt in der Seite“). Von Hand sind es vier Schritte:

1. Wählen Sie die Darstellung **Verbindungen** und den Zeitraum: „1m" oder „5m" für das, was gerade läuft, „1h" oder „Alles" für die letzten Stunden. Weiter als die Speicherdauer reicht der Blick nicht zurück (Abschnitt „Zeitraum und Speicherdauer“).
2. Wählen Sie bei den Geräten die Sortierung **Daten**. Das Gerät mit den meisten Daten steht dann oben.
3. Öffnen Sie bei den Geräten **Felder anzeigen** und haken Sie „Datenmenge im Zeitraum" und „Verlaufskurve mit aktueller Rate" an. Dann steht an jedem Gerät, wie viel es überträgt.
4. Klicken Sie das oberste Gerät an. Links stehen dann nur noch seine Server. Wählen Sie auch dort die Sortierung **Daten**: Oben steht der Server, mit dem das Gerät die meisten Daten austauscht.

Meist ist es Video, gelegentlich aber auch ein Gerät, das im Hintergrund unbemerkt Daten überträgt, etwa ein laufendes Backup. Wie viel über das Funknetz und wie viel über Kabel läuft, zeigt der Schalter Netzwerk-Anschlüsse (Abschnitt „Die drei Darstellungen“).

9.7 Statistiken: Blockierungen über lange Zeiträume

Der Monitor zeigt das Jetzt und die letzten Stunden. Für die lange Sicht gibt es **Verwaltung → Statistiken**: eine Übersicht aller *blockierten* Verbindungen, getrennt nach Webfilter-Blockierungen (Proxy) und Firewall-Blockierungen, mit den Zahlen für „Letzte 60 Minuten", „Heute", „Diesen Monat" und „Insgesamt" sowie einem Diagramm „Blockierungen pro Tag". „Letzte 60 Minuten" zählt gleitend die Stunde bis eben, „Heute" ab Mitternacht; kurz nach Mitternacht kann die erste Zahl deshalb größer sein als die zweite.

Zwei Reiter schlüsseln auf: **Ziele** zeigt, welche Adressen am häufigsten blockiert wurden; **Geräte** zeigt, welches Gerät wie viele Blockierungen ausgelöst hat. Über den Reitern sitzt der Umschalter **Beides** / **Proxy** / **Firewall**: Er bestimmt, ob beide Herkünfte zusammen ausgewertet werden oder nur die Blockierungen des Webfilters oder nur die der Firewall. Das ist der schnellste Weg zu der

Frage, ob eine auffällige Zahl vom Webfilter oder von der Firewall stammt. Ein Klick auf ein Ziel verrät, welche Geräte es wie oft aufgerufen haben.

Die Statistik ein- und ausschalten

Ab Werk zeichnet die TrutzBox die Statistik auf; die ersten Zahlen erscheinen wenige Minuten nach dem Setup, das Tagesdiagramm füllt sich über die nächsten Tage. Wer keine Statistik möchte, schaltet sie ab:

1. Öffnen Sie **Verwaltung → Statistiken**.
2. Schalten Sie **Statistiken speichern** aus. Ab diesem Moment zählt die TrutzBox nicht mehr mit.

Zum Aufräumen dient auf derselben Seite **Zurücksetzen**: Es löscht alle bisher gesammelten Statistikdaten und beginnt bei null. Die Aufzeichnung selbst läuft danach weiter.

Einzelne Server sperren oder freigeben Sie nicht hier, sondern im Monitor (Abschnitt „Untersuchen und eingreifen“).

9.8 Eine Seite zeigt eine Sperrseite: die Seitenanalyse

Manche Seiten zeigen statt ihres Inhalts nur einen Hinweis: „Bitte schalten Sie Ihren Werbeblocker aus." Die Seite hat gemerkt, dass die TrutzBox ihre Werbetechnik sperrt, und weigert sich. Meist nutzen solche Seiten dafür einen fremden Dienst, einen sogenannten Werbeblocker-Blocker. Die Seitenanalyse findet heraus, welche Adresse die Sperre auslöst, und schlägt die kleinste Freigabe vor, mit der die Seite wieder läuft. Mehr als nötig gibt sie nie frei.

Menüpfad: Monitor → Sperren / Freischalten → Analysieren

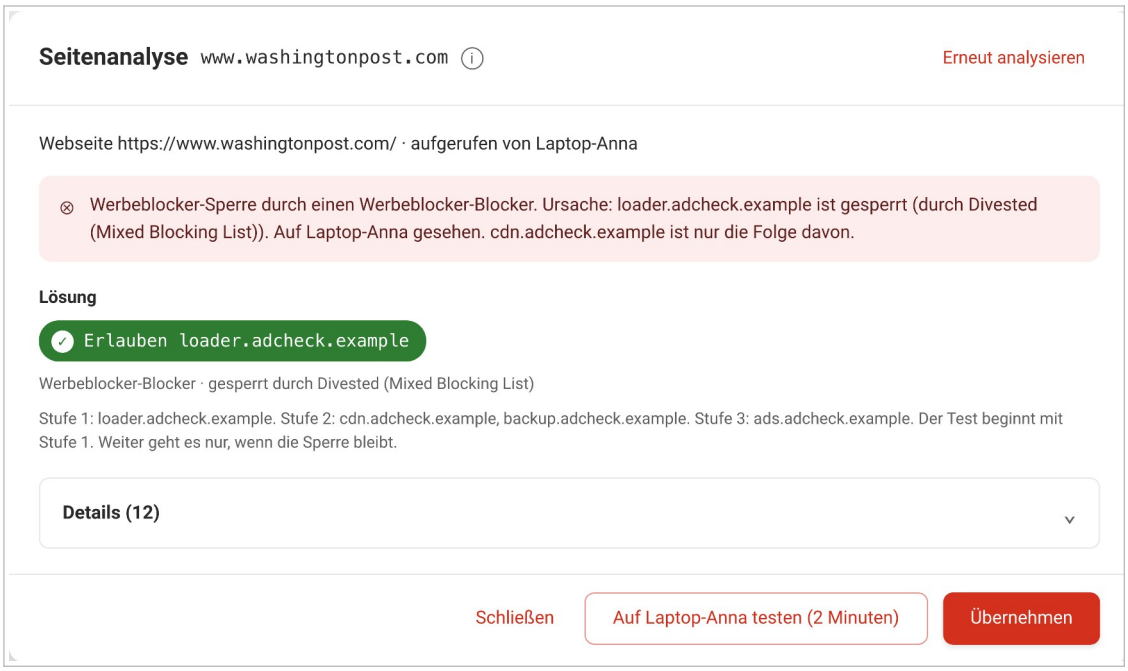


Abbildung 9-7: Die Seitenanalyse: oben das Ergebnis in einem Satz, darunter die Lösung, alles Weitere unter „Details". (© 2026 Comidio GmbH)

Analysieren

1. Klicken Sie im Monitor auf die Seite, die nicht lädt, oder auf eine der Adressen, die sie nachlädt. Im Menü **Sperren / Freischalten** wählen Sie **Analysieren**.
2. Die TrutzBox sucht das Gerät, das die Seite aufgerufen hat, ruft die Seite ab, liest deren Ladeskripte und prüft die Adressen gegen Ihre Listen. Den Fortschritt sehen Sie im Dialog; nach wenigen Sekunden steht das Ergebnis.
3. Oben steht das Ergebnis in einem Satz, im Bild für die Seite www.washingtonpost.com zum Beispiel: „Werbeblocker-Sperre durch einen Werbeblocker-Blocker. Ursache: loader.adcheck.example ist gesperrt. Auf Laptop-Anna gesehen." Die Adressen im Bild sind nur Beispiele; welche Dienste eine Seite tatsächlich nutzt, zeigt erst die Analyse auf Ihrer TrutzBox. Darunter folgt unter **Lösung** die vorgeschlagene Freigabe. Alles Weitere, etwa weitere Vorschläge und Hinweise zur Seite, liegt zusammengeklappt unter **Details**.

Die Lösung ist bereits angekreuzt. Meist ist es eine einzige Adresse. Weitere Adressen, die der Dienst vielleicht noch braucht, hält die TrutzBox in Stufen bereit und nennt sie unter der Lösung, zum Beispiel: „Stufe 1: loader.adcheck.example. Stufe 2: cdn.adcheck.example, … Stufe 3: ads.adcheck.example."

Testen, bevor Sie etwas eintragen

Eine Freigabe gilt für alle Geräte. Darum probieren Sie die Lösung erst aus: Klicken Sie **Auf Laptop-Anna testen (2 Minuten)**. Die Freigabe gilt dann zwei Minuten lang nur für dieses eine Gerät, und nichts wird eingetragen.

1. Tippen Sie auf dem Gerät die Adresse der Seite neu ein. Laden Sie nicht die Sperrseite neu, die lädt sich nur immer wieder selbst. Auf Geräten mit TrutzBrowse lädt die Seite von allein neu.
2. Erscheint die Seite: Klicken Sie **Seite funktioniert: Behalten**. Die TrutzBox trägt genau diese Freigabe ein, nicht mehr.
3. Bleibt die Sperrseite: Klicken Sie **Sperre bleibt: Stufe 2**. Die TrutzBox gibt die nächste Gruppe von Adressen frei, verlängert den Test um 30 Sekunden, und Sie tippen die Adresse erneut ein. Bis zu drei Stufen sind möglich. So sehen Sie, welche Stufe wirklich nötig ist.
4. Klicken Sie nichts, ist nach Ablauf der Zeit alles wieder wie vorher. **Rückgängig** beendet den Test sofort.

> **Nach dem Eintragen: Cache des Browsers leeren**
>
> Der Werbeblocker-Blocker merkt sich im Browser bis zu vier Stunden lang, dass er gesperrt war, und zeigt so lange weiter die Sperrseite, obwohl die TrutzBox längst freigibt. Leeren Sie nach „Behalten" oder „Übernehmen" den Cache des Browsers auf dem Gerät und öffnen Sie die Seite neu. Umgekehrt gilt dasselbe: Läuft eine Seite nach dem Test scheinbar weiter, obwohl nichts eingetragen wurde, hat der Browser das Skript noch aus der Testzeit.

Übernehmen trägt die angekreuzte Lösung ohne Test ein. Alle Einträge der Seitenanalyse landen in der Ausnahmeliste *Standard-TrutzContent-WL* (Kapitel „Filterlisten verwalten“) mit der Seite als Herkunft, im Beispiel „Seitenanalyse: washingtonpost.com", und lassen sich dort jederzeit wieder

löschen. Wer alle bekannten Werbeblocker-Blocker auf einmal freigeben möchte, findet dafür den Schalter „Werbeblocker-Blocker erlauben" unter Eigene Sperren und Ausnahmen (Kapitel „Eigene Sperren und Ausnahmen“); er gibt allerdings mehr frei als die Seitenanalyse.

Was die Analyse sonst noch findet

Nicht jede hängende Seite liegt an einem Werbeblocker-Blocker. Die Analyse erkennt weitere Ursachen und sagt es im Ergebnis-Satz:

- **Cookie-Dialog gesperrt:** Die Seite wartet vergeblich auf ihren Einwilligungs-Dienst und bleibt leer. Die Freigabe dieses Dienstes steht als Vorschlag bereit.
- **Die Seite selbst ist gesperrt:** Sie steht auf einer Ihrer Sperrlisten. Die Analyse nennt die Liste und bietet die Freigabe an, nicht vorgewählt.
- **Beim Laden gesperrte Adressen:** Die TrutzBox zählt nur, was zur Seite gehört. Was das Gerät nebenbei anfragt, etwa die Netzprüfung eines Smartphones, steht als „Hintergrundverkehr" nur unter Details.
- **Die Seite prüft selbst, ob Werbenetze laden:** Manche Seiten bringen ihre Prüfung gegen Werbeblocker im eigenen Seitencode mit, ohne fremden Dienst. Die Sperrseite verschwindet dann erst, wenn alle geprüften Werbenetze laden. Die Analyse nennt diese Adressen einzeln und kreuzt keine davon vor: Es sind Netze für Werbung und für die Aufzeichnung dessen, was man tut, und eine Freigabe gilt für alle Geräte.

Dazu kommen Hinweise, die keine Freigabe brauchen, aber gut zu wissen sind: Dienste, die über die eigene Domain der Seite mitschreiben, was Besucher tun, solche Dienste getarnt hinter einer eigenen Subdomain, Fingerprinting (das Wiedererkennen eines Geräts ohne Cookies), eine Weiterleitung auf eine andere Seite, eine Domain mit versteckten Sonderzeichen, ein Formular, das an eine fremde Domain sendet, oder eine Seite aus einer Warnkategorie. Vorschläge zum Sperren sind nie vorgewählt; Sie entscheiden.

> **Warum in Stufen?**
> Ein Werbeblocker-Blocker wie Ad-Shield lädt sein Skript von einer Adresse. Ist sie gesperrt, weicht er auf Ersatzadressen aus. Läuft das Skript, prüft es, ob Werbenetze erreichbar sind, und lädt Werbung über weitere Adressen nach. Die Seitenanalyse liest das Skript und sortiert diese Adressen: die eine, die zuerst geladen wird, die Ersatzadressen, die Nachlade-Adressen. Meist reicht die erste. Ob mehr nötig ist, zeigt nur der Test auf dem Gerät. Deshalb schaltet die TrutzBox nie von allein weiter, sondern erst auf Ihren Klick.

Häufige Fragen zum Monitor

Die Seitenanalyse sagt „nicht gesperrt", der Browser zeigt aber weiter die Sperrseite.

Dann hat der Browser das Skript des Werbeblocker-Blockers noch im Cache und mit ihm die alte Entscheidung. Leeren Sie den Cache des Browsers auf dem Gerät und tippen Sie die Adresse neu ein. Die TrutzBox zeigt den Zustand ihrer Listen, und der stimmt.

Die Seitenanalyse findet kein Gerät.

Die TrutzBox weiß nur von Aufrufen, die über sie gelaufen sind, und merkt sie sich so lange wie die Speicherdauer des Monitors (Kapitel „Zeitraum und Speicherdauer“), ab Werk eine Stunde. Rufen Sie die Seite auf dem Gerät auf und starten Sie die Analyse danach. Ohne Gerät fehlt der Test; „Übernehmen" funktioniert trotzdem.

In der Internet-Spalte stehen Adressen, die mit 10. beginnen. Ist das bedenklich?

Nein. Das sind private Adressen, und in der Internet-Spalte stehen sie, weil der Weg zu ihnen über den Router führt (Abschnitt „Der Aufbau: Geräte, TrutzBox, Internet“). Tauchen viele davon auf einmal auf, steckt meist eine App auf einem Handy dahinter, das per VPN verbunden ist: Apps für Lautsprecher, Drucker oder Smart-Home-Geräte suchen das Netz nach passenden Geräten ab, auch durch den Tunnel. Diese Anfragen laufen ins Leere, weil unter diesen Adressen niemand antwortet. Mit einem Klick auf die Gerätekarte sehen Sie, von welchem Gerät sie kommen. Wer das abstellen möchte, entzieht der App in den Einstellungen des Handys den Zugriff auf das lokale Netzwerk.

Sieht Comidio, was der Monitor aufzeichnet?

Nein. Alle Daten entstehen und bleiben auf Ihrer TrutzBox. Nur wenn Sie den Schalter „IP-Infos aus dem Internet ergänzen" einschalten, fragt die TrutzBox nach Ihrer Zustimmung die öffentlichen Registrierungsdienste zu den angezeigten Server-Adressen ab.

Es wird nichts angezeigt, nur „Warte auf Daten…". Woran liegt das?

Meist ist der Anzeigezeitraum leer, etwa weil gerade erst gelöscht wurde, weil die Speicherdauer auf „Aus" steht oder weil sie kürzer ist als der gewählte Ausschnitt. Prüfen Sie zuerst die Speicherdauer: Schnellwahl-Knöpfe, die über sie hinausreichen, sind gesperrt. Stellen Sie die Schnellwahl dann auf „5m", die Voreinstellung, und erzeugen Sie mit einem Gerät etwas Verkehr; nach wenigen Sekunden erscheinen die ersten Einträge.

Bremst der Monitor die TrutzBox?

Ein Teil der Erfassung läuft dauerhaft, auch ohne geöffnete Monitor-Ansicht (Abschnitt „Zeitraum und Speicherdauer“). Die TrutzBox ist dafür ausgelegt, im Alltag ist davon nichts zu spüren. Längere Speicherdauern kosten zusätzlich etwas Platz, deshalb steht die Voreinstellung nicht auf dem Maximum.

10 TrutzMail: sichere E-Mail

Gewöhnliche E-Mail ist eine Postkarte: unterwegs für viele Stellen lesbar, und selbst wenn der Inhalt verschlüsselt ist, bleibt sichtbar, wer wem wann schreibt. TrutzMail macht daraus einen versiegelten Brief. Ihre TrutzBox ist dabei selbst der Mail-Server: Ihre Post lagert zuhause oder in der Firma bei Ihnen statt bei einem Anbieter, die Verschlüsselung übernimmt die TrutzBox automatisch, und bei Mails zwischen TrutzBoxen werden sogar die Begleitdaten (Metadaten) versteckt. Sichere Adressen erkennen Sie an der Endung `@comidio.email`.

Der Unterschied zum gewohnten Postfach beim großen Anbieter ist damit grundsätzlicher, als es zunächst aussieht. Sie werden zu Ihrem eigenen Mail-Anbieter. Wird ein großer Anbieter aufgebrochen und werden dabei Millionen Adressen samt Passwörtern erbeutet, sind Ihre TrutzMail-Zugangsdaten schlicht nicht dabei, weil sie dort nie lagen. Und weil die geheimen Schlüssel ausschließlich auf Ihrer TrutzBox entstehen und dort bleiben, kann Comidio verschlüsselte Post zwischen TrutzBoxen weder lesen noch herausgeben.

Die TrutzBox gehört eingeschaltet

Ihre TrutzBox ist Ihr eigener Mail-Server. Damit TrutzMails jederzeit ankommen, sollte die TrutzBox durchgehend laufen; sie ist für den Dauerbetrieb gebaut. Ist sie zeitweise aus, geht nichts verloren: Die TrutzBox der Gegenseite versucht die Zustellung über mehrere Tage in regelmäßigen Abständen weiter, bis Ihre TrutzBox wieder erreichbar ist.

Anleitung zum Anklicken

Schlüssel, Status und Webmail einmal gesehen erklären sich leichter. Die Anleitung „TrutzMail und ihre Schlüssel" zeigt die Stationen dieses Kapitels mit Bild, Text und Ton im Browser: trutzbox.de/videodokumentation.

10.1 Drei Wege des Mail-Austauschs

Wie sicher eine E-Mail unterwegs ist, hängt davon ab, welche technischen Möglichkeiten Ihr Kommunikationspartner hat. Es gibt drei Wege, jeder mit eigenen Stärken:

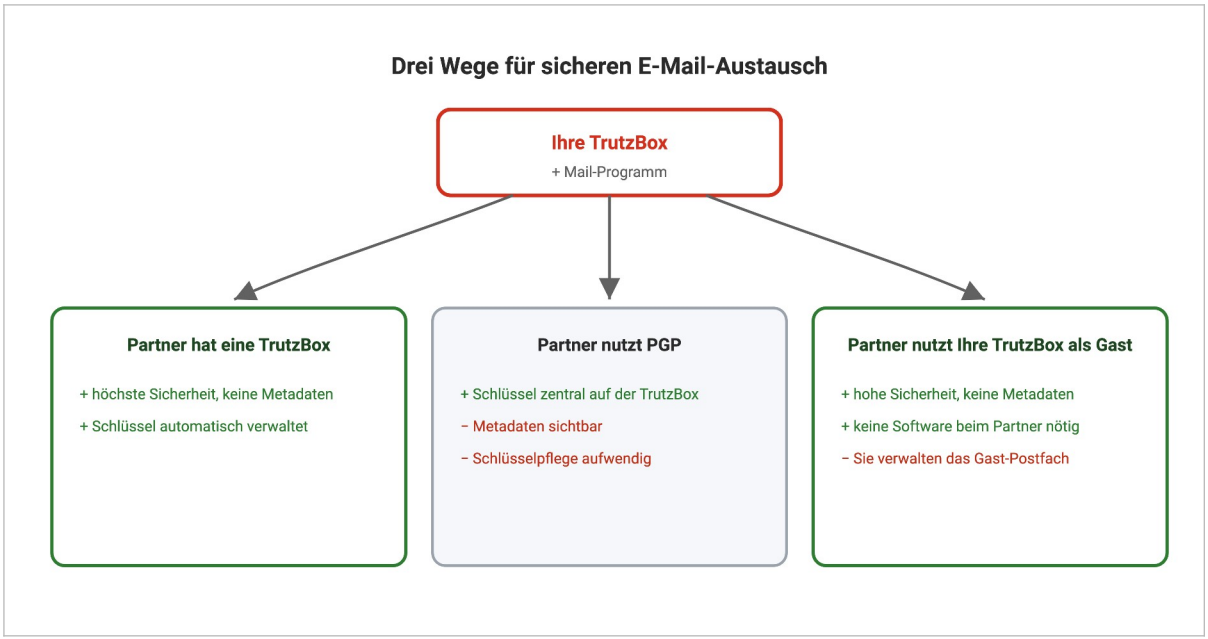


Abbildung 10-1: Drei Wege, je nach Gegenstelle: Partner mit TrutzBox, Partner mit PGP, Partner als Gast auf Ihrer TrutzBox. (© 2026 Comidio GmbH)

Weg A, der Partner hat eine eigene TrutzBox: der Königsweg. Beide schreiben mit ihrem normalen Mail-Programm, und die TrutzBoxen erledigen den Rest: Inhalt und Metadaten verschlüsselt, Absender und Empfänger gegenseitig beglaubigt, Schlüssel vollautomatisch verwaltet. Sie müssen nichts einrichten und nichts wissen; es funktioniert einfach. Die beiden TrutzBoxen finden sich dabei nicht über das offene Internet, sondern über versteckte Adressen im Tor-Netzwerk, und ein zentraler Server ist an der Übertragung nicht beteiligt.

Ein Beispiel aus dem Alltag: Ihre Schwester besitzt ebenfalls eine TrutzBox. Sie schreiben ihr aus Ihrem gewohnten Mail-Programm an ihre Adresse mit der Endung `@comidio.email`. Weder Sie noch sie haben dafür etwas eingerichtet, keine Schlüssel getauscht, keine Erweiterung installiert. In ihrer Antwort steht vor dem Betreff die Kennzeichnung **[SE]**, und daran erkennen Sie: Absender geprüft und verschlüsselt, der ganze Weg über.

Weg B, der Partner nutzt PGP: für Partner ohne TrutzBox, die aber PGP-Verschlüsselung beherrschen (ein offener Standard, den es für alle gängigen Mail-Programme gibt). Die öffentlichen Schlüssel der Partner verwaltet die TrutzBox zentral für Sie, das erspart die PGP-Bastelei am eigenen Rechner. Die Inhalte sind verschlüsselt; sichtbar bleiben allerdings die Metadaten, und die Schlüsselpflege beim Partner bleibt dessen Sache.

Ein Beispiel aus dem Alltag: Ihre Steuerberaterin hat keine TrutzBox, arbeitet aber seit Jahren mit PGP. Sie schickt Ihnen einmalig ihren öffentlichen Schlüssel, Sie hinterlegen ihn in der Schlüsselverwaltung Ihrer TrutzBox. Ab diesem Moment verschlüsselt die TrutzBox jede Mail an sie von selbst, ganz gleich, aus welchem Programm Sie schreiben. Damit sie Ihnen ebenso verschlüsselt antworten kann, laden Sie umgekehrt Ihren eigenen öffentlichen Schlüssel herunter und schicken ihn ihr einmal zu.

Weg C, der Partner nutzt Ihre TrutzBox als Gast: Sie legen dem Partner ein eigenes Benutzerkonto mit TrutzMail-Adresse auf Ihrer TrutzBox an (Kapitel „Benutzer, Postfächer, Passwörter“). Er liest und schreibt dann per Webbrowser über das eingebaute Webmail oder mit seinem Mail-Programm, ganz ohne Zusatzsoftware und Schlüsselwissen. Die Kommunikation

bleibt komplett auf Ihrer TrutzBox, ohne Metadaten nach außen. Dafür verwalten Sie das Konto, und der Partner muss dem Betreiber der TrutzBox, also Ihnen, vertrauen.

Ein Beispiel aus dem Alltag: In Ihrem Verein soll der Vorstand vertraulich korrespondieren. Der Kassenwart möchte sich aber mit Technik nicht beschäftigen. Sie legen ihm ein Konto auf Ihrer TrutzBox an und nennen ihm Adresse und Passwort. Er ruft das Webmail im Browser auf und schreibt los; von unterwegs nutzt er dafür den VPN-Zugang (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Für ihn sieht es aus wie jedes andere Postfach.

Weg	Inhalt geschützt	Metadaten geschützt	Aufwand beim Partner
A: Partner mit TrutzBox	ja, automatisch	ja	keiner
B: Partner mit PGP	ja	nein	PGP im eigenen Programm einrichten und pflegen
C: Partner als Gast auf Ihrer TrutzBox	ja	ja, alles bleibt auf Ihrer TrutzBox	keiner, Sie verwalten das Konto

Und gewöhnliche E-Mail von Absendern ohne TrutzBox? Dafür verbinden Sie die TrutzBox mit Ihrem bisherigen Postfach bei einem Mail-Anbieter (Abschnitt „Weg B einrichten: Postfach beim Anbieter verbinden“). Je nach Einstellung holt sie dort alle Mails oder nur die verschlüsselten ab und legt sie in Ihr TrutzMail-Postfach; unverschlüsselte Mails sind im Betreff markiert. Nur in eine Richtung ist die TrutzBox konsequent streng: *Unverschlüsselt senden kann sie grundsätzlich nicht.* Wer es versucht, bekommt eine Fehlermeldung zurück. Für unverschlüsselte Alltagspost an beliebige Empfänger nutzen Sie Ihre bisherige Mail-Adresse deshalb weiter wie gewohnt; beide lassen sich im selben Mail-Programm nutzen.

10.2 Webmail benutzen

Der schnellste Zugang zu Ihrem Postfach ist der eingebaute Web-Mailer: Öffnen Sie `https://trutzbox/mail` und melden Sie sich mit Ihrer TrutzMail-Adresse und Ihrem Passwort an. Lesen, schreiben, Anhänge, Ordner: alles Gewohnte ist da, von jedem Gerät im internen Netz und unterwegs über den VPN-Zugang (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Technisch steckt dahinter Roundcube, ein weit verbreiteter quelloffener Web-Mailer, der auf der TrutzBox selbst läuft.

Das Webmail ist besonders praktisch für drei Situationen: für den ersten Test einer frisch angelegten Adresse, für Gast-Konten nach Weg C, deren Inhaber gar kein Mail-Programm einrichten möchten, und für den schnellen Blick ins Postfach an einem fremden Gerät, auf dem Sie nichts installieren wollen. Wer dauerhaft viel Post bearbeitet, ist mit dem gewohnten Mail-Programm am Ende meist schneller.

10.3 Ein Mail-Programm einrichten

Genauso gut arbeiten Sie mit Ihrem gewohnten Programm, ob Thunderbird, Outlook oder Apple Mail, am Rechner wie auf Telefon und Tablet. Sie legen darin ein zusätzliches Konto an. Besondere

Erweiterungen braucht es nicht, denn alle Verschlüsselung passiert auf der TrutzBox. Jedes Programm verlangt dieselben Angaben:

Angabe	Wert
Benutzername	die TrutzMail-Adresse
Passwort	das Passwort des TrutzMail-Accounts
Server für Eingang und Ausgang	der Name Ihrer TrutzBox, ab Werk trutzbox
Eingang	IMAP, Port 993, SSL/TLS
Ausgang	SMTP, Port 587, STARTTLS

Die TrutzBox zeigt diese Angaben auch selbst, mit ihrem tatsächlichen Namen: unter **Verwaltung → Benutzer** hinter dem „i" neben der TrutzMail-Adresse. Die Schritte für die einzelnen Programme stehen im Anhang, Kapitel „Mail-Programme für TrutzMail einrichten“. Schicken Sie nach dem Einrichten eine Testmail an die eigene Adresse. Kommt sie an, ist alles richtig.

Zwei Dinge sind zu beachten. Erstens verbindet sich das Mail-Programm direkt mit der TrutzBox, und deshalb muss das Gerät der TrutzBox vertrauen: Auf dem Gerät gehört das Root-Zertifikat installiert (Kapitel „Das Root-Zertifikat installieren“). Ohne es meldet das Programm eine Zertifikatswarnung oder verweigert die Verbindung ganz. Zweitens erreicht das Gerät die TrutzBox unter ihrem Namen im Netz der TrutzBox und im lokalen Netz am Internet-Router. Unterwegs brauchen Sie dafür TrutzVPN (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Ist die VPN-Verbindung aufgebaut, funktioniert das Konto genau wie im Netz der TrutzBox.

Eingang und Ausgang erledigen zwei verschiedene Aufgaben, die auf der TrutzBox auch von zwei getrennten Diensten übernommen werden: Über den Eingangsserver holt Ihr Programm die Post aus dem Postfach ab, über den Ausgangsserver übergibt es neue Nachrichten an die TrutzBox, die sie dann verschlüsselt und weiterschickt. Beide laufen auf Ihrer TrutzBox, deshalb steht bei beiden derselbe Name.

Ihr bisheriges Konto beim alten Anbieter bleibt daneben bestehen. So haben Sie sichere und normale Post im selben Programm. In einem Programm lassen sich auch mehrere TrutzMail-Adressen gleichzeitig einrichten, etwa eine private und eine für den Verein.

> **Warum eine Mail größer ist als ihre Anhänge**
>
> Bevor eine E-Mail verschickt werden kann, müssen Anhänge in reine Textzeichen umcodiert werden, denn nur solche verträgt der Mail-Weg. Dadurch wächst eine Nachricht deutlich über die Summe ihrer Anhänge hinaus. Eine feste Obergrenze gibt es bei TrutzMail nicht, die Grenze setzt der freie Arbeitsspeicher der beteiligten TrutzBoxen. Bei ungewöhnlich großen Sendungen lässt sich deshalb kaum vorhersagen, ob sie durchgehen. Hakt es, hilft meist ein Neustart der TrutzBox, weil der Arbeitsspeicher dabei geleert wird.

10.4 Die Kennzeichnung im Betreff: [SE], [UE], [UU]

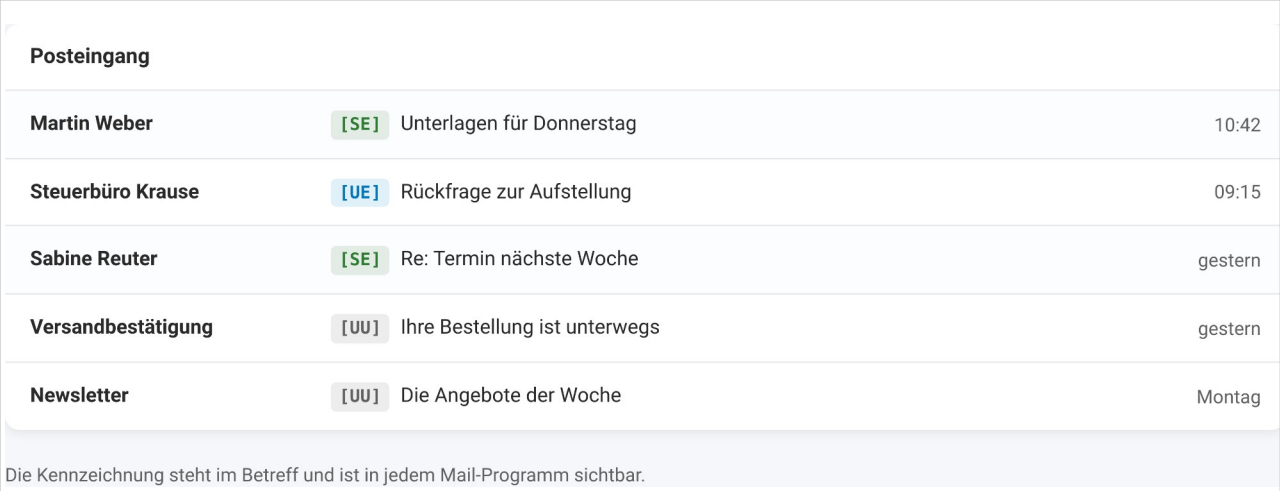


Abbildung 10-2: Die Kennzeichnung im Posteingang: [SE] von TrutzBox zu TrutzBox, [UE] mit PGP, [UU] unverschlüsselt. (© 2026 Comidio GmbH)

Bei jeder eingehenden Mail stellt die TrutzBox dem Betreff zwei Buchstaben in eckigen Klammern voran, damit Sie die Vertrauenswürdigkeit auf einen Blick sehen. Der erste Buchstabe bewertet den Absender: **S** für signiert (Signatur geprüft), **U** für unsigniert. Der zweite die Übertragung: **E** für verschlüsselt (encrypted), **U** für unverschlüsselt.

Kennzeichen	Bedeutung
[SE]	Signiert und verschlüsselt: eine echte TrutzMail von TrutzBox zu TrutzBox. Absender geprüft, Inhalt und Metadaten geschützt.
[UE]	Verschlüsselt, aber Absender nicht geprüft: PGP-Post von Partnern ohne TrutzBox, solange ihr Schlüssel nicht bestätigt ist (Abschnitt „Weg B einrichten: Postfach beim Anbieter verbinden“).
[UU]	Unverschlüsselt und unsigniert: gewöhnliche Post, etwa aus Ihrem Postfach beim Anbieter abgeholt. Behandeln Sie den Inhalt entsprechend, wie eine Postkarte.

Bei **[SE]** sehen Sie im Mail-Programm keinen Signatur-Anhang. Das ist Absicht: Nach erfolgreicher Prüfung entfernt die TrutzBox die Signatur wieder und bestätigt sie stattdessen über das S im Betreff. Bleibt ein sichtbarer Signatur-Anhang stehen, konnte die TrutzBox die Prüfung nicht durchführen. Das S ist ein Prüfergebnis der TrutzBox, keine Beglaubigung. Weil die Signatur danach fehlt, lässt sich die Mail im Postfach nicht mehr unabhängig prüfen; das Original liegt beim Anbieter, solange es dort nicht gelöscht wird (Abschnitt „Weg B einrichten: Postfach beim Anbieter verbinden“).

Kommt von einem TrutzBox-Partner unerwartet einmal [UU] oder [UE] statt [SE], steckt meist ein veralteter Schlüssel dahinter; das korrigiert sich in der Regel automatisch (Abschnitt „Schlüssel und Zertifikate“). Gewöhnliche Post, die die TrutzBox bei Ihrem Anbieter abholt, trägt dagegen immer [UU], und genau dafür ist die Kennzeichnung gedacht: Sie sehen sofort, wie weit Sie dem Absender trauen dürfen, bevor Sie einen Anhang öffnen.

> **Und was ist mit Werbemüll?**

Einen eigenen Spam-Filter hat die TrutzBox nicht. Sie holt die Mail aus dem Posteingang Ihres Anbieters ab, und dessen Spam-Filter hat Werbemüll in der Regel schon vorher in einen eigenen Ordner sortiert. Gewöhnliche Post trägt immer die Kennzeichnung [UU]; daran erkennen Sie sie sofort und können sie im Mail-Programm auch automatisch in einen eigenen Ordner sortieren lassen. Wer nur verschlüsselte Mails abholen lässt, bekommt gewöhnliche Post gar nicht erst ins TrutzMail-Postfach.

Auch eine Größenbegrenzung für Ihr Postfach gibt es nicht. Die Grenze setzt allein der freie Platz auf der TrutzBox, und wie viel das ist, zeigt die Startseite (Kapitel „Die Startseite lesen“).

10.5 Weg B einrichten: Postfach beim Anbieter verbinden

Für Partner ohne TrutzBox verbinden Sie die TrutzBox mit einem Postfach, das Sie ohnehin bei einem Mail-Anbieter haben, etwa bei GMX, IONOS oder Posteo. Darüber sendet sie verschlüsselte Mail an den Partner, und dort holt sie seine Antworten ab. TrutzMail selbst stellt keine Mail an gewöhnliche Adressen zu und nimmt keine von dort an; dafür ist dieses Postfach da.

1. Öffnen Sie **Verwaltung → Benutzer**, klappen Sie den Benutzer auf und gehen Sie zum Bereich **E-Mail-Austausch mit normalen Adressen**. Tragen Sie die **E-Mail-Adresse** und das **Passwort** Ihres Postfachs beim Anbieter ein. Bekannte Anbieter erkennt die TrutzBox an der Adresse und trägt die Server selbst ein. Verlangt der Anbieter ein eigenes App-Passwort, weist die TrutzBox darauf hin und verlinkt die Anleitung.
2. Wählen Sie unter **Mail abholen**, was die TrutzBox aus dem Postfach holt: **alle Mails** (das TrutzMail-Postfach wird zum gemeinsamen Posteingang, unverschlüsselte Mails sind im Betreff markiert), **nur verschlüsselte** (Standard: alles andere bleibt beim Anbieter und lässt sich dort wie gewohnt lesen) oder **nicht abholen** (die TrutzBox sendet nur, Antworten kommen beim Anbieter an).
3. Wählen Sie unter **Beim Anbieter**, was mit einer abgeholten Mail dort geschieht: **behalten** (Standard: die Mail bleibt zusätzlich beim Anbieter, etwa für ein Mail-Programm am Telefon), **abgleichen** (die Mail bleibt beim Anbieter, Löschen und die Markierungen gelesen, beantwortet und markiert übernimmt die TrutzBox jede Minute in beide Richtungen), **löschen nach … Tagen** (1 bis 365 Tage, vorbelegt 14) oder **sofort löschen**. Bei den beiden Wahlen zum Löschen zeigt die TrutzBox einen orangen Hinweis, dass danach beim Anbieter kein Original mehr liegt.
4. Klicken Sie **Speichern und prüfen**. Die TrutzBox meldet sich beim Postausgang an und, wenn Abholen eingeschaltet ist, beim Posteingang. Gespeichert wird nur, wenn beides funktioniert. Danach zeigt der Bereich, mit welchem Postfach die TrutzBox verbunden ist und wie Senden und Abholen stehen; der erste Abruf folgt nach einer Minute.
5. Geben Sie dem Partner Ihren eigenen öffentlichen Schlüssel: Unter **E-Mail → Schlüsselverwaltung** lässt er sich per Klick auf Ihr Konto herunterladen.

Wer Mails als Nachweis aufbewahren muss, wählt „behalten“

Die Mail im TrutzMail-Postfach ist eine bearbeitete Kopie: Verschlüsselte Mail ist entschlüsselt,

die Signatur ist nach der Prüfung entfernt (Abschnitt „Die Kennzeichnung im Betreff: [SE], [UE], [UU]“), und der Betreff trägt das Prüfergebnis. Diese Kopie lässt sich nachträglich nicht mehr unabhängig prüfen. Das unveränderte Original mit der ursprünglichen Signatur liegt nur beim Anbieter, und nur so lange, wie es dort nicht gelöscht wird.

Mit **löschen nach … Tagen** oder **sofort löschen** entfernt die TrutzBox dieses Original. Das gilt für jede abgeholte Mail, auch für unverschlüsselte, wenn **alle Mails** abgeholt werden. Brauchen Sie Mails später als Nachweis, etwa für geschäftliche Post, bleiben Sie bei **behalten**. Das Original rufen Sie dann jederzeit beim Anbieter ab, mit dessen Webmail oder einem Mail-Programm.

Den Schlüssel des Partners sucht die TrutzBox selbst: in seinen Mails und in öffentlichen Schlüsselverzeichnissen, über das Tor-Netzwerk. Einen so gefundenen Schlüssel nutzt sie sofort zum Verschlüsseln. Als Unterschrift gilt er erst, wenn Sie ihn bestätigen; bis dahin beginnt die Kennzeichnung im Betreff mit U, etwa [UE]. Zum Bestätigen vergleichen Sie unter **E-Mail → Schlüsselverwaltung** den Fingerabdruck mit dem Partner, etwa am Telefon, und klicken **Bestätigen**. Schickt Ihnen der Partner seinen Schlüssel als Datei, fügen Sie ihn dort über **Schlüssel hinzufügen** ein; ein so hinzugefügter Schlüssel gilt gleich als bestätigt. Ohne Schlüssel des Empfängers sendet die TrutzBox nicht.

Die Prüfung beim Speichern läuft in Etappen ab und benennt einen Fehler dort, wo er auftritt: beim Namen des Postausgangs, bei der Verbindung, bei der Anmeldung und beim Abholen zusätzlich am Posteingang und beim Öffnen des Ordners. Scheitert es an der Anmeldung, obwohl das Passwort stimmt, ist fast immer das App-Passwort die Lösung. Ob der Anbieter den Versand unter der Adresse auch erlaubt, zeigt **Test-Mail senden**: Die TrutzBox schickt dabei eine echte Mail an Ihre TrutzMail-Adresse. Mit **Ändern** passen Sie die Angaben an, mit **Trennen** lösen Sie die Verbindung; die Mails im TrutzMail-Postfach bleiben erhalten.

Anmeldename und Absenderadresse

Bei den meisten Anbietern meldet man sich mit der E-Mail-Adresse an. Dann bleibt das Feld **Anmeldename** unter **Erweitert** leer, und die TrutzBox verwendet die Adresse für beides. Manche Anbieter, vor allem bei Webhosting-Paketen, vergeben dagegen einen eigenen Anmeldenamen, der keine E-Mail-Adresse ist, etwa eine Kennung aus Buchstaben und Ziffern. Diesen tragen Sie unter **Erweitert** in das Feld **Anmeldename** ein. Dort stehen auch die Server für Postausgang und Posteingang, falls die TrutzBox Ihren Anbieter nicht kennt. In das Feld **E-Mail-Adresse** gehört in jedem Fall die vollständige Absenderadresse mit @ und Domain, denn unter ihr geht die Mail hinaus.

Führen Sie beim Anbieter unter demselben Zugang mehrere Absenderadressen, sogenannte Aliase, tragen Sie diese unter **Erweitert** in das Feld **Weitere Absenderadressen** ein, eine pro Zeile. Wählen Sie im Mail-Programm eine davon als Absender, geht die Mail unter ihr hinaus; alle anderen Mails verschickt die TrutzBox unter der Adresse im Feld **E-Mail-Adresse**. Die Aliase müssen beim Anbieter für dieses Postfach freigeschaltet sein. Mails unter einem Alias sind verschlüsselt, tragen aber keine PGP-Signatur.

Menüpfad: E-Mail → Schlüsselverwaltung

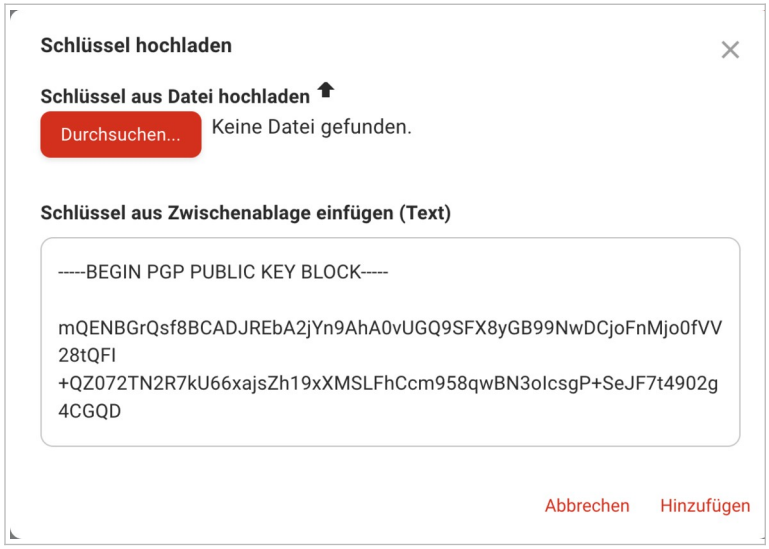


Abbildung 10-3: Den Schlüssel eines Partners hinzufügen: als Datei hochladen oder als Text einfügen. (© 2026 Comidio GmbH)

10.6 Schlüssel und Zertifikate

Menüpfad: E-Mail → Schlüsselverwaltung

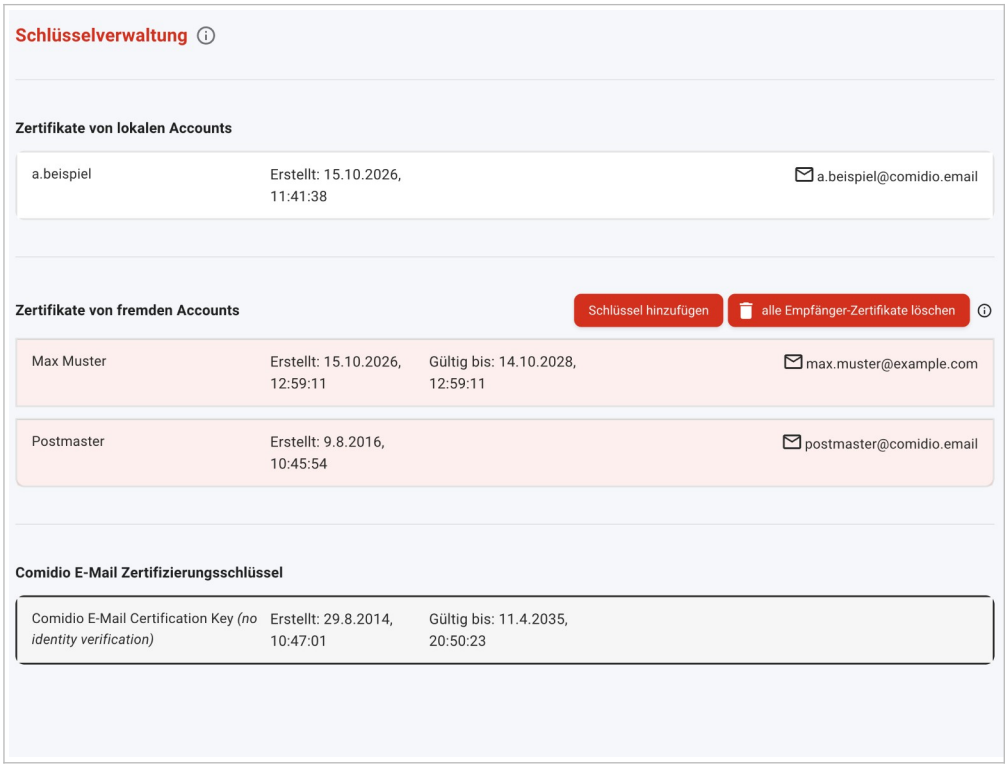


Abbildung 10-4: Die Schlüsselverwaltung: eigene Schlüssel oben, zwischengespeicherte fremde darunter, zuletzt der Comidio-Zertifizierungsschlüssel. (© 2026 Comidio GmbH)

Unter **E-Mail → Schlüsselverwaltung** sehen Sie drei Bereiche: die Zertifikate Ihrer lokalen Konten, die zwischengespeicherten Zertifikate fremder Konten und den Comidio-Zertifizierungsschlüssel. Anfassen müssen Sie hier normalerweise nichts, denn die Pflege läuft automatisch: Jede TrutzMail trägt im geschützten Teil einen Hinweis auf den aktuellen Absenderschlüssel, und die Empfänger-TrutzBox holt sich neue Schlüssel einmalig aus dem

zentralen Comidio-Adressbuch. Dem mitgeschickten Schlüssel selbst vertraut sie bewusst nicht, und Comidio erfährt dabei nicht, wer mit wem schreibt. Wurde an einen veralteten Schlüssel verschlüsselt, schickt die Gegenseite automatisch eine Korrektur-Notiz.

Menüpfad: E-Mail → Schlüsselverwaltung



Abbildung 10-5: Die Detail-Ansicht eines eigenen Schlüssels: Vertrauensstufe, Fingerabdruck und die versteckte Zustelladresse. (© 2026 Comidio GmbH)

- **Zertifikate von lokalen Accounts:** die Schlüssel der TrutzMail-Adressen auf dieser TrutzBox. Ein Klick öffnet die Detail-Ansicht mit Erstellungsdatum, Vertrauensstufe, Fingerabdruck und der versteckten Adresse im Tor-Netzwerk, über die Ihre Post zugestellt wird. Von hier laden Sie auch Ihren öffentlichen Schlüssel für PGP-Partner herunter.
- **Zertifikate von fremden Accounts:** der Zwischenspeicher für die Schlüssel Ihrer Gegenstellen. Schlüssel anderer TrutzBoxen landen hier automatisch, Schlüssel gewöhnlicher Adressen haben Sie selbst eingefügt. Einzelne Einträge lassen sich löschen, mit **Alle Empfänger-Zertifikate löschen** auch der ganze Speicher.
- **Comidio E-Mail Zertifizierungsschlüssel:** der öffentliche Schlüssel, mit dem Ihre TrutzBox die Signaturen eingehender TrutzMails prüft.

Beim Hinzufügen nimmt die TrutzBox nur Schlüssel an, mit denen sie unbeaufsichtigt arbeiten kann. Enthält eine Datei einen privaten Schlüssel, der durch eine Passphrase geschützt ist, lehnt sie ihn mit einem Hinweis ab, denn ihre Mail-Dienste laufen im Hintergrund und könnten die Passphrase nicht abfragen. Für einen PGP-Partner genügt ohnehin sein öffentlicher Schlüssel. Soll ein Eintrag gelöscht werden, der einen privaten Schlüssel enthält, fragt die TrutzBox vorher nach: Mit diesem Schlüssel verschlüsselte Post ließe sich danach nicht mehr öffnen.

Einmal täglich gleicht die TrutzBox zusätzlich ab, ob eines der gespeicherten fremden Zertifikate inzwischen ungültig geworden ist, etwa weil eine TrutzBox gestohlen oder zurückgesetzt wurde. Ungültige Einträge verschwinden dann aus dem Speicher und werden bei Bedarf frisch geholt. Abgefragt wird dabei nur ein Prüfwert der Adresse, nicht die Adresse selbst; aus diesen Abfragen lässt sich also keine Adressliste gewinnen. Ein einmal gesperrter Schlüssel wird nie wieder angenommen: Sperrung geht immer vor Aktualisierung.

Wenn sich ein Schlüssel ändert

Schlüssel sind nicht für die Ewigkeit: Wird ein Konto neu angelegt, eine Adresse reaktiviert oder die TrutzBox ohne Sicherung neu aufgesetzt, entsteht ein neuer Schlüssel. Was dann passiert, hängt davon ab, auf welcher Seite der Wechsel stattfindet:

- **Der Schlüssel eines Partners ändert sich:** Ihre TrutzBox merkt das von selbst. Verschlüsselt sie noch an den alten Schlüssel, schickt die Gegenseite automatisch eine Korrektur-Notiz, und

Ihre TrutzBox holt sich den aktuellen Schlüssel frisch. Zusätzlich prüft sie einmal täglich, ob gespeicherte fremde Schlüssel zurückgezogen wurden. Sie müssen nichts tun; schlimmstenfalls braucht der erste Briefwechsel nach dem Wechsel einen zweiten Anlauf.

- **Ihr eigener Schlüssel ändert sich:** TrutzBox-Partner merken davon nichts, deren TrutzBoxen holen sich den neuen Schlüssel automatisch. An eines müssen Sie aber selbst denken: PGP-Partner ohne TrutzBox (Weg B) verschlüsseln weiter an Ihren alten öffentlichen Schlüssel, bis Sie ihnen den neuen zugeschickt haben. Laden Sie ihn dafür aus der Detail-Ansicht herunter und senden Sie ihn einmal an jeden PGP-Partner.
- **Alte Post bleibt lesbar,** solange der alte geheime Schlüssel noch da ist. Genau deshalb lohnt die Sicherung (Kapitel „Sichern, Wiederherstellen und Zurücksetzen“): Sie bringt nach einem Neuaufbau den bisherigen Schlüssel zurück, und weder Partner noch Postfach merken etwas vom Umzug. Ohne Sicherung ist ein neuer Schlüssel unvermeidlich, und mit dem alten verschlüsselte Post bleibt verschlossen.

Wenn es mit genau einem Partner klemmt

Löschen Sie in der Schlüsselverwaltung den zwischengespeicherten Schlüssel genau dieses Partners und senden Sie erneut; die TrutzBox lädt den aktuellen Schlüssel dann frisch. Das behebt die allermeisten Verschlüsselungsprobleme mit Einzelnen. Erst wenn es mit mehreren Partnern gleichzeitig hakt, lohnt sich das Leeren des gesamten Speichers.

10.7 Wenn eine Mail nicht ankommt

Unter **E-Mail → Status** sehen Sie, was Ihre TrutzBox gerade mit Ihrer Post macht. Die Seite hat zwei Bereiche: die **Warteschlange** mit allem, was noch nicht zugestellt werden konnte, und das **Mailprotokoll** mit allen abgeschlossenen Ein- und Ausgängen.

Die Warteschlange

Jede wartende Mail steht hier mit Datum, Art der Warteschlange, Größe, Absender, Empfänger, Status und der Fehlermeldung im Klartext. Die Spalte **nach** nennt die Empfängeradresse. Häufig lesen Sie dort, dass die Verbindung zur Ziel-TrutzBox in eine Zeitüberschreitung gelaufen ist; das heißt schlicht, dass die TrutzBox der Gegenseite gerade nicht erreichbar war. In diesem Fall ist nichts zu tun, Ihre TrutzBox versucht es von selbst weiter.

- **Aktualisieren** (das Pfeil-Symbol über der Liste): lädt die Liste neu.
- **Mail anschauen:** zeigt den Inhalt der noch nicht versendeten Nachricht.
- **Mail erneut senden:** stößt einen sofortigen neuen Zustellversuch an.
- **Mail löschen:** entfernt nach einer Rückfrage genau diese Nachricht aus der Warteschlange.
- **Alle Mails löschen:** leert die Sende-Warteschlange vollständig. Die Nachrichten sind danach weg und werden nicht mehr zugestellt.

Das Mailprotokoll

Darunter listet das Mailprotokoll jeden abgeschlossenen Vorgang mit Datum, Größe, Absender, Empfänger und Status, etwa dass eine Mail erfolgreich gesendet wurde oder dass Sie eine Mail erhalten haben. Ein Pfeil nach rechts kennzeichnet ausgehende, ein Pfeil nach links eingehende

Post. Zu jeder einzelnen Zeile lässt sich über das Protokoll-Symbol das technische Rohprotokoll dieser einen Mail öffnen, das der Support für eine genaue Fehlersuche braucht.

Fünf Voraussetzungen für die Zustellung

Damit eine TrutzMail zugestellt werden kann, müssen fünf Dinge stimmen. Die Warteschlange nennt den Grund im Klartext, sodass Sie in aller Regel sofort sehen, an welchem Punkt es hakt:

- Die Empfängeradresse existiert und ist als aktive TrutzMail-Adresse registriert.
- Das TrutzMail-Zertifikat des Empfängers ist gültig.
- Die Empfänger-TrutzBox ist eingeschaltet und online. Ist sie es vorübergehend nicht, wiederholt Ihre TrutzBox die Zustellung selbsttätig.
- Ihr eigenes TrutzMail-Zertifikat ist gültig. Nach Ablauf des Service-Vertrags wird es nicht mehr erneuert, und die Gegenseite nimmt die Mail dann nicht mehr an.
- Die Mail wurde nicht an einen veralteten Schlüssel des Empfängers verschlüsselt. In diesem Fall schickt die Empfänger-TrutzBox automatisch eine Korrektur-Notiz zurück.

10.8 Adressen anlegen, löschen und reaktivieren

Eine TrutzMail-Adresse entsteht immer zusammen mit einem Benutzerkonto unter **Verwaltung → Benutzer** (Kapitel „Benutzer, Postfächer, Passwörter“). Setzen Sie dort beim Anlegen das Häkchen **Als TrutzMail-Adresse registrieren**, prüft die TrutzBox drei Dinge bei Comidio nach, bevor sie die Adresse einrichtet: ob die Service-Laufzeit Ihrer TrutzKennung noch läuft, ob der gewünschte Name überhaupt noch frei ist, denn TrutzMail-Adressen sind weltweit eindeutig, und ob Ihr Service-Vertrag noch eine freie Adresse im Kontingent hat.

Passt etwas nicht, nennt die Oberfläche den Grund in einer roten Meldung:

- *„Die Service-Laufzeit dieser TrutzKennung ist abgelaufen. TrutzMail-Adressen lassen sich erst nach der Verlängerung wieder anlegen oder reaktivieren."* Das gilt für neue Adressen wie fürs Reaktivieren. Verlängert wird der Vertrag nicht über die TrutzBox, sondern über www.trutzbox.de oder per Mail an support@trutzbox.de; danach versuchen Sie es erneut.
- *„Adresskontingent erschöpft."* Alle Adressen Ihres Vertrags sind vergeben (Kapitel „Löschen, Reaktivieren und das Kontingent“).
- *„Diese E-Mail-Adresse ist bereits registriert."* Der Name ist schon vergeben; wählen Sie einen anderen.
- *„Die Comidio-Server erkennen diese TrutzBox nicht. Bitte die Aktivierung der TrutzBox prüfen."* Comidio nimmt die Anfrage dieser TrutzBox nicht an. Ob sie aktiviert ist, steht unter **Systemeinstellungen → Vertrag und Pakete**. Hilft das nicht weiter, wenden Sie sich mit der Meldung an den Support (Kapitel „Support kontaktieren“).
- *„Verbindung zu Comidio-Servern nicht möglich. Bitte überprüfen Sie Ihre Internetverbindung."* Die TrutzBox erreicht Comidio gerade nicht.

Erst wenn alles passt, erzeugt die TrutzBox das Schlüsselpaar und das zugehörige Mail-Zertifikat. Der geheime Teil verlässt die TrutzBox dabei nie und ist auch Comidio nicht bekannt. Comidio kennt ausschließlich die Adressen und die dazugehörigen öffentlichen Schlüssel, die im zentralen Adressbuch stehen, damit andere TrutzBoxen Ihnen verschlüsselt schreiben können.

Löschen Sie später einen Benutzer mit TrutzMail-Adresse, wird die Adresse deaktiviert und das Zertifikat zentral als ungültig markiert. Verloren ist die Adresse damit aber nicht: Sie bleibt für Ihre TrutzLegitimation reserviert. Niemand sonst kann sie übernehmen, auch nicht nach einem Zurücksetzen Ihrer TrutzBox. In der Benutzerliste erscheint sie farblich abgesetzt unter **Reaktivierbare Benutzer** und kehrt über **Reaktivieren** zurück: Im Fenster *„Benutzer reaktivieren"* ist der Anmeldename schon eingetragen, Sie vergeben ein Passwort und bestätigen mit **Reaktivieren**. Auch dabei fragt die TrutzBox bei Comidio nach; mit abgelaufener Service-Laufzeit lässt sich eine Adresse also auch nicht reaktivieren.

> **Reaktivieren holt die Adresse zurück, nicht die Post**
>
> Nach einer Reaktivierung erhält die Adresse einen neuen Schlüssel. Die alten Postfachinhalte und den alten geheimen Schlüssel bringt nur eine Sicherung zurück (Kapitel „Sichern, Wiederherstellen und Zurücksetzen"). Ihre TrutzBox-Partner merken vom Schlüsselwechsel nichts: Deren TrutzBoxen bemerken ihn selbst und holen den neuen Schlüssel beim nächsten Briefwechsel automatisch nach. PGP-Partner ohne TrutzBox (Weg B) brauchen dagegen Ihren neuen öffentlichen Schlüssel; schicken Sie ihn ihnen einmal zu (Abschnitt „Schlüssel und Zertifikate").

10.9 Was Comidio sieht und was nicht

TrutzMail kommt nicht ganz ohne eine zentrale Stelle aus, denn irgendwo muss hinterlegt sein, unter welchem öffentlichen Schlüssel eine Adresse zu erreichen ist. Diese Stelle ist das Comidio-Adressbuch. Es ist bewusst so gebaut, dass es so wenig wie möglich erfährt.

- **Comidio kennt:** alle vergebenen TrutzMail-Adressen und deren öffentliche Schlüssel, die Laufzeit Ihres Service-Vertrags und die Tatsache, dass eine Adresse gesperrt oder wieder freigegeben wurde.
- **Comidio kennt nicht:** Ihre geheimen Schlüssel, den Inhalt Ihrer Mails, Ihre Postfächer und die Frage, wer wem schreibt. Für den Versand einer Mail wird kein zentraler Server gefragt; die TrutzBoxen sprechen direkt miteinander.

Den Schlüssel einer Gegenstelle holt Ihre TrutzBox nur beim ersten Kontakt und nach einem Schlüsselwechsel oder einer Sperrung aus dem Adressbuch und behält ihn sonst. Auch der tägliche Abgleich über gesperrte Zertifikate läuft ausschließlich über Prüfwerte, nicht über Klartext-Adressen. Alles andere, von der Verschlüsselung über die Zustellung bis zur Ablage, geschieht auf Ihrer eigenen TrutzBox.

Häufige Fragen zu TrutzMail

Kann ich mit TrutzMail an ganz normale Adressen schreiben?

Verschlüsselt ja, über Weg B (PGP) oder Weg C (Gast-Konto). Unverschlüsselt bewusst nicht; dafür nutzen Sie parallel Ihre bisherige Adresse. Empfangen können Sie über Ihr Postfach beim Anbieter (Abschnitt „Weg B einrichten: Postfach beim Anbieter verbinden") auch unverschlüsselte Post, dann mit [UU] markiert.

Was passiert bei sehr großen Mails?

Eine feste Größengrenze gibt es nicht. Weil Anhänge für den Versand umcodiert werden, wird eine Mail aber immer deutlich größer als die Summe ihrer Dateien, und die Grenze setzt am Ende der Arbeitsspeicher der beteiligten TrutzBoxen. Hakt es bei einer ungewöhnlich großen Mail, hilft ein Neustart der TrutzBox. Der Dateiversand über TrutzChat (Kapitel „TrutzChat und Videokonferenz“) ist oft der bequemere Weg, allerdings nur bis 25 MB je Datei.

Kann Comidio meine Mails lesen?

Nein. Comidio betreibt nur das Adressbuch mit den öffentlichen Schlüsseln; die geheimen Schlüssel und Ihre Postfächer liegen ausschließlich auf Ihrer TrutzBox. Für gewöhnliche, unverschlüsselte Post gilt dasselbe wie für jede E-Mail: Sie ist offen unterwegs und liegt bei Ihrem Anbieter, bis die TrutzBox sie abholt. Deshalb trägt sie das Kennzeichen [UU].

Was passiert, wenn mein Service-Vertrag ausläuft?

Das TrutzMail-Zertifikat wird dann nicht mehr erneuert. Empfänger-TrutzBoxen nehmen Ihre Mails danach nicht mehr an, und die Warteschlange weist auf das ungültige eigene Zertifikat hin. Neue TrutzMail-Adressen lassen sich nicht mehr anlegen oder reaktivieren; die Oberfläche meldet dann, dass die Service-Laufzeit abgelaufen ist (Abschnitt „Adressen anlegen, löschen und reaktivieren“). Die übrigen Schutzfunktionen der TrutzBox arbeiten weiter.

Mein Anbieter lehnt die Absenderadresse ab. Woran liegt das?

Die Fehlermeldung nennt dann die abgelehnte Adresse. Meist steht im Feld **E-Mail-Adresse** nicht die vollständige Adresse, sondern der Anmeldename des Anbieters, oder die Mail ging unter einer Adresse hinaus, die beim Anbieter nicht für dieses Postfach freigeschaltet ist. Tragen Sie unter **Verwaltung → Benutzer** im Bereich E-Mail-Austausch mit normalen Adressen die vollständige Absenderadresse ein und den Anmeldenamen unter Erweitert in das Feld Anmeldename (Kapitel „Weg B einrichten: Postfach beim Anbieter verbinden“).

Muss ich meine Mails selbst sichern?

Die Sicherung unter **Systemeinstellungen → Sichern und Wiederherstellen** nimmt die Postfächer samt geheimer Schlüssel mit (Kapitel „Sichern, Wiederherstellen und Zurücksetzen“). Ohne sie sind die Schlüssel nach einem Zurücksetzen unwiederbringlich verloren, denn niemand sonst hat eine Kopie davon.

11 TrutzDynDNS: Ihre TrutzBox aus dem Internet erreichbar machen

Im Netz der TrutzBox funktioniert alles ohne dieses Kapitel. Sobald aber ein Gerät von unterwegs zu Ihrer TrutzBox soll oder ein Gast von außen in Ihre Videokonferenz, muss die TrutzBox im Internet zu finden sein. Dafür sorgt **TrutzDynDNS**: ein fester Name für Ihre TrutzBox, der immer auf die aktuelle IP-Adresse Ihres Internet-Anschlusses zeigt. Dieses Kapitel erklärt, wozu das gut ist, welche Kehrseite es hat, wie Sie es einschalten und an welchen Internet-Anschlüssen es überhaupt möglich ist.

11.1 Wozu Ihre TrutzBox von außen erreichbar sein muss

Die IP-Adresse Ihres Internet-Anschlusses vergibt Ihr Internet-Anbieter, und sie wechselt immer wieder. Ein Gerät unterwegs kann sie sich deshalb nicht merken. Der Name unter `mytrutzbox.de` bleibt dagegen gleich: Die TrutzBox meldet jede neue IP-Adresse von selbst dorthin. Diesen Namen brauchen:

- **TrutzVPN:** Ihre Geräte unterwegs bauen den Tunnel zu diesem Namen auf (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).
- **Videokonferenz und Anrufe aus dem Chat:** Gäste kommen über einen Link mit diesem Namen in Ihre Konferenz, und die TrutzBox holt für ihn ein anerkanntes Zertifikat, damit niemand eine Warnung sieht (Kapitel „TrutzChat und Videokonferenz“).

Wer nichts davon nutzt, braucht TrutzDynDNS nicht und lässt es aus.

> **Die Kehrseite: Angriffsversuche von außen**
>
> Der Name allein öffnet nichts. Erreichbar wird Ihre TrutzBox erst durch die Freigaben, die Sie am Internet-Router für TrutzVPN oder die Videokonferenz einrichten. Jede solche Freigabe ist eine Tür nach außen, und an jede Tür im Internet klopft früher oder später jemand: Automatische Suchprogramme probieren rund um die Uhr Adressen und Anschlüsse durch, ob mit oder ohne Namen. Solche Versuche sehen Sie dann auch bei Ihrer TrutzBox.
>
> Die TrutzBox lässt durch eine Freigabe nur den einen Dienst erreichen, für den sie gedacht ist, die Verwaltungsoberfläche bleibt von außen verschlossen. Wer es wiederholt versucht, wird gesperrt (Abschnitt „Angriffsschutz: Firewall und Wächter“). Sie selbst halten das Risiko klein, wenn Sie nur die Freigaben anlegen, die Sie wirklich brauchen, Dienste abschalten, die Sie gerade nicht nutzen, und gute Passwörter verwenden. Ganz ausschließen lässt sich ein Risiko bei keiner Tür nach außen.

11.2 TrutzDynDNS einschalten

1. Öffnen Sie im Admin-Panel **Netzwerk → Fernzugriff**. Dieselbe Karte steht auch auf der Seite **Videokonferenz und Chat**; es ist gleich, wo Sie sie einschalten.
2. Schalten Sie in Karte **1. Domain-Namen festlegen** den Schalter **TrutzDynDns** ein.
3. Notieren Sie sich den angezeigten Namen, etwa `beispiel.mytrutzbox.de`. Unter diesem Namen ist Ihre TrutzBox künftig von außen zu finden.

Damit ist die TrutzBox gefunden, aber noch nicht erreichbar. Was danach am Internet-Router einzurichten ist, beschreiben die Kapitel der Dienste: für TrutzVPN der Abschnitt „Schritt 2: Portweiterleitung am Internet-Router“, für die Videokonferenz der Abschnitt „Reiter Videokonferenz: einmalig einrichten“. Ob danach von außen etwas ankommt, misst die TrutzBox selbst (Abschnitt „Netzwerk-Übersicht: außen und innen“).

> **Was speichert Comidio dabei?**
> Nur Ihre jeweils aktuelle IP-Adresse, verknüpft mit Ihrem Domain-Namen. Jede neue Adresse ersetzt die alte, einen Verlauf führt Comidio nicht. Damit bei einem Ausfall nichts verloren geht, sichert Comidio seine Server regelmäßig; in diesen Sicherungskopien bleiben ältere Stände bis zu 90 Tage erhalten und werden danach gelöscht. Schalten Sie TrutzDynDNS ab, löscht Comidio Ihre Adresse. Der Name bleibt für Ihre TrutzKennung reserviert, damit ihn niemand anderes bekommt.

11.3 Welcher Anschluss ist von außen erreichbar?

Ein Name und eine Freigabe am Internet-Router genügen nur, wenn Ihr Internet-Anbieter Verbindungen aus dem Internet überhaupt bis zu Ihrem Internet-Router durchlässt. Das hängt von der Art Ihres Anschlusses ab. Das Internet kennt dafür zwei Adressarten, um über das Internet Ihren Internet-Router zu erreichen: das ältere **IPv4** mit kurzen Adressen aus vier Zahlen und das neuere **IPv6** mit langen Adressen. Für jede der beiden gilt etwas anderes. Vier Fälle kommen häufig vor:

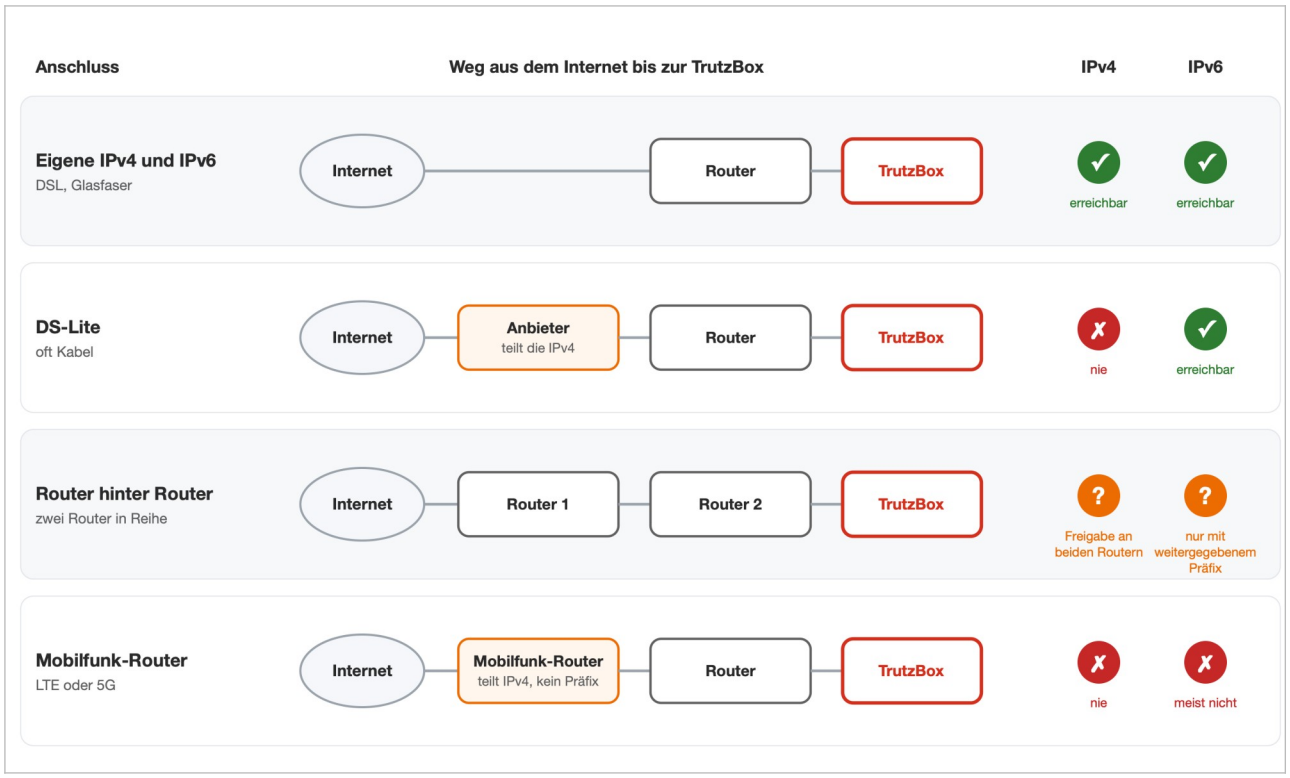


Abbildung 11-1: Vier Arten von Internet-Anschlüssen und ob die TrutzBox dahinter von außen erreichbar ist: über IPv4 (oben in jeder Zeile) und über IPv6 (unten). (© 2026 Comidio GmbH)

Anschluss	Von außen erreichbar	Was hilft
Eigene IPv4 und IPv6	Über IPv4 und IPv6. Das ist der Normalfall bei vielen DSL- und manchen Glasfaser-Anschlüssen.	Freigaben am Internet-Router wie in den Kapiteln der Dienste beschrieben.
DS-Lite	Nur über IPv6. Die IPv4-Adresse teilen Sie sich mit anderen Kunden des Anbieters, sie führt nie zu Ihnen. Verbreitet bei Kabel- und Glasfaser-Anschlüssen.	IPv6-Freigabe am Internet-Router und der Schalter **TrutzDynDNS nur mit IPv6** (nächster Abschnitt). Oder beim Internet-Anbieter eine eigene öffentliche IPv4-Adresse erfragen, damit die TrutzBox auch über IPv4 von außen erreichbar ist. Viele Anbieter richten das auf Wunsch ein, oft gegen eine zusätzliche Gebühr und unter der Bezeichnung „Dual-Stack" oder „öffentliche IPv4-Adresse".
Router hinter Router	Nur, wenn beide Router mitspielen. Über IPv4 braucht dann jeder der beiden Router eine Freigabe. Über IPv6 bekommt die TrutzBox nur eine öffentliche Adresse, wenn der vordere Router einen eigenen Adressbereich an den hinteren weitergibt.	Den vorderen Router als reines Modem betreiben (oft „Bridge-Modus" genannt), dann bleibt nur ein Router übrig. Sonst Freigaben an beiden Routern.
Mobilfunk-Router (LTE oder 5G)	Meist gar nicht. Eine eigene IPv4-Adresse gibt es im Mobilfunk praktisch nie, und viele dieser Router geben keinen IPv6-Adressbereich an einen angeschlossenen Router weiter.	Beim Internet-Anbieter fragen, ob der Router einen IPv6-Adressbereich weitergeben kann und ob Verbindungen von außen über IPv6 erlaubt sind. Manche Anbieter bieten auch eine öffentliche IPv4-Adresse an, meist gegen eine zusätzliche Gebühr. Sonst bleibt nur ein Festnetz-Anschluss.

So erkennen Sie Ihren Anschluss an einer FRITZ!Box

Die FRITZ!Box zeigt alles Nötige auf einer Seite. Öffnen Sie in ihrer Oberfläche **Internet → Online-Monitor**. Wichtig sind drei Angaben:

Menüpfad: FRITZ!Box: Internet → Online-Monitor

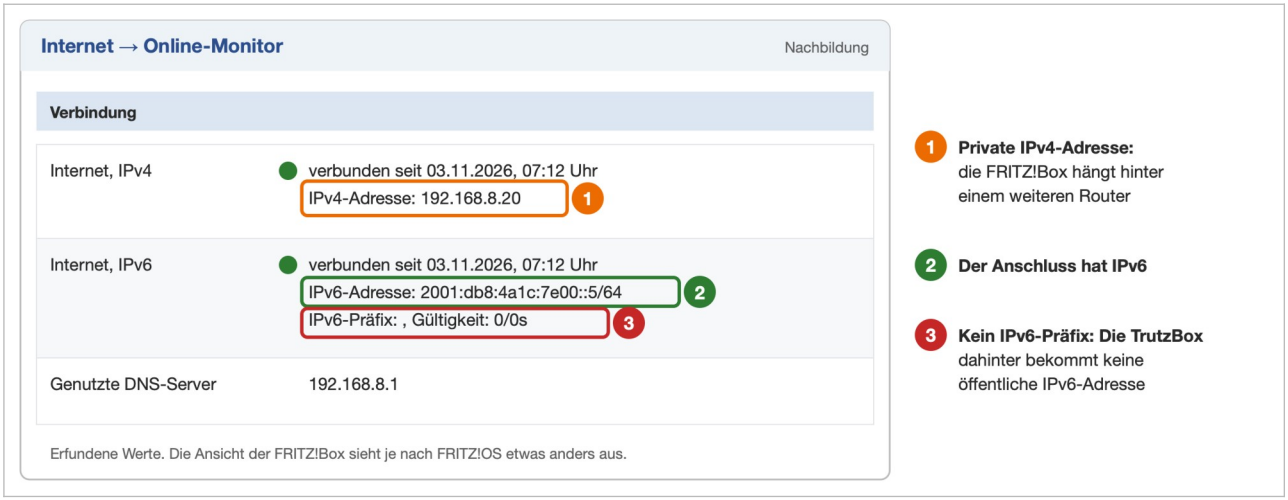


Abbildung 11-2: Nachbildung des Online-Monitors einer FRITZ!Box an einem Mobilfunk-Router, mit erfundenen Werten: private IPv4-Adresse, eine IPv6-Adresse, aber kein IPv6-Präfix. (© 2026 Comidio GmbH)

- **Internet, IPv4:** Beginnt die Adresse mit `192.168.`, `10.` oder `172.16.` bis `172.31.`, ist sie privat: Die FRITZ!Box hängt hinter einem weiteren Router. Steht dort ein Hinweis auf einen **DS-Lite-Tunnel** oder eine Adresse ab `192.0.0.`, haben Sie DS-Lite. Adressen ab `100.64.` bis `100.127.` teilt sich der Anbieter mit anderen Kunden; auch sie führen nicht zu Ihnen.
- **Internet, IPv6:** Steht hier eine Adresse, die mit 2 oder 3 beginnt, hat der Anschluss IPv6.
- **IPv6-Präfix:** Das ist der Adressbereich, aus dem die FRITZ!Box den Geräten dahinter, also auch der TrutzBox, ihre IPv6-Adressen gibt. Ist das Feld leer, bekommt die TrutzBox keine öffentliche IPv6-Adresse und ist über IPv6 nicht erreichbar.

Andere Router zeigen dieselben Angaben meist auf ihrer Übersichtsseite oder unter einem Punkt wie *Status* oder *Internet*. Ob am Ende wirklich etwas ankommt, misst die TrutzBox selbst mit Testpaketen von außen (Abschnitt „Netzwerk-Übersicht: außen und innen“).

11.4 TrutzDynDNS nur mit IPv6

Bei DS-Lite gehört die IPv4-Adresse, die von außen sichtbar ist, dem Internet-Anbieter und führt nie zu Ihrer TrutzBox. Trägt TrutzDynDNS trotzdem beide Adressarten ein, wählen die VPN-Apps von Android, iPhone und Windows, die WireGuard-App eingeschlossen, immer die IPv4 und kommen nie an.

Dafür gibt es im Domain-Bereich den Schalter **TrutzDynDNS nur mit IPv6 (Anschluss ohne eigene IPv4-Adresse, DS-Lite)**. Eingeschaltet veröffentlicht TrutzDynDNS nur noch die IPv6-Adresse, und die Apps verbinden zuverlässig. Voraussetzung ist eine IPv6-Freigabe am Internet-Router (Abschnitt „VPN auch über IPv6 anbieten“), bei OpenVPN zusätzlich der Schalter **VPN auch über IPv6 anbieten**. Der Schalter gilt auch für Videokonferenz, Chat und Mail über den TrutzDynDNS-Namen; 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 (Abschnitt „Netzwerk-Übersicht: außen und innen“). Von Hand brauchen Sie ihn dann nicht zu stellen.

Geräte im Netz der TrutzBox und im Tunnel arbeiten nur mit IPv4 und fänden zu einem Namen, der nur die IPv6-Adresse trägt, keinen Weg. Solange der Schalter gesetzt ist, beantwortet die TrutzBox ihren Namen dort deshalb selbst mit ihrer internen Adresse. Videokonferenz und Oberfläche bleiben so auch von innen unter dem Namen erreichbar; nach außen ändert sich nichts.

Grenzen des Wegs über IPv6

- **Netze ohne IPv6:** Ist Ihre TrutzBox nur über IPv6 erreichbar, kommen Geräte und Gäste nur aus Netzen herein, die selbst IPv6 haben. Mobilfunknetze in Deutschland haben das meist, manche Hotel-, Gäste- oder Firmen-WLANs nicht. Ein Gast in einem solchen Netz kommt nicht in Ihre Videokonferenz.
- **Geräte im Netz des Routers:** Die FRITZ!Box schützt ihr Netz vor Namen, die auf Adressen im eigenen Netz zeigen (DNS-Rebind-Schutz). Trägt der Name der TrutzBox nur noch die IPv6-Adresse, nennt die FRITZ!Box ihn deshalb Geräten in ihrem eigenen WLAN nicht, und dort öffnet sich weder die Videokonferenz noch der VPN-Zugang. Abhilfe: in der FRITZ!Box unter **Heimnetz → Netzwerk → Netzwerkeinstellungen** im Feld **DNS-Rebind-Schutz** den Namen Ihrer TrutzBox als Ausnahme eintragen, etwa `beispiel.mytrutzbox.de`. Geräte im Netz der TrutzBox betrifft das nicht.

11.5 Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden

Haben Sie TrutzDynDNS eingeschaltet (Abschnitt „TrutzDynDNS einschalten“), erreichen Ihre Geräte die TrutzBox von außen unter ihrem TrutzDynDNS-Namen, etwa unter `beispiel.mytrutzbox.de`. Wer eine eigene Domain besitzt und ihren Namen ohnehin pflegt, etwa weil der Internet-Router die Adresse bei einem DynDNS-Anbieter einträgt, kann stattdessen diesen Namen verwenden. Die Einstellung dafür steht unter **Netzwerk → Fernzugriff** im Domain-Bereich und heißt **Eigener Domain-Name**. Solange kein eigener Name eingetragen ist, ist sie zugeklappt. Ein Klick auf die Zeile klappt sie auf.

Wichtig zum Verständnis: Den Eintrag im Internet pflegen weiterhin Ihr Internet-Router oder Ihr Internet-Anbieter. Die TrutzBox trägt dort nichts ein und prüft nur, ob der Name auf Ihren Anschluss zeigt. Sie können den eigenen Namen auch dann nutzen, wenn Sie TrutzDynDNS gar nicht eingerichtet haben.

1. Die Zeile **Eigener Domain-Name** aufklappen, den Schalter **Eigenen Domain-Namen verwenden** einschalten und den Namen eintragen, zum Beispiel `vpn.beispiel.de`.
2. Unter **Verwenden für** ankreuzen, wofür der Name gelten soll: **VPN-Zugangsdateien (WireGuard und OpenVPN)** und **Videokonferenz und Chat von unterwegs**.
3. Für Videokonferenz und Chat ein Zertifikat für diesen Namen hochladen, im PEM-Format, wie es Let’s Encrypt oder Ihr Domain-Anbieter liefert. Der Schlüssel darf nicht mit einem Kennwort geschützt sein. Für die VPN-Zugänge wird kein Zertifikat gebraucht.
4. Mit **Testen** prüfen. Die TrutzBox prüft vier Schritte einzeln: Schreibweise, Namensauflösung, Zertifikat und ob die Videokonferenz über den Namen erreichbar ist.
5. Mit **Speichern** übernehmen.

6. Die Zugänge auf den Geräten ersetzen, sonst steht dort weiter der alte Name: WireGuard-Zugänge über **Datei** oder **Bildcode** neu holen (Abschnitt „Schritt 5: Zugänge für die WireGuard-App anlegen“), OpenVPN-Profile unter **Benutzer** neu herunterladen (Abschnitt „OpenVPN statt WireGuard verwenden“), und jeweils in der App neu importieren.

Direkt darunter steht das Feld **Port von außen für VPN** mit dem eigenen Knopf **Port speichern**. Es gilt für beide Tunnel und auch ohne eigenen Namen. Weicht der Port, den Ihr Internet-Router nach außen anbietet, vom Anschluss der TrutzBox ab, tragen Sie ihn dort ein. Das ist der übliche Weg, wenn eine zweite TrutzBox am selben Internet-Router hängt: Die erste behält 1194, die zweite bekommt am Internet-Router etwa 1195, und die TrutzBox setzt das intern wieder auf ihren eigenen Anschluss um. Auch danach die Zugänge auf den Geräten ersetzen.

Das Zertifikat erneuert die TrutzBox nicht

Ein hochgeladenes Zertifikat läuft irgendwann ab, meist nach drei Monaten. Die TrutzBox erneuert es nicht selbst, sie erinnert aber rechtzeitig: Die Karte *„Eigener Name"* im Betriebszustand wird gelb, bevor es so weit ist, und rot, sobald es abgelaufen ist. Dann laden Sie unter Fernzugriff einfach das neue Zertifikat hoch. Für den TrutzDynDNS-Namen gilt das nicht, dort besorgt und erneuert die TrutzBox das Zertifikat selbst.

Für Neugierige: Beide Namen gleichzeitig

Der eigene Name ersetzt den TrutzDynDNS-Namen nicht, er tritt daneben. In den OpenVPN-Zugangsdateien steht der eigene Name zuerst, der TrutzDynDNS-Name bleibt als Rückfall darunter. Ein WireGuard-Zugang kennt nur einen Weg; dort steht dann allein der eigene Name. Videokonferenz und Chat antworten unter beiden Namen, jeder mit seinem eigenen Zertifikat. Welcher Weg benutzt wird, entscheidet also das Gerät, nicht die TrutzBox.

12 TrutzChat und Videokonferenz

Nachrichten und Videokonferenzen laufen sonst über die Server großer Anbieter. Ihre TrutzBox kann beides selbst: **TrutzChat** für Nachrichten, Gruppen und Dateiaustausch, **TrutzMeeting** für Videokonferenzen, zu denen Gäste ohne App und ohne Konto einfach per Link dazustoßen. Alles läuft auf Ihrer TrutzBox; kein fremder Server sitzt dazwischen. Beide Funktionen gehören zur TrutzBox-Business-Ausstattung, eingerichtet werden sie gemeinsam auf der Seite **Videokonferenz und Chat**.

Der Unterschied zu den bekannten Diensten liegt weniger bei der Verschlüsselung der Nachrichten, die viele inzwischen beherrschen, als bei den Begleitdaten. Wer den Dienst betreibt, sieht bei jeder Nachricht, wer wann mit wem geschrieben hat, auch wenn er den Text nicht lesen kann. Genau diese Stelle fällt weg, wenn der Dienst auf der eigenen TrutzBox läuft. TrutzChat setzt dabei auf den offenen Standard **XMPP**, sodass Sie nicht an ein einzelnes Programm gebunden sind.

Voraussetzungen

• Mindestens ein Benutzer mit TrutzMail-Adresse (Kapitel „Benutzer, Postfächer, Passwörter“); damit meldet man sich an Chat und Videokonferenz an.

• Ein öffentlicher Name für die TrutzBox: der TrutzDynDNS-Name oder ein eigener Name (Kapitel „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“). Ohne ihn lässt sich der gemeinsame Server von Videokonferenz und Chat nicht einschalten, und ohne eingeschalteten Server arbeitet auch TrutzChat nicht.

• Für Teilnehmer von außerhalb zusätzlich Portfreigaben am Router (unten beschrieben). Im eigenen Netz und zwischen TrutzBoxen sind keine nötig. Den Chat erreichen Sie von unterwegs über den VPN-Zugang (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

• Für eine Videokonferenz braucht nur der Einladende eine TrutzMail-Adresse. Alle anderen Teilnehmer kommen ohne Konto und ohne eigene TrutzBox aus.

12.1 Die Seite Videokonferenz und Chat

Eingerichtet und verwaltet wird beides an einer Stelle: im Menü unter **Videokonferenz und Chat**. Die Seite beginnt mit dem gemeinsamen Schritt **1. Domain-Namen festlegen** und teilt sich darunter in zwei Reiter: **Videokonferenz** für den Konferenz-Server und **TrutzChat** für den Nachrichtendienst. Dieses Kapitel folgt genau dieser Aufteilung: zuerst der Reiter Videokonferenz, danach der Reiter TrutzChat, zum Schluss die Benutzung im Alltag.

Menüpfad: Videokonferenz und Chat

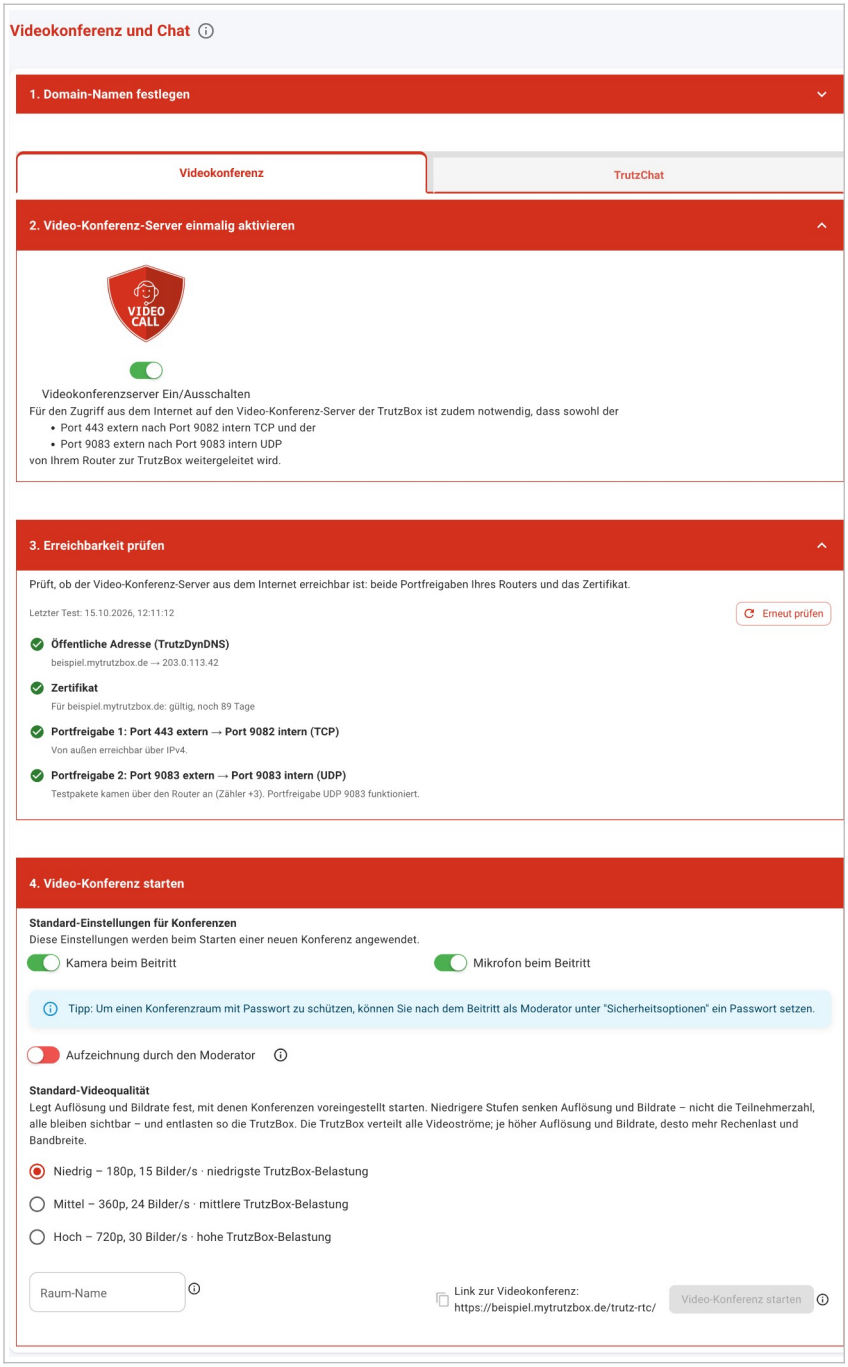


Abbildung 12-1: Die Seite Videokonferenz und Chat: oben Karte 1 zugeklappt, darunter der Reiter Videokonferenz mit Karte 2 (Server eingeschaltet), Karte 3 (Prüfung bestanden) und Karte 4 mit den Standard-Einstellungen für Konferenzen. (© 2026 Comidio GmbH)

Wenn der Server von außen nicht erreichbar ist

Meldet die Prüfung auf dieser Seite, dass Ihre TrutzBox von außen nicht erreichbar ist, liegt das fast nie an Chat oder Konferenz selbst, sondern an der Erreichbarkeit Ihres Internet-Anschlusses: Entweder fehlt eine Portfreigabe am Router, oder Ihr Anschluss lässt von außen nichts oder nur IPv6 herein, etwa bei DS-Lite oder an einem Mobilfunk-Router. Woran Sie das erkennen und was hilft, steht im Abschnitt „Welcher Anschluss ist von außen erreichbar?“. Die Portfreigabe am Router beschreibt der Abschnitt „Schritt 2: Portweiterleitung am Internet-Router“, die Freigabe

über IPv6 der Abschnitt „VPN auch über IPv6 anbieten“. Die dortigen Schritte gelten für die Videokonferenz genauso.

12.2 Reiter Videokonferenz: einmalig einrichten

Menüpfad: Videokonferenz und Chat

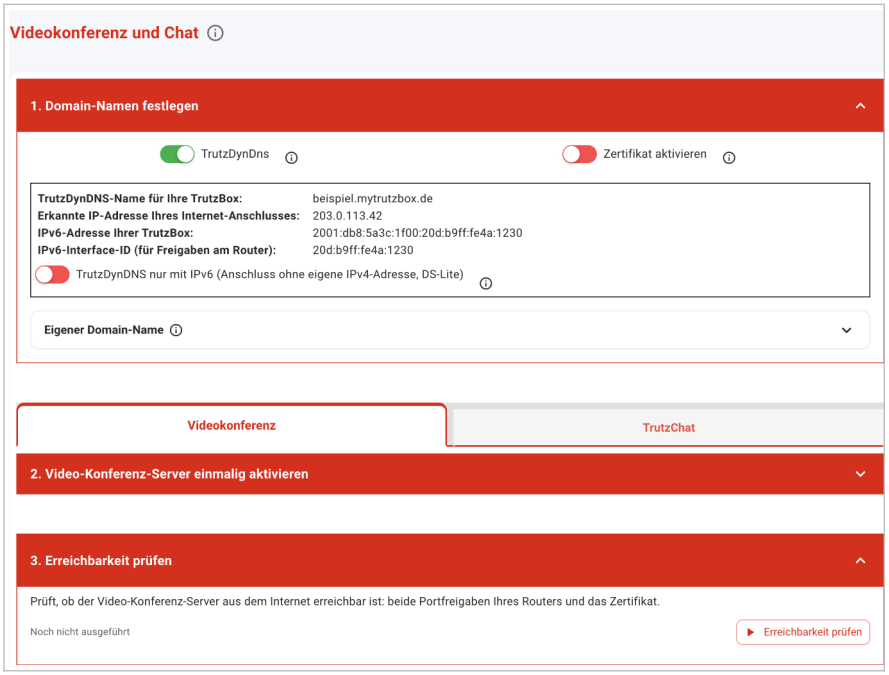


Abbildung 12-2: Karte 1 aufgeklappt: TrutzDynDNS-Name, erkannte Adresse des Anschlusses, IPv6-Angaben und der zugeklappte Bereich „Eigener Domain-Name“. Darunter die Reiter Videokonferenz und TrutzChat und Karte 3, bevor die Prüfung lief. (© 2026 Comidio GmbH)

Die Videokonferenz braucht einmalig vier Schritte; Karte 1 steht über den Reitern, die Karten 2 bis 4 im Reiter **Videokonferenz**. Die Seite führt der Reihe nach hindurch:

1. **Domain-Namen festlegen:** TrutzDynDNS einschalten (Abschnitt „TrutzDynDNS einschalten“) und zusätzlich mit dem Schalter **Zertifikat aktivieren** das kostenlose Zertifikat von Let’s Encrypt holen. Schlägt die Ausstellung fehl, nennt die Fehlermeldung die konkrete Ursache. Statt TrutzDynDNS ist auch ein eigener Name möglich, mit einem hochgeladenen Zertifikat und dem Haken **Videokonferenz und Chat von unterwegs** im Bereich **Eigener Domain-Name** (Kapitel „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“).
2. **Video-Konferenz-Server einmalig aktivieren:** den Schalter **Videokonferenzserver Ein/Ausschalten** einschalten und am Internet-Router zwei Portweiterleitungen einrichten: extern **443** auf intern **9082 (TCP)** und **9083 auf 9083 (UDP)**. Das Vorgehen am Router beschreibt Abschnitt „Schritt 2: Portweiterleitung am Internet-Router“, mit Bildern für eine FRITZ!Box Abschnitt „Beispiel: die Freigaben in einer FRITZ!Box“. Fehlt ein öffentlich anerkanntes Zertifikat, fragt die TrutzBox beim Einschalten unter *„Zertifikat nicht öffentlich anerkannt“* nach: Jeder Teilnehmer sieht dann eine Browser-Warnung, auch Gäste mit einem

Einladungslink. Mit **Trotzdem starten** läuft der Server dennoch; mit einem Zertifikat etwa von Let's Encrypt entfällt die Warnung.

3. **Erreichbarkeit prüfen:** Der Selbsttest prüft in vier Zeilen die öffentliche Adresse, das Zertifikat und beide Portfreigaben und meldet das Ergebnis jeweils im Klartext. Er ist erst möglich, wenn der Server läuft. Für die Portfreigaben nimmt er die regelmäßige Messung von außen dazu, bei der ein Server von Comidio Testpakete über IPv4 und IPv6 an die TrutzBox schickt (Kapitel „Netzwerk-Übersicht: außen und innen"), und urteilt je Weg, etwa *„Von außen erreichbar über IPv4 und IPv6."* Fehlt eine Freigabe für einen der beiden Wege, sagt er es, ebenso wenn auf Port 443 ein anderes Gerät antwortet als die TrutzBox. Der Zusatz *„Gemessen von außen:"* mit Zeitpunkt zeigt, dass das Urteil auf dieser Messung beruht.
4. **Video-Konferenz starten:** Raumnamen eingeben (nur Buchstaben und Ziffern) und los. Der Link hat die Form `https://beispiel.mytrutzbox.de/trutz-rtc/raumname`. Unter **Standard-Einstellungen für Konferenzen** legen Sie hier außerdem fest, ob Kamera und Mikrofon beim Beitritt an oder aus sind (**Kamera beim Beitritt**, **Mikrofon beim Beitritt**), ob der Moderator aufzeichnen darf (**Aufzeichnung durch den Moderator**, ab Werk aus) und mit welcher **Standard-Videoqualität** Konferenzen starten (Abschnitt „Konferenzen im Alltag").

Die Vorgabe für Kamera und Mikrofon gilt nur, wenn jemand die Adresse eines Raums von Hand öffnet, etwa den Link von dieser Seite; wer über einen Einladungslink oder einen Anruf aus dem Chat kommt, beginnt mit beidem ausgeschaltet (Abschnitt „Konferenzen im Alltag").

Ist der externe Port 443 an Ihrem Anschluss schon für etwas anderes vergeben, dürfen Sie auch einen anderen äußeren Port weiterleiten. Ihre Gäste müssen ihn dann im Link mit angeben, etwa `https://beispiel.mytrutzbox.de:4443/trutz-rtc/raumname`. Verfügt Ihr Anschluss über IPv6, ist der Konferenz-Server zusätzlich direkt über die globale IPv6-Adresse der TrutzBox erreichbar, ohne Portweiterleitung; dafür genügt am Router eine IPv6-Freigabe für die TrutzBox auf 443 (TCP) und 9083 (UDP), ohne Umleitung auf 9082. Wie eine IPv6-Freigabe angelegt wird, zeigt Abschnitt „Die IPv6-Freigabe in einer FRITZ!Box".

Das Zertifikat nicht ständig neu anfordern

Let's Encrypt stellt pro Woche nur eine begrenzte Zahl von Zertifikaten für denselben Namen aus. Schalten Sie den Schalter für das Zertifikat deshalb nicht mehrfach hintereinander aus und wieder ein, sondern lassen Sie ihn eingeschaltet. Als Faustregel: höchstens fünf Anläufe pro Woche.

Was die Freigabe außerdem erreichbar macht

Über die Freigabe auf 443 ist neben den Konferenzräumen auch die Anmeldung am Chat-Server aus dem Internet erreichbar, denn die Videokonferenz braucht sie: Wer einen Raum eröffnet, meldet sich dort mit seiner TrutzMail-Adresse und seinem TrutzMail-Passwort an. Damit niemand dieses Passwort durch Ausprobieren errät, wacht der Angriffsschutz der TrutzBox über diese Anmeldung (Kapitel „Angriffsschutz: Firewall und Wächter"). Nach fünf Fehlversuchen innerhalb von 30 Minuten sperrt er die Internet-Adresse, von der sie kommen, für sechs Stunden, bei Wiederholung immer länger, höchstens eine Woche. Geräte im eigenen Netz und über VPN sperrt

er nie.

Ein starkes Passwort bleibt trotzdem der beste Schutz. Neue und geänderte Passwörter prüft die TrutzBox deshalb nach festen Regeln (Kapitel „Passwörter ändern“).

12.3 Konferenzen im Alltag

Einen Raum eröffnen kann nur, wer sich mit einer TrutzMail-Adresse Ihrer TrutzBox anmeldet; er ist damit der Moderator des Raums. Ihre Gäste brauchen dagegen nur den Link und einen modernen Browser, keine App, kein Konto und keine eigene TrutzBox. Existiert der Raum bereits, verbindet sich der Browser einfach damit. Nach dem Beitritt vergibt jeder seinen Anzeigenamen, indem er sein eigenes Bildfenster anklickt; die Bedienleiste erscheint, sobald Sie die Maus bewegen, und bietet das Übliche: Kamera und Mikrofon, Bildschirm teilen, Chat.

Einladungslinks, die aus der Konferenz heraus weitergegeben werden, und Anrufe aus dem Chat führen ohne Vorschauseite direkt in den Raum, auf Smartphone und Tablet ebenso wie am Rechner und ohne Frage nach einer App. Kamera und Mikrofon sind dann zuerst aus. Kommt ein Gast vor dem Gastgeber, sieht er keine Anmeldung, sondern nur den Hinweis *„Die Konferenz hat noch nicht begonnen. Sie kommen von selbst hinein, sobald der Gastgeber da ist.“* Wer dagegen die Adresse eines Raums von Hand öffnet, sieht zuerst die Vorschauseite.

Beim ersten Beitritt fragt der Browser nach der Erlaubnis, Kamera und Mikrofon zu benutzen. Diese Frage stellt der Browser, nicht die TrutzBox, und ohne ein „Erlauben" bleibt das eigene Bild schwarz und der Ton stumm. Wer versehentlich abgelehnt hat, findet die Einstellung im Browser links neben der Adresszeile hinter dem Schloss- oder Kamerasymbol und kann sie dort für diese Adresse wieder freigeben.

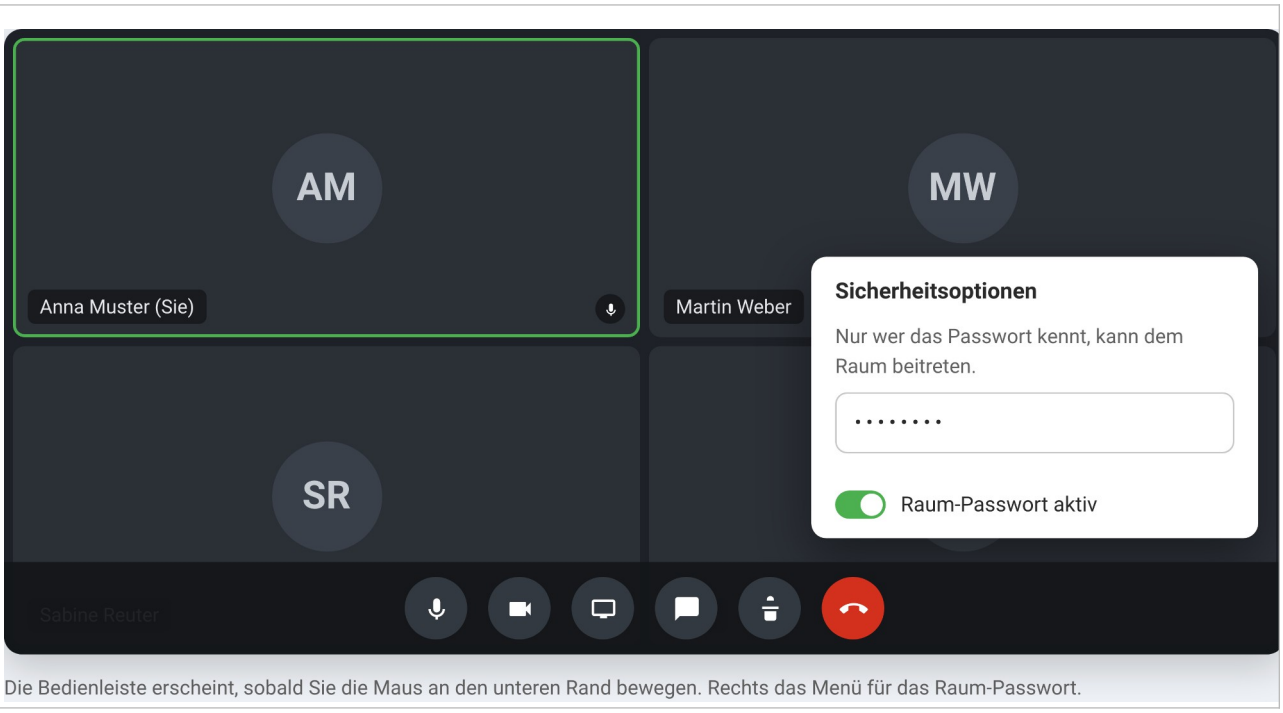


Abbildung 12-3: Das Konferenzfenster mit Bedienleiste und geöffneten Sicherheitsoptionen für das Raum-Passwort. (© 2026 Comidio GmbH)

Den Raum mit einem Passwort schützen

Solange kein Passwort gesetzt ist, kann jeder mitmachen, der den Link kennt. Für vertrauliche Runden setzt der Moderator deshalb nach dem Beitritt unter **Sicherheitsoptionen** ein Raum-Passwort. Wer später beitritt, muss es eingeben. Geben Sie Link und Passwort möglichst auf getrennten Wegen weiter, damit nicht beides in derselben Nachricht steht.

Aufzeichnen

Ist im Reiter Videokonferenz der Schalter **Aufzeichnung durch den Moderator** eingeschaltet, kann der Moderator, also wer den Raum mit Anmeldung eröffnet hat, die Konferenz aufzeichnen. Die Aufzeichnung läuft in seinem eigenen Browser, die Datei landet auf seinem Rechner; die TrutzBox speichert nichts. Das funktioniert nur am Rechner mit Chrome, Edge oder Firefox. Alle Teilnehmer sehen den Hinweis, dass aufgezeichnet wird. Ab Werk ist der Schalter aus.

> **Nur mit Einverständnis aller**
>
> Eine Konferenz darf nur aufgezeichnet werden, wenn alle Teilnehmer einverstanden sind. Die Seite weist beim Einschalten des Schalters ausdrücklich darauf hin: Die Verantwortung liegt beim Moderator.

Videoqualität und Bandbreite

Die Standard-Videoqualität lässt sich in drei Stufen einstellen: **Niedrig** (180p, 15 Bilder je Sekunde), **Mittel** (360p, 24 Bilder) und **Hoch** (720p, 30 Bilder). Voreingestellt ist Niedrig, was für Gespräche völlig reicht und die TrutzBox spürbar entlastet; für Präsentationen mit feiner Schrift stellen Sie höher. Eine niedrigere Stufe verringert nur Auflösung und Bildrate, nicht die Zahl der gezeigten Teilnehmer: Alle bleiben sichtbar.

Für die reine Sprachübertragung genügen etwa 40 kbit je Sekunde pro Teilnehmer, in beide Richtungen. Kommt eine Kamera oder ein geteilter Bildschirm dazu, sollten je Richtung rund 800 kbit je Sekunde zur Verfügung stehen, abhängig von Auflösung und davon, wie oft sich das Bild ändert. Bei üblichen DSL-Anschlüssen wird deshalb meist die Internet-Anbindung knapp, bevor die TrutzBox an ihre Grenze kommt. Solche Engpässe lassen sich am besten am Internet-Router beurteilen.

Als Praxisgrenze haben sich rund 15 Teilnehmer erwiesen, wenn nur einer von ihnen seinen Bildschirm teilt oder eine Kamera eingeschaltet hat. Reicht die Leistung bei vielen Kameras nicht, senken Sie zuerst die Standard-Videoqualität. Und weil die Konferenz komplett auf Ihrer TrutzBox läuft, gilt auch hier: Keine Gesprächsdaten landen bei Dritten.

Eine Einwahl per Telefon in eine Konferenz gibt es nicht. Das dafür nötige Zusatzmodul ist auf der TrutzBox bewusst nicht installiert und wird von Comidio nicht unterstützt.

12.4 Reiter TrutzChat: Selbsttest, Aufbewahrung, Gruppen

Für Verwaltung und Aufräumen gibt es auf der Seite **Videokonferenz und Chat** den Reiter **TrutzChat**. Ganz oben steht der Knopf **TrutzChat öffnen**, der den Web-Chat in einem neuen Fenster öffnet, daneben *„Im eigenen Netz erreichbar unter:"* mit der Adresse, etwa `https://trutzbox/chat/`, und *„Von unterwegs erreichbar über TrutzVPN"*. Darunter steht

ausdrücklich: Die Chat-Oberfläche ist aus dem Internet bewusst nicht erreichbar, und der Port 5222 wird am Router nicht freigegeben. Von unterwegs erreichen Sie den Chat über den VPN-Zugang (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

TrutzChat teilt sich den Server mit der Videokonferenz. Ist er aus, steht in diesem Reiter der Hinweis, ihn im Reiter Videokonferenz einzuschalten (Abschnitt „Reiter Videokonferenz: einmalig einrichten“, Schritt 2). Portfreigaben braucht der Chat dafür nicht.

Der Chat-Selbsttest

Im Bereich **Prüfung** startet der Knopf **Prüfen** den **Chat-Selbsttest**. Er prüft den kompletten Nachrichtenweg auf der TrutzBox: Zwei Testteilnehmer melden sich an und tauschen eine Nachricht aus. Das dauert etwa zehn Sekunden, und das Ergebnis erscheint im Klartext. Scheitert der Test, liegt es am Chat-Dienst auf der TrutzBox selbst, und der Support hat sofort einen Anhaltspunkt.

Ein bestandener Test sagt allerdings nur, dass der Nachrichtenweg auf Ihrer TrutzBox arbeitet. Ausdrücklich nicht geprüft werden drei Dinge: der Chat mit Teilnehmern auf anderen TrutzBoxen, der über das Tor-Netzwerk läuft, die Erreichbarkeit von unterwegs über den VPN-Zugang sowie die Anmeldung mit Ihren echten TrutzMail-Konten, denn der Test verwendet zwei Gastkonten. Klemmt es trotz bestandenem Test, suchen Sie die Ursache also zuerst in diesen drei Bereichen.

Aufbewahrungsdauer und Speicherplatz

Im Bereich **Speicherplatz und Aufbewahrung** legen Sie unter **Verläufe aufbewahren (Tage)** fest, wie viele Tage Chat-Verläufe aufbewahrt werden. Die Änderung wird mit dem nächsten Start des Chat-Dienstes wirksam; Älteres löscht die TrutzBox danach selbsttätig. Die Frist gilt für Einzelgespräche und Gruppen gleichermaßen. Anhänge räumt die TrutzBox unabhängig davon schon nach 30 Tagen ab. Daneben sehen Sie den Platzbedarf der Verläufe und können sie über **Alle Verläufe löschen** in einem Schritt gesammelt entfernen. Getrennt davon nennt die Karte den **Platzbedarf der Anhänge**; mit **Alle Anhänge löschen** räumen Sie die gespeicherten Dateien in einem Zug ab, ohne die Verläufe anzutasten.

Gruppen auf dieser TrutzBox

Der Bereich **Gruppen auf dieser TrutzBox** macht alle Gruppen der TrutzBox sichtbar. Je Gruppe stehen in einer Zeile die Zahl der gerade verbundenen Teilnehmer, die Zahl der Mitglieder und der Zeitpunkt der Gründung. Aufgeklappt zeigt die Karte jedes Mitglied mit dem Zeitpunkt seiner Aufnahme und seiner letzten Anmeldung. Gerade bei offenen Einladungen ist das nützlich: Sie sehen sofort, seit wann jemand noch nicht reagiert hat.

- **Neue Gruppe anlegen:** erzeugt eine Gruppe samt Ersteller, ganz ohne Chat-Programm.
- **Teilnehmer aufnehmen:** macht ein weiteres TrutzMail-Konto zum Mitglied; die Einladung erscheint sofort in dessen Chat-Programm.
- **Papierkorb-Symbol:** entfernt eine ganze Gruppe oder ein einzelnes Mitglied.
- **Mitglieder dürfen weitere Teilnehmer einladen:** ein Schalter je Gruppe. Ist er aus, lädt nur der Ersteller ein; ist er an, darf jedes Mitglied weitere Teilnehmer aufnehmen.

Darunter listet die Karte außerdem die gerade angemeldeten Chat-Sitzungen. Daran sehen Sie auf einen Blick, wer aktuell verbunden ist und über wie viele Geräte.

12.5 TrutzChat benutzen: im Browser und mit einer Chat-App

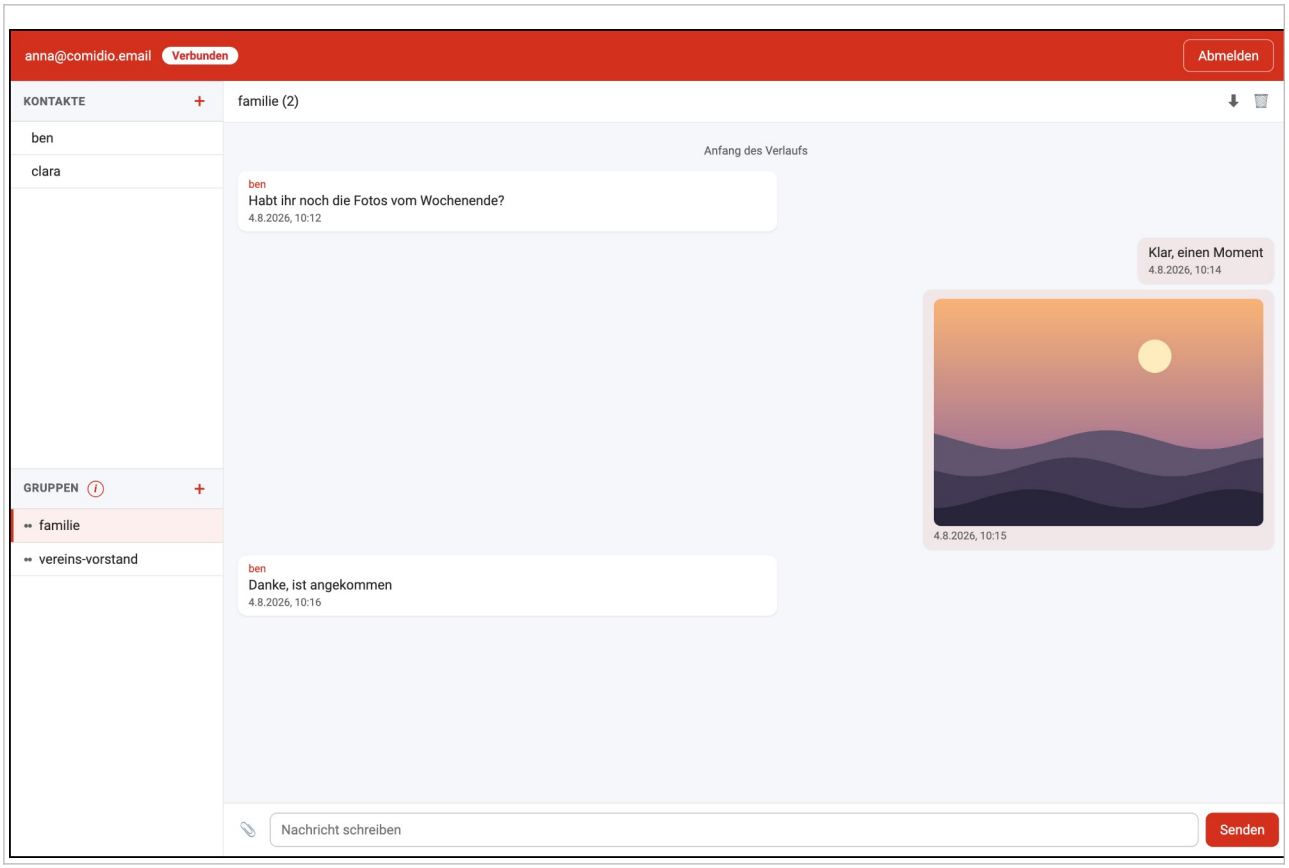


Abbildung 12-4: TrutzChat im Browser: links Kontakte und Gruppen, rechts das Gespräch mit Bildern und Dateien. (© 2026 Comidio GmbH)

Der eingebaute Web-Chat ist der einfachste Einstieg: Im eigenen Netz öffnen Sie `https://trutzbox/chat/` oder klicken im Reiter TrutzChat auf **TrutzChat öffnen**, und melden sich mit TrutzMail-Adresse und Passwort an. Von unterwegs bauen Sie zuerst die VPN-Verbindung auf (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“); danach funktioniert dieselbe Adresse wie im Netz der TrutzBox. Über den TrutzDynDNS-Namen ist der Web-Chat nicht erreichbar.

Kontakte und Kontaktanfragen

Einen Kontakt fügen Sie mit dem Pluszeichen neben **Kontakte** hinzu: TrutzMail-Adresse eintragen oder unter *„Benutzer dieser TrutzBox:"* ankreuzen. Zwischen zwei Benutzern derselben TrutzBox ist der Kontakt sofort in beiden Richtungen bestätigt. Bei einer Adresse auf einer anderen TrutzBox bestätigt die Gegenseite einmal. Danach zeigt ein farbiger Punkt die Erreichbarkeit.

Schreibt Ihnen eine Adresse, die noch kein Kontakt ist, oder möchte sie Ihre Erreichbarkeit sehen, entsteht daraus eine **Kontaktanfrage** und noch kein Gespräch. Der Web-Chat fragt *„Als Kontakt aufnehmen? Beide Seiten sehen danach, wann der andere erreichbar ist."* und nennt, wie viele Nachrichten von dieser Adresse warten. Mit **Aufnehmen** wird die Adresse Kontakt, und die wartenden Nachrichten erscheinen. **Ablehnen** sperrt die Adresse: Von dort kommen dann keine Nachrichten mehr an. Die Sperre endet, sobald Sie die Adresse selbst über **Kontakt hinzufügen** aufnehmen.

Nachrichten, Zustellung und Lesebestätigungen

Hinter der Uhrzeit jeder eigenen Nachricht steht ein Zeichen für ihren Zustand; zeigen Sie mit der Maus darauf, steht er in Worten da: eine kleine Uhr für *„Wird gesendet“*, ein Haken für *„Von der TrutzBox angenommen“*, zwei Haken für *„Zugestellt“* oder *„Gelesen“*, ein Ausrufezeichen für *„Nicht zugestellt“*. Im Kopf des Gesprächs sehen Sie, wenn die Gegenseite gerade *„tippt …“*, und sonst, wann sie zuletzt online war. Meldet eine Nachricht an eine andere TrutzBox „Nicht zugestellt", war die Gegenseite nicht erreichbar oder die Adresse nicht aktiv; die TrutzBox stellt sie nicht später von selbst zu, sondern sagt im Gespräch, woran es lag. Senden Sie die Nachricht dann später noch einmal (Kapitel „… ein Chat-Kontakt dauerhaft als nicht erreichbar erscheint“).

Unten in der Liste der Kontakte und Gruppen steht der Schalter **Lesebestätigungen senden**. Ist er aus, verschickt der Web-Chat keine Lesebestätigung, und die Lesebestätigungen der anderen bleiben Ihnen ebenfalls verborgen. Zustellbestätigungen gelten weiterhin.

Fotos, Dateien, Sprachnachricht und Standort

Dateien und Bilder wandern per Büroklammer und **Fotos und Dateien** oder einfach mit der Maus ins Fenster, auch mehrere auf einmal. Vor dem Senden zeigt eine Liste jede Datei mit Vorschau und Größe. Für Fotos wählen Sie unter **Auflösung der Fotos** zwischen **Klein (1024 px)**, **Mittel (2048 px)**, der Vorgabe, **Groß (4096 px)** und **Original**. Fotos im Format JPEG oder HEIC, wie Telefonkameras sie liefern, schreibt der Web-Chat vor dem Senden neu. Dabei fällt der Aufnahmeort heraus, den die Kamera in jedes Foto schreibt, auch bei **Original**. Je Datei sind höchstens 25 MB möglich.

Bilder erscheinen als Vorschau direkt im Gespräch, andere Dateien als anklickbarer Verweis; die Gegenseite lädt einen Anhang erst dann von Ihrer TrutzBox, wenn sie ihn öffnet. Nach 30 Tagen räumt die TrutzBox Anhänge selbsttätig ab.

Ist das Eingabefeld leer, steht rechts daneben das Mikrofon für eine **Sprachnachricht** von bis zu 5 Minuten. Über die Büroklammer und **Standort senden** schicken Sie nach einer Rückfrage Ihren Standort, den die Gegenseite auf einer Karte öffnen kann. Mikrofon und Standort gibt der Browser nur über die verschlüsselte Adresse `https://trutzbox/chat/` frei, und nur, wenn auf dem Gerät das Root-Zertifikat der TrutzBox installiert ist (Kapitel „Das Root-Zertifikat installieren“).

Anrufe aus dem Gespräch

Ist die Videokonferenz unter einem öffentlichen Namen eingerichtet (Abschnitt „Reiter Videokonferenz: einmalig einrichten“), stehen im Kopf eines Gesprächs zwei weitere Knöpfe: **Videoanruf starten** und **Anruf ohne Bild starten**; in Gruppen gibt es nur den Videoanruf. Ein Klick legt auf Ihrer TrutzBox einen Konferenzraum mit zufälligem Namen an, schreibt die Einladung ins Gespräch und öffnet die Konferenz in einem neuen Fenster, ohne zweite Anmeldung. Der Anruf ohne Bild ist derselbe Raum, nur mit zuerst ausgeschalteter Kamera. Bei der Gegenseite erscheint die Einladung als Knopf **Zum Videoanruf** bzw. **Zum Anruf**, der direkt in den Raum führt. Auch Adressen in Nachrichten lassen sich anklicken.

Der Gesprächsverlauf kommt aus dem Archiv Ihrer TrutzBox, nicht aus dem Browser. Deshalb steht er nach einem Browserwechsel oder an einem anderen Gerät unverändert bereit, und Nachrichten, die während Ihrer Abwesenheit eintreffen, liefert die TrutzBox beim nächsten Öffnen nach. Über die beiden Symbole rechts oben im Gespräch sichern oder löschen Sie den Verlauf:

Beim Sichern holt TrutzChat den vollständigen Verlauf von der TrutzBox; enthält das Gespräch Anhänge, entsteht ein ZIP-Archiv mit dem Text und allen Dateien, in der Reihenfolge des Gesprächs nummeriert. Das Löschen entfernt den Verlauf nach einer Rückfrage endgültig. Auch beim Entfernen eines Kontakts oder einer Gruppe können Sie den gespeicherten Verlauf gleich mitlöschen.

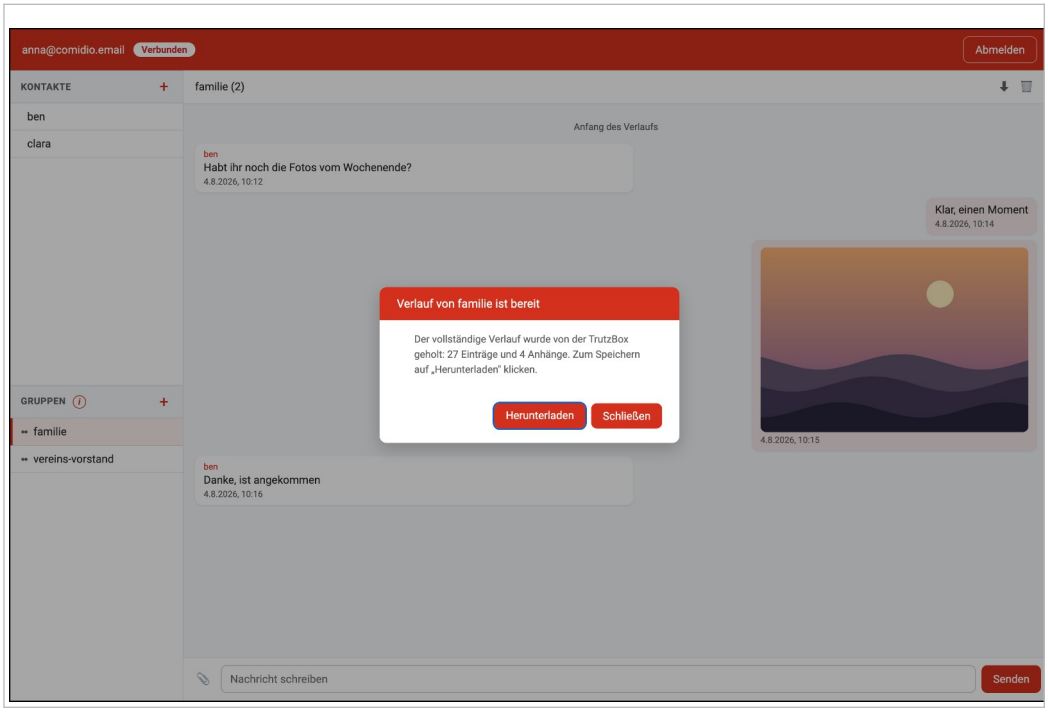


Abbildung 12-5: Verlauf sichern oder löschen: Der Gesprächsverlauf liegt auf Ihrer TrutzBox, nicht im Browser. (© 2026 Comidio GmbH)

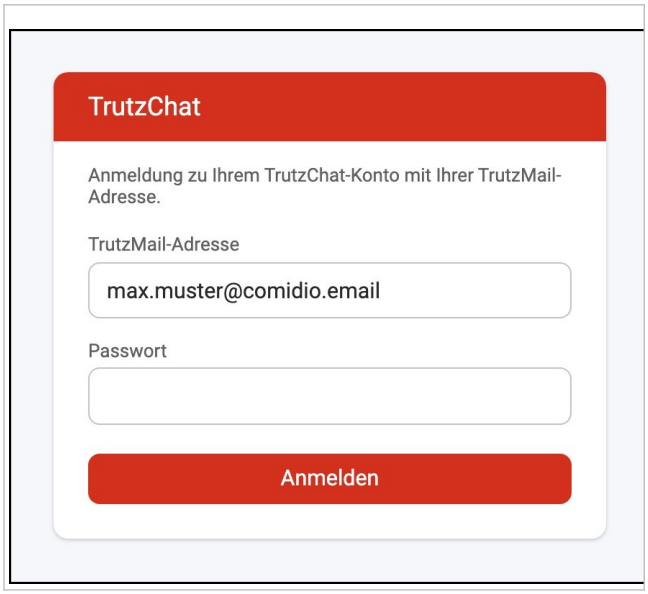


Abbildung 12-6: Die Anmeldung am Web-Chat mit TrutzMail-Adresse und Passwort. (© 2026 Comidio GmbH)

Eine Chat-App einrichten

Lieber eine App? TrutzChat spricht den offenen Chat-Standard XMPP, den viele Programme auf allen Systemen beherrschen. Sie melden sich darin mit TrutzMail-Adresse und Passwort an, als

Server tragen Sie den Namen Ihrer TrutzBox ein, ab Werk `trutzbox`. Die empfohlenen Programme je Betriebssystem und die Schritte stehen in Kapitel „Chat-Programme für TrutzChat einrichten“.

Für unterwegs führt der Weg über den VPN-Zugang (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“), für die App ebenso wie für den Web-Chat: Ist die VPN-Verbindung aufgebaut, funktioniert die App mit dem Servernamen `trutzbox` genau wie im Netz der TrutzBox. Eine Freigabe des Chat-Ports am Router ist nicht vorgesehen: Chat-Programme nimmt die TrutzBox nur aus dem eigenen Netz und über den VPN-Zugang an.

Welche Ports der Zugang von unterwegs braucht

Keine zusätzlichen. Web-Chat und Chat-Programme erreichen Sie von unterwegs über den Fernzugriff per VPN (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Der Chat läuft dann vollständig innerhalb der VPN-Verbindung, am Router braucht es nur die Freigabe für den VPN-Zugang. Port **5222/TCP** für Chat-Programme wird am Router nicht freigegeben. Im eigenen Netz und zwischen TrutzBoxen ist gar keine Freigabe nötig.

Die Freigabe auf **443/TCP** für die Videokonferenz führt nicht zum Web-Chat. Sie macht aber die Anmeldung am Chat-Server von außen erreichbar, die der Angriffsschutz bewacht (Abschnitt „Reiter Videokonferenz: einmalig einrichten“).

12.6 Kontakte und Gruppen

Menüpfad: Videokonferenz und Chat → TrutzChat



Abbildung 12-7: Gruppenverwaltung: Gruppen anlegen, Mitglieder aufnehmen und Verläufe im Blick behalten. (© 2026 Comidio GmbH)

Gruppen legen Sie direkt im Web-Chat an: Name vergeben, Mitglieder über ihre TrutzMail-Adressen eintragen, fertig; alle werden automatisch eingeladen. Das funktioniert auch TrutzBox-übergreifend, die TrutzBoxen der Teilnehmer verbinden sich dann verschlüsselt untereinander. Wer eingeladen wird, bekommt die Frage, ob er der Gruppe beitreten will, und antwortet mit **Beitreten** oder **Ablehnen**.

Das Stift-Symbol einer Gruppe (*„Teilnehmer anzeigen"*) öffnet die Mitglieder. Bei jedem steht seine Rolle: *„Ersteller"* oder *„Mitglied"*, dazu *„gerade nicht da"* für alle, die gerade nicht angemeldet sind; sie bleiben trotzdem Mitglied. Unter *„Aus den Kontakten einladen:"* kreuzen Sie bekannte Kontakte an, darunter lässt sich zusätzlich eine weitere TrutzMail-Adresse eintragen; **Einladen** schickt die Einladungen. Das × neben einem Namen nimmt jemanden aus der Gruppe. Die vollständige Liste sieht nur der Ersteller, die übrigen Mitglieder sehen die gerade Anwesenden. Der Ersteller kann eine Gruppe zusätzlich „Für alle löschen" oder sie wahlweise nur bei sich selbst entfernen.

Die Gruppenliste führt die TrutzBox selbst, nicht Ihr Chat-Programm. Wer in eine Gruppe aufgenommen wird, sieht sie deshalb automatisch in jedem seiner Chat-Programme, und eine gelöschte Gruppe verschwindet überall von selbst. Auch der Gruppenverlauf liegt im Archiv der TrutzBox, sodass Liste und Verlauf auf jedem Gerät gleich aussehen, ohne dass ein Programm selbst etwas speichern muss.

Solche Gruppen sind der Grund, warum die TrutzBox gern von Vereinen, Freundeskreisen, Schulen und Projektteams genutzt wird: Eine geschlossene Runde kann darüber gemeinsam schreiben, Dateien austauschen und bei Bedarf in dieselbe Videokonferenz wechseln, ohne dass ein fremder Dienst beteiligt ist. Wie lange die Verläufe aufbewahrt werden, legen Sie zentral fest (Abschnitt „Reiter TrutzChat: Selbsttest, Aufbewahrung, Gruppen“).

12.7 Was im Hintergrund für Sicherheit sorgt

Bei Nachrichten zwischen zwei TrutzBoxen greifen drei Schutzschichten ineinander. Die Nachricht selbst ist verschlüsselt, die Verbindung zwischen den TrutzBoxen ist zusätzlich verschlüsselt, und der Netzweg läuft über versteckte Dienste im Tor-Netzwerk. Dadurch bleibt nicht nur der Inhalt geschützt: Wer den Internet-Verkehr beobachtet, kann kaum erkennen, dass hier überhaupt gechattet wird oder welche Adressen beteiligt sind. Ein zentraler Server außerhalb der beteiligten TrutzBoxen ist nicht im Spiel.

Adressiert wird dabei immer die TrutzMail-Adresse, und beim Verbindungsaufbau prüft die TrutzBox die Beglaubigung der Gegenseite. Eine erfundene TrutzMail-Adresse nützt einem Angreifer deshalb nichts: Er kann sich damit nicht als jemand anderes ausgeben. Für Chat und Videokonferenz nutzt die TrutzBox genau dieselben Schlüssel und Zertifikate wie für TrutzMail. Eine einmal angelegte TrutzMail-Adresse ist damit ohne jede weitere Einrichtung auch die Chat-Adresse.

Die Videokonferenz arbeitet anders, aber nach demselben Grundgedanken: Der Konferenz-Server steht auf Ihrer TrutzBox und nimmt zu keinem anderen Server im Internet Verbindung auf. Die Browser der Teilnehmer sprechen ausschließlich mit Ihrer TrutzBox, und diese Verbindung ist verschlüsselt. Restrisiken bleiben, wie immer: ein befallenes Endgerät etwa, oder aufwendige Verkehrsanalysen. Gegen den Betreiber eines fremden Dienstes müssen Sie sich hier aber nicht absichern, denn es gibt keinen.

Häufige Fragen zu Chat und Videokonferenz

Können Chat-Partner auf anderen TrutzBoxen erreicht werden?

Ja. Nachrichten zwischen TrutzBoxen laufen verschlüsselt von TrutzBox zu TrutzBox, ohne zentralen Server, mit denselben Schlüsseln wie TrutzMail. Es genügt die TrutzMail-Adresse des Partners.

Die Videokonferenz klappt von außen nicht. Was prüfen?

Erst den Selbsttest „Erreichbarkeit prüfen" laufen lassen: Er unterscheidet fehlende Portfreigaben je Weg (IPv4 oder IPv6), ein anderes Gerät auf Port 443 und Zertifikatsprobleme. Zertifikatswarnungen bei Gästen deuten auf ein fehlendes Zertifikat von Let’s Encrypt oder ein nicht öffentlich anerkanntes eigenes Zertifikat. Endet eine Zeile mit „Gemessen von außen:", beruht das Urteil auf Testpaketen aus dem Internet und gilt so, wie es dasteht. Fehlt dieser Zusatz und meldet der Test, dass keine Verbindung zustande kam, fehlt entweder die Freigabe, oder der Router kann eine Anfrage aus dem eigenen Netz nicht über die öffentliche Adresse zurückleiten; im zweiten Fall funktioniert die Konferenz für Gäste von außen trotzdem.

Funktioniert der Chat auch ohne Internet-Zugang von außen?

Im eigenen Netz und zwischen TrutzBoxen ja, dafür braucht es keine Portfreigaben. Eingeschaltet sein muss aber der gemeinsame Server im Reiter Videokonferenz, und der setzt einen TrutzDynDNS-Namen oder einen eigenen Namen voraus (Abschnitt „Reiter Videokonferenz: einmalig einrichten“). Von unterwegs erreichen Sie Web-Chat und Chat-Programme über den VPN-Zugang.

Ich habe eine Kontaktanfrage versehentlich abgelehnt. Wie hebe ich die Sperre auf?

Nehmen Sie die Adresse selbst über **Kontakt hinzufügen** auf. Damit endet die Sperre, und Nachrichten von dieser Adresse kommen wieder an (Abschnitt „TrutzChat benutzen: im Browser und mit einer Chat-App“).

Kann ich einen Verlauf aufheben, bevor die Aufbewahrungsfrist ihn löscht?

Ja. Sichern Sie den Verlauf im Gespräch über das Symbol rechts oben. Enthält er Anhänge, erhalten Sie ein ZIP-Archiv mit Text und Dateien in der Reihenfolge des Gesprächs.

Warum sehe ich eine Gruppe in meiner App, die ich nie hinzugefügt habe?

Weil die TrutzBox die Gruppenliste führt und an jedes Ihrer Chat-Programme weitergibt. Jemand hat Sie in diese Gruppe aufgenommen; entfernen Sie sich, verschwindet sie überall.

13 TrutzBox unterwegs nutzen (TrutzVPN)

Zuhause oder in der Firma schützt die TrutzBox alle Geräte, die an ihr angeschlossen sind. Aber was ist im Hotel-WLAN, im Zug oder im Café? Genau dafür gibt es **TrutzVPN**: eine verschlüsselte Verbindung („Tunnel") von Ihrem Smartphone oder Laptop zu Ihrer TrutzBox. Sobald der Tunnel steht, läuft Ihr gesamter Internet-Verkehr erst durch die TrutzBox und dann ins Netz, mit allen Filtern und Schutzfunktionen, als wären Sie vor Ort. Niemand im fremden WLAN kann mitlesen.

Voraussetzungen

• Ihre TrutzBox ist fertig eingerichtet (Kapitel „TrutzBox einrichten (Setup)“) und Sie kennen das Admin-Passwort.

• Sie können sich an der Verwaltungsoberfläche Ihres Internet-Routers anmelden. Dort wird eine Portweiterleitung eingerichtet.

• Ihr Internet-Anschluss lässt Verbindungen von außen zu. Bei den meisten Anschlüssen ist das so, bei manchen nur über IPv6 und bei manchen, etwa vielen Mobilfunk-Routern, gar nicht. Welcher Fall bei Ihnen vorliegt, klärt der Abschnitt „Welcher Anschluss ist von außen erreichbar?“.

• Zeitbedarf: Die Einrichtung auf der TrutzBox dauert nur wenige Minuten. Dazu kommen die Portfreigabe am Router und etwa 5 Minuten je Endgerät.

Anleitung zum Anklicken

Von der Freigabe am Router bis zum ersten Verbindungstest: Die Anleitung „Fernzugriff mit TrutzVPN" zeigt die Stationen dieses Kapitels mit Bild, Text und Ton im Browser: trutzbox.de/videodokumentation.

13.1 So funktioniert TrutzVPN

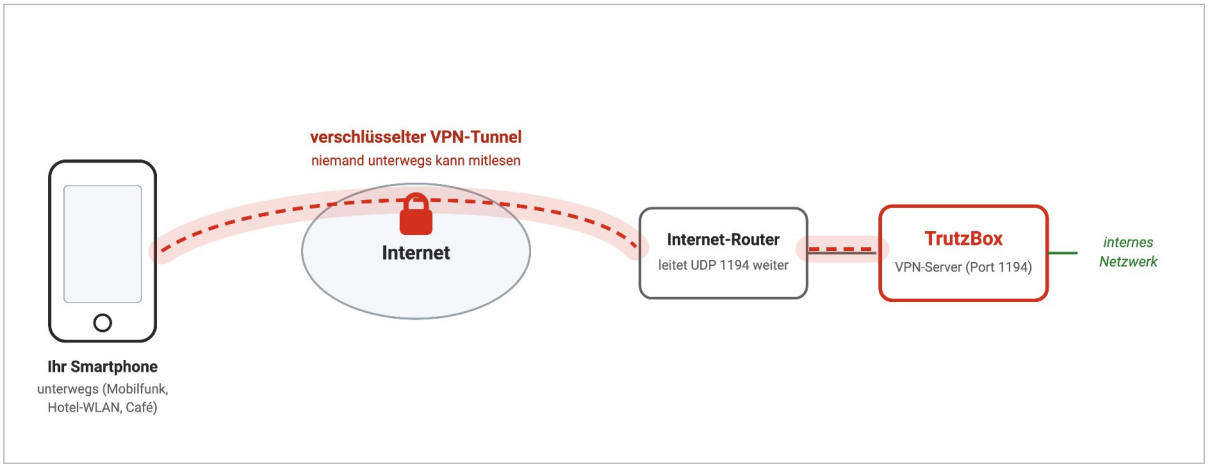


Abbildung 13-1: Der VPN-Tunnel: vom Smartphone unterwegs verschlüsselt durch das Internet bis zur TrutzBox. (© 2026 Comidio GmbH)

Drei Stationen spielen zusammen: Ihr Gerät unterwegs baut den Tunnel auf, Ihr Internet-Router reicht ihn durch, und die TrutzBox nimmt ihn an. Deshalb besteht die Einrichtung auch aus drei Teilen: einer auf der TrutzBox, einer am Router und einer auf jedem Endgerät. Fast alles auf der

TrutzBox erledigen Sie unter **Netzwerk → Fernzugriff**. Die OpenVPN-Profile gibt es unter **Verwaltung → Benutzer** (Abschnitt „OpenVPN statt WireGuard verwenden“).

TrutzVPN kennt zwei Tunnel. **WireGuard** ist die Vorgabe: der neuere, schlankere Weg. Er verbindet nach einem Netzwechsel in Sekunden neu und schont den Akku. **OpenVPN** ist der ältere, überall verbreitete Weg. Verschlüsselt wird bei beiden gleich stark. Es läuft immer nur einer der beiden, und beide benutzen denselben Anschluss UDP 1194. Am Router braucht es deshalb nur eine Freigabe, gleich welcher Tunnel läuft.

Die Fernzugriff-Seite ist in nummerierte Karten gegliedert. Ganz oben steht Karte **1. Domain-Namen festlegen** (Abschnitt „Schritt 1: Domain-Name festlegen (TrutzDynDNS)“). Darunter folgt der Bereich **Fernzugriff (TrutzVPN)** mit Karte 2 **Tunnel wählen** (Abschnitt „Schritt 3: Tunnel wählen“). Was danach kommt, hängt vom gewählten Tunnel ab:

- **WireGuard läuft:** Karte 3 gehört OpenVPN. Sie heißt **VPN-Server einrichten**, solange OpenVPN nie eingerichtet war, sonst **OpenVPN-Server** mit dem Hinweis, dass OpenVPN ruht. Karte 4 **TrutzVPN über WireGuard** enthält alles für den Tunnel: den Schalter, die Erreichbarkeitsprüfung und die Zugänge der Geräte (Abschnitte „Schritt 4: Erreichbarkeit von WireGuard prüfen“ und „Schritt 5: Zugänge für die WireGuard-App anlegen“).
- **OpenVPN läuft:** Karte 3 **Erreichbarkeit prüfen**, Karte 4 **OpenVPN-Server** und Karte 5 **TrutzVPN über WireGuard**, die dann nur sagt, dass WireGuard ruht oder noch nicht eingerichtet ist (Abschnitt „OpenVPN statt WireGuard verwenden“).
- **Noch kein Tunnel:** Auf einer frisch eingerichteten TrutzBox läuft noch keiner. Bis Sie in Karte 2 einen Tunnel einschalten, zeigt die Seite dieselben Karten wie bei OpenVPN; nur heißt Karte 4 dort noch **VPN-Server einrichten**.

Die Portweiterleitung aus Abschnitt „Schritt 2: Portweiterleitung am Internet-Router“ hat bewusst keine eigene Karte, denn sie wird nicht auf der TrutzBox, sondern am Internet-Router eingerichtet. Dieses Kapitel beschreibt zuerst den Weg mit WireGuard (Abschnitte „Schritt 1: Domain-Name festlegen (TrutzDynDNS)“ bis „Ihre Geräte einrichten“). Wer OpenVPN nutzen will, etwa weil auf den Geräten schon OpenVPN-Profile eingerichtet sind, findet alles dazu in Abschnitt „OpenVPN statt WireGuard verwenden“.

Menüpfad: Netzwerk → Fernzugriff

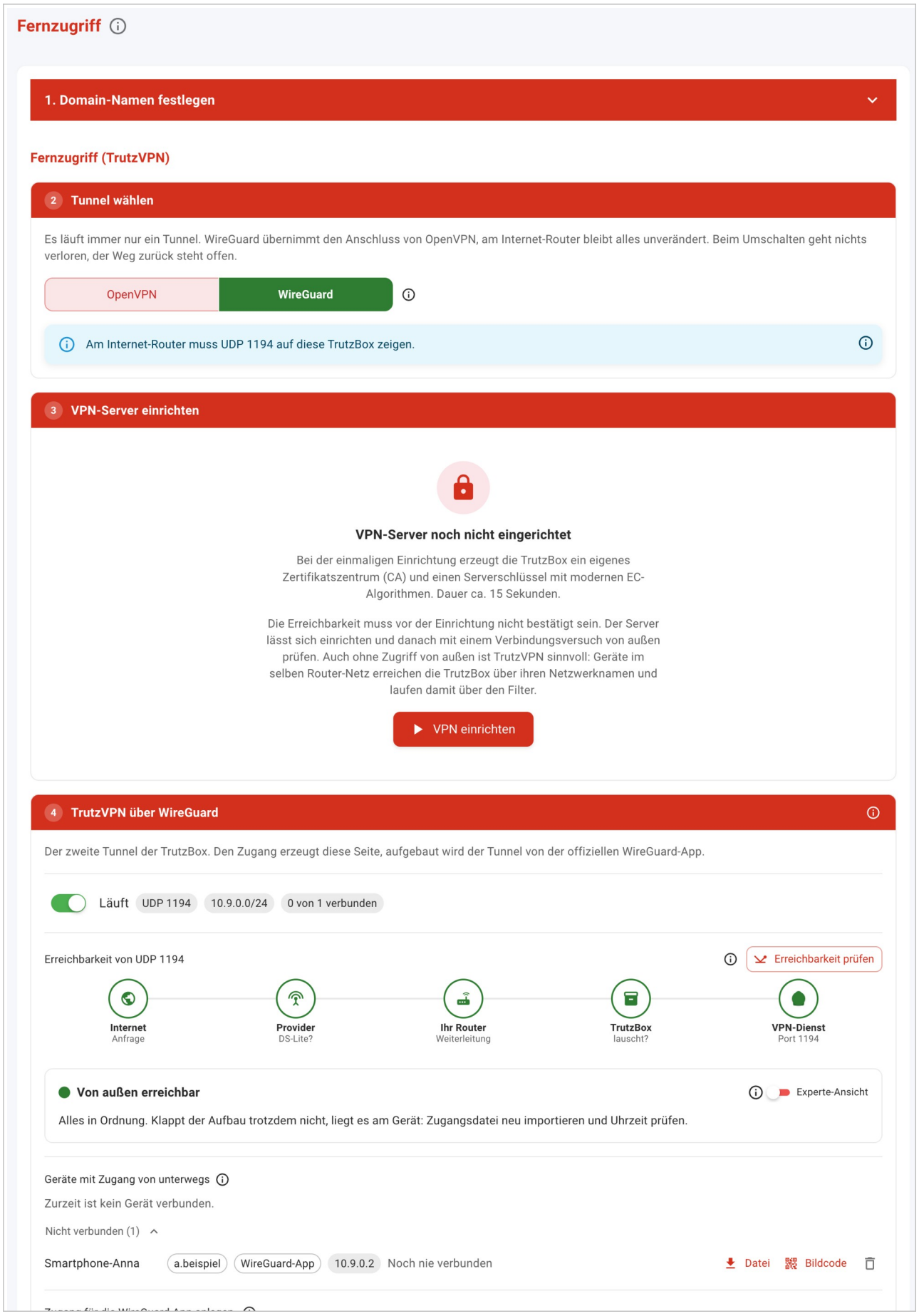

Fernzugriff
1. Domain-Namen festlegen
Fernzugriff (TrutzVPN)
2 Tunnel wählen
Es läuft immer nur ein Tunnel. WireGuard übernimmt den Anschluss von OpenVPN, am Internet-Router bleibt alles unverändert. Beim Umschalten geht nichts verloren, der Weg zurück steht offen.
OpenVPN
WireGuard
Am Internet-Router muss UDP 1194 auf diese TrutzBox zeigen.
3 VPN-Server einrichten
VPN-Server noch nicht eingerichtet
Bei der einmaligen Einrichtung erzeugt die TrutzBox ein eigenes Zertifikatszentrum (CA) und einen Serverschlüssel mit modernen EC-Algorithmen. Dauer ca. 15 Sekunden.
Die Erreichbarkeit muss vor der Einrichtung nicht bestätigt sein. Der Server lässt sich einrichten und danach mit einem Verbindungsversuch von außen prüfen. Auch ohne Zugriff von außen ist TrutzVPN sinnvoll: Geräte im selben Router-Netz erreichen die TrutzBox über ihren Netzwerknamen und laufen damit über den Filter.
VPN einrichten
4 TrutzVPN über WireGuard
Der zweite Tunnel der TrutzBox. Den Zugang erzeugt diese Seite, aufgebaut wird der Tunnel von der offiziellen WireGuard-App.
Läuft
UDP 1194
10.9.0.0/24
0 von 1 verbunden
Erreichbarkeit von UDP 1194
Erreichbarkeit prüfen
Internet
Anfrage
Provider
DS-Lite?
Ihr Router
Weiterleitung
TrutzBox
lauscht?
VPN-Dienst
Port 1194
Von außen erreichbar
Experte-Ansicht
Alles in Ordnung. Klappt der Aufbau trotzdem nicht, liegt es am Gerät: Zugangsdatei neu importieren und Uhrzeit prüfen.
Geräte mit Zugang von unterwegs
Zurzeit ist kein Gerät verbunden.
Nicht verbunden (1)
Smartphone-Anna
a.beispiel
WireGuard-App
10.9.0.2
Noch nie verbunden
Datei
Bildcode

Abbildung 13-2: Die Seite Fernzugriff, wenn WireGuard läuft: Karte 1 zugeklappt, Karte 2 „Tunnel wählen“ mit WireGuard, Karte 3 für OpenVPN (hier noch nicht eingerichtet) und Karte 4 „TrutzVPN über WireGuard“ mit dem Zugang „Smartphone-Anna“. (© 2026 Comidio GmbH)

> **Für Neugierige: Die Technik dahinter**
> Der Server des jeweiligen Tunnels läuft auf der TrutzBox und ist über den UDP-Port 1194 erreichbar. Jeder Zugang trägt einen eigenen Schlüssel, bei OpenVPN in Form eines eigenen Zertifikats; ein Passwort allein genügt Angreifern also nicht. Die Verbindung selbst ist nach aktuellem Stand der Technik verschlüsselt, und der Server gibt sich Unbefugten gegenüber gar nicht erst zu erkennen: Wer den passenden Schlüssel nicht hat, bekommt schlicht keine Antwort.

13.2 Schritt 1: Domain-Name festlegen (TrutzDynDNS)

Ihr Gerät muss Ihre TrutzBox im Internet finden können. Dafür bekommt sie einen festen Namen, der immer auf die aktuelle Adresse Ihres Anschlusses zeigt. Schalten Sie dazu TrutzDynDNS ein, wie im Kapitel „TrutzDynDNS: Ihre TrutzBox aus dem Internet erreichbar machen“ beschrieben, und notieren Sie den angezeigten Namen, etwa `beispiel.mytrutzbox.de`. Ohne einen solchen Namen lässt sich WireGuard nicht einschalten; die Seite weist dann darauf hin.

Lesen Sie dort vorher auch den Abschnitt „Welcher Anschluss ist von außen erreichbar?“. An manchen Anschlüssen kommt von außen nichts an, ganz gleich, was Sie am Router einstellen. Das lässt sich in zwei Minuten klären, bevor Sie Zeit in die weiteren Schritte stecken.

13.3 Schritt 2: Portweiterleitung am Internet-Router

Ihr Router lässt Verbindungsversuche aus dem Internet normalerweise nicht ins interne Netz. Das ist gut so. Für TrutzVPN brauchen Sie eine einzige, gezielte Ausnahme: Der Router soll alles, was auf **Port 1194** mit dem Protokoll **UDP** ankommt, an die TrutzBox weiterreichen. Das nennt sich **Portweiterleitung** oder Portfreigabe. Diese eine Freigabe gilt für beide Tunnel: WireGuard übernimmt beim Umschalten den Anschluss von OpenVPN, am Router ändert sich nichts.

Wie die Einrichtung genau aussieht, unterscheidet sich von Router zu Router, und die Hersteller ändern ihre Oberflächen laufend. Deshalb steht hier das Prinzip. Wie das in einer FRITZ!Box aussieht, mit Bildern, und wo die Anleitungen der anderen Hersteller stehen, zeigt Kapitel „Ports und Freigaben am Internet-Router“. Im Grundsatz sind es immer dieselben fünf Schritte:

1. Melden Sie sich an der Verwaltungsoberfläche Ihres Routers an. Die Adresse steht meist auf einem Aufkleber am Gerät, z. B. `http://fritz.box`.
2. Suchen Sie den Menüpunkt „Portfreigabe", „Portweiterleitung" oder englisch „Port Forwarding", oft unter „Internet" oder „Freigaben".
3. Legen Sie eine neue Freigabe an und wählen Sie als Gerät die **TrutzBox** aus. Sie erscheint in der Geräteliste des Routers unter dem Namen „trutzbox".
4. Tragen Sie Port **1194** ein und stellen Sie das Protokoll auf **UDP**, nicht TCP.
5. Speichern Sie die Freigabe.

Häufigster Stolperstein: TCP statt UDP

Wenn der Fernzugriff später nicht klappt, ist in den allermeisten Fällen die Portfreigabe schuld: Protokoll versehentlich auf TCP gestellt, falscher Port oder falsches Zielgerät. Prüfen Sie diese drei Angaben zuerst.

Brauchen Sie auch die Videokonferenz, legen Sie deren Freigaben gleich mit an. Alle Freigaben auf einen Blick stehen in Abschnitt „Welche Ports die TrutzBox braucht“.

IPv6-Freigabe und mehrere TrutzBoxen

Wollen Sie TrutzVPN auch über IPv6 anbieten, kommt am Router eine zweite Regel hinzu, die IPv6-Freigabe (Abschnitt „VPN auch über IPv6 anbieten“). Für die Grundeinrichtung genügt die Portweiterleitung oben.

Hängen mehrere TrutzBoxen am selben Router, lässt sich Port 1194 über IPv4 nur an eine davon weiterleiten. Jede weitere TrutzBox bekommt am Router einen eigenen Port von außen (Abschnitt „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“) oder wird über IPv6 erreicht (Abschnitt „VPN auch über IPv6 anbieten“).

13.4 Schritt 3: Tunnel wählen

Welcher Tunnel läuft, legen Sie in Karte 2 **Tunnel wählen** fest. Die Karte trägt einen Schalter aus zwei Hälften: links **OpenVPN**, rechts **WireGuard**. Die gewählte Hälfte ist grün, die andere blass rot. WireGuard ist die Vorgabe und steht deshalb auch auf einer frisch eingerichteten TrutzBox grün. Eingeschaltet ist damit aber noch nichts. Darunter steht dann *„Noch läuft kein Tunnel. Ein Klick auf OpenVPN oder WireGuard schaltet ihn ein.“*

Menüpfad: Netzwerk → Fernzugriff

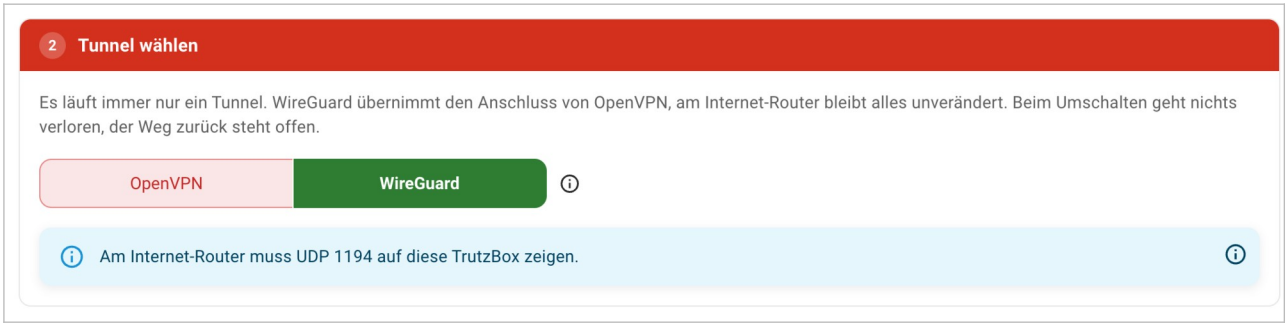


Abbildung 13-3: Karte 2 „Tunnel wählen“: WireGuard ist gewählt und grün, OpenVPN blass rot. Darunter der Hinweis, welcher Anschluss am Router auf die TrutzBox zeigen muss. (© 2026 Comidio GmbH)

1. Prüfen Sie, dass Karte 1 einen Namen nennt, also TrutzDynDNS oder Ihr eigener Name eingeschaltet ist (Abschnitt „Schritt 1: Domain-Name festlegen (TrutzDynDNS)“).
2. Klicken Sie in Karte 2 auf **WireGuard**.
3. Warten Sie, bis der Balken unter dem Schalter verschwindet. Beim ersten Mal richtet die TrutzBox WireGuard dabei ein und lädt die nötigen Pakete aus dem Internet nach; das dauert einen Moment länger. Danach läuft der Tunnel, und Karte 4 **TrutzVPN über WireGuard** zeigt den Schalter **Läuft**.

Unter dem Schalter steht der Hinweis *„Am Internet-Router muss UDP 1194 auf diese TrutzBox zeigen.“* Das „i" an seinem rechten Rand sagt, womit sich die Geräte verbinden; das „i" neben dem Schalter vergleicht die beiden Tunnel.

Läuft schon ein Tunnel und Sie klicken auf den anderen, fragt die TrutzBox unter **Tunnel umschalten** nach. Mit **Umschalten** hält sie den laufenden Tunnel an und startet den anderen. Gelöscht wird dabei nichts: Ausgestellte OpenVPN-Profile und angelegte WireGuard-Zugänge bleiben erhalten und gelten wieder, sobald Sie zurückschalten. Während WireGuard läuft, kommen OpenVPN-Profile allerdings nicht durch, und umgekehrt. Läuft auf Ihrer TrutzBox schon OpenVPN, etwa seit einer früheren Einrichtung, bleibt es dabei, bis Sie umschalten; die Karte zeigt dann OpenVPN grün.

> **Nicht umschalten, während Sie selbst über das VPN verbunden sind**
> Die Oberfläche warnt Sie in diesem Fall. Mit dem Umschalten bricht genau die Verbindung ab, über die Sie gerade arbeiten. Aus dem Netz der TrutzBox erreichen Sie die Oberfläche danach wie gewohnt, von unterwegs erst wieder über den neuen Tunnel.

13.5 Schritt 4: Erreichbarkeit von WireGuard prüfen

Läuft WireGuard, liegt alles Weitere in Karte 4 **TrutzVPN über WireGuard**. Oben stehen der Schalter **Läuft** und drei Plaketten: der Anschluss (UDP 1194), das Netz im Tunnel (10.9.0.0/24; daraus bekommt jedes Gerät seine eigene Adresse) und wie viele Geräte gerade verbunden sind, etwa „0 von 1 verbunden".

Menüpfad: Netzwerk → Fernzugriff

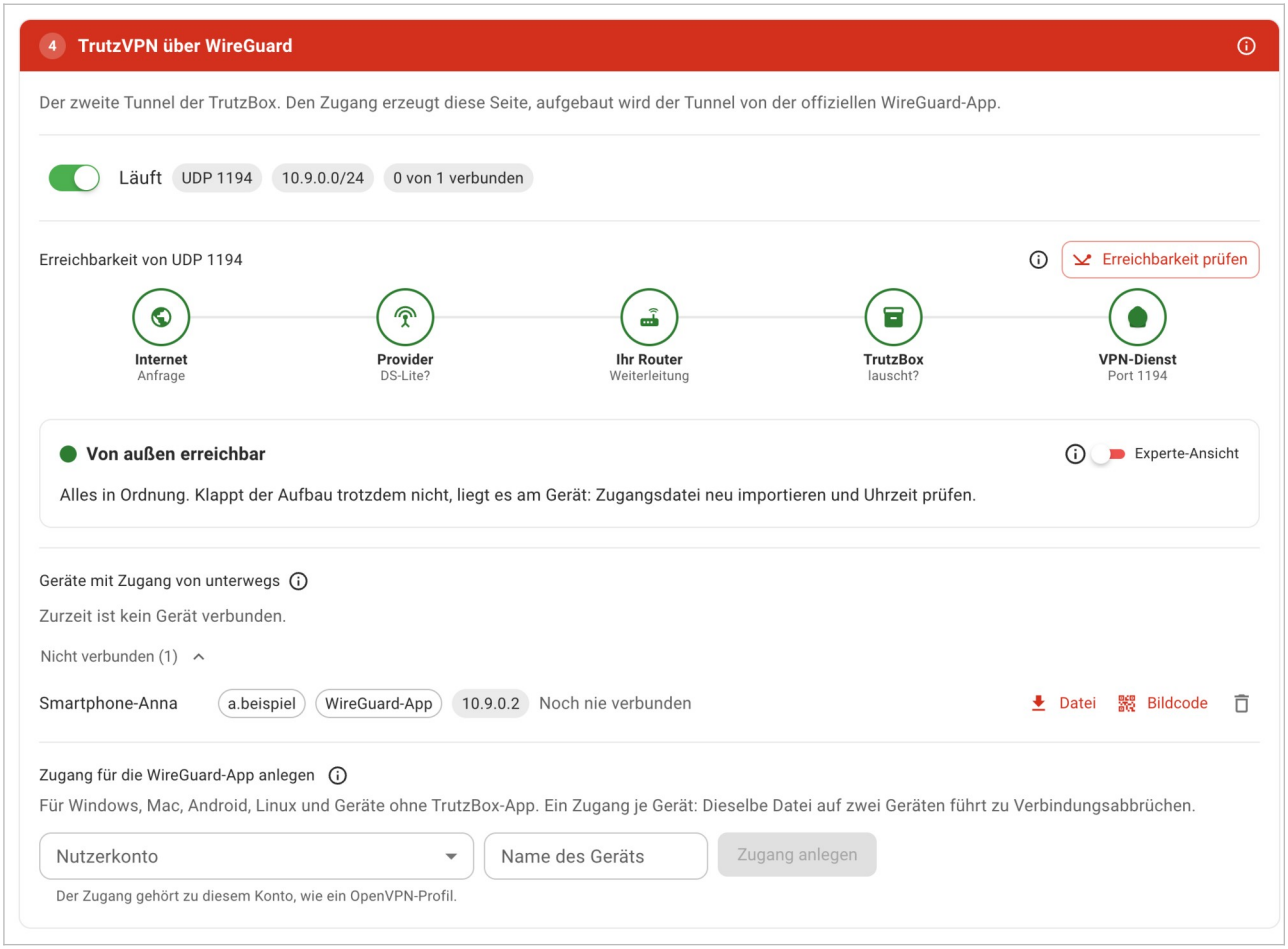


Abbildung 13-4: Karte 4 „TrutzVPN über WireGuard“: Der Tunnel läuft, die Prüfung meldet „Von außen erreichbar“. Darunter die Liste der Geräte mit dem Zugang „Smartphone-Anna“ und der Bereich zum Anlegen weiterer Zugänge. (© 2026 Comidio GmbH)

Darunter steht **Erreichbarkeit von UDP 1194** mit dem Knopf **Erreichbarkeit prüfen**. Die TrutzBox schickt sich dabei selbst ein Testpaket über den Internet-Router und zählt an ihrer Firewall, ob es zurückkommt. Der laufende Tunnel stört dabei nicht. Gleich nach dem Umschalten auf WireGuard prüft die Karte das von selbst. Das Ergebnis zeigt sie als Kette mit fünf Stationen:

- **Internet:** die Anfrage von außen, also der Verbindungsversuch selbst.
- **Provider:** ob die TrutzBox ihre öffentliche Internet-Adresse ermitteln kann.
- **Ihr Router:** ob die Portweiterleitung für UDP 1194 greift.
- **TrutzBox:** ob die TrutzBox auf diesem Port überhaupt lauscht.
- **VPN-Dienst:** ob die Verbindung am Ende beim VPN-Server ankommt.

Unter der Kette steht das Ergebnis im Klartext, im besten Fall *„Von außen erreichbar“*. Die übrigen Ergebnisse und was dann hilft, stehen in Abschnitt „Wenn es nicht klappt“. Der Schalter **Experte-Ansicht** blendet zusätzlich die technischen Werte ein, die der Support gelegentlich braucht. Ist die Kette durchgehend grün, können Sie direkt mit Abschnitt „Schritt 5: Zugänge für die WireGuard-App anlegen“ weitermachen.

Warum die Prüfung bei WireGuard so wichtig ist

WireGuard schickt nie eine Fehlermeldung. Ein Gerät, dessen Anfrage nicht bis zur TrutzBox kommt, erlebt dasselbe wie eines mit falschem Schlüssel: Stille. Die App auf dem Gerät kann deshalb nicht sagen, woran es liegt. Die Prüfung auf der TrutzBox schon.

Trotz richtiger Portfreigabe kommt nichts an?

Dann liegt es meist am Internet-Anschluss selbst: Bei DS-Lite fehlt die eigene öffentliche IPv4-Adresse, und an vielen Mobilfunk-Routern kommt von außen gar nichts an. Woran Sie Ihren Anschluss erkennen und was jeweils hilft, steht im Abschnitt „Welcher Anschluss ist von außen erreichbar?“. Fehlt nur die IPv4-Adresse, bieten Sie TrutzVPN über IPv6 an (Abschnitt „VPN auch über IPv6 anbieten“).

Test meldet „Von außen nicht bestätigt“, obwohl alles stimmt?

Manche Router reichen ein Paket, das die TrutzBox an ihre eigene öffentliche Adresse schickt, nicht an sich selbst zurück (das „Hairpin"-Verfahren). Dann sagt der Selbsttest nichts über den Weg von außen, und das Ergebnis bleibt unbestätigt, obwohl der Zugang funktioniert. Machen Sie im Zweifel einen echten Verbindungsversuch: mit dem Smartphone über Mobilfunk, WLAN dabei ausschalten. Kommt dabei ein Handschlag an, ist der Weg bewiesen. Der Handschlag ist die kurze Anmeldung, mit der sich ein Gerät beim Verbinden mit seinem Schlüssel bei der TrutzBox meldet. Sie erkennen ihn in Karte 4 unter **Geräte mit Zugang von unterwegs**: Das Gerät steht dann bei den verbundenen Geräten oder trägt „Zuletzt verbunden" statt „Noch nie verbunden" (Abschnitt „Schritt 5: Zugänge für die WireGuard-App anlegen“).

Unabhängig von diesem Selbsttest prüft die TrutzBox ihre Erreichbarkeit regelmäßig mit Testpaketen aus dem Internet. Das Ergebnis steht unter **Netzwerk → Status** im Abschnitt **Erreichbarkeit von außen** und hängt nicht vom Router ab (Kapitel „Netzwerk-Übersicht: außen und innen“).

Tunnel aus = Tür zu

Wenn Sie längere Zeit keinen Fernzugriff brauchen, schalten Sie den Schalter **Läuft** einfach aus. Dann erreicht kein Gerät die TrutzBox von unterwegs über WireGuard, Port 1194 ist aus dem Internet nicht mehr erreichbar, und automatische Scanner können erst gar keinen Anlauf nehmen. Die Zugänge bleiben erhalten. Zur nächsten Reise schalten Sie den Tunnel mit einem Klick wieder ein.

13.6 Schritt 5: Zugänge für die WireGuard-App anlegen

Jedes Gerät, das sich von unterwegs verbinden soll, braucht einen eigenen **Zugang**. Er gehört zu einem Nutzerkonto der TrutzBox, wie ein OpenVPN-Profil. Anders als bei OpenVPN braucht eine Person mit mehreren Geräten aber keinen zweiten Benutzer: Unter einem Konto legen Sie so viele Zugänge an, wie die Person Geräte hat, je Gerät einen.

1. Wählen Sie in Karte 4 im Bereich **Zugang für die WireGuard-App anlegen** unter **Nutzerkonto** das Konto aus.
2. Tragen Sie unter **Name des Geräts** einen Namen ein, etwa `Smartphone-Anna`. Erlaubt sind Buchstaben, Ziffern, Punkt, Strich und Unterstrich, höchstens 31 Zeichen.
3. Klicken Sie auf **Zugang anlegen**. Es öffnet sich das Fenster **Zugang Smartphone-Anna** mit Bildcode und Text.
4. Bringen Sie den Zugang auf das Gerät (Abschnitt „Ihre Geräte einrichten“): am Telefon den Bildcode einlesen, am Rechner über **Datei** die `.conf`-Datei herunterladen. **Kopieren** legt den Text in die Zwischenablage. Danach **Schließen**.

Menüpfad: Netzwerk → Fernzugriff

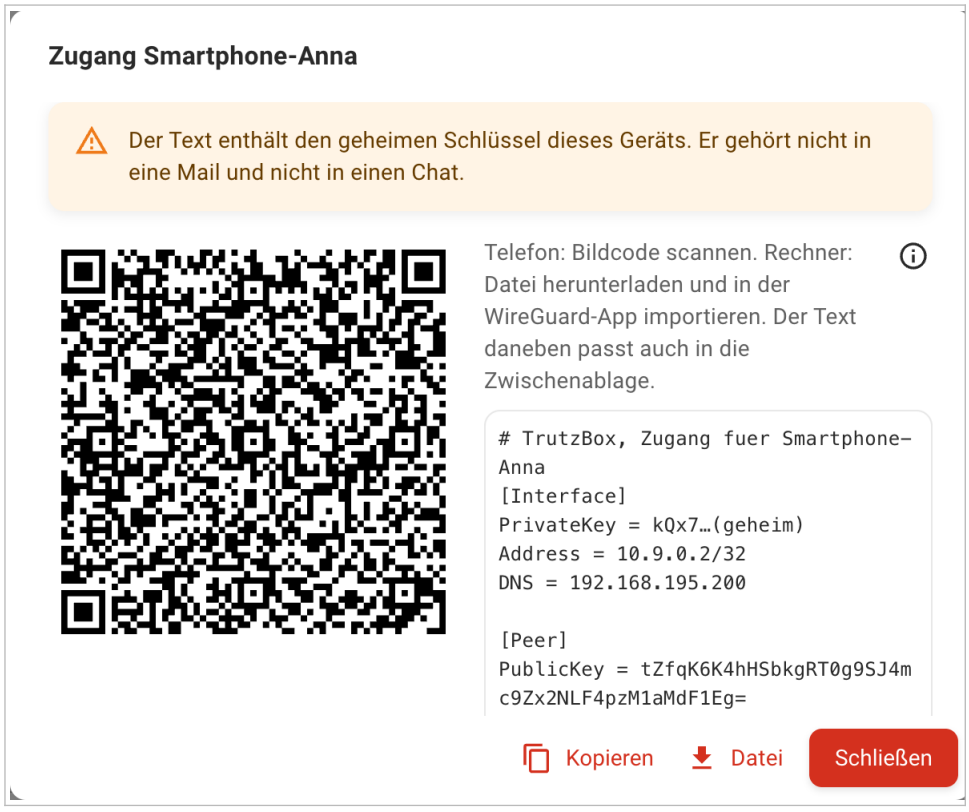


Abbildung 13-5: Das Fenster „Zugang Smartphone-Anna“: links der Bildcode für das Telefon, rechts derselbe Inhalt als Text, darunter „Kopieren“ und „Datei“. (© 2026 Comidio GmbH)

Ein Zugang gehört zu einem Gerät

Jeder Zugang trägt seinen eigenen Schlüssel. Das Fenster warnt deshalb: *„Der Text enthält den geheimen Schlüssel dieses Geräts. Er gehört nicht in eine Mail und nicht in einen Chat.“* Dieselbe Datei auf zwei Geräten führt zu ständigen Verbindungsabbrüchen, weil beide dieselbe Adresse im Tunnel beanspruchen. Legen Sie deshalb je Gerät einen eigenen Zugang an, und entfernen Sie verlorene Zugänge.

Alle Zugänge stehen in Karte 4 unter **Geräte mit Zugang von unterwegs**. Oben stehen die Geräte, die gerade verbunden sind; ist keines verbunden, steht dort *„Zurzeit ist kein Gerät verbunden.“* Die übrigen liegen zugeklappt unter **Nicht verbunden** mit ihrer Anzahl in Klammern. Jede Zeile nennt

den Namen des Geräts, das Konto, die Art („WireGuard-App"), die Adresse im Tunnel und den letzten Kontakt, etwa „Noch nie verbunden". Über **Datei** und **Bildcode** holen Sie einen Zugang jederzeit erneut, das Papierkorb-Symbol entfernt ihn. Ein entfernter Zugang verbindet sich nicht mehr.

Hatte ein Zugang über 90 Tage keinen Kontakt, kennzeichnet ihn die Liste mit „Über 90 Tage unbenutzt". Darüber erscheint ein Hinweis mit dem Knopf **Unbenutzte entfernen**. Nach der Rückfrage *„Unbenutzte Zugänge entfernen?“* entfernt er alle diese Zugänge auf einmal. Die Geräte verbinden sich danach nicht mehr; ein neuer Zugang lässt sich jederzeit anlegen. Den letzten Kontakt merkt sich die TrutzBox auch über einen Neustart hinweg.

Zugänge lassen sich auch beim Benutzer anlegen: Läuft WireGuard, zeigt unter **Verwaltung → Benutzer** der Bereich **Fernzugriff (VPN)** die WireGuard-Zugänge dieses Kontos samt dem Knopf **WireGuard-Zugang anlegen** (Kapitel „Die Detail-Einstellungen eines Benutzers“).

13.7 Ihre Geräte einrichten

Auf dem Endgerät baut die offizielle **WireGuard-App** den Tunnel auf, kostenlos vom WireGuard-Projekt. Liest die App Bildcodes, genügt der Bildcode; sonst nehmen Sie die Datei. Das Vorgehen ist überall gleich und besteht aus drei Handgriffen:

1. WireGuard-App installieren (Bezugsquelle je System in Kapitel „VPN-Apps für TrutzVPN einrichten“).
2. Zugang hineinbringen: am Telefon den Bildcode einlesen, am Rechner die `.conf`-Datei importieren.
3. Verbindung einschalten. Fertig.

Die App je Betriebssystem und die Handgriffe darin beschreibt Kapitel „VPN-Apps für TrutzVPN einrichten“.

> **Läuft die TrutzBox auf OpenVPN?**
> Dann brauchen Ihre Geräte statt der WireGuard-App das Programm OpenVPN Connect und statt des Zugangs ein OpenVPN-Profil mit der Endung `.ovpn`. Welcher Tunnel läuft, zeigt Karte 2 auf der Fernzugriff-Seite. Alles zu OpenVPN steht in Abschnitt „OpenVPN statt WireGuard verwenden“, die Programme je Betriebssystem in Abschnitt „Geräte mit OpenVPN einrichten“.

13.8 Unterwegs verbinden

Unterwegs genügt künftig ein Fingertipp in der WireGuard-App, bei OpenVPN in OpenVPN Connect. Sobald die Verbindung steht, erkennbar am Schlüssel- oder VPN-Symbol in der Statusleiste, läuft Ihr gesamter Datenverkehr durch den Tunnel zu Ihrer TrutzBox. Die Filter gegen unerwünschten Datenverkehr greifen also auch unterwegs: gegen Werbung, gegen die Aufzeichnung dessen, was Sie tun, und gegen Verbindungen zu gefährlichen Servern. Im Monitor der TrutzBox taucht Ihr Gerät wie gewohnt auf, die Einwahl selbst ist als „TrutzVPN-Einwahl (Fernzugang)" gekennzeichnet. Auch die Dienste in Ihrem Netzwerk erreichen Sie so von unterwegs.

Wenn Sie den Schutz nicht brauchen, trennen Sie die Verbindung einfach wieder im Programm, etwa um Akku zu sparen. Ein dauerhaft verbundenes Smartphone verbraucht durch den Tunnel etwas mehr Datenvolumen und Energie.

Den Weg zur TrutzBox bestimmt der Zugang auf dem Gerät. Ein WireGuard-Zugang kennt genau einen Weg: den öffentlichen Namen der TrutzBox, also den TrutzDynDNS-Namen oder Ihren eigenen Namen (Abschnitt „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“). Ein OpenVPN-Profil kennt mehrere: Im lokalen Netz verbindet es sich über IPv4 mit dem Netzwerknamen der TrutzBox. Haben Sie **VPN auch über IPv6 anbieten** eingeschaltet (Abschnitt „VPN auch über IPv6 anbieten“), probiert es unterwegs zuerst IPv6 und weicht sonst auf IPv4 aus. Ob der Zugang von außen funktioniert, zeigt deshalb nur ein Versuch unterwegs, etwa über Mobilfunk bei ausgeschaltetem WLAN.

13.9 Wenn es nicht klappt

Der häufigste Fall: Das VPN-Programm baut keine Verbindung auf oder bleibt beim Verbinden hängen. Die WireGuard-App zeigt dabei grundsätzlich keinen Fehler (Abschnitt „Schritt 4: Erreichbarkeit von WireGuard prüfen“). Ihre TrutzBox hilft bei der Ursachensuche mit der Erreichbarkeitsprüfung auf der Fernzugriff-Seite: bei WireGuard in Karte 4 (Abschnitt „Schritt 4: Erreichbarkeit von WireGuard prüfen“), bei OpenVPN in Karte 3 (Abschnitt „OpenVPN statt WireGuard verwenden“). Die Kette zeigt Station für Station, wie weit eine Anfrage von außen kommt und woran sie scheitert, darunter steht das Ergebnis. Die folgende Tabelle nennt die Ergebnisse, die etwas zu tun geben, und die übrigen häufigen Fälle:

Menüpfad: Netzwerk → Fernzugriff

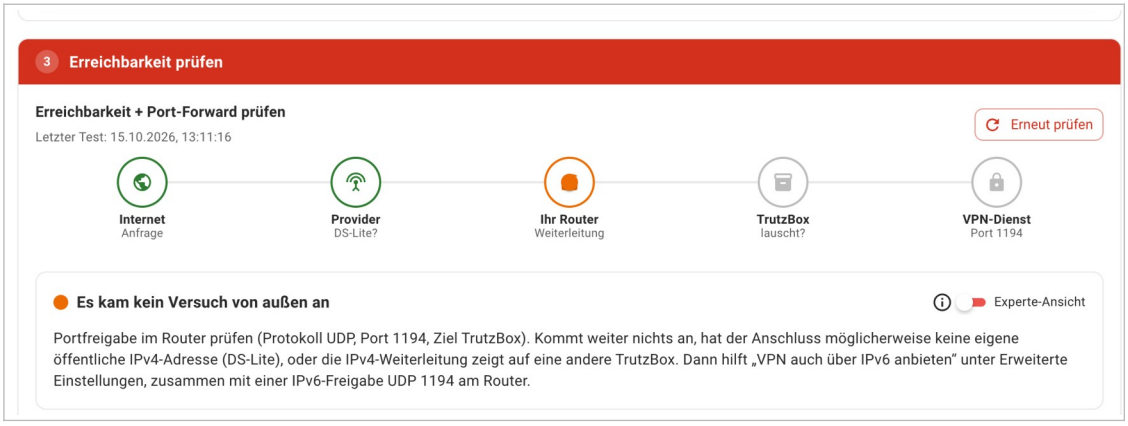


Abbildung 13-6: Ein gescheiterter Test bei OpenVPN: Die Kette bleibt bei „Ihr Router“ stehen, das Ergebnis lautet „Es kam kein Versuch von außen an“, darunter steht, was zu prüfen ist. (© 2026 Comidio GmbH)

Anzeige oder Symptom	Wahrscheinliche Ursache	Das hilft
„Der Router leitet diesen Anschluss nicht hierher" (nur WireGuard, Kette stoppt bei „Ihr Router")	Ein Testpaket auf einen anderen, nachweislich freigegebenen Anschluss kam zurück, das auf UDP 1194 nicht. Die Freigabe für UDP 1194 fehlt oder zeigt auf ein anderes Gerät, etwa eine zweite TrutzBox	Im Router nachsehen, wohin UDP 1194 zeigt (Abschnitt „Schritt 2: Portweiterleitung am Internet-Router“). Mehrere TrutzBoxen an einem Anschluss bekommen je einen eigenen Port von außen (Abschnitt „Einen eigenen Namen statt des TrutzDynDNS-Namens

Anzeige oder Symptom	Wahrscheinliche Ursache	Das hilft
		verwenden“)
„Von außen nicht bestätigt" (nur WireGuard)	Das Testpaket kam nicht zurück, und von außen kam noch nie ein Handschlag an, also nie die Anmeldung eines Geräts (Abschnitt „Schritt 4: Erreichbarkeit von WireGuard prüfen“). Entweder fehlt die Weiterleitung, oder der Router reicht eigene Pakete nicht an sich selbst zurück	Freigabe prüfen: UDP, Port 1194, Ziel TrutzBox. Danach einmal mit dem Smartphone über Mobilfunk verbinden; kommt ein Handschlag an, ist der Weg bewiesen
„Es kam kein Versuch von außen an" (nur OpenVPN, nach dem Live-Test)	Während der Wartezeit kam kein Paket von außen an der TrutzBox an. Meist fehlt die Portfreigabe oder steht auf TCP; seltener fehlt dem Anschluss eine eigene IPv4-Adresse (DS-Lite)	Freigabe prüfen: UDP, Port 1194, Ziel TrutzBox (Abschnitt „Schritt 2: Portweiterleitung am Internet-Router“); bei DS-Lite siehe Abschnitte „Schritt 4: Erreichbarkeit von WireGuard prüfen“ und „VPN auch über IPv6 anbieten“
„Bisher nur aus dem eigenen Netz erreicht"	Alle bisherigen Verbindungen kamen aus dem eigenen Netz oder über den eigenen Router zurück. Ein Gerät im Internet hat die TrutzBox noch nie erreicht	Einmal von außen verbinden, am Smartphone also WLAN ausschalten. Bleibt es dabei, fehlt die Weiterleitung im Router, oder das Gerät nimmt IPv4, während nur IPv6 offen ist (Abschnitt „VPN auch über IPv6 anbieten“)
„Kein Internetzugang oder keine öffentliche Adresse" (Kette stoppt beim „Provider")	Die TrutzBox kann ihre öffentliche Internet-Adresse nicht ermitteln	Internetverbindung der TrutzBox prüfen und den Test wiederholen
„Der VPN-Dienst auf der TrutzBox läuft nicht" (Kette stoppt bei „TrutzBox")	Der Tunnel ist angehalten oder noch nicht eingerichtet	WireGuard: Schalter „Läuft" in Karte 4 einschalten. OpenVPN: Schalter „OpenVPN-Server aktiv" einschalten (Abschnitt „OpenVPN statt WireGuard verwenden“)
„Von außen erreichbar", Verbindung klappt trotzdem nicht	Problem liegt am Endgerät	Zugang neu importieren; Datum und Uhrzeit des Geräts prüfen. Bei OpenVPN notfalls das Häkchen beim Benutzer aus- und wieder einschalten und das neue Profil verwenden
Verbindung klappt im eigenen WLAN nicht	Test findet innerhalb des eigenen Netzes statt	Zum Testen Mobilfunk verwenden, WLAN am Smartphone ausschalten
OpenVPN: IPv6 eingeschaltet, aber unterwegs	Meist steckt in der App noch das alte Profil; seltener fehlt die	Profil neu herunterladen und in der App ersetzen, Freigabe prüfen,

Anzeige oder Symptom	Wahrscheinliche Ursache	Das hilft
keine Verbindung	IPv6-Freigabe oder das Netz unterwegs hat kein IPv6	Mobilfunk verwenden (Abschnitt „VPN auch über IPv6 anbieten“)
OpenVPN: Smartphone braucht bis zu einer Minute zum Verbinden	IPv6 eingeschaltet, aber keine IPv6-Freigabe am Router	IPv6-Freigabe einrichten oder den Schalter wieder ausschalten und die Profile neu laden (Abschnitt „VPN auch über IPv6 anbieten“)
Zweite TrutzBox am selben Router: keine Verbindung, keine klare Meldung	Der Zugang landet über IPv4 bei der anderen TrutzBox, die ihn abweist	Für diese TrutzBox einen eigenen Port von außen einrichten (Abschnitt „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“) oder IPv6 mit eigener IPv6-Freigabe (Abschnitt „VPN auch über IPv6 anbieten“); danach den Zugang neu laden

Führt das alles nicht weiter, schalten Sie unter dem Ergebnis die **Experte-Ansicht** ein. Sie zeigt unter *„Technische Details (für Support)"* einen Diagnosetext, den Sie mit **Kopieren** in die Zwischenablage legen und dem Comidio-Support schicken können. Mehr dazu in Kapitel „Support kontaktieren“.

13.10 Was der Fernzugriff sonst noch ermöglicht

Der VPN-Tunnel bringt Sie nicht nur geschützt ins Internet, er bringt Sie auch ins Netz der TrutzBox. Solange die Verbindung steht, erreichen Sie von unterwegs:

- das **Admin-Panel** Ihrer TrutzBox unter `https://trutzbox`, als säßen Sie davor, etwa um im Urlaub eine Filtergruppe zu ändern;
- Ihr **Webmail** unter `https://trutzbox/mail` und den **TrutzChat** unter `https://trutzbox/chat/` (Kapitel „TrutzMail: sichere E-Mail“ und „TrutzChat und Videokonferenz“);
- Geräte in Ihrem Netzwerk, etwa einen Netzwerkspeicher oder einen Drucker, sofern diese das erlauben.

Comidio empfiehlt diesen Weg ausdrücklich gegenüber der Alternative, einzelne Dienste am Router ins Internet zu öffnen: Beim VPN bleibt genau ein einziger, streng abgesicherter Zugang offen, und alles dahinter bleibt unsichtbar.

13.11 VPN auch über IPv6 anbieten

Das Internet kennt zwei Adressarten: das ältere **IPv4** und das neuere **IPv6**. Ab Werk verbindet sich TrutzVPN über IPv4. Auf Wunsch nimmt es unterwegs den Weg über IPv6. Das lohnt sich in zwei Fällen:

- **Anschluss ohne eigene IPv4-Adresse (DS-Lite).** Von außen ist Ihre TrutzBox dann nur über IPv6 erreichbar (Abschnitt „Welcher Anschluss ist von außen erreichbar?“). Verbinden können Sie sich deshalb nur aus Netzen, die selbst IPv6 haben. Mobilfunknetze in

Deutschland haben das meist, manche Hotel- oder Gäste-WLANs dagegen nicht; dort klappt es dann nicht.

- **Mehrere TrutzBoxen am selben Router.** Alle teilen sich eine öffentliche IPv4-Adresse, und Port 1194 lässt sich über IPv4 nur an eine davon weiterleiten. Jede weitere TrutzBox braucht entweder einen eigenen Port von außen (Abschnitt „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“) oder den Weg über IPv6 mit einer eigenen Freigabe am Router. Landet ein Zugang über IPv4 bei der falschen TrutzBox, weist diese ihn ab, und die App zeigt keinen verständlichen Fehler.

Der Tunnel selbst bleibt dabei unverändert, IPv6 ist nur der Weg zur TrutzBox. Wie dieser Weg eingeschaltet wird, hängt vom Tunnel ab:

- **WireGuard:** Ein Zugang nennt den Namen der TrutzBox. Trägt TrutzDynDNS unter diesem Namen beide Adressarten ein, nehmen die WireGuard-Apps immer die IPv4. Über IPv6 verbinden sie sich deshalb erst, wenn der Name nur noch die IPv6-Adresse trägt. Das bewirkt der Schalter **TrutzDynDNS nur mit IPv6** (Abschnitt „TrutzDynDNS nur mit IPv6“). Die Zugänge auf den Geräten bleiben dabei gleich.
- **OpenVPN:** Ein Profil nennt seine Wege einzeln. Den Weg über IPv6 nimmt es erst auf, wenn Sie den Schalter **VPN auch über IPv6 anbieten** einschalten. Danach braucht jedes Gerät ein neues Profil.

Für beide Tunnel muss die TrutzBox eine globale, also im ganzen Internet gültige IPv6-Adresse haben, und am Router muss eine IPv6-Freigabe stehen. Fehlt die Adresse, steht beim OpenVPN-Schalter *„Nicht verfügbar: Die TrutzBox hat keine globale IPv6-Adresse."* So gehen Sie vor:

1. Öffnen Sie **Netzwerk → Fernzugriff** und notieren Sie im Domain-Bereich der Seite den Wert **IPv6-Interface-ID (für Freigaben am Router)**. Die **Interface-ID** ist die hintere Hälfte der IPv6-Adresse Ihrer TrutzBox. Sie wird aus der Hardware-Adresse der TrutzBox gebildet und bleibt gleich, wenn Ihr Anbieter den vorderen Teil der Adresse wechselt. Sie tragen sie also nur einmal ein.
2. Richten Sie am Internet-Router zusätzlich zur Portweiterleitung aus Abschnitt „Schritt 2: Portweiterleitung am Internet-Router“ eine **IPv6-Freigabe** für die TrutzBox ein: Protokoll **UDP**, Port **1194**. Eine Weiterleitung auf eine andere Adresse gibt es unter IPv6 nicht; der Router öffnet den Port direkt für die IPv6-Adresse der TrutzBox und fragt dafür die Interface-ID ab.
3. Bei **WireGuard**: Führt über IPv4 kein Weg zu dieser TrutzBox, etwa bei DS-Lite oder als zweite TrutzBox am selben Router, schalten Sie im Domain-Bereich **TrutzDynDNS nur mit IPv6** ein. Sonst ist hier nichts weiter zu tun.
4. Bei **OpenVPN**: Klappen Sie in der Karte **OpenVPN-Server** den Bereich **Erweiterte Einstellungen** auf und schalten Sie in der ersten Zeile **VPN auch über IPv6 anbieten** ein. Das ist erst möglich, wenn der OpenVPN-Server läuft (Abschnitt „OpenVPN statt WireGuard verwenden“). Laden Sie danach für jeden Benutzer das Profil neu herunter, löschen Sie in der App das alte und importieren Sie das neue.
5. Testen Sie unterwegs, etwa mit dem Smartphone über Mobilfunk bei ausgeschaltetem WLAN.

Wie Sie die IPv6-Freigabe in einer FRITZ!Box anlegen, auch für die Videokonferenz, zeigt Abschnitt „Die IPv6-Freigabe in einer FRITZ!Box“.

OpenVPN: nur mit Freigabe einschalten, danach Profile ersetzen

Ist der Schalter **VPN auch über IPv6 anbieten** an, fehlt aber die IPv6-Freigabe am Router, probieren Smartphones zuerst IPv6 und weichen erst nach bis zu einer Minute auf IPv4 aus. Schalten Sie IPv6 deshalb erst ein, wenn die Freigabe steht.

Jedes Umschalten schreibt alle OpenVPN-Profile auf der TrutzBox neu, die schon in Apps importierten Profile bleiben aber, wie sie sind. Ein altes Profil kennt den Weg über IPv6 nicht. Jeder Benutzer muss sein Profil deshalb neu herunterladen und in der App ersetzen.

Für Neugierige: Was im Zugang steht

Ein OpenVPN-Profil enthält mehrere Adressen, die die VPN-App der Reihe nach probiert. Ist der Schalter aus, sind es zwei: der Netzwerkname der TrutzBox im lokalen Netz und der TrutzDynDNS-Name, beide über IPv4. Ist er an, sind es drei: der Netzwerkname über IPv4, der TrutzDynDNS-Name über IPv6 und derselbe Name über IPv4 als Rückfall. Deshalb nimmt die App im lokalen Netz immer IPv4 und IPv6 nur unterwegs. Der VPN-Server auf der TrutzBox nimmt Verbindungen über beide Wege an; welchen Weg ein Gerät versucht, bestimmt allein das Profil.

Ein WireGuard-Zugang nennt dagegen nur einen Weg, den öffentlichen Namen der TrutzBox mit dem Anschluss. Welche Adresse dahinter genommen wird, bestimmt der Eintrag bei TrutzDynDNS.

13.12 OpenVPN statt WireGuard verwenden

OpenVPN ist der ältere, überall verbreitete Tunnel. Jedes Gerät braucht dafür ein eigenes Profil, eine Datei mit der Endung `.ovpn`, und ein VPN-Programm wie OpenVPN Connect. Sinnvoll ist OpenVPN etwa, wenn auf Ihren Geräten schon OpenVPN-Profile eingerichtet sind. Am Router ändert sich nichts: OpenVPN benutzt denselben Anschluss UDP 1194 wie WireGuard.

Den OpenVPN-Server einrichten und einschalten

Solange OpenVPN noch nicht eingerichtet ist, schaltet ein Klick auf OpenVPN in Karte 2 nichts um; die Karte verweist dann auf die Karte **VPN-Server einrichten**. So gehen Sie vor:

1. Klicken Sie in der Karte **VPN-Server einrichten** auf **VPN einrichten**. Die TrutzBox erzeugt dabei einmalig ihr eigenes Zertifikatszentrum und die nötigen Schlüssel. Das dauert laut Seite etwa 15 Sekunden, den Fortschritt sehen Sie live. Die Erreichbarkeit muss dafür noch nicht bestätigt sein.
2. Lief bisher kein Tunnel, startet OpenVPN damit gleich, und Karte 2 zeigt OpenVPN grün. Lief WireGuard, klicken Sie danach in Karte 2 auf **OpenVPN** und bestätigen die Rückfrage mit **Umschalten** (Abschnitt „Schritt 3: Tunnel wählen“).

Menüpfad: Netzwerk → Fernzugriff

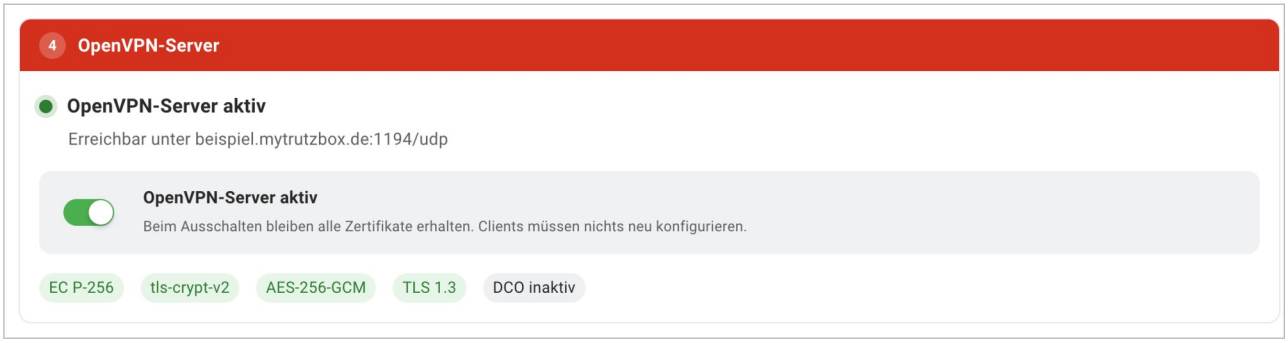


Abbildung 13-7: Karte 4 „OpenVPN-Server“: Der Server ist aktiv und unter beispiel.mytrutzbox.de:1194/udp erreichbar, darunter der Schalter und die verwendeten Verfahren. (© 2026 Comidio GmbH)

Danach heißt die Karte **OpenVPN-Server**. Sie zeigt *„OpenVPN-Server aktiv“*, die Adresse, unter der der Server erreichbar ist, den Schalter **OpenVPN-Server aktiv** und die verwendeten Verfahren als Plaketten. Über den Schalter halten Sie den Server jederzeit an. Alle Zertifikate bleiben dabei erhalten, und Ihre Geräte müssen nichts neu einrichten. Solange der Server aus ist, ist Port 1194 aus dem Internet nicht erreichbar. Läuft stattdessen WireGuard, steht in der Karte *„OpenVPN ruht, WireGuard hat den Anschluss“*.

Die Erreichbarkeit prüfen

Menüpfad: Netzwerk → Fernzugriff

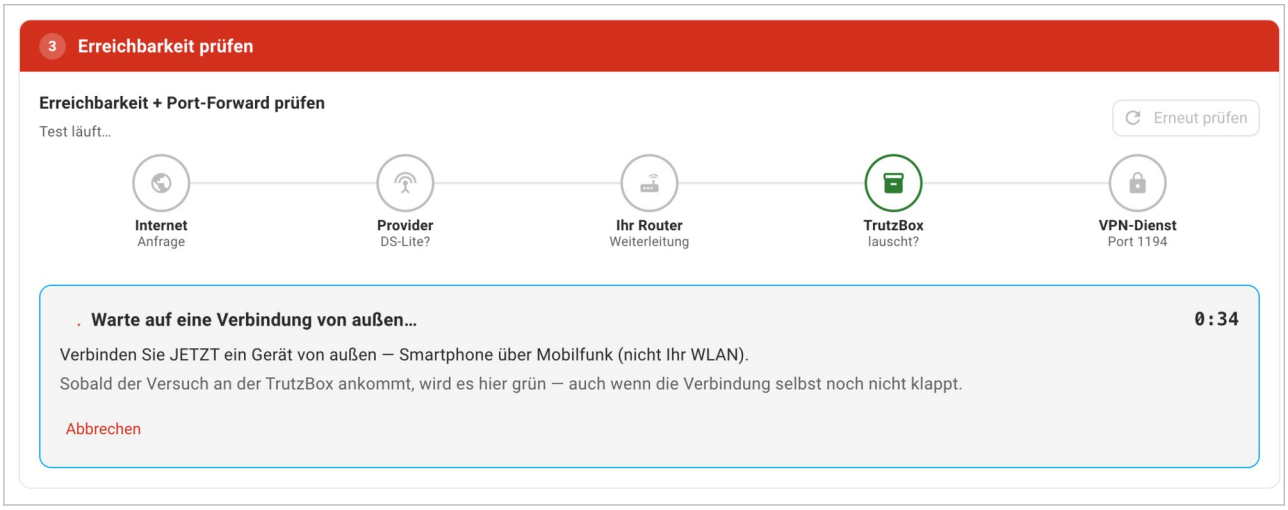


Abbildung 13-8: Karte 3 „Erreichbarkeit prüfen“ bei OpenVPN: Der Live-Test wartet auf einen Verbindungsversuch von außen und zählt die verbleibende Zeit herunter. (© 2026 Comidio GmbH)

Bei OpenVPN steht die Prüfung in einer eigenen Karte über dem Server, Karte 3 **Erreichbarkeit prüfen**. Sie zeigt dieselbe Kette mit fünf Stationen wie bei WireGuard (Abschnitt „Schritt 4: Erreichbarkeit von WireGuard prüfen“) und startet mit dem gleichnamigen Knopf, später mit **Erneut prüfen**. Solange der Server noch nicht läuft, schickt sich die TrutzBox ein Testpaket über den Router. Läuft er, ist kein Gerät verbunden und kam noch nie ein Paket von außen an, kann die TrutzBox den Weg nicht selbst prüfen. Dann führt die Karte durch einen Live-Test: Sie zeigt *„Warte auf eine Verbindung von außen…“* und zählt 90 Sekunden herunter.

Verbinden Sie in dieser Zeit ein Gerät mit eingerichtetem Profil von außen, am einfachsten das Smartphone über Mobilfunk, nicht über Ihr WLAN. Sobald der Versuch an der TrutzBox ankommt,

wird die Kette grün, auch wenn die Verbindung selbst noch nicht klappt. Kommt nichts an, lautet das Ergebnis *„Es kam kein Versuch von außen an“* (Abschnitt „Wenn es nicht klappt“). Mit **Abbrechen** beenden Sie das Warten. Für Anschlüsse ohne eigene IPv4-Adresse und für Router ohne Rückleitung gelten die Kästen in Abschnitt „Schritt 4: Erreichbarkeit von WireGuard prüfen“ genauso.

Benutzer freischalten und Profil herunterladen

Wer die OpenVPN-Verbindung nutzen darf, legen Sie pro Benutzer fest, und zwar in der Benutzerverwaltung unter **Verwaltung → Benutzer**. Dorthin führt auch der Verweis *„VPN-Zugang für Nutzer:innen freischalten"* auf der Fernzugriff-Seite. Für jeden freigeschalteten Benutzer erzeugt die TrutzBox eine persönliche Konfigurationsdatei, das **VPN-Profil** mit der Endung `.ovpn`. Diese eine Datei enthält alles, was ein Endgerät braucht.

Menüpfad: Verwaltung → Benutzer

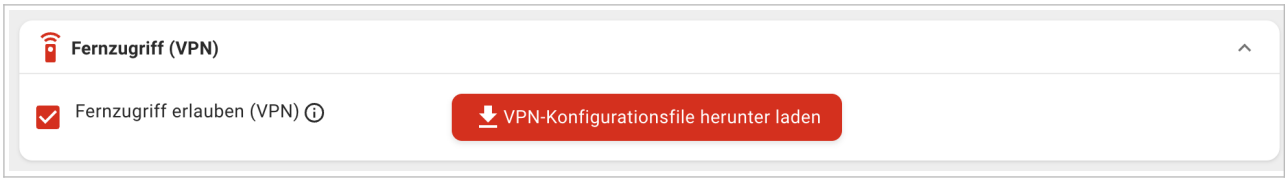


Abbildung 13-9: Der Bereich „Fernzugriff (VPN)“ eines Benutzers, wenn OpenVPN läuft: das Häkchen „Fernzugriff erlauben (VPN)“ und der Knopf zum Herunterladen des Profils. (© 2026 Comidio GmbH)

1. Öffnen Sie **Verwaltung → Benutzer** und klappen Sie den gewünschten Benutzer auf.
2. Setzen Sie im Bereich **Fernzugriff (VPN)** das Häkchen *„Fernzugriff erlauben (VPN)"*.
3. Klicken Sie auf **VPN-Konfigurationsfile herunter laden**. Sie erhalten eine Datei wie `a.beispiel-vpn.ovpn`.
4. Bringen Sie die Datei auf das Endgerät, am einfachsten per USB-Kabel, AirDrop oder über einen verschlüsselten Kanal wie TrutzMail.

> **Das Profil ist ein Schlüssel: Behandeln Sie es auch so**
> Wer diese Datei besitzt, kann sich mit Ihrem Netzwerk verbinden. Verschicken Sie sie deshalb nicht per unverschlüsselter E-Mail und löschen Sie Kopien aus Downloads-Ordnern, sobald das Profil importiert ist. Falls eine Datei in falsche Hände gerät: Häkchen beim Benutzer entfernen. Damit wird das Zertifikat sofort gesperrt.

Gut zu wissen: Jedes OpenVPN-Profil erlaubt **eine** Verbindung gleichzeitig. Sollen Laptop und Smartphone derselben Person zeitgleich verbunden sein, braucht sie bei OpenVPN einen zweiten Benutzer (Kapitel „Benutzer, Postfächer, Passwörter“). Bei WireGuard genügt dafür ein zweiter Zugang unter demselben Konto (Abschnitt „Schritt 5: Zugänge für die WireGuard-App anlegen“). Läuft WireGuard, zeigt der Bereich **Fernzugriff (VPN)** beim Benutzer statt Häkchen und Profil die WireGuard-Zugänge des Kontos.

Ein schon importiertes Profil ändert sich nicht von selbst. Schalten Sie später **VPN auch über IPv6 anbieten** ein oder aus, laden Sie das Profil deshalb neu herunter, löschen Sie in der App das alte und importieren Sie das neue (Abschnitt „VPN auch über IPv6 anbieten“).

Auf dem Endgerät brauchen Sie ein VPN-Programm, das OpenVPN-Profile versteht: Programm installieren, die `.ovpn`-Datei importieren, Verbindung einschalten. Die bewährten Programme je Betriebssystem nennt Abschnitt „Geräte mit OpenVPN einrichten“.

Zurück zu WireGuard kommen Sie jederzeit über Karte 2 (Abschnitt „Schritt 3: Tunnel wählen“). Die OpenVPN-Profile bleiben dabei erhalten und gelten wieder, sobald Sie erneut auf OpenVPN umschalten.

Häufige Fragen zu TrutzVPN

Können mehrere Geräte gleichzeitig verbunden sein?

Ja. Bei WireGuard bekommt jedes Gerät einen eigenen Zugang, auch mehrere unter demselben Nutzerkonto (Abschnitt „Schritt 5: Zugänge für die WireGuard-App anlegen“). Bei OpenVPN lässt ein Profil bewusst nur eine Verbindung gleichzeitig zu; ein zweites Gerät derselben Person braucht dort einen zweiten Benutzer mit eigenem Profil.

Was passiert, wenn ich zwischen OpenVPN und WireGuard umschalte?

Die TrutzBox hält den einen Tunnel an und startet den anderen; beide teilen sich den Anschluss UDP 1194, an der Freigabe im Router ändert sich nichts. Nichts wird gelöscht: Profile und Zugänge bleiben erhalten. Die Geräte brauchen aber das passende Programm, also die WireGuard-App für WireGuard und OpenVPN Connect für OpenVPN. Wer unterwegs umstellt, sollte daran denken, dass die eigene Verbindung dabei abbricht (Abschnitt „Schritt 3: Tunnel wählen“).

Funktioniert TrutzVPN auch an einem Anschluss mit DS-Lite?

Ja, über IPv6: am Router die IPv6-Freigabe einrichten und den Schalter **TrutzDynDNS nur mit IPv6** setzen; das tut die TrutzBox auch von selbst, wenn ihre Messung von außen es ergibt. Bei OpenVPN zusätzlich **VPN auch über IPv6 anbieten** einschalten und die Profile neu laden (Abschnitt „VPN auch über IPv6 anbieten“). Mehr zum Schalter steht im Abschnitt „TrutzDynDNS nur mit IPv6“. Verbinden können Sie sich dann aus allen Netzen mit IPv6, also meist im Mobilfunk, in manchen Hotel-WLANs aber nicht.

Warum bietet OpenVPN den Weg über IPv6 nicht ab Werk an?

Der Weg über IPv6 braucht eine eigene Freigabe am Router, und ob sie eingerichtet ist, bestimmt, wer den Router verwaltet. Fehlt sie, probieren Smartphones zuerst IPv6 und weichen erst nach bis zu einer Minute auf IPv4 aus, und OpenVPN Connect auf iPhone und iPad bricht dabei teils ganz ab. Die TrutzBox prüft zwar selbst, ob sie über IPv6 erreichbar ist, und nimmt eine unerreichbare IPv6-Adresse aus ihrem TrutzDynDNS-Namen (Kapitel „Netzwerk-Übersicht: außen und innen“). Den Weg über IPv6 in den OpenVPN-Profilen schaltet sie aber nicht von selbst ein, denn jedes Umschalten verlangt neue Profile auf allen Geräten. Deshalb entscheiden Sie selbst.

Ist meine TrutzBox angreifbar, wenn der VPN-Server läuft?

Ehrliche Antwort: Mit der Portfreigabe öffnen Sie tatsächlich eine Tür von außen zu Ihrer TrutzBox, und jede offene Tür ist grundsätzlich ein mögliches Ziel. Die TrutzBox-Entwickler haben diese Tür deshalb so gebaut, dass sie Unbefugten möglichst wenig bietet: Ohne gültigen Schlüssel gibt der Server nicht einmal eine Antwort, ein erratenes Passwort nützt Angreifern nichts, und die Verschlüsselung entspricht aktuellem Stand der Technik. Zusätzlich wacht der Angriffsschutz über alle von außen erreichbaren Dienste und sperrt auffällige Absender automatisch aus (Kapitel

„Angriffsschutz: Firewall und Wächter“). Wer das Restrisiko weiter senken will, schaltet den Tunnel einfach ab, wenn er längere Zeit nicht gebraucht wird: bei WireGuard mit dem Schalter **Läuft**, bei OpenVPN mit **OpenVPN-Server aktiv**.

14 TrutzBrowse: zusätzlicher Schutz für Browser und Apps

Der Webfilter aus Kapitel „Webfilter und Jugendschutz (TrutzContent)“ entscheidet, *wohin* ein Gerät Verbindungen aufbauen darf. **TrutzBrowse** geht einen Schritt weiter und verändert, *was dabei über Sie verraten wird*: Es entfernt identifizierende Merkmale aus dem Datenverkehr, damit Werbenetze und Analyse-Dienste aus den Angaben von Browser und Apps keinen wiedererkennbaren „Fingerabdruck" Ihres Geräts bilden können. TrutzBrowse ist für erfahrene Anwender gedacht und wird je Gerät einzeln eingeschaltet.

14.1 Was TrutzBrowse leistet

Beim Aufruf einer einzigen Webseite melden sich im Hintergrund oft Dutzende Drittserver: Werbenetze, Analyse-Dienste, Schriftarten-Lieferanten. Jeder davon erfährt normalerweise eine Menge über Sie, denn Browser plaudern freimütig: Gerätetyp, Betriebssystem, Bildschirmauflösung, Zeitzone, installierte Schriften. Zusammen ergibt das einen nahezu eindeutigen Fingerabdruck, der Sie über Webseiten hinweg wiedererkennbar macht, ganz ohne Cookies.

TrutzBrowse arbeitet als Vermittler (Proxy) mitten im Datenstrom und filtert diese Merkmale heraus. Wie gründlich, bestimmt der **Security-Slider**: ein Regler mit zehn Stufen, L1 bis L10, von „maximale Anonymität" bis „wenig Eingriff, alles funktioniert". Neun davon, L1 bis L9, stellen Sie durch Schieben ein; die zehnte schaltet TrutzBrowse für einen Server ganz ab (Abschnitt „Was der Security-Slider praktisch bewirkt“). Wichtig dabei: Auch alle im Hintergrund kontaktierten Drittserver werden mit demselben Niveau behandelt wie die eigentliche Seite. Für einzelne Server können Sie das Niveau gezielt ändern oder TrutzBrowse ganz abschalten, und das sehr fein: Sogar einzelne Pfade einer Domain lassen sich unterschiedlich behandeln, das Skript zur Wiedererkennung blockiert, der Inhalt daneben erlaubt.

Vier Aufgaben erledigt TrutzBrowse dabei nebeneinander:

- **Verräterische Kennzeichen glätten:** Die technischen Angaben, die Ihr Browser bei jedem Aufruf mitschickt, werden ersetzt oder unterdrückt.
- **Cookies eindämmen:** Cookies von fremden Seiten, das klassische Werkzeug seitenübergreifender Wiedererkennung, werden zurückgehalten.
- **Fingerabdrücke verkleinern:** Die Menge der Merkmale, aus denen ein Werbenetz oder Analyse-Dienst einen Fingerabdruck zusammensetzen kann, schrumpft.
- **Unsichtbare Folgeaufrufe prüfen:** Die Server, die eine Webseite im Hintergrund nachlädt, werden gegen eigene, schärfere Sperrlisten geprüft. Genau hier liegt eine Stärke, die reine Domain-Sperren nicht bieten.

TrutzBrowse kümmert sich um Web-Verkehr. Geräte, die eigene, nicht webbasierte Protokolle sprechen, erreicht der Proxy nicht; dort greifen Firewall und Angriffsschutz mit ihren IP-Sperren (Kapitel „Angriffsschutz: Firewall und Wächter“).

> **Für Neugierige: in der Masse verschwinden**

> Gar keine Angaben zu senden wäre keine gute Idee. Erstens brauchen viele Webseiten diese Angaben, um die Darstellung an Ihr Gerät anzupassen. Zweitens fiele ein Gerät, das gar nichts verrät, selbst wieder auf. TrutzBrowse setzt deshalb bewusst Allerwelts-Werte ein, die möglichst viele andere Nutzer ebenso senden. Ihr Gerät wird damit nicht unsichtbar, sondern gewöhnlich, und das ist der wirksamere Schutz.

14.2 Woraus ein Fingerabdruck entsteht

Um zu verstehen, woran TrutzBrowse ansetzt, hilft ein Blick auf das, was ein Skript zur Wiedererkennung in wenigen Sekundenbruchteilen abfragen kann. Der Browser meldet ungefragt Betriebssystem und dessen Version, Browser und dessen Version sowie die Art des Prozessors. Dazu kommen Bildschirmauflösung und Farbtiefe, Zeitzone, Systemsprache, die vorhandenen Erweiterungen und die Liste der installierten Schriftarten.

Drei Verfahren gehen darüber hinaus, weil sie die Eigenheiten Ihrer Hardware messen statt sie zu erfragen:

- **Canvas:** Ein unsichtbares Skript lässt den Browser einen kurzen Text oder eine einfache Form zeichnen, die niemand zu sehen bekommt. Weil Grafikkarte, Treiber und Betriebssystem denselben Auftrag minimal unterschiedlich ausführen, entsteht ein Bild, das für Ihre Gerätekombination fast einzigartig ist.
- **WebGL:** Dieselbe Idee mit 3D-Grafik. Gemessen werden die Fähigkeiten und Eigenheiten der Grafikeinheit.
- **Ton:** Ein Skript erzeugt ein Tonsignal, das nie hörbar wird, und wertet aus, wie Ihr Gerät es verrechnet. Auch dabei kommen bei jeder Geräteart leicht andere Zahlen heraus.

Die Kombination all dieser Merkmale ist sehr aussagekräftig: In der viel zitierten Studie „Panopticlick" der Bürgerrechtsorganisation EFF waren 84 Prozent der untersuchten Browser allein daran eindeutig zu erkennen. Neuere Untersuchungen kommen auf niedrigere, aber weiterhin erhebliche Anteile; in einer Studie von Google-Forschern aus dem Jahr 2025 war der Fingerabdruck von rund 60 Prozent der Teilnehmer eindeutig. Das Unangenehme daran: Cookies löschen hilft nicht, ein neuer Browser hilft kaum, und im Netzwerkverkehr ist von alledem nichts Auffälliges zu sehen. Genau deshalb setzt TrutzBrowse eine Ebene früher an, nämlich an den Daten, die überhaupt erst zum Server gelangen.

14.3 Webfilter und TrutzBrowse: zwei Stufen, ein Ziel

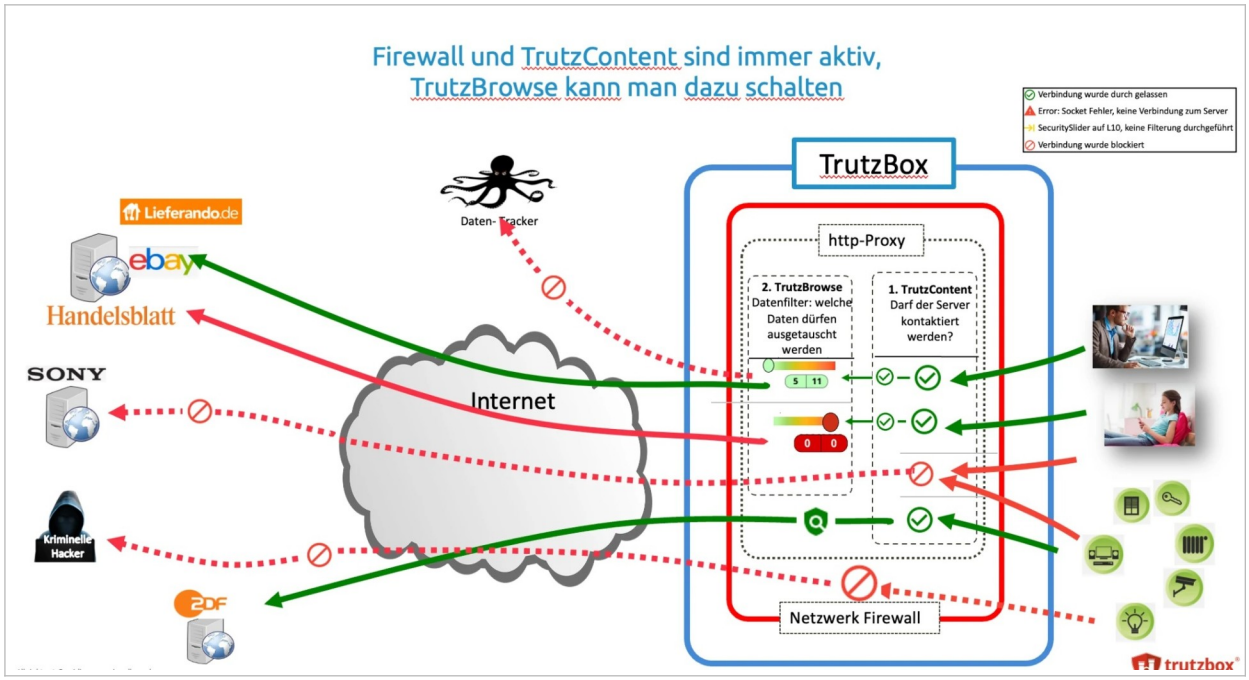


Abbildung 14-1: Firewall und TrutzContent sind immer aktiv; TrutzBrowse lässt sich als zweite Stufe dazuschalten. (© 2026 Comidio GmbH)

Die beiden Schutzfunktionen greifen nacheinander und ergänzen sich. Der Webfilter TrutzContent prüft den Verbindungsaufbau: Er vergleicht die Zieladresse mit den Filterlisten der Filtergruppe, die für dieses Gerät gilt, und lässt gar nicht erst Daten fließen, wenn das Ziel bekanntermaßen unerwünschten Datenverkehr bringt: Werbung, die Aufzeichnung dessen, was Sie tun, oder Schadcode. TrutzBrowse setzt danach an: Es entschärft die Verbindungen, die den Webfilter passiert haben, inhaltlich.

	Webfilter (TrutzContent)	**TrutzBrowse**
Zustand	immer aktiv, sobald Verkehr über die TrutzBox läuft	zusätzlich einschaltbar, je Gerät
Setzt an	am Verbindungsaufbau, also an der Zieladresse	am Inhalt der Kommunikation
Schützt	alle Geräte im Netz	nur Geräte mit installiertem Root-Zertifikat
Wirkt auf	Server für Werbung, für die Aufzeichnung dessen, was Sie tun, und für Schadcode	Kennzeichen des Browsers, Cookies, Fingerabdrücke, unsichtbare Folgeaufrufe
Nötig am Gerät	nichts	TrutzBox-Root-Zertifikat

Der Preis für die zweite Stufe ist der Eingriff in verschlüsselte Verbindungen. TrutzBrowse muss sie öffnen, um überhaupt hineinsehen zu können, und baut sie danach neu auf. Damit Ihr Gerät das akzeptiert, muss dort das TrutzBox-Root-Zertifikat liegen (Kapitel „Das Root-Zertifikat

installieren“). Ist TrutzBrowse für ein Gerät ausgeschaltet, reicht die TrutzBox das Zertifikat des besuchten Servers unverändert bis zum Gerät durch, und der Webfilter arbeitet trotzdem weiter.

14.4 Was der Security-Slider praktisch bewirkt

Der Security-Slider kennt zehn Stufen, L1 bis L10. Der Regler selbst bewegt sich über die neun Stufen L1 bis L9; L10 ist eine Sonderstellung (siehe unten). Links, auf L1, sind alle Filter aktiv, die Anonymität ist am höchsten. Je weiter der Regler nach rechts wandert, desto mehr echte Angaben gehen an den Server, und desto wahrscheinlicher funktioniert eine anspruchsvolle Seite fehlerfrei. Ab Werk steht der Regler auf L1, und bei den allermeisten Seiten bleibt er dort auch.

Grob gesagt geben die Stufen der Reihe nach frei: zuerst einzelne Kopfzeilen der Anfrage, dann Ihre Spracheinstellung, dann die Angabe zu Gerät und Browser, danach die Zugriffe auf Server aus den TrutzBrowse-Sperrlisten und zuletzt die Cookies fremder Seiten. Die Sperrlisten führen Server für Werbung und für die Aufzeichnung dessen, was Sie tun; die Slider-Definition nennt die Stufe, die sie freigibt, „Datentracker erlaubt". Zwei Voreinstellungen sind besonders praxisnah: Zugriffe aus den TrutzBrowse-Sperrlisten bleiben bis einschließlich L6 blockiert, und Cookies von fremden Seiten bleiben bis einschließlich L7 zurückgehalten. Eine Seite, die ohne solche Server gar nicht funktioniert, lässt sich damit auf L7 benutzen, ohne dass diese Server dort viel ausrichten könnten: Ohne Cookie fehlt ihnen der Faden, an dem sie Sie wiedererkennen.

Zwei Punkte werden dabei leicht missverstanden. Erstens die Cookies: Die Cookies der Seite, die Sie gerade besuchen, sind auf allen Stufen erlaubt, sonst funktionierte kaum eine Anmeldung. Zurückgehalten werden bis einschließlich L7 ausschließlich die fremden Cookies, also die von Drittservern, die eine Seite im Hintergrund einbindet. Zweitens die Stufe L9: Sie ist für zukünftige Erweiterungen reserviert und gibt derzeit nichts zusätzlich frei. Wer den Regler von L8 auf L9 zieht, ändert an der Behandlung einer Seite also nichts.

L10 ist ein Sonderfall und lässt sich nicht durch Schieben erreichen. Sie stellen L10 ein, indem Sie im Fenster des Reglers für einen Server den Haken **TrutzBrowse deaktivieren** setzen; die Slider-Definition nennt die Stufe „Keine Filter aktiv". Auf L10 greift der Proxy überhaupt nicht mehr ein: Verschlüsselte Verbindungen laufen komplett an ihm vorbei. Das ist der Notausgang für einen einzelnen, besonders empfindlichen Dienst, nicht die Einstellung für den Alltag.

Menüpfad: Browseranonymität

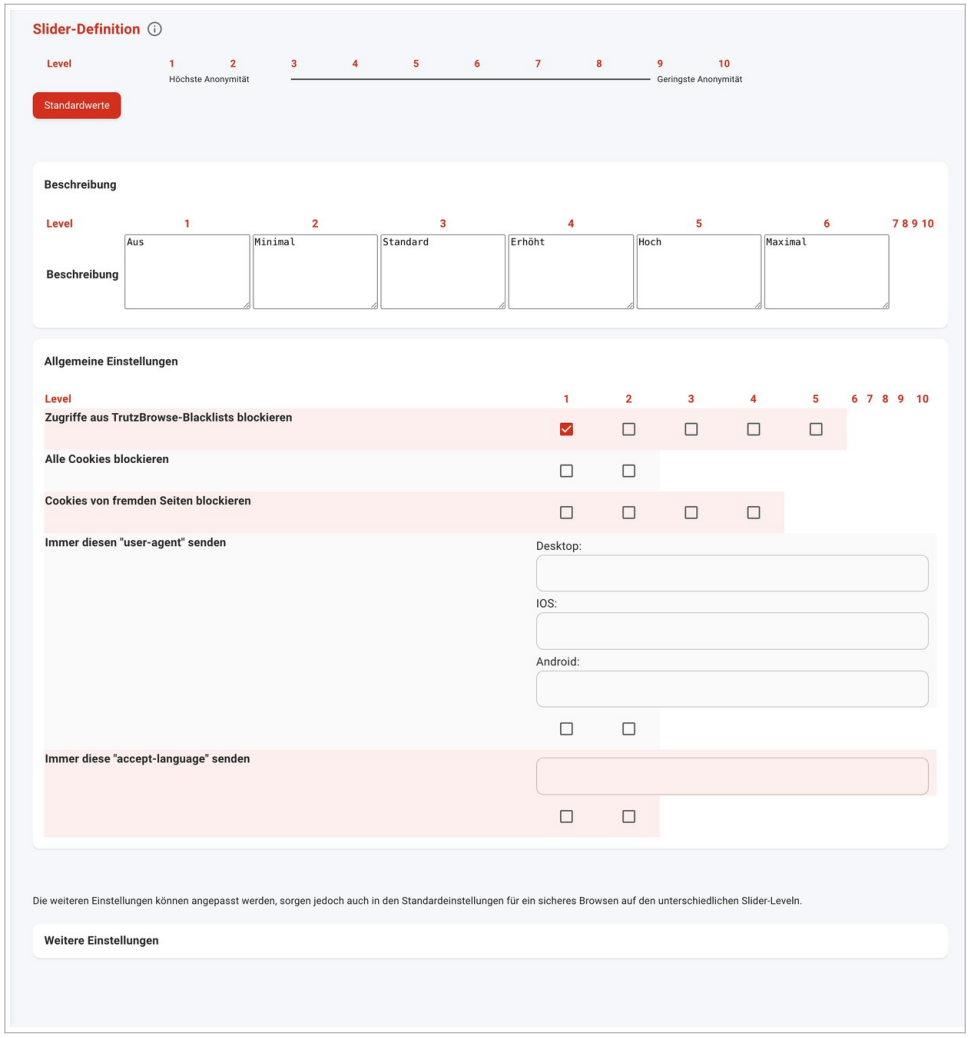


Abbildung 14-2: Die Slider-Definition: die zehn Stufen L1 bis L10 in den Spalten, die einzelnen Filter in den Zeilen. (© 2026 Comidio GmbH)

Wer wissen möchte, was genau auf welcher Stufe passiert, findet das im Admin-Panel: **Slider-Definition** zeigt eine Tabelle mit den zehn Stufen L1 bis L10 in den Spalten und den einzelnen Filtern in den Zeilen; ein Häkchen je Feld sagt, ob der Filter auf dieser Stufe arbeitet. Über **Standardwerte** lässt sich die gesamte Definition auf die Comidio-Voreinstellung zurücksetzen. Unter **Slider-Positionen** steht, für welche Server der Regler jemals von der Voreinstellung abgewichen ist, samt Angabe, wer das eingestellt hat; die Liste lässt sich gruppieren, sodass sich alle Einstellungen eines Verursachers gemeinsam entfernen lassen.

> **Erst die Seite, dann das Gerät**
>
> Schieben Sie den Regler nach Möglichkeit nur für die eine Seite weiter nach rechts, die zickt, nicht gleich für das ganze Gerät. Die Einstellung bleibt für diesen Server gespeichert, alle anderen Seiten behalten den vollen Schutz.

14.5 Das TrutzBurg-Menü im Browser

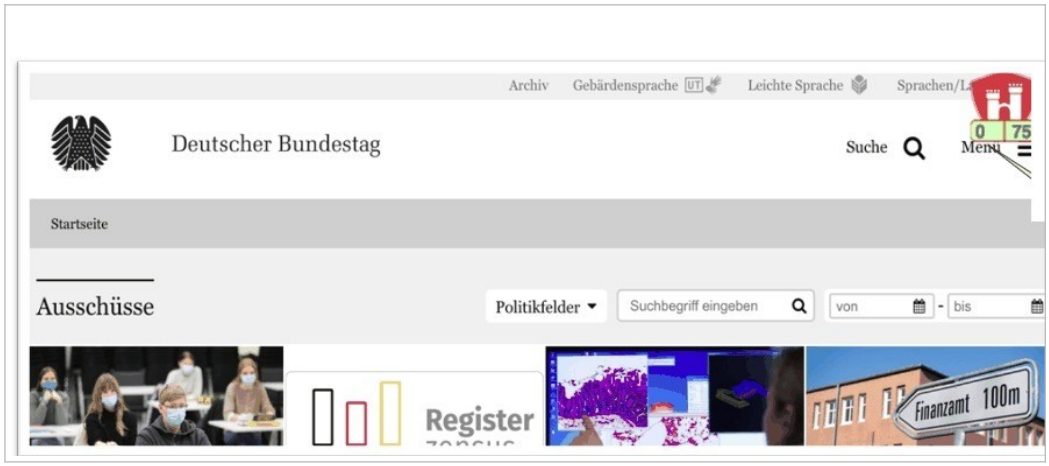


Abbildung 14-3: Das TrutzBurg-Icon oben rechts in einer aufgerufenen Seite. Grün heißt geschützt; die Zahlen nennen blockierte und erlaubte Hintergrund-Zugriffe. (© 2026 Comidio GmbH)

Damit Sie den Regler nicht jedes Mal im Admin-Panel suchen müssen, blendet TrutzBrowse ein kleines Bedienelement in die aufgerufene Seite ein: das **TrutzBurg-Icon**. Ein Klick darauf öffnet ein Menü, in dem sich unter anderem der Security-Slider für genau diese Seite verschieben lässt. Die Wirkung ist sofort nach dem Neuladen zu sehen.

Das TrutzBurg-Icon lässt sich je Gerät abschalten, unter **Verwaltung → Geräte** im Reiter **Proxy** über die Einstellung **TrutzBurg Symbol anzeigen**; auch die Bildschirmecke, in der es erscheint, ist dort wählbar. Sinnvoll ist das Abschalten, wenn das Icon stört, etwa beim Ausdrucken einer Seite oder beim Filmschauen auf dem Fernseher. Eine Einschränkung ergibt sich von selbst: Auf der Stufe L10 arbeitet der Proxy nicht mehr in der Seite, also kann er dort auch das TrutzBurg-Icon nicht einbauen.

Menüpfad: Browseranonymität

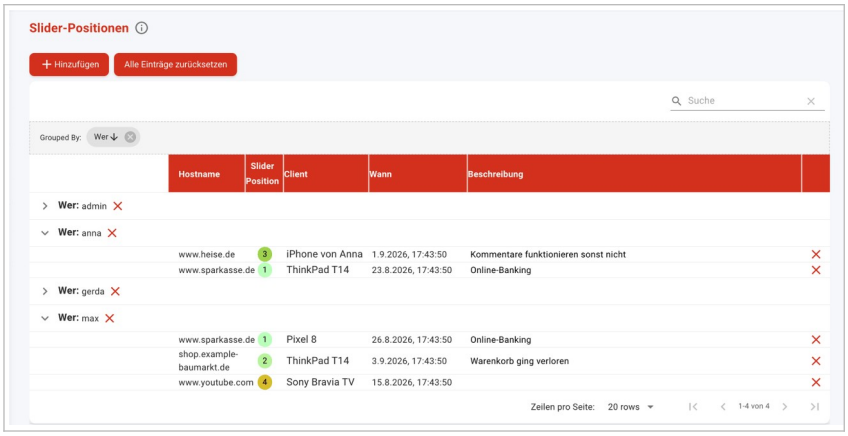


Abbildung 14-4: Slider-Positionen: für welche Server der Regler jemals verstellt wurde, gruppierbar nach Verursacher. (© 2026 Comidio GmbH)

14.6 TrutzBrowse je Gerät einschalten



Abbildung 14-5: TrutzBrowse je Gerät: Schalter und Security-Slider bestimmen den Anonymisierungsgrad. (© 2026 Comidio GmbH)

1. Installieren Sie auf dem Gerät das TrutzBox-Root-Zertifikat (Kapitel „Das Root-Zertifikat installieren“). Ohne Zertifikat kann TrutzBrowse verschlüsselte Seiten nicht bearbeiten. Die Datei dazu liegt unter **Verwaltung → Allgemeine Einstellungen** hinter **Root Zertifikat herunterladen**.
2. Öffnen Sie **Verwaltung → Geräte**, klappen Sie das gewünschte Gerät auf und schalten Sie im Reiter **Proxy** den Schalter **TrutzBrowse aktivieren** ein.
3. Lassen Sie die **Standardposition Slider** zunächst auf der Werkseinstellung L1. Dort ist der Schutz am höchsten, und bei den allermeisten Seiten bleibt der Regler auch dauerhaft dort. Schieben Sie ihn nur dann auf eine höhere Stufe, wenn eine bestimmte Seite es verlangt.
4. Benutzen Sie das Gerät ein paar Tage normal und schauen Sie gelegentlich in den Monitor. Dort sehen Sie, was TrutzBrowse tatsächlich abfängt, und dort korrigieren Sie auch die wenigen Seiten, die eine Ausnahme brauchen.

Ein guter Startpunkt sind ein oder zwei Geräte, auf denen Sie selbst arbeiten und Auffälligkeiten sofort bemerken. Geräte, die andere Personen im Haushalt oder in der Firma benutzen, kommen später dazu, wenn die ersten Ausnahmen eingespielt sind.

> **Wo TrutzBrowse ausbleiben sollte**
>
> Auf Geräten ohne installierbares Zertifikat, typisch Fernseher, Haustechnik und Gastgeräte, gehört TrutzBrowse ausgeschaltet, sonst scheitern deren verschlüsselte Verbindungen. Diese Geräte bleiben trotzdem geschützt: Webfilter, Firewall und Angriffsschutz arbeiten unabhängig davon.
>
> Dasselbe gilt, wenn die TrutzBox im halböffentlichen Raum steht und fremde Geräte mitversorgt, etwa im Wartebereich einer Praxis. Dort lässt sich auf den Geräten der Gäste kein Zertifikat einrichten, und TrutzBrowse bliebe wirkungslos.

14.7 Wenn eine Seite nicht richtig funktioniert

Je weiter links der Regler steht, je stärker also der Schutz, desto eher stolpert einmal eine Seite, denn manche Login- und Bezahlseiten bestehen auf genau den Merkmalen, die TrutzBrowse verschleiert. Typische Kandidaten sind Anmeldeseiten, Online-Banking, aufwendige Web-Anwendungen und einzelne Streaming-Dienste. Das Bild ist dabei meist harmlos: Ein Bereich der

Seite bleibt leer, ein Knopf reagiert nicht, oder die Anmeldung bricht ohne erkennbaren Grund ab. Die Abhilfe ist immer dieselbe Reihenfolge:

1. Den Regler für diese Seite eine Stufe weiter nach rechts schieben und die Seite neu laden, am schnellsten über das TrutzBurg-Menü.
2. Hilft das nicht, weiter nach rechts schieben. Auf L7 sind die Zugriffe aus den TrutzBrowse-Sperrlisten erlaubt, Cookies fremder Seiten aber weiterhin blockiert; sehr viele hartnäckige Fälle lösen sich genau hier.
3. Bleibt es dabei, im Monitor prüfen, ob stattdessen der Webfilter blockiert (Kapitel „Untersuchen und eingreifen“); dann ist die Freigabe dort einen Klick entfernt.
4. Blockiert der Webfilter nicht, für genau diesen Server eine Ausnahme setzen, also TrutzBrowse für ihn abschalten: im Fenster des Reglers den Haken **TrutzBrowse deaktivieren** setzen (Abschnitt „Was der Security-Slider praktisch bewirkt“). Alle übrigen Seiten behalten dabei ihren Schutz.
5. Betrifft es nicht eine Seite, sondern ein ganzes Programm oder eine App, hilft nur, TrutzBrowse für dieses Gerät abzuschalten. Manche Apps bringen ihre eigene Zertifikatsprüfung mit und akzeptieren das Root-Zertifikat der TrutzBox grundsätzlich nicht.

14.8 Den Nutzen im Monitor sehen

Ob sich der Aufwand lohnt, müssen Sie nicht glauben, Sie können es nachsehen. In der Listen-Darstellung des Monitors (Kapitel „Die drei Darstellungen“) zeigt die Spalte „Ergebnis" vorn in jeder Zeile als Symbol, wie der Webfilter den Kontakt behandelt hat: durchgelassen, blockiert, ungefiltert oder mit Verbindungsfehler. Sie hat keinen Spaltenkopf; im Menü **Spalten** heißt sie „Ergebnis: durchgelassen oder gesperrt". Für Geräte mit eingeschaltetem TrutzBrowse kommt die Spalte **Trutz Browse** dazu. Sie zeigt zweierlei: als Farbe die tatsächlich wirksame Slider-Stufe und als zwei Zahlen nebeneinander, wie viele der unsichtbaren Folgeaufrufe blockiert wurden, etwa 3 und 17 für drei blockierte von siebzehn angeforderten.

Beides ist nicht nur Anzeige, sondern Bedienung. Ein Klick auf das farbige Feld in der Spalte **Trutz Browse** öffnet den Regler und passt die Stufe für genau diesen Server an. Der Pfeil am Anfang einer aufgeklappten Zeile öffnet die einzelnen Folgeaufrufe mit ihrer jeweiligen Bewertung; dort sehen Sie schwarz auf weiß, welche Drittserver eine Seite im Hintergrund kontaktiert und welche davon die TrutzBox zurückgehalten hat.

Häufige Fragen zu TrutzBrowse

Wird das Surfen mit TrutzBrowse langsamer?

Ja, merklich. Die TrutzBox muss jede verschlüsselte Verbindung öffnen, den Inhalt prüfen und neu verschlüsseln, und das kostet bei jedem Seitenaufbau Zeit. Wie stark es auffällt, hängt von der Seite und der Slider-Stufe ab. Das ist der Preis der Anonymisierung und einer der Gründe, warum TrutzBrowse als Zusatz für erfahrene Anwender gedacht ist, nicht als Voreinstellung für alle Geräte. Noch einmal deutlich langsamer wird es, wenn zusätzlich das Tor-Netzwerk eingeschaltet ist.

Ersetzt TrutzBrowse meine Browser-Erweiterungen?

Nicht vollständig. TrutzBrowse arbeitet unabhängig vom Browser und erfasst auch Apps und andere Programme; einiges, was eine Erweiterung direkt in der Seite erledigt, etwa das Wegräumen von Cookie-Bannern oder das Blockieren einzelner Seitenelemente, kann ein Proxy dagegen nicht leisten. Eine gute Browser-Erweiterung kann deshalb auch neben TrutzBrowse sinnvoll bleiben; beides ergänzt sich.

Muss ich den Slider ständig nachstellen?

Nein. Jede Einstellung bleibt für den betroffenen Server gespeichert. In den ersten Wochen kommen ein paar Ausnahmen zusammen, danach ist meist über Monate nichts mehr zu tun.

Warum ist TrutzBrowse nicht einfach ab Werk überall eingeschaltet?

Weil es ein Zertifikat auf jedem Gerät braucht und weil gelegentlich eine Seite Aufmerksamkeit verlangt. Comidio empfiehlt es deshalb erfahrenen Anwendern. Der Webfilter allein ist bereits ein sehr wirksamer Schutz und läuft ohne jedes Zutun auf allen Geräten.

15 TrutzBox-Netzwerk: Schutz und Verwaltung

Dieses Kapitel versammelt alles rund um das Netzwerk der TrutzBox: das eigene WLAN, die verschlüsselte Namensauflösung, den Angriffsschutz und die Netzwerk-Einstellungen bis hin zum Experten-Zugang Webmin.

Auf Netzwerk-Ebene arbeitet die TrutzBox wie ein Router. Sie trennt das unsichere äußere Netz vom geschützten inneren und leitet für jede Anwendung, die auf der TrutzBox selbst bereitsteht (Mail, Web-Proxy, Chat, Videokonferenz), den passenden Verkehr auf diese Anwendung um. Genau daraus entsteht die Fähigkeit, den Datenverkehr in beiden Richtungen zu prüfen, Unerwünschtes zu blockieren und Verräterisches zu entschärfen. Im Alltag müssen Sie an keiner der hier beschriebenen Stellen etwas einstellen; die Voreinstellungen sind bewusst so gewählt, dass sie ohne Zutun das Richtige tun.

15.1 Netzwerk-Übersicht: außen und innen

Die TrutzBox trennt zwei Welten. Außen, am Anschluss **LAN-Ext**, bezieht sie vom Internet-Router automatisch eine Adresse und meldet sich dort unter dem Namen „trutzbox". Zusätzlich kündigt sie sich im Netz des Routers und im internen Netz selbst unter dem Namen trutzbox.local an, damit Geräte sie auch dann finden, wenn der Router ihren Namen nicht kennt (Kapitel „Das Setup im Browser öffnen"). Innen betreibt sie ihr geschütztes Netz: die Anschlüsse LAN-Int1 und LAN-Int2 sowie das WLAN bilden zusammen einen Verbund (eine sogenannte Brücke), in dem alle angeschlossenen Geräte ungehindert miteinander sprechen können. Die VPN-Einwahl gehört nicht zu diesem Verbund. Sie bildet ein eigenes Netz, das die TrutzBox getrennt vom internen Netzwerk führt; von dort leitet die TrutzBox den Verkehr in das interne Netz weiter. Den Zustand beider Seiten samt Live-Anzeige und Geräteliste zeigt **Netzwerk → Status**.

Der innere Adressbereich

Im inneren Netz vergibt die TrutzBox die Adressen selbst. Sie brauchen dafür nichts einzustellen: Ein Gerät, das Sie anschließen oder ins WLAN einbuchen, bekommt seine Adresse automatisch aus dem Bereich 192.168.195.50 bis 199; die TrutzBox selbst hat immer die 192.168.195.200. Wer einem Gerät ausnahmsweise eine feste Adresse geben will, etwa einem Netzwerkdrucker, findet die nötigen Werte in Kapitel „Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen".

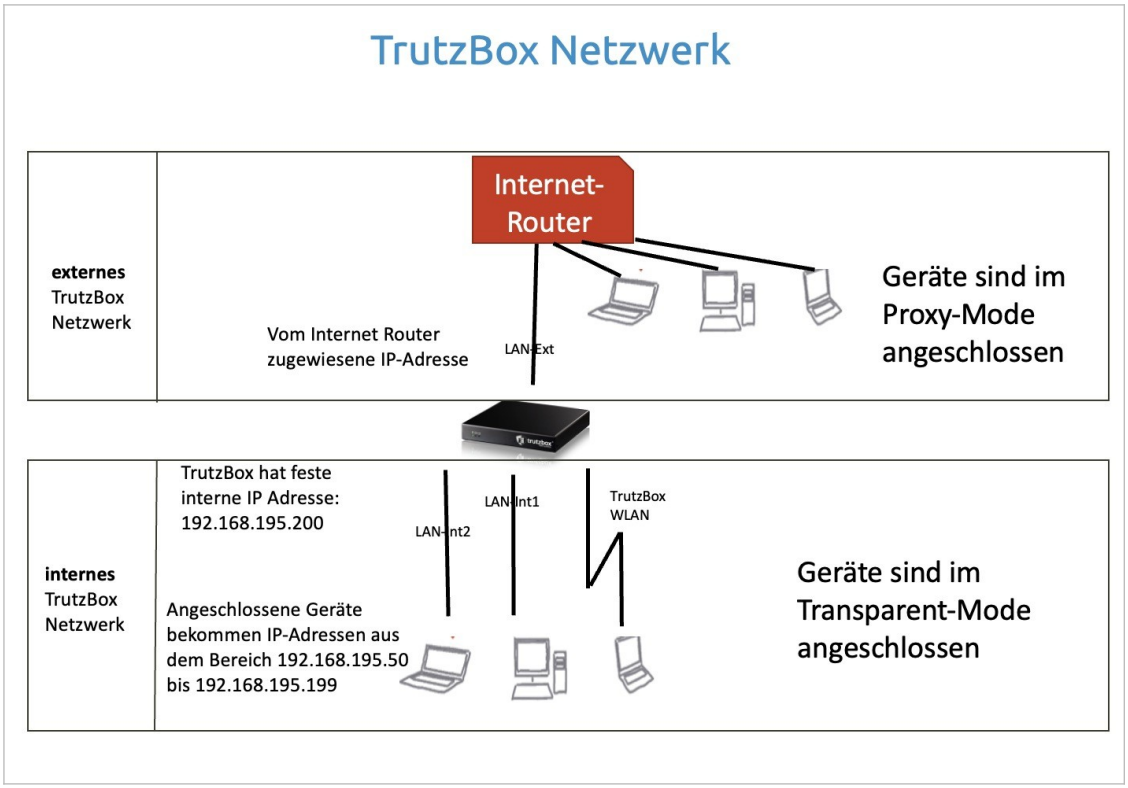


Abbildung 15-1: Außen das Netz des Internet-Routers, innen das geschützte TrutzBox-Netz mit den Adressen ab 192.168.195.50. (© 2026 Comidio GmbH)

Im inneren Netz vergibt die TrutzBox ausschließlich IPv4-Adressen. Reichen die beiden internen Anschlüsse nicht aus, erweitern Sie sie mit einem gewöhnlichen Switch; alles, was daran hängt, gehört weiterhin zum geschützten Netz. Eine bestehende VPN-Verbindung endet zwar in ihrem eigenen Adressbereich, wird von der TrutzBox aber in dieses Netz weitergeleitet, weshalb Sie von unterwegs genau dieselben Dienste erreichen wie im Netz der TrutzBox selbst.

Die Status-Seite

Die Seite **Netzwerk → Status** ist in zwei Bereiche gegliedert; darüber steht, sobald Fernzugriff oder Videokonferenz laufen, die Erreichbarkeit von außen (weiter unten in diesem Abschnitt). Der erste Bereich ist **LAN-Ext**, die zum Internet-Router gerichtete Seite. Hier wählen Sie zwischen **Automatisch IP Adresse zuweisen** (die Voreinstellung) und **Manuell IP Adresse konfigurieren**; bei der manuellen Variante tragen Sie Adresse, Netzmaske, Gateway und DNS selbst ein. Empfohlen bleibt die automatische Zuweisung. Manche Glasfaser- und DSL-Anschlüsse verlangen eine VLAN-Kennung: eine Nummer, die jedes Datenpaket trägt und auf der Leitung den Internetzugang von anderen Diensten wie der Telefonie trennt. Gewöhnlich setzt sie der Router. Hängt die TrutzBox ohne Router direkt an einer solchen Leitung und hat der Support dafür an LAN-Ext eine VLAN-Kennung eingerichtet, steht daneben zusätzlich der Haken **IPv6 für die TrutzBox anfordern**. Manche Anschlüsse vergeben IPv6 nur an ein Gerät; braucht ein zweiter Router am selben Anschluss IPv6, entfernen Sie den Haken. Hinter einem Router erscheint der Haken nicht. Darunter zeigt ein Live-Diagramm die gesendete und empfangene Datenrate, und eine Tabelle listet die am Router erreichbaren Geräte mit Name, Adresse und Zustand.

Der zweite Bereich ist das innere Netz. Die Brücke fasst dort das WLAN und die internen LAN-Anschlüsse zusammen; die VPN-Einwahl wird als eigene Schnittstelle daneben geführt. Alle lassen

sich einzeln über Kontrollkästchen ein- und ausblenden und besitzen jeweils ein eigenes Live-Diagramm. Eine weitere Tabelle listet die Geräte im inneren Netz. Zu jeder Schnittstelle lassen sich über einen Detail-Dialog die technischen Netzwerkdaten einsehen, was vor allem für den Support hilfreich ist.

Neben dem Namen eines Anschlusses steht die Geschwindigkeit, die er mit der Gegenstelle ausgehandelt hat, etwa „1000 Mbit/s“. Bei einer virtuellen Netzwerkkarte, also wenn die TrutzBox in einer virtuellen Maschine läuft, steht dort „virtuell“: Eine solche Karte hat keine Leitung und handelt keine Geschwindigkeit aus. Das „i“ daneben erklärt beides.

Erreichbarkeit von außen

Menüpfad: Netzwerk → Status

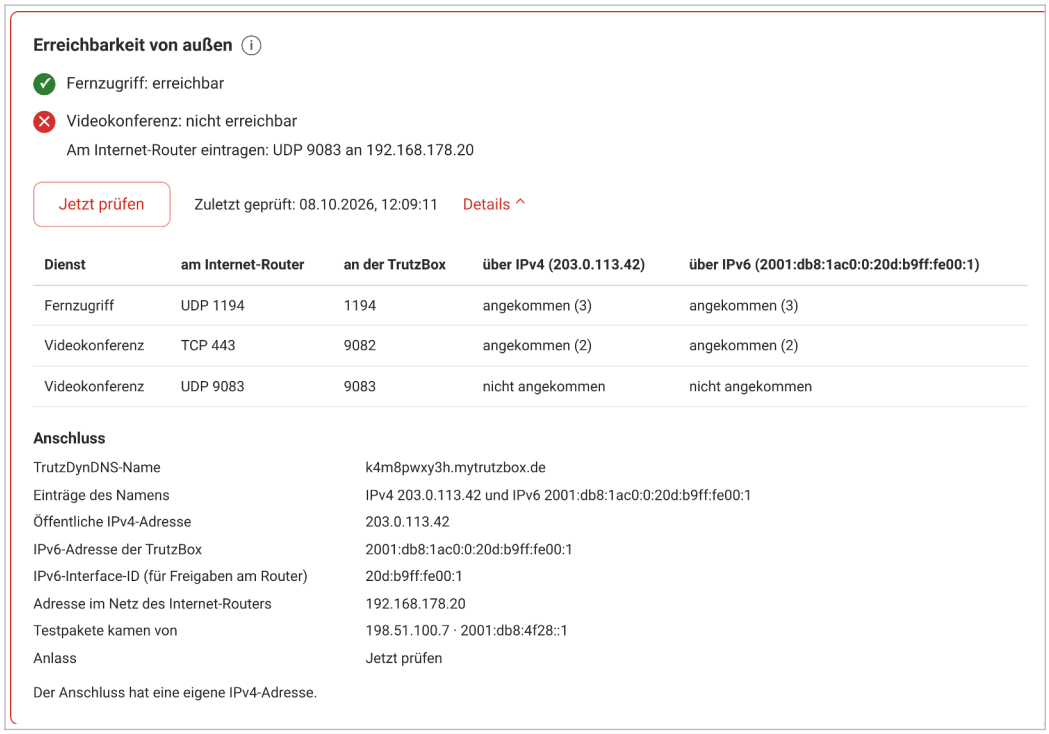


Abbildung 15-2: Der Abschnitt „Erreichbarkeit von außen": je Dienst das Ergebnis, darunter, was am Internet-Router noch einzutragen ist, und die aufgeklappten Details. (© 2026 Comidio GmbH)

Läuft der Fernzugriff oder die Videokonferenz, steht ganz oben auf der Seite 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 in diesem Fall 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.

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.

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. 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, die viele Router für eine IPv6-Freigabe verlangen, 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, steht dort, dass das für einen Anschluss ohne eigene IPv4-Adresse (DS-Lite) oder für fehlende Freigaben am Internet-Router spricht. Dieselben Angaben stehen im Bericht an den Support (Kapitel „Was in den Support-Bericht gehört“).

> **Was der Server von Comidio dabei tut und was nicht**
>
> Der Server schickt Testpakete nur, wenn Ihre 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 Ihrer TrutzBox auf (Kapitel „Was Comidio nicht kann und nicht tut“).

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** (Abschnitt „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 steht unter **Systemeinstellungen → Betriebszustand** in der Karte TrutzDynDNS in der Zeile „Veröffentlicht": „nur IPv6 (über IPv4 kommt nichts an)" oder „nur IPv4 (über IPv6 kommt nichts an)". Haben Sie den Schalter von Hand gesetzt, steht dort „nur IPv6 (Anschluss ohne eigene IPv4-Adresse)".

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 (Abschnitt „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“), bekommt die Anzeige ebenfalls; umgestellt wird dann nichts.

15.2 Das WLAN der TrutzBox

Menüpfad: Netzwerk → WLAN

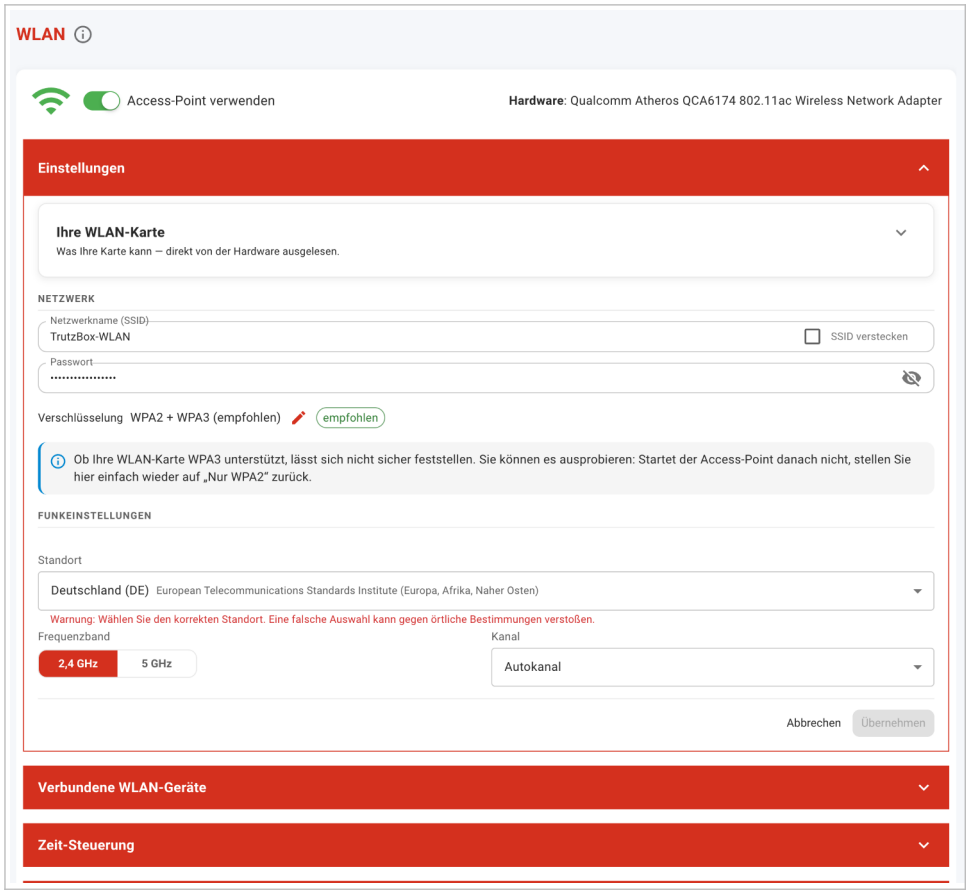


Abbildung 15-3: Die Seite WLAN mit dem Funknetz „TrutzBox-WLAN": Schalter „Access-Point verwenden", Netzwerkname, Passwort und Verschlüsselung, darunter Standort, Frequenzband und Kanal. (© 2026 Comidio GmbH)

Steckt in Ihrer TrutzBox ein WLAN-Modul, stellt sie unter **Netzwerk → WLAN** ein eigenes Funknetz bereit. Der Menüpunkt ist immer vorhanden; fehlt die passende Hardware, meldet die Seite „Kein WLAN Modul gefunden". Alles in diesem Funknetz ist Teil des internen Netzes und damit automatisch komplett geschützt. Eingeschaltet wird es über den Schalter **Access-Point verwenden**. Er lässt sich erst umlegen, wenn Name (SSID) und Passwort gespeichert sind; beides legen Sie darunter unter **Einstellungen** fest, auf Wunsch mit versteckter SSID, sodass der Name in den Netzwerklisten anderer Geräte nicht auftaucht.

Die Karte **Ihre WLAN-Karte** zeigt vorab, was die eingebaute Funkhardware überhaupt kann: ob sie WPA3 beherrscht, ob das 5-GHz-Band zur Verfügung steht und welcher WLAN-Generation sie angehört. Der angebotene Funktionsumfang der Seite richtet sich danach.

Das WLAN einrichten

Ab Werk ist der Zugangspunkt ausgeschaltet, und der Schalter **Access-Point verwenden** ist gesperrt. Darunter steht: „Schalter gesperrt: Es sind noch kein Netzwerkname und Passwort gespeichert. Bitte unter Einstellungen eintragen und übernehmen." In fünf Schritten steht Ihr eigenes Funknetz:

1. Öffnen Sie **Netzwerk → WLAN**.

2. Vergeben Sie unter **Einstellungen** im Feld **Netzwerkname (SSID)** einen Namen für das Funknetz. Er darf beliebig lauten; verwenden Sie am besten nicht denselben Namen wie das WLAN Ihres Routers, sonst wissen die Geräte später nicht, in welchem der beiden Netze sie eigentlich sind.
3. Vergeben Sie ein Passwort von mindestens 8 und höchstens 63 Zeichen. Nehmen Sie ein anderes als das des Router-WLANs und notieren Sie es; jedes Gerät braucht es beim ersten Verbinden einmal.
4. Klicken Sie auf **Übernehmen**. Damit ist der Schalter oben frei.
5. Schalten Sie **Access-Point verwenden** ein. Das Funknetz ist nach wenigen Sekunden verfügbar. Verbinden Sie danach Ihre Geräte damit; sie sind dann automatisch komplett geschützt (Kapitel „Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen“).

Die übrigen Einstellungen können Sie zunächst so lassen, wie sie sind. Was sie bedeuten und wann sich ein Eingriff lohnt, steht hier:

- **Verschlüsselung:** Voreingestellt ist „WPA2 + WPA3 (empfohlen)", ein Übergangsbetrieb, in dem alte und neue Geräte gleichermaßen funktionieren. Wer nur moderne Geräte hat, stellt auf „Nur WPA3" (höchste Sicherheit, sehr alte Geräte bleiben außen vor); „Nur WPA2" gibt es für Sonderfälle. Für „WPA2 + WPA3" betreibt die TrutzBox das WLAN mit dem Programm hostapd, denn nur damit funken alte und neue Geräte gleichzeitig im selben Netz. Die Umstellung erledigt sie selbst. Startet das WLAN auf diesem Weg nicht, läuft es mit der vorherigen Einstellung weiter, und die Seite zeigt einen Hinweis. Welches Programm gerade arbeitet, hostapd oder NetworkManager, nennt die Karte **Ihre WLAN-Karte** in der Zeile „Verwaltet von".
- **Frequenzband und Kanal:** Zur Wahl stehen 2,4 GHz und, wenn die Karte es am gewählten Standort nutzen kann, 5 GHz (siehe unten). Die Voreinstellung „Autokanal" wählt selbst den am wenigsten belegten Kanal. Wer von Hand wählt, sieht zu jedem Kanal Frequenz, zulässige Sendeleistung und Besonderheiten, etwa Kanäle, die auf Wetterradar Rücksicht nehmen müssen.
- **Standort:** Damit wird die zuständige Funkregulierung gewählt, für Deutschland und Europa also die europäische. Die Angabe bestimmt, welche Kanäle und Sendeleistungen am Aufstellort überhaupt erlaubt sind, und muss deshalb korrekt gesetzt sein. Erst wenn der gewählte Standort wirksam ist, bietet die Seite das 5-GHz-Band an. Beim Ändern startet die TrutzBox das WLAN kurz intern neu, damit die Einstellung sicher greift.
- **Zeit-Steuerung:** Ein Wochenplan kann das WLAN automatisch schalten. Ab Werk ist kein Zeitplan aktiv; richten Sie einen ein, schlägt der Dialog 07:00 bis 22:00 vor.
- **Verbundene WLAN-Geräte:** listet jedes eingebuchte Gerät mit Namen aus der Geräteliste, Adresse, Signalstärke, aktueller Empfangs- und Sende-Datenrate sowie der Dauer der Verbindung.
- **Andere WLAN-Netzwerke die stören könnten:** eine Übersicht der Nachbar-WLANs, hilfreich bei Funkproblemen.

Zeit-Steuerung im Detail

Die Zeit-Steuerung zeigt für jeden Wochentag ein 24-Stunden-Raster: Grün hinterlegte Abschnitte sind die Zeiten, in denen der Zugangspunkt sendet, graue die, in denen das Funkmodul ausgeschaltet ist. Über **Einstellen** passen Sie die Fenster an. Der manuelle Schalter hat dabei Vorrang: Schalten Sie das WLAN von Hand ein oder aus, gilt diese Entscheidung bis zum nächsten im Plan hinterlegten Schaltzeitpunkt, danach übernimmt wieder der Plan. Außerhalb der aktiven Zeiten verbraucht das Funkmodul keinen Strom und sendet keine Funkwellen, was den Energieverbrauch senkt und die Funkbelastung in den Räumen reduziert, ohne dass jemand abends einen Knopf drücken muss.

Andere WLANs in der Umgebung

Am unteren Rand der Seite zeigt die TrutzBox einen Scan der Funknetze in Reichweite, die das eigene stören könnten. Zu jedem gefundenen Netz stehen die Signalstärke in Prozent, der belegte Kanal mit Frequenz, die angekündigte Höchstgeschwindigkeit und die unterstützten Verschlüsselungsstandards. Der Scan funktioniert auch, während die TrutzBox selbst sendet; angezeigt werden die Netze des gerade aktiven Frequenzbands. Auf manchen WLAN-Karten bleibt die Liste leer, solange das WLAN mit hostapd läuft; die Seite sagt das dann ausdrücklich. Wählen Sie für Ihr eigenes WLAN nach Möglichkeit einen Kanal, den kein starkes Nachbarnetz belegt. Im 2,4-GHz-Band haben sich die Kanäle 1, 6 und 11 bewährt, weil sie sich gegenseitig nicht überlappen.

Ob Ihre TrutzBox überhaupt auf 5 GHz funkt, hängt von der jeweils eingebauten WLAN-Karte ab. Die Seite zeigt den Knopf **5 GHz** nur, wenn der gewählte Standort wirksam ist und die Karte dort nutzbare 5-GHz-Kanäle für den Betrieb als Zugangspunkt hat. Manche Karten haben ihre Funkregion fest im Chip hinterlegt und geben das Band nicht frei; das lässt sich über den Standort nicht ändern, nur eine andere WLAN-Karte hilft. Warum Ihre Karte kein 5 GHz anbietet, steht in der Karte **Ihre WLAN-Karte**.

Früher gab es für manche dieser Karten den Knopf „5 GHz freischalten“. Ihn gibt es nicht mehr. Ein WLAN, das auf diesem Weg auf 5 GHz lief, hat ein Software-Update von selbst auf 2,4 GHz mit Autokanal umgestellt.

15.3 DNS-Schutz und verschlüsselte Namensauflösung

Menüpfad: Netzwerk → Netzwerkdienste

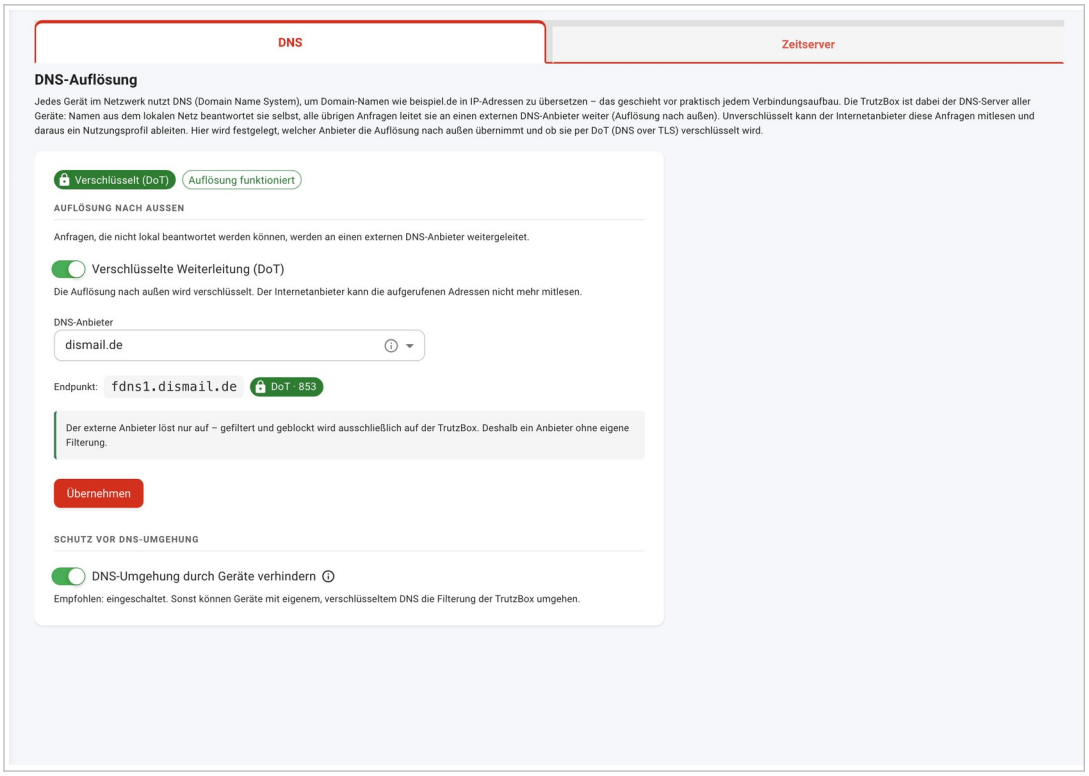


Abbildung 15-4: Verschlüsseltes DNS: Status, Anbieterwahl und der Schutz vor DNS-Umgehung. (© 2026 Comidio GmbH)

Bevor ein Gerät irgendeine Verbindung aufbaut, fragt es per DNS nach der Adresse des Ziels. Unverschlüsselt ist diese Namensauflösung ein offenes Buch: Jeder auf dem Weg kann mitlesen, welche Seiten Sie ansteuern. Anfragen aus Ihrem Netz beantwortet die TrutzBox zunächst selbst; nur was sie nicht lokal beantworten kann, reicht sie nach außen weiter. Genau diese Weiterleitung verschlüsselt sie ab Werk (DoT, DNS über TLS). Zu finden ist alles unter **Netzwerk → Netzwerkdienste**, Reiter **DNS**.

Zwei Anzeigen sagen Ihnen, woran Sie sind: die eine, ob die Weiterleitung gerade verschlüsselt läuft oder nicht, die andere, ob die Auflösung überhaupt funktioniert. Die TrutzBox schaltet die Verschlüsselung selbsttätig ein und prüft sie selbst. Lässt der Anschluss sie gerade nicht zu, löst die TrutzBox vorübergehend unverschlüsselt auf, damit die Geräte Internet haben. Sie versucht es in der ersten Stunde alle fünf Minuten erneut, danach alle 30 Minuten, und schaltet von selbst zurück, sobald es wieder klappt. Das hilft auch nach einem Umzug an einen anderen Anschluss. Nur wenn Sie die Verschlüsselung bewusst abschalten, bleibt sie dauerhaft aus.

Als Anbieter für die Auflösung nach außen stehen geprüfte Dienste zur Wahl, jeweils mit einer kurzen Einordnung zu Betreiber und Rechtsraum: **DNS4EU** (ein EU-gefördertes Projekt ohne eigene Filterung, empfohlen), **Quad9** (eine gemeinnützige Schweizer Stiftung, ungefiltert), **Cloudflare** und **Google** (beides US-Unternehmen) sowie **Benutzerdefiniert** für einen eigenen Server. Wichtig zur Einordnung: Der externe Anbieter löst nur auf. Gefiltert und geblockt wird ausschließlich auf Ihrer TrutzBox, weshalb bewusst ein Anbieter ohne eigene Filterung empfohlen wird. Die Kontrolle bleibt so vollständig bei Ihnen.

Schutz vor DNS-Umgehung

Ebenfalls empfohlen eingeschaltet: **DNS-Umgehung durch Geräte verhindern**. Viele Smart-Geräte und Apps ignorieren den Namensdienst im eigenen Netz und fragen fest einprogrammierte Server im Internet, um Filter zu umgehen. Der Schalter unterbindet das: Egal auf welchem Weg ein Gerät es versucht, ob unverschlüsselt oder verschlüsselt, die TrutzBox fängt die Anfrage ab und beantwortet sie selbst. Betroffen ist davon auch Apples „Private Relay"; Apple-Geräte zeigen dann einen entsprechenden Hinweis an.

Kann ein Gerät danach keine Namen mehr auflösen, hat jemand dort einen eigenen verschlüsselten DNS-Dienst fest eingetragen; entfernen Sie diese Einstellung am Gerät. Jede Änderung wird mit **Übernehmen** wirksam. Die TrutzBox prüft die Umschaltung dabei selbst, was bis zu einer Minute dauern kann, und stellt bei einem Fehlschlag automatisch den vorherigen Zustand wieder her, damit die Namensauflösung nicht ausfällt.

Der Reiter Zeitserver

Menüpfad: Netzwerk → Netzwerkdienste → Zeitserver

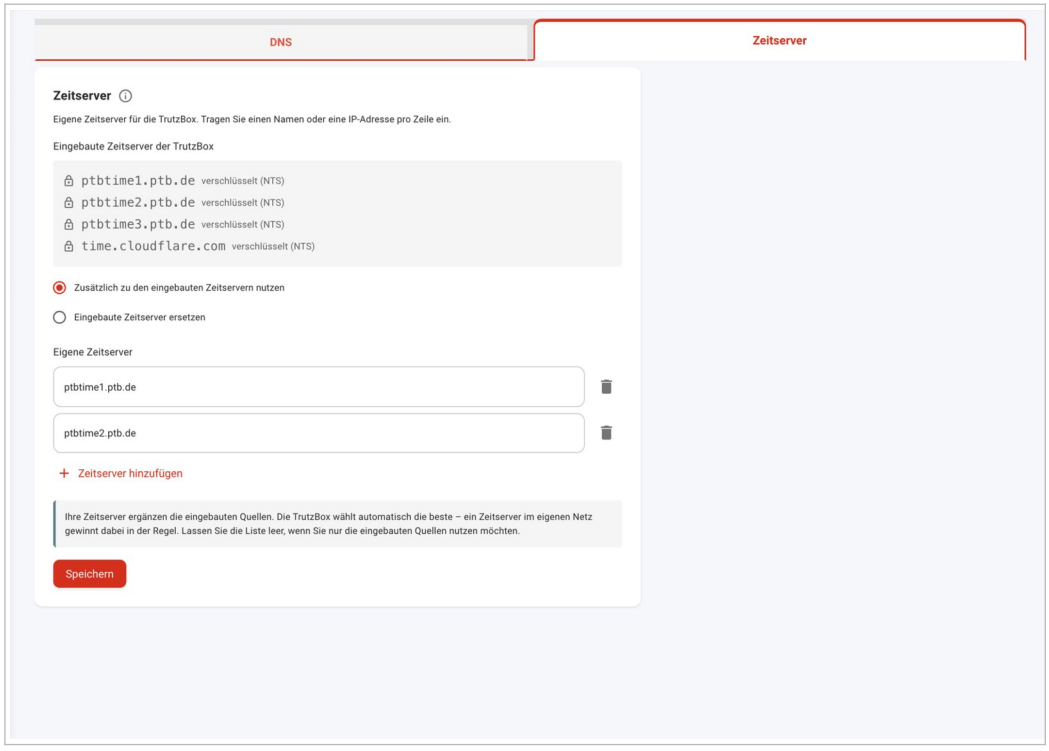


Abbildung 15-5: Der Reiter Zeitserver: eigene Zeitquellen ergänzen die eingebauten, ersetzen sie aber nicht. (© 2026 Comidio GmbH)

Der zweite Reiter derselben Seite verwaltet die Zeitquellen. Korrekte Zeit ist die Grundlage jeder Zertifikatsprüfung, deshalb holt die TrutzBox ihre Uhrzeit von vertrauenswürdigen Quellen: von vier Zeitservern der Physikalisch-Technischen Bundesanstalt, also der deutschen Atomuhr, und von Netnod. Alle fünf Quellen sind kryptografisch gesichert, die Zeit lässt sich unterwegs also nicht unbemerkt verfälschen. Zusätzlich lassen sich bis zu acht eigene Zeitserver eintragen, etwa ein Zeitserver im eigenen Netz. Eigene Server ergänzen die eingebauten Quellen, sie ersetzen sie nicht: Die TrutzBox wählt automatisch die beste Quelle, wobei ein Server im eigenen Netz in der Regel gewinnt. Bleibt die Liste leer, nutzt die TrutzBox nur die eingebauten Quellen.

15.4 Angriffsschutz: Firewall und Wächter

Menüpfad: Netzwerk → Angriffsschutz

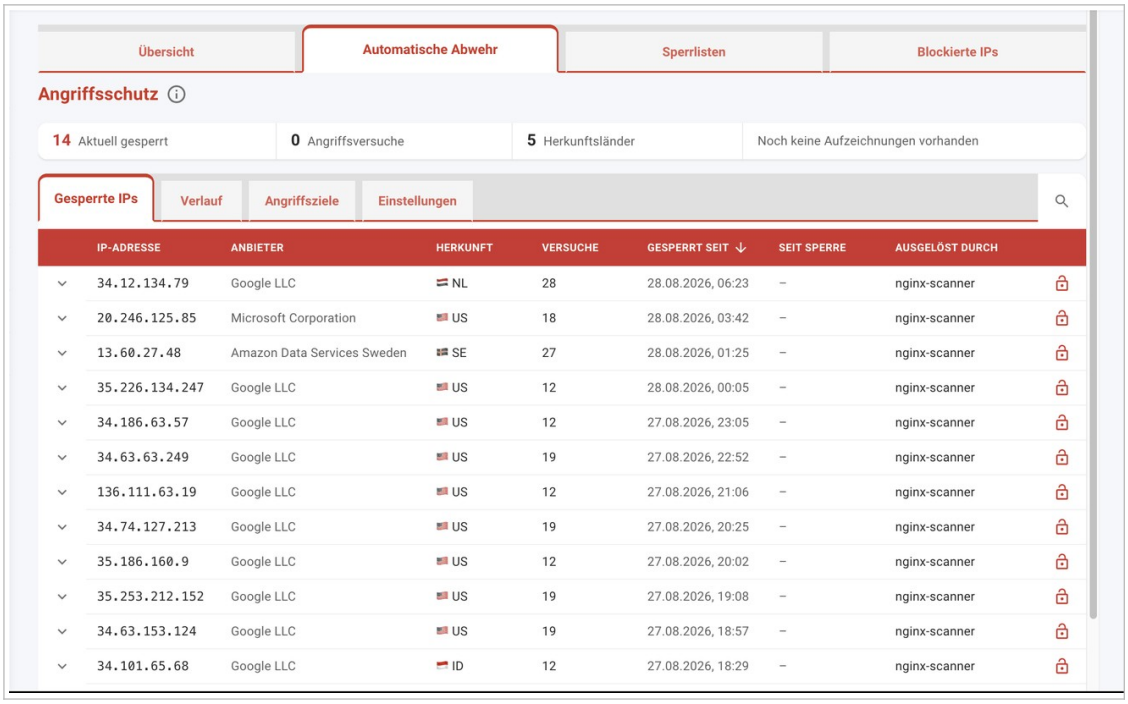


Abbildung 15-6: Die Angriffsschutz-Seite: Kennzahlen, gesperrte Adressen und die Angriffsziele in Alltagssprache. (© 2026 Comidio GmbH)

Jeder Internet-Anschluss wird pausenlos von automatischen Scannern abgeklopft; das ist kein Grund zur Sorge, sondern Alltag im Netz. Die TrutzBox beantwortet es zweistufig: Die **Firewall** verwirft unerwünschte Zugriffe von außen, und der **Angriffsschutz** beobachtet die von außen erreichbaren Dienste der TrutzBox. Wer dort wiederholt mit Fehlversuchen auffällt, etwa beim Passwort-Raten, dessen Adresse wird automatisch gesperrt und wandert in die Firewall-Blockliste. Geräte in Ihrem eigenen Netz sperrt der Wächter dabei nie, und auch die eigene Internet-Adresse ist fest ausgenommen: Die TrutzBox kann sich nicht selbst aussperren.

Alles dazu bündelt die Seite **Netzwerk → Angriffsschutz** in vier Reitern.

> **Anleitung zum Anklicken**
>
> Die vier Reiter und ihre Zahlen im Zusammenhang: Die Anleitung „Angriffsschutz der TrutzBox" zeigt die Stationen dieses Kapitels mit Bild, Text und Ton im Browser: trutzbox.de/videodokumentation.

Reiter Übersicht: der Firewall-Monitor

Der erste Reiter ist die Live-Sicht auf alle Verbindungen, die auf Netzwerk-Ebene abgewehrt wurden, über alle Ports und Protokolle hinweg. Die Darstellung entspricht dem gewohnten Spaltenbild des Monitors: links die betroffenen Server im Internet, in der Mitte die Firewall mit der Zahl der Blockierungen, rechts Ihre Geräte. Rot gestrichelte Linien markieren die blockierten Verbindungen. Die Kopfzeile fasst die Kennzahlen zusammen und nennt unter anderem die am

Internet-Router freigegebenen Ports, sodass Sie jederzeit sehen, welche Türen tatsächlich offen stehen.

Der Knopf **Warum?** erklärt jede einzelne Blockierung im Klartext: Schweregrad, wahrscheinliche Art des Vorgangs (etwa ein Port-Scan), die zugrunde liegende Regel, sämtliche Verbindungsangaben und eine Handlungsempfehlung. Diese lautet in den allermeisten Fällen, dass keine Maßnahme erforderlich ist, denn genau dafür ist die Firewall da. Zu jeder Adresse bietet der Dialog außerdem vorbereitete Links zu externen Auskunftsdiensten an. Die TrutzBox ruft diese Dienste nicht von sich aus auf; ob Sie dort nachschlagen, entscheiden Sie.

Reiter Automatische Abwehr

Hier arbeitet der Wächter. Drei Kennzahlen fassen die Lage zusammen: die Zahl der gesperrten Adressen, die Zahl der Angriffsversuche und die Herkunftsländer. Darunter gliedert sich die Ansicht weiter auf:

- **Gesperrte IPs:** die derzeit gesperrten Adressen, jeweils mit dem Namen des Anbieters statt nur der nackten Zahlenadresse, dazu Herkunftsland, Zahl der Versuche, Sperrzeitpunkt und der Dienst, der die Sperre ausgelöst hat. Der Pfeil am Zeilenanfang klappt auf, wonach diese Adresse gesucht hat. Über das Schloss-Symbol entsperren Sie versehentlich Gesperrtes wieder.
- **Verlauf:** Sperrungen und Freigaben in zeitlicher Reihenfolge, die neuesten zuerst.
- **Angriffsziele:** in Alltagssprache, wonach die gesperrten Adressen gesucht haben, etwa nach Zugangsdaten und Schlüsseln, Router-Zugängen, Webmail-Servern, VPN-Portalen, Überwachungskameras oder Datenbank-Verwaltungen. Wichtig zur Einordnung: Keiner dieser Dienste läuft auf der TrutzBox. Die Liste zeigt nur, wonach automatische Scanner überall im Internet suchen.
- **Einstellungen:** Sperrdauer, Beobachtungszeitraum und die Zahl der Versuche bis zur Sperre, jeweils für jeden Wächter einzeln. Zusätzliche eigene Ausnahmen lassen sich ergänzen; die fest hinterlegten Ausnahmen für das eigene Netz und die eigene Internet-Adresse lassen sich bewusst nicht entfernen. Die Wächter für Anmeldungen lassen sich nur strenger einstellen, nicht lockerer.

In der Spalte, die den Auslöser nennt, erkennen Sie verschiedene Wächter, und sie sind ab Werk unterschiedlich eingestellt. Der Wächter für Scan-Versuche greift nach drei Versuchen innerhalb eines Tages und sperrt die Adresse dann dauerhaft. Die Wächter für fehlgeschlagene Anmeldungen, einer für den Chat und einer für Mail-Programme, die sich von außen am Postfach anmelden, greifen nach fünf Fehlversuchen innerhalb von 30 Minuten und sperren zunächst für sechs Stunden, bei Wiederholung immer länger, höchstens eine Woche. Dahinter steckt nämlich meist ein eigenes Gerät mit einem alten Passwort, das sich sonst dauerhaft selbst aussperren würde. Ein dritter Anmelde-Wächter bewacht die Kommandozeile (SSH, Abschnitt „Webmin: der Experten-Zugang“). Er zählt genauso, sperrt beim ersten Mal aber nur für eine Stunde, denn dort sitzt ein Mensch an der Tastatur und kein Programm, das immer wieder anklopft. Geräte im eigenen Netz, im Netz vor der TrutzBox mit privaten Adressen und im VPN sperren diese Wächter nie.

Reiter Sperrlisten

Hier verwalten Sie Adressen, die auf Netzwerk-Ebene grundsätzlich blockiert werden sollen, unabhängig vom Protokoll. Einzelne Adressen oder ganze Bereiche tragen Sie selbst ein, größere Mengen importieren Sie aus einer Textdatei; öffentlich gepflegte Listen bekannter schädlicher Adressen lassen sich auf diesem Weg ebenfalls einspielen. Ab Werk ist die Liste leer, und Comidio verteilt keine Adresslisten. Eine eingespielte Liste holt die TrutzBox auch nicht von selbst neu, anders als Filterlisten aus dem Internet (Kapitel „Filterlisten aus dem Internet laden und automatisch aktualisieren“): Sie bleibt auf dem Stand der Datei, bis Sie eine neuere einspielen (Kapitel „Filter- und Sperrlisten-Updates“). Einträge lassen sich einzeln über das Papierkorb-Symbol oder in einem Schritt über die Auswahlkästchen entfernen. Die Sperren gelten für IPv4 und IPv6 gleichermaßen, und auch die automatischen Sperren des Wächters landen in genau dieser Liste. Es gibt also keine zweite, unsichtbare Sperrwelt daneben.

Auf demselben Reiter sitzt der Schalter **QUIC sperren**, ab Werk eingeschaltet. QUIC ist ein neueres Übertragungsverfahren, das von Anfang an verschlüsselt ist und für den Webfilter der TrutzBox deshalb undurchsichtig bleibt. Wird es gesperrt, weichen die Programme automatisch auf das herkömmliche, prüfbare Verfahren aus, und der Webfilter kann wieder arbeiten. Genau darum ist die Sperre voreingestellt.

Unterhalb der Sperrliste steht der Abschnitt **Ausnahmen (IP-Whitelist)**. Eine Ausnahme ist eine ausdrückliche Freigabe für eine Adresse oder einen Adressbereich, die die Sperrliste übersteuert, ohne deren Eintrag zu löschen. Genau darin liegt ihr Wert: Spielen Sie später eine Liste ein, die die Adresse wieder enthält, bleibt die Adresse trotzdem frei. Als eigene Ausnahme bleibt die Freigabe dauerhaft bestehen. Eingetragen werden eine einzelne Adresse oder ein Bereich, dazu eine kurze Angabe, woher die Adresse stammt, und ein freier Kommentar.

Jede Ausnahme führt einen eigenen Trefferzähler, an dem Sie ablesen, ob sie überhaupt noch gebraucht wird. Nicht jede Freigabe wird angenommen: Ausnahmen auf reservierte Adressbereiche, auf allzu große Bereiche und auf eine gerade aktive Sperre des Wächters lehnt die TrutzBox ab. Sonst genügte eine einzige zu weit gefasste Ausnahme, um den Angriffsschutz wirkungslos zu machen.

Reiter Blockierte IPs

Menüpfad: Netzwerk → Angriffsschutz → Blockierte IPs

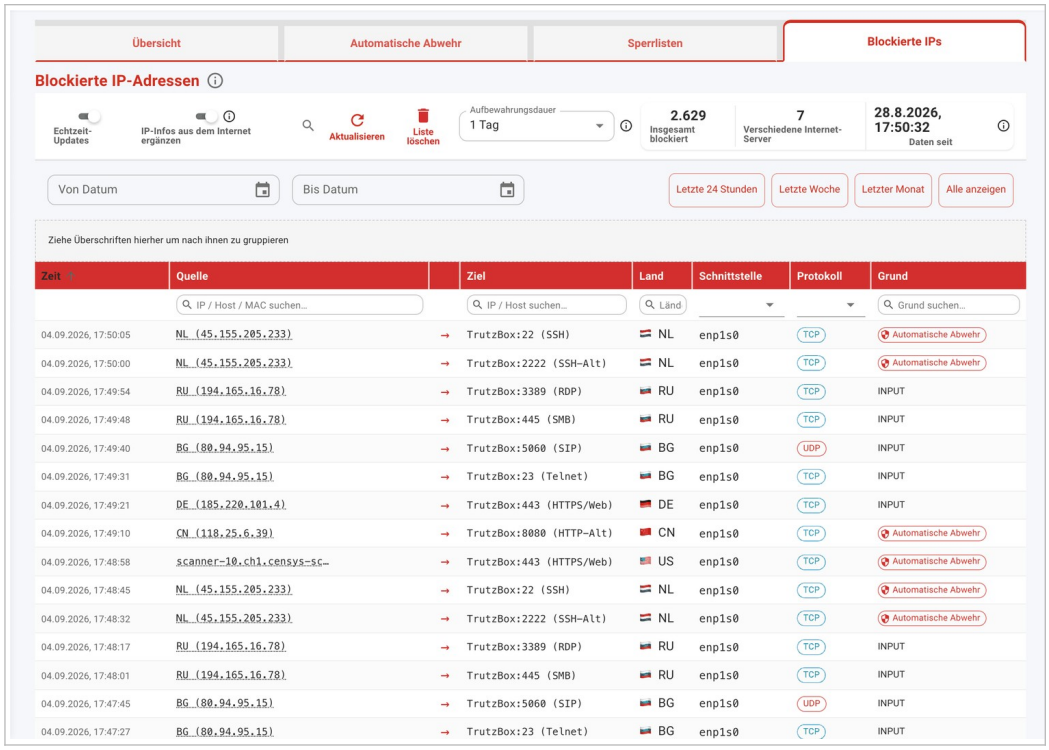


Abbildung 15-7: Der Reiter Blockierte IPs: jeder abgewehrte Verbindungsversuch mit Quelle, Ziel und Land. (© 2026 Comidio GmbH)

Der vierte Reiter ist das durchsuchbare Protokoll aller von der Firewall blockierten Verbindungsversuche. Ab Werk werden die Einträge einen Tag lang aufbewahrt; zur Wahl stehen aus, 5 Minuten, 1 Stunde, 1 Tag, 7 Tage und, als längste Aufbewahrung, 31 Tage. Sie können den Zeitraum eingrenzen (letzte 24 Stunden, letzte Woche, letzter Monat oder alles), je Spalte suchen und die Liste nach Quelle, Ziel, Land oder Grund gruppieren. Die Ports erscheinen dabei mit ihrem Dienstnamen, was das Lesen erheblich erleichtert. Über den CSV-Export nehmen Sie die angezeigten Einträge für eine eigene Auswertung mit.

Der Zustand des Angriffsschutzes erscheint zusätzlich als Karte auf der Betriebszustand-Seite; im Alltag müssen Sie hier nichts tun.

Warum manche Verbindungen keinen Namen zeigen

Im Monitor und in den Sperrlisten stehen Einträge, die statt eines Domain-Namens nur eine Adresse tragen. Das ist kein Fehler, sondern eine Entwicklung im Netz: Der Name einer Verbindung verschwindet zusehends aus dem Datenstrom, und die beiden namensbasierten Schutzwege, die Namenssperre und der Webfilter, greifen dann nicht mehr.

- Fernseher, sprachgesteuerte Lautsprecher und Spielkonsolen fragen oft einen fest eingebauten Namensdienst im Internet statt den der TrutzBox. Der Schutz vor DNS-Umgehung fängt das ab (Abschnitt „DNS-Schutz und verschlüsselte Namensauflösung“).
- Browser und Apps verschlüsseln ihre Namensanfragen zunehmend selbst. Die TrutzBox sperrt deshalb die bekannten Anbieter solcher Dienste und erzwingt den eigenen Weg (Abschnitt „DNS-Schutz und verschlüsselte Namensauflösung“).

- Bei neueren Verfahren ist selbst im Verbindungsaufbau kein Name mehr zu sehen; übrig bleibt die Adresse. Dort greifen die Sperrlisten, und das Server-Detail im Monitor nennt Betreiber und Land zur Einordnung.
- Etwa jede fünfte Web-Verbindung nutzt inzwischen ein Übertragungsverfahren, das am Webfilter vorbeiläuft. Der Schalter **QUIC sperren** schließt diesen Weg.
- Push-Dienste der Betriebssysteme verbinden sich teils ohne vorherige Namensabfrage direkt mit hinterlegten Adressen. Solche Verbindungen sieht nur eine Firewall, die nach Adressen arbeitet.

Daraus folgt die Arbeitsteilung in der TrutzBox: Der Webfilter filtert genau, wo er Namen und Adresse einer Seite sieht; der Angriffsschutz sperrt nach Adresse, wo kein Name mehr sichtbar ist. Der Monitor zeigt beides und bietet zu jeder Verbindung die passende Aktion an (Kapitel „Untersuchen und eingreifen“).

15.5 Netzwerk-Einstellungen ändern

Änderungen an der Außenseite (feste Adresse statt automatischer, andere DNS-Vorgaben) nehmen Sie unter **Netzwerk → Status** vor. Die TrutzBox testet neue Einstellungen erst und stellt bei Fehlschlag den vorherigen Zustand automatisch wieder her, das kennen Sie schon aus dem Setup. Für das interne Netz gilt: Der Adressbereich ist bewusst fest; Geräte, Adressvergabe und interne Namensauflösung verwaltet die TrutzBox vollautomatisch.

Diese Zurückhaltung hat einen praktischen Grund. Ein falsch gesetzter Wert an dieser Stelle kann die TrutzBox aus dem eigenen Netz unerreichbar machen, und dann bliebe im ungünstigsten Fall nur das Zurücksetzen. Solange Sie keinen bestimmten Anlass haben, etwa eine Vorgabe Ihrer Firmen-IT, ändern Sie hier am besten nichts.

Häufige Fragen zum Netzwerk

Brauche ich das WLAN des Internet-Routers noch?

Nur für Geräte, die bewusst ungeschützt bleiben sollen. Am konsequentesten ist es, alle Geräte ins TrutzBox-WLAN umzuziehen und das Router-WLAN abzuschalten; dann führt kein Funkweg mehr am Schutz vorbei.

Auf der Angriffsschutz-Seite stehen viele gesperrte Adressen. Muss ich etwas tun?

Nein, im Gegenteil: Die Einträge zeigen, dass der Wächter arbeitet. Die Versuche gelten nicht Ihnen persönlich; automatische Scanner klopfen jeden Anschluss im Internet ab.

Mein WLAN ist abends nicht da. Ist etwas kaputt?

Vermutlich nicht. Prüfen Sie die Zeit-Steuerung unter **Netzwerk → WLAN**. Ab Werk ist dort kein Zeitplan hinterlegt; wurde einer eingerichtet, ist das Funkmodul außerhalb der grün hinterlegten Zeiten bewusst ausgeschaltet.

Die DNS-Anzeige steht auf „Unverschlüsselt". Was heißt das?

Der Anschluss ließ die verschlüsselte Weiterleitung im Moment nicht zu. Die Namensauflösung funktioniert weiterhin, sie ist auf dem Weg nach außen nur nicht verschlüsselt. Die TrutzBox

versucht es von selbst erneut, in der ersten Stunde alle fünf Minuten, danach alle 30 Minuten (Abschnitt „DNS-Schutz und verschlüsselte Namensauflösung“).

Ein Gerät kommt seit dem Einschalten des Umgehungsschutzes nicht mehr ins Internet.

Auf diesem Gerät ist wahrscheinlich ein eigener verschlüsselter Namensdienst fest eingetragen. Entfernen Sie diese Einstellung am Gerät, dann nutzt es wieder die TrutzBox. Notfalls lässt sich der Schutz auch vorübergehend abschalten.

16 Updates

Aktuelle Software ist die halbe Sicherheit. Bei der TrutzBox müssen Sie sich darum nicht kümmern: Sie hält sich selbst auf dem neuesten Stand. Jede Nacht und bei jedem Start prüft sie, ob Neues bereitsteht, lädt es und spielt es ein, ohne Ihr Zutun und ohne dass mitten am Tag etwas stehen bleibt. Dieses Kapitel erklärt trotzdem, was da passiert, denn wer weiß, wie die TrutzBox sich versorgt, kann auch einschätzen, warum das sicher ist.

16.1 Die drei Arten von Updates

Menüpfad: Systemeinstellungen → Vertrag und Pakete

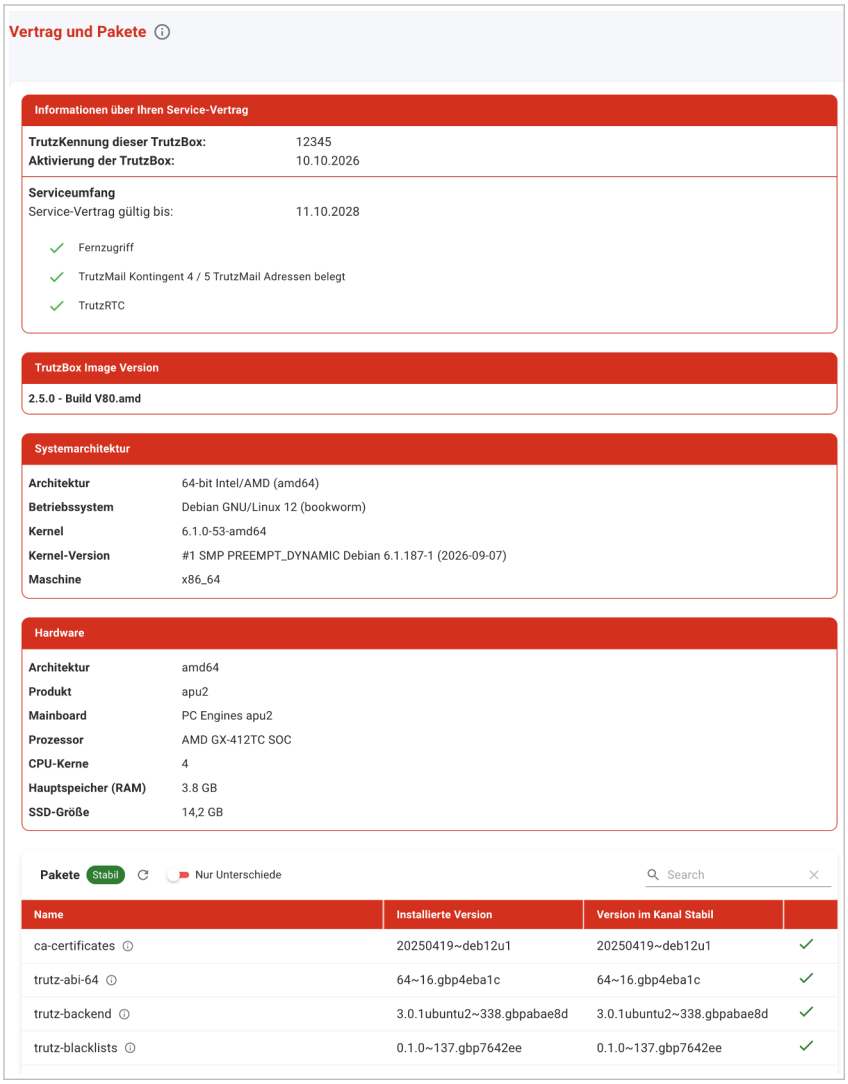


Abbildung 16-1: Die Seite Vertrag und Pakete: Service-Vertrag der TrutzKennung 12345, Image-Version 2.5.0 Build V80.amd, Systemarchitektur, Hardware und die Paketliste im Kanal Stabil mit installierter Version und Version im Kanal. (© 2026 Comidio GmbH)

Auf der TrutzBox werden drei Arten von Updates unterschieden. Die ersten beiden laufen täglich und unbemerkt, die dritte ist ein seltener Ausnahmefall:

- **Software-Paket-Updates:** Einzelne Programmbestandteile der TrutzBox werden gegen neuere Versionen getauscht. Das betrifft die von Comidio entwickelten Teile ebenso wie geprüfte Pakete des zugrunde liegenden Betriebssystems.
- **Filter- und Sperrlisten-Updates:** Die Listen, mit denen die TrutzBox unerwünschten Datenverkehr erkennt, werden täglich erneuert. Gemeint sind etwa Werbung, die Aufzeichnung dessen, was Sie im Netz tun, Schadcode-Quellen und andere gefährliche Server.
- **Komplette Image-Updates:** Das gesamte Betriebssystem der TrutzBox wird neu aufgespielt. Das ist die Ausnahme und kein Teil des täglichen Ablaufs (Abschnitt „Der Ausnahmefall: ein komplettes Image“).

16.2 Software-Paket-Updates

Die Programme der TrutzBox stammen aus zwei Quellen, und beide werden unterschiedlich behandelt.

Von Comidio entwickelte Pakete

Hierzu gehören die Teile, die es nur auf der TrutzBox gibt: der Webfilter, die Mail-Komponenten, die Verwaltungsoberfläche und alles, was daran hängt. Sie enthalten Fehlerbehebungen und neue Funktionen und werden vor der Auslieferung intern getestet. Was ein Software-Update bringt, beschreibt Comidio im TrutzBox-Forum.

Pakete des Betriebssystems

Die TrutzBox baut auf der Linux-Distribution Debian auf, für die laufend Sicherheits- und Stabilitäts-Updates erscheinen. Comidio übernimmt diese nicht ungeprüft. Sie werden zuerst in einer eigenen Umgebung gegen die TrutzBox-Software getestet, und erst wenn feststeht, dass sie nichts beeinträchtigen, gehen sie an die TrutzBoxen der Kunden. Das kostet ein paar Tage, verhindert aber, dass eine fremde Änderung Ihre TrutzBox aus dem Tritt bringt.

Software-Updates schon beim ersten Start

Die TrutzBox spielt die neueren Software-Pakete schon beim ersten Einschalten ein, meist noch bevor Sie im Setup beim Schritt Netzwerkeinstellungen angekommen sind. Nach diesem Schritt zeigt das Setup die Warteseite „Software-Updates werden installiert“ nur in zwei Fällen: wenn der Lauf vom Einschalten noch arbeitet, oder wenn die TrutzBox beim Einschalten noch kein Internet hatte, etwa weil sie am Router eine feste Adresse braucht. Dann startet das Setup den Lauf selbst und wartet, bis er fertig ist (Kapitel „Software-Updates während der Einrichtung“). Eine frisch eingerichtete TrutzBox ist damit auf demselben Stand wie eine, die seit Jahren läuft.

Der Ablauf im Betrieb

Im laufenden Betrieb sucht die TrutzBox jede Nacht zu einer zufälligen Zeit zwischen 3 und 6 Uhr nach neuen Paketen, und zusätzlich bei jedem Start. Was sie findet, spielt sie selbst ein. Die Karte **Software-Updates** im Betriebszustand sagt es so: „Die TrutzBox sucht jede Nacht und bei jedem Start nach Software-Updates und spielt sie selbst ein.“

Scheitert ein Lauf, versucht es die TrutzBox gleich noch einmal, insgesamt bis zu dreimal, mit zwei Minuten Pause dazwischen. Klappt es auch dann nicht, folgt der nächste Versuch in der

kommenden Nacht oder beim nächsten Start. Für Software-Updates startet die TrutzBox nie neu; nur einzelne Dienste starten kurz neu.

Öffnen Sie die Oberfläche, während Software-Updates eingespielt werden, erscheint statt der Startseite die Seite „Software-Updates werden installiert“. Sie zeigt den Fortschritt, etwa „5 von 12 Paketen“. Meist dauert das wenige Minuten, bei einer neuen TrutzBox bis zu einer halben Stunde; spätestens nach 65 Minuten öffnet sich die Oberfläche von selbst. Ein Browserfenster, in dem die Oberfläche schon offen war, lädt die neue Version von selbst, sobald dabei nichts verloren geht, etwa wenn dort eine Minute lang niemand etwas tut. Bis dahin steht dort der Hinweis „Die Oberfläche der TrutzBox wurde aktualisiert.“ mit dem Knopf **Neu laden**.

Ein manuelles Einspielen gibt es bewusst nicht, und es fehlt Ihnen auch nichts: Es gibt schlicht nichts zu tun.

16.3 Filter- und Sperrlisten-Updates

Die Schutzwirkung der TrutzBox lebt von aktuellen Listen, denn Server für Werbung und für die Aufzeichnung dessen, was Menschen im Netz tun, wechseln ihre Adressen ständig. Drei Dinge pflegt Comidio zentral, und jede TrutzBox gleicht sich täglich damit ab:

- **Filterlisten für Webfilter und TrutzBrowse:** Comidio pflegt rund vierzig Listen zur Erkennung von Servern für Werbung und Aufzeichnung, Schadcode-Quellen und thematischen Sperrkategorien. Sie werden täglich aktualisiert und an alle TrutzBoxen verteilt (Kapitel „Filterlisten verwalten“).
- **Sperrliste kompromittierter TrutzMail-Adressen:** Wird eine TrutzMail-Adresse kompromittiert, etwa weil eine TrutzBox gestohlen wurde, führt Comidio sie zentral auf einer Sperrliste. Jede TrutzBox gleicht täglich ab und entfernt gespeicherte Schlüssel solcher Adressen, damit niemand über eine solche Adresse weiter vertrauenswürdig kommunizieren kann.
- **Empfänger-Zertifikate:** Auch die gespeicherten Zertifikate Ihrer Mail-Partner werden täglich gegen den zentralen Comidio-Server abgeglichen, damit ungültig gewordene zeitnah aussortiert werden. Übertragen werden dabei aus Datenschutzgründen nur Prüfsummen der Adressen, nicht die Adressen selbst.

Anders die IP-Blockliste der Firewall (Kapitel „Angriffsschutz: Firewall und Wächter“). Sie verteilt Comidio nicht, und nachts aktualisiert wird sie auch nicht. Ab Werk ist sie leer. Was darin steht, kommt von Ihrer TrutzBox selbst: Der Angriffsschutz trägt auffällige Adressen ein, Sie sperren Adressen von Hand (im Reiter Sperrlisten, im Monitor oder unter **Verwaltung → Eigene Sperren und Ausnahmen**, Kapitel „Eigene Sperren und Ausnahmen“), oder Sie spielen eine Adressliste als Datei ein. Eine solche Liste bleibt auf dem Stand der Datei; einen neueren Stand bringt nur eine neuere Datei, die Sie wieder einspielen. Freigaben, die Sie als Ausnahme angelegt haben, bleiben dabei bestehen.

16.4 Warum diese Updates sicher sind

Ein Update-Weg ist ein empfindlicher Punkt: Wer ihn übernimmt, könnte eigene Software auf die TrutzBox bringen. Deshalb ist er dreifach abgesichert.

- **Signatur:** Jedes Paket und jedes Image trägt eine kryptografische Signatur von Comidio. Passt sie nicht, wird nicht installiert. Manipulierte oder untergeschobene Pakete fallen damit auf.
- **Verschlüsselter Kanal:** Die Übertragung läuft verschlüsselt zum Comidio-Repository.
- **Gegenseitige Beglaubigung:** Nicht nur Ihre TrutzBox prüft den Server, auch der Server prüft Ihre TrutzBox. Ein fremder Server kann sich damit nicht als Comidio ausgeben.

Dazu kommt eine schlichte, aber wirksame Vorsichtsmaßnahme: Die TrutzBox stellt nach außen nur die Dienste bereit, die sie für ihren Betrieb wirklich braucht. Was nicht erreichbar ist, kann auch nicht angegriffen werden.

> **Sichere Voreinstellungen ab Werk**
>
> Automatische Software-Updates sind ab Werk eingeschaltet, die Prüfung läuft jede Nacht zwischen 3 und 6 Uhr und bei jedem Start, alle Update-Kanäle sind verschlüsselt und gegenseitig beglaubigt, und jedes Paket ist signiert. An diesen Voreinstellungen etwas zu ändern ist im Normalfall weder nötig noch ratsam.

16.5 Voraussetzung: ein gültiger Service-Vertrag

Die hier beschriebenen Update-Arten sind Leistungen des Service-Vertrags. Solange er läuft, erhält Ihre TrutzBox laufend Sicherheits- und Funktions-Updates, ohne zusätzliche Kosten und ohne Ihr Zutun.

Läuft der Vertrag aus, liefert Comidio keine neuen Pakete und keine neuen Listen mehr. Ihre TrutzBox hört deswegen nicht auf zu arbeiten: Sie filtert mit dem Stand weiter, den sie hat. Nur nutzt sich dieser Stand ab, weil neue Server für Werbung, Aufzeichnung und Angriffe in den alten Listen naturgemäß fehlen. Dienste, die einen gültigen Vertrag voraussetzen, darunter TrutzMail und TrutzRTC mit Chat und Videokonferenz, stehen ohne Verlängerung nicht mehr zur Verfügung. Ihre gesetzlichen Aktualisierungsansprüche als Verbraucher nach § 475b BGB bleiben davon unberührt; sie hängen nicht am Service-Vertrag. Wenden Sie sich dafür an den Support. Comidio empfiehlt, den Vertrag durchgehend zu verlängern.

16.6 Stand und Verlauf einsehen

Ob alles aktuell ist, sehen Sie an mehreren Stellen, je nachdem, wie genau Sie es wissen möchten:

- **Startseite:** der schnelle Blick, ob es etwas zu beachten gibt.
- **Betriebszustand, Karte Software-Updates:** Sie zeigt, wann die TrutzBox den Update-Server zuletzt erreicht und zuletzt Pakete eingespielt hat, wie der letzte Update-Lauf endete und wann der nächste ansteht. Bietet der Update-Server neuere Pakete an und hat die TrutzBox sie nach 7 Tagen nicht eingespielt, wird die Karte gelb, nach 14 Tagen rot; dasselbe gilt, wenn sie den Update-Server so lange nicht erreicht. Gezählt wird nur die Zeit, in der die TrutzBox eingeschaltet ist. Gelb wird die Karte auch, wenn ein Lauf abgebrochen ist. Eine Woche ohne neue Pakete ist dagegen normal. Mehr dazu mit Abbildung in Kapitel „Betriebszustand: die Karten im Einzelnen“.

- **Betriebszustand, Karte Filterlisten:** Sie nennt Stand und Installationszeitpunkt der Listen sowie die Zahl der veränderten Listen. Stehen neuere Listen länger als zwei Tage bereit, ohne installiert zu sein, färbt sich die Karte gelb und nennt die verfügbare Version und den Zeitpunkt, seit dem die TrutzBox zurückliegt. Gefiltert wird in dieser Zeit unverändert weiter.
- **Filterlisten-Verlauf:** über **Verlauf durchsuchen** auf derselben Karte. Er zeigt je Liste, wann sie aktualisiert wurde, wie viele Einträge sie enthält und was sich gegenüber dem vorherigen Stand geändert hat. Bei eigenen importierten Listen lässt sich zusätzlich die Überschneidung mit den vorhandenen Listen abrufen.
- **Vertrag und Pakete:** unter **Systemeinstellungen → Vertrag und Pakete** steht zu jedem von Comidio gepflegten Paket die installierte neben der aktuell verfügbaren Version.
- **Vollständige Paketliste:** unter **Systemeinstellungen → Rechtliche Hinweise** listet der Abschnitt **Anlage B - Paketliste** lückenlos alle Software-Bestandteile der TrutzBox auf, einschließlich der zugrunde liegenden Debian-Pakete. Das macht die Zusammensetzung der TrutzBox nachprüfbar, auch für eine externe Prüfung.
- **Verwaltung, Filterlisten:** an jeder einzelnen Liste steht dort das Datum der letzten Aktualisierung.

16.7 Der Ausnahmefall: ein komplettes Image

Ein Image-Update tauscht das gesamte Betriebssystem aus. Es gehört nicht zum täglichen Ablauf und kommt nur in drei Lagen zum Einsatz: wenn ein Versionssprung über die normalen Paket-Updates nicht sauber durchführbar ist, wenn das interne Speichermedium defekt war und getauscht wurde, oder wenn die TrutzBox nach einer schweren Störung anders nicht mehr in einen funktionsfähigen Zustand kommt.

Dafür gibt es zwei Wege. Der erste ist das **System zurücksetzen** aus der Oberfläche heraus: Alle Daten werden gelöscht, ein aktuelles Betriebssystem wird aus dem Internet geladen und dabei anhand einer Prüfsumme auf Unversehrtheit geprüft, danach durchlaufen Sie das Setup erneut mit Ihrer TrutzLegitimation. Zugänglich unter **Systemeinstellungen → Sichern und Wiederherstellen**, ausführlich beschrieben in Kapitel „System zurücksetzen (Werksreset)“. Der zweite ist der USB-Stick, den der folgende Abschnitt komplett beschreibt. Für beide gilt: Legen Sie vorher eine Sicherung an, sofern die TrutzBox das noch hergibt, sonst sind Postfächer und Schlüssel verloren (Kapitel „Sichern, Wiederherstellen und Zurücksetzen“).

Das System per USB-Stick neu aufspielen

Dieser Weg funktioniert auch dann noch, wenn die TrutzBox gar nicht mehr startet oder das Speichermedium getauscht wurde, denn er braucht weder die Oberfläche noch ein lauffähiges System auf der TrutzBox. Sie erstellen an einem PC einen Start-Stick mit dem kompletten TrutzBox-System und lassen die TrutzBox davon booten; der Stick schreibt das System dann selbsttätig auf das interne Speichermedium. Comidio nennt diesen Stick auch „Tank-Stick", weil die TrutzBox daraus betankt wird.

Sie brauchen dafür einen **USB-Stick mit 32 GB**, einen PC mit gutem Internet-Anschluss und etwa eine Stunde Zeit, das meiste davon Wartezeit. Auf dem Stick belegt das System gut 17 GB; ein Stick mit der Aufschrift 16 GB fasst weniger und ist deshalb zu klein. Ein Stick mit mehr als 32 GB schadet nicht, bringt aber keinen Vorteil, denn der übrige Platz bleibt leer.

Nehmen Sie dafür am besten einen gewöhnlichen USB-Speicherstick, gern auch einen älteren mit USB 2.0. Geräte, die als **USB-SSD** verkauft werden, funktionieren erst mit den Image-Dateien ab V79. Ältere Versionen erkennen sie nicht: Die TrutzBox startet zwar vom Stick, bleibt dann aber beim Suchen des Datenträgers stehen, sichtbar daran, dass LED 1 dauerhaft leuchtet und LED 2 blinkt.

Der Stick überschreibt jeden Rechner, der von ihm startet

Seit Image V80 betankt der Tank-Stick nicht nur die TrutzBox, sondern jeden Rechner mit gewöhnlicher PC-Hardware (x86) und jede virtuelle Maschine. Startet ein Rechner von diesem Stick, überschreibt der Stick dessen eingebaute Platte vollständig, ohne Rückfrage. Alles, was darauf war, ist danach weg.

Stecken Sie den Stick deshalb nur in die TrutzBox oder in den Rechner, der wirklich neu betankt werden soll. Ziehen Sie ihn nach dem Beschreiben gleich aus dem PC, damit er bei dessen nächstem Neustart nicht dort steckt, und beschriften Sie ihn. Nur auf der PC Engines APU1, einem älteren Modell mit dem Prozessor AMD G-T40E, bricht der Stick ab, ohne etwas zu verändern.

1. Laden Sie die aktuelle Image-Datei für den Tank-Stick auf Ihren PC herunter. Sie steht auf trutzbox.de unter Downloads im Abschnitt „TrutzBox-Images“: trutzbox.de/downloads. Dort finden Sie immer die aktuelle Version. Die Datei ist rund 1,5 GB groß.
2. Entpacken müssen Sie nichts: Das Schreibprogramm im nächsten Schritt liest die gepackte Datei unmittelbar. Wer sichergehen will, dass der Download unversehrt ist, lädt von derselben Seite die Prüfsumme (SHA256) dazu und vergleicht sie.
3. Installieren Sie das kostenlose Programm **balenaEtcher** (etcher.balena.io). Es überträgt Image-Dateien sicher auf USB-Sticks und läuft auf Windows, macOS und Linux.
4. Starten Sie Etcher, wählen Sie die heruntergeladene Image-Datei und Ihren USB-Stick aus und starten Sie das Schreiben. Achtung: Der Stick wird dabei vollständig überschrieben. **Hinweis für Windows:** Schreibt die aktuelle Etcher-Version unter Windows 10 nicht, nehmen Sie die ältere Version 1.18.11 (github.com/balena-io/etcher/releases/tag/v1.18.11). Fragt Windows nach dem Schreiben, ob der Stick formatiert werden soll, klicken Sie jedes Mal auf Abbrechen.
5. Trennen Sie die TrutzBox vom Strom und stecken Sie den fertigen Stick in eine USB-Buchse auf der Rückseite.
6. Schließen Sie den Strom wieder an. Die TrutzBox startet automatisch vom Stick und beginnt von selbst; einen Knopf müssen Sie nicht drücken. Ab jetzt heißt es warten und auf die drei LEDs an der Front achten.
7. Am Ende blinken alle drei LEDs gleichzeitig, und die TrutzBox piept dreimal; etwa 30 Sekunden später schaltet sie sich selbst ab.
8. Trennen Sie die TrutzBox vom Strom, ziehen Sie den Stick ab und schließen Sie den Strom wieder an. Die TrutzBox startet nun mit dem frischen System und meldet sich mit dem Setup (Kapitel „TrutzBox einrichten (Setup)“).

9. Durchlaufen Sie das Setup mit Ihrer TrutzLegitimation und spielen Sie im Schritt „TrutzBox registrieren" über „Backup laden" Ihre Sicherung ein, bevor Sie registrieren (Kapitel „Wiederherstellen: im Betrieb oder im Setup“).

Was die LEDs während des Vorgangs bedeuten:

Die drei Leuchtdioden	Was gerade passiert
	Die TrutzBox startet vom Stick.
	Der Stick wird gesucht.
	Das interne Speichermedium wird gesucht.
	Lauflicht von links nach rechts: Das System wird geschrieben. Auf aktueller Hardware dauert das etwa 5 bis 10 Minuten, auf älteren TrutzBoxen deutlich länger.
	Lauflicht von rechts nach links: Das Geschriebene wird geprüft, noch einmal etwa 5 bis 10 Minuten.
	Fertig, dazu drei Pieptöne. Die TrutzBox schaltet sich in etwa 30 Sekunden selbst ab.
	Außen und Mitte blinken im Wechsel, ein Piepton pro Minute: fehlgeschlagen. Strom trennen, Stick neu beschreiben und erneut versuchen; klappt es wieder nicht, hilft der Support.

- **Der Stick prüft, was er geschrieben hat:** Nach dem Schreiben vergleicht er das System auf dem internen Speichermedium anhand einer Prüfsumme mit dem Image. Stimmt sie nicht, meldet er einen Fehler.
- **Denken Sie an das Root-Zertifikat:** Nach dem Neuaufspielen erzeugt die TrutzBox beim Setup neue Zertifikate. Spielen Sie Ihre Sicherung ein, kehrt das bisherige Root-Zertifikat zurück, und auf den Geräten ist nichts zu tun. Richten Sie dagegen ohne Sicherung neu ein, löschen Sie auf allen Geräten das alte Zertifikat und installieren das neue (Kapitel „Nach einem Zurücksetzen der TrutzBox“).
- **Wenn die TrutzBox nicht vom Stick startet:** Das kommt praktisch nicht vor, denn der Stick hat beim Starten Vorrang vor dem internen Speichermedium. Startet die TrutzBox dennoch normal, sitzt der Stick nicht richtig oder wurde nicht korrekt beschrieben; wiederholen Sie das Schreiben mit Etcher. Führt auch das nicht weiter, übernimmt der Support.

Eigene Hardware und virtuelle Maschinen

Ab V80 spielt der Tank-Stick die TrutzBox-Software auch auf einen eigenen Rechner mit gewöhnlicher PC-Hardware (x86) oder in eine virtuelle Maschine. Die Platte muss mindestens 16 GB groß sein. Der Rechner muss im klassischen BIOS-Verfahren starten, nicht über UEFI; bei einer virtuellen Maschine stellen Sie das so ein. Die drei LEDs der TrutzBox fehlen dort. Das Ende erkennen Sie daran, dass sich der Rechner nach Schreiben und Prüfen selbst ausschaltet. Nehmen

Sie dann den Stick heraus, bei einer virtuellen Maschine die Stick-Datei, sonst betankt er beim nächsten Start von vorn.

Beim ersten Start dehnt die TrutzBox ihren Datenbereich bis zum Ende der Platte aus, sofern dahinter mindestens 256 MB frei sind; mehr als 2 TB nutzt sie dafür nicht. Dasselbe geschieht nach jedem Zurücksetzen und auf einer TrutzBox, deren SSD gegen eine größere getauscht und neu betankt wurde. Eine virtuelle Platte, die erst bei Bedarf wächst, belegt beim späteren Zurücksetzen ihre volle Größe, weil die TrutzBox dabei den freien Platz einmal überschreibt. Aus demselben Grund dauert das Zurücksetzen auf einer großen Platte deutlich länger (Kapitel „System zurücksetzen (Werksreset)“).

16.8 Ankündigungen, Fragen und Meldungen

Größere Neuerungen kündigt Comidio im TrutzBox-Forum unter forum.trutzbox.de im Bereich „TrutzBox-Updates" an und beschreibt dort auch, was ein Software-Update konkret verbessert. Wer die Entwicklung mitverfolgen möchte, schaut dort gelegentlich vorbei; nötig ist es nicht.

Umgekehrt nimmt Comidio auch Meldungen entgegen. Vermutete Schwachstellen, ungewöhnliches Verhalten oder allgemeine Sicherheitsfragen können Sie jederzeit an support@trutzbox.de senden oder im Forum ansprechen. Comidio bewertet die Meldung, entwickelt eine Korrektur und liefert sie über den normalen nächtlichen Weg an alle TrutzBoxen aus. Bei besonders kritischen Fällen geschieht das auch außerhalb des Tagesrhythmus.

Häufige Fragen zu Software-Updates

Startet die TrutzBox nach einem Software-Update neu?

Nein. Die TrutzBox spielt Software-Updates im laufenden Betrieb ein und startet dafür nie neu. Einzelne Dienste starten dabei kurz neu, was Sie im Alltag nicht bemerken.

Wann kommen Software-Updates?

Jede Nacht zu einer zufälligen Zeit zwischen 3 und 6 Uhr und zusätzlich bei jedem Start der TrutzBox. Scheitert ein Lauf, versucht es die TrutzBox insgesamt bis zu dreimal (Abschnitt „Software-Paket-Updates“).

Kann ich ein Software-Update selbst anstoßen oder verschieben?

Verschieben nicht, und das ist Absicht. Ein einheitlicher, automatischer Ablauf lässt keine TrutzBox mit veralteter Software zurück. Einen eigenen Knopf zum Anstoßen gibt es nicht, aber bei jedem Start sucht die TrutzBox von selbst nach Software-Updates. Sollte im Einzelfall etwas nachzuhelfen sein, leitet der Support Sie an.

Die Oberfläche zeigt „Software-Updates werden installiert“. Was tun?

Nichts, nur warten. Die TrutzBox spielt gerade Software-Updates ein, die Seite zeigt den Fortschritt. Meist dauert das wenige Minuten, bei einer neuen TrutzBox bis zu einer halben Stunde; spätestens nach 65 Minuten öffnet sich die Oberfläche von selbst. Trennen Sie die TrutzBox in dieser Zeit nicht vom Strom.

Oben steht „Die Oberfläche der TrutzBox wurde aktualisiert.“ Was heißt das?

Ein Software-Update hat die Oberfläche erneuert, Ihr Browserfenster zeigt aber noch die alte Version. Klicken Sie auf **Neu laden**. Meist lädt die Seite ohnehin von selbst neu, sobald dabei nichts verloren geht.

Nach einem Software-Update verhält sich etwas anders als vorher. Was tun?

Erst im Forum nachsehen, ob die Änderung dort beschrieben ist, dann im Betriebszustand die Karte **Software-Updates** ansehen: Sie zeigt, ob der letzte Lauf fertig wurde. Bleibt es unklar, hilft der Support weiter (Kapitel „… nach einem Software-Update etwas nicht mehr funktioniert“ und Kapitel „Support kontaktieren“).

17 Sichern, Wiederherstellen und Zurücksetzen

Auf Ihrer TrutzBox liegen Dinge, die es nur einmal gibt: die geheimen Schlüssel Ihrer TrutzMail-Konten und die zugehörigen versteckten Adressen. Geht die TrutzBox verloren oder wird sie zurückgesetzt, sind diese Schlüssel unwiederbringlich weg. Niemand hat eine Kopie davon, auch Comidio nicht, denn genau darauf beruht die Sicherheit des ganzen Verfahrens. Eine Sicherung ist deshalb keine Fleißaufgabe, sondern Pflicht. Sie finden alles unter **Systemeinstellungen → Sichern und Wiederherstellen**.

Auf derselben Seite sitzen zwei Funktionen, die man auseinanderhalten sollte: das **Speichern** und **Laden** der vollständigen Sicherung und, deutlich abgesetzt, das **System zurücksetzen** auf den Werkszustand. Das erste ist harmlos und sollte zur Routine gehören, das zweite löscht alles.

17.1 Was in der Sicherung steckt

Menüpfad: Systemeinstellungen → Sichern und Wiederherstellen

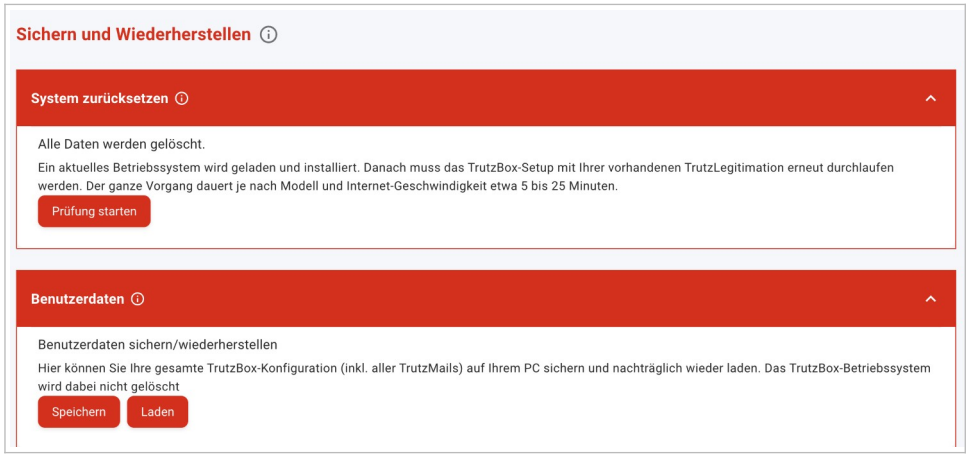


Abbildung 17-1: Die Seite Sichern und Wiederherstellen: oben „System zurücksetzen“ mit dem Knopf „Prüfung starten“, darunter „Benutzerdaten“ mit „Speichern“ und „Laden“. (© 2026 Comidio GmbH)

Die Sicherung fasst den kompletten Zustand Ihrer TrutzBox in einer einzigen, mit einer Passphrase verschlüsselten Datei zusammen. Weil die Datei verschlüsselt ist, können Sie sie gefahrlos auf Ihrem PC oder einem USB-Stick aufbewahren. Enthalten sind unter anderem:

- die allgemeinen Einstellungen der TrutzBox samt Netzwerkname, DNS-Anbieter und den Einstellungen des Angriffsschutzes,
- die Filtergruppen und Sicherheitsstufen,
- die eigenen Sperren und Ausnahmen samt der Schalter für die mitgelieferten Ausnahmen („Werbeblocker-Blocker erlauben“ und „App-Grundbausteine durchlassen“) sowie die IP-Sperrlisten,
- die Benutzer mit ihren Passwörtern und sämtliche TrutzMail-Konten samt ihrer persönlichen Schlüssel und der zugehörigen versteckten Adressen im Tor-Netzwerk,
- die TrutzChat-Daten mit Gesprächsverläufen und Gruppen,
- das Root-Zertifikat der TrutzBox, TrutzDynDNS samt Zertifikat und der Angabe, ob der Name nur IPv6 oder nur IPv4 trägt, sowie das Zertifikat eines eigenen Namens (Kapitel „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“),

- der Fernzugriff: die Zugänge für OpenVPN und für WireGuard und die Wahl, welcher der beiden Tunnel läuft (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“),
- die Schalter für die LED-Anzeige und die Töne, die Zeit-Steuerung des WLAN und der Haken „IPv6 für die TrutzBox anfordern“ am Anschluss LAN-Ext (Kapitel „TrutzBox-Netzwerk: Schutz und Verwaltung“),
- die SSH-Schlüssel der TrutzBox, an denen Programme für die Kommandozeile sie wiedererkennen (Abschnitt „Die Kommandozeile: Terminal und SSH“).

Nicht enthalten ist das Betriebssystem der TrutzBox. Das ist Absicht und ein Vorteil: Beim Einspielen einer Sicherung bleibt das System unangetastet, es werden nur Ihre Daten und Einstellungen zurückgeschrieben. Umgekehrt heißt das aber auch, dass eine Sicherung kein Ersatz für das Zurücksetzen ist, wenn die TrutzBox selbst nicht mehr sauber läuft.

Ebenfalls nicht in der Sicherung stehen:

- Name und Passwort des WLAN der TrutzBox. Nach einem Zurücksetzen oder auf neuer Hardware tragen Sie beide neu ein (Kapitel „Das WLAN der TrutzBox“).
- eine VLAN-Kennung am Anschluss LAN-Ext (Kapitel „Netzwerk-Übersicht: außen und innen“). Gebraucht wird sie nur, wenn die TrutzBox ohne Router direkt an der Leitung hängt. In der Oberfläche lässt sie sich nicht setzen; eingerichtet hat sie in diesem Fall der Support.
- das Systemprotokoll der TrutzBox.

> **Die Passphrase gut aufbewahren**
>
> Ohne die Passphrase lässt sich die Sicherungsdatei nicht mehr öffnen, auch nicht von Comidio. Notieren Sie sie an einem sicheren Ort, am besten getrennt von der Sicherungsdatei selbst.
>
> Eine Sicherung, deren Passphrase niemand mehr kennt, ist genauso wertlos wie gar keine. Ein Passwort-Manager oder ein verschlossener Umschlag beim Vereinsvorstand sind bewährte Aufbewahrungsorte.

17.2 Eine Sicherung anlegen

1. Öffnen Sie **Systemeinstellungen → Sichern und Wiederherstellen**.
2. Klicken Sie unter **Benutzerdaten** auf **Speichern**, vergeben Sie eine Passphrase und laden Sie die Datei auf Ihren PC herunter. Im Fenster „Benutzerdaten sichern“ heißt das Feld für die Passphrase „Passwort“.
3. Bewahren Sie die Datei außerhalb der TrutzBox auf, zum Beispiel auf einem USB-Stick im Schrank.
4. Notieren Sie sich Datum und Passphrase getrennt von der Datei.

Legen Sie eine Sicherung an, bevor Sie größere Änderungen vornehmen, und danach regelmäßig, etwa monatlich. Besonders wichtig sind zwei Zeitpunkte: unmittelbar nachdem Sie eine neue TrutzMail-Adresse eingerichtet haben, denn erst dann existiert deren Schlüssel, und bevor Sie irgendetwas Grundlegendes an der TrutzBox verändern. Bewahren Sie ruhig die letzten zwei oder drei Sicherungen auf, statt immer dieselbe Datei zu überschreiben.

Eine zweite, kleinere Sicherung nur für Teilbereiche, etwa allein für die Filter-Einstellungen, gibt es nicht. Wollen Sie an Filtergruppen, Ausnahmen oder Sperrlisten etwas ausprobieren und im Zweifel schnell zum vorherigen Stand zurückkehren, legen Sie vorher eine vollständige Sicherung an.

17.3 Wiederherstellen: im Betrieb oder im Setup

Eine Sicherung lässt sich auf zwei Wegen einspielen:

- **Im laufenden Betrieb:** über **Laden** auf derselben Seite. Die Dienste starten dabei kurz neu, das Betriebssystem bleibt unangetastet. Das ist der Weg, wenn die TrutzBox läuft und Sie nur auf einen früheren Stand zurück möchten.
- **Während des Setups:** im Schritt „TrutzBox registrieren" über die Schaltfläche **Backup laden**, bevor Sie registrieren (Kapitel „Schritt „TrutzBox registrieren" und Sicherung einspielen“). Genau dieser Weg ist gedacht, wenn Sie eine TrutzBox ersetzen oder nach einem Zurücksetzen wieder aufbauen: Die TrutzBox übernimmt den gesicherten Zustand, und **Zur Administration** führt anschließend direkt ins Admin-Panel. Das Setup ist damit beendet, die übrigen Schritte entfallen, weil die Sicherung sie bereits mitbringt.

Eine Sicherung, die sich nicht einspielen lässt, richtet keinen Schaden an. Ist das Passwort falsch, die Datei beschädigt oder ihre Datenbank nicht lesbar, bricht die TrutzBox ab, bevor sie etwas an ihren Einstellungen ändert, und nennt den Grund. Ihre bisherigen Einstellungen bleiben dann, wie sie sind.

Wiederherstellen auf neuer Hardware

Eine Sicherung lässt sich auch auf ausgetauschte Hardware einspielen, solange dieselbe **TrutzLegitimation** verwendet wird. Das ist der entscheidende Punkt: Ihre TrutzMail-Adressen hängen nicht am Gerät, sondern an der TrutzLegitimation. Richten Sie also die neue TrutzBox mit derselben TrutzKennung und demselben TrutzSchlüssel ein und spielen Sie im Setup Ihre Sicherung ein. Postfächer, Schlüssel und versteckte Adressen wandern damit unverändert mit; Ihre Kommunikationspartner merken vom Gerätewechsel nichts.

Auf den Geräten ist danach in der Regel nichts zu tun. Die Sicherung bringt das Root-Zertifikat der TrutzBox mit, ebenso die Zugänge für OpenVPN und WireGuard; die Zertifikate und VPN-Profile auf den Geräten gelten weiter. Prüfen Sie aber am Internet-Router, ob die Freigaben für Fernzugriff und Videokonferenz auf die Adresse der neuen TrutzBox zeigen. Nur wenn Sie ohne Sicherung neu einrichten, entsteht ein neues Root-Zertifikat; dann löschen Sie auf allen Geräten das alte und importieren das neue (Kapitel „Das Root-Zertifikat installieren“), sonst zeigen die Browser Warnungen an.

17.4 System zurücksetzen (Werksreset)

Das Zurücksetzen löscht alle Daten auf der TrutzBox und installiert das aktuelle Betriebssystem neu. Es ist das letzte Mittel bei Störungen, die sich anders nicht mehr beheben lassen, und der richtige Schritt vor einem Besitzerwechsel. Danach durchlaufen Sie das Setup erneut mit Ihrer TrutzLegitimation (Kapitel „TrutzBox einrichten (Setup)“). Die Seite nennt für den ganzen Vorgang „je nach Modell und Internet-Geschwindigkeit etwa 5 bis 25 Minuten“.

Mit einer größeren SSD oder in einer virtuellen Maschine dauert es deutlich länger, auf einer großen Platte auch Stunden. Der Grund: Ab Image V80 dehnt die TrutzBox ihren Datenbereich beim ersten Start auf die ganze Platte aus (Kapitel „Der Ausnahmefall: ein komplettes Image“), und beim Zurücksetzen überschreibt sie den freien Platz dieses Bereichs einmal, damit von den alten Daten nichts lesbar bleibt. Je größer die Platte, desto länger dauert das. Auf einer SSD mit 16 GB fällt es kaum ins Gewicht. Hat die TrutzBox noch nie mit Image V80 oder neuer gestartet, ist ihr Datenbereich noch klein, und das erste Zurücksetzen ist entsprechend schnell fertig; erst danach wächst der Datenbereich.

Ausgeführt wird das Zurücksetzen von einem kleinen Wartungssystem. Es liegt auf der Rettungspartition, einem eigenen, kleinen Bereich auf dem Speichermedium, den der Vorgang selbst nicht anrührt. Gestartet wird es über den Bootloader, das kleine Startprogramm, das beim Einschalten festlegt, welches System startet; dafür trägt der Bootloader einen eigenen Rettungs-Eintrag.

Der Ablauf Schritt für Schritt

1. Legen Sie zuerst eine vollständige Sicherung an und laden Sie sie auf Ihren PC (Abschnitt „Eine Sicherung anlegen“). Ohne sie sind Postfächer und Schlüssel verloren.
2. Öffnen Sie **Systemeinstellungen → Sichern und Wiederherstellen** und klicken Sie im Bereich zum Zurücksetzen auf **Prüfung starten**.
3. Die TrutzBox prüft nun sieben Voraussetzungen der Reihe nach: die Internetverbindung, das Betriebssystem-Image auf dem Update-Server, das Vorhandensein der Rettungspartition, deren Startfähigkeit und Vollständigkeit, die Konfiguration des Bootloaders, den Rettungs-Eintrag darin und zuletzt, ob das angebotene Image überhaupt auf den Systembereich Ihrer TrutzBox passt. Erst wenn alle sieben Punkte erfüllt sind, lässt sich das Zurücksetzen überhaupt auslösen.
4. Werfen Sie dabei einen Blick auf die Zeile zum Betriebssystem-Image. Sie nennt, was der Update-Server für genau Ihre TrutzBox bereithält: Version und Bau-Nummer, die entpackte Größe und die enthaltenen Betriebssystem-Kerne, etwa *Gefunden: TrutzBox 2.5.0 Build V80.amd, 6,0 GiB*. So sehen Sie vor dem Auslösen, auf welchen Stand die TrutzBox zurückkehren wird.
5. Bestätigen Sie den Vorgang. Ab jetzt läuft alles selbsttätig durch. Lassen Sie das Browserfenster offen: Es zeigt die vergangene Zeit, sucht die TrutzBox alle fünf Sekunden unter ihrem Namen und unter ihren bisherigen Adressen und öffnet von selbst das Setup, sobald sie wieder antwortet. Meldet sie sich binnen 45 Minuten nicht, nennt die Seite stattdessen die Adresse zum Eintippen und bietet **Erneut suchen** an. Auf einer großen Platte ist das kein Fehler: Solange zwei LEDs leuchten und die dritte blinkt, arbeitet die TrutzBox noch (Tabelle unten). Trennen Sie die TrutzBox in dieser Zeit keinesfalls vom Strom.
6. Am Ende meldet sich die TrutzBox von selbst wieder zurück, und zwar unter ihrem Auslieferungsnamen `trutzbox`. Hatten Sie ihr einen anderen Netzwerknamen gegeben, ist der damit weg; eine Sicherung bringt ihn zurück. Das Setup liegt unter `http://trutzbox/setup/`, an einer FRITZ!Box auch unter `http://trutzbox.fritz.box/setup/`. Kennt Ihr Router den Namen nicht oder hat er sich noch die alte Adresse gemerkt, führt `http://trutzbox.local/setup/` zum Ziel

(Kapitel „Das Setup im Browser öffnen“). Durchlaufen Sie dann das Setup mit Ihrer TrutzLegitimation und spielen Sie im Schritt „TrutzBox registrieren" über „Backup laden" Ihre Sicherung ein, bevor Sie registrieren.

Ein Sonderfall betrifft nur den Sprung am Ende: Haben Sie die Verwaltung über eine `https`-Adresse geöffnet, öffnet die Seite das Setup nicht von selbst. Ein Browser darf aus einer verschlüsselten Seite heraus keine unverschlüsselte Adresse abfragen. Rufen Sie das Setup in diesem Fall von Hand auf; die Adresse steht auf der Warteseite.

Wenn Sie das Admin-Panel nicht mehr erreichen

Der Weg über die Oberfläche ist der bequemste, aber nicht der einzige. Die TrutzBox lässt sich auch dann zurücksetzen, wenn Sie sich nicht mehr anmelden können.

- **Taste am Gehäuse in den ersten 2 Minuten:** Gemeint ist bei der TrutzBox AMD die Taste an der Gerätefront, bei der TrutzBox ARM die Taste „reset“ neben der Strombuchse. Schalten Sie die TrutzBox ein. Sie startet ganz normal und wartet nicht auf die Taste. Halten Sie innerhalb der ersten 2 Minuten nach dem Einschalten die Taste 3 Sekunden lang gedrückt. Solange Sie drücken, blinken die drei grünen LEDs gemeinsam. Nach 3 Sekunden leuchten sie dauerhaft: Lassen Sie jetzt los. Erst das Loslassen löst das Zurücksetzen aus. Vom Loslassen bis zum Neustart in das Wartungssystem leuchten die drei LEDs weiter dauerhaft. In dieser Zeit wartet die TrutzBox auf ihre Internetverbindung und führt dieselbe Prüfung durch wie in der Oberfläche. Fällt sie durch, etwa weil kein Netzwerk anliegt, blitzen die drei LEDs fünfmal gemeinsam auf, und die TrutzBox arbeitet normal weiter.
- **Wann die Taste wirkt:** Lassen Sie vor Ablauf der 3 Sekunden los, geschieht nichts, und die LEDs zeigen wieder ihre gewohnte Anzeige. Innerhalb der 2 Minuten können Sie es dann noch einmal versuchen. Bleibt die Taste nach dem dauerhaften Leuchten länger als 30 Sekunden gedrückt, etwa weil sie klemmt, löst sie ebenfalls nichts aus. Nach den 2 Minuten bewirkt die Taste nichts mehr. Halten Sie die Taste schon beim Einschalten, beginnt das Blinken erst, sobald die TrutzBox die Taste liest: bei der TrutzBox AMD etwa 40 Sekunden nach dem Einschalten, bei der TrutzBox ARM nach etwa 10 Sekunden.
- **Startmenü der TrutzBox:** Beim Einschalten zeigt die TrutzBox für wenige Sekunden ein Auswahlmenü, in dem sich das Wartungssystem starten lässt. Dieser Weg ist für den Support gedacht: Es gibt dort weder eine Rückfrage noch eine Prüfung, das Zurücksetzen läuft sofort an.

Was die LEDs bei der Taste anzeigen

Bei der TrutzBox AMD sind es die drei grünen LEDs an der Front, bei der TrutzBox ARM die drei grünen LEDs WAN, LAN und WLAN (von links nach rechts). In den Bildern steht ein grauer Kreis für eine dunkle LED, ein grüner für eine leuchtende und ein grüner mit gestricheltem Ring für eine blinkende.

Die drei Leuchtdioden	Was gerade passiert
	Die Taste ist gedrückt. Alle drei LEDs blinken gemeinsam, zweimal je Sekunde. Halten Sie die Taste weiter.
	Nach 3 Sekunden leuchten alle drei dauerhaft: Lassen Sie jetzt los. Nach dem Loslassen bleibt die Anzeige so, bis die TrutzBox in das Wartungssystem neu startet. Für Netz und Prüfung hat sie bis zu 3 Minuten Zeit.
	Alle drei blitzen fünfmal schnell auf, danach zeigen sie wieder die gewohnte Anzeige: Die Prüfung ist nicht bestanden, etwa weil kein Netzwerk anliegt. Es wird nichts zurückgesetzt, die TrutzBox arbeitet normal weiter.

Was die LEDs währenddessen anzeigen

Sobald die TrutzBox neu gestartet ist, zeigen die drei grünen LEDs an der Front, wie weit der Vorgang ist. Erledigte Schritte leuchten dauerhaft, der gerade laufende Schritt blinkt. Bei der TrutzBox ARM übernehmen die grünen LEDs WAN, LAN und WLAN die Rolle der linken, mittleren und rechten LED.

Die drei Leuchtdioden	Was gerade passiert
	Die TrutzBox wartet auf Netzwerk und Namensauflösung und holt die Beschreibungsdatei vom Update-Server. Das dauert nur wenige Sekunden.
	Das Image wird geladen, auf die Systempartition geschrieben und die Prüfsumme kontrolliert. Das dauert etwa vier Minuten.
	Nacharbeit: Der Startbereich wird erneuert, das Datenverzeichnis auf den Werkszustand gebracht und sein freier Platz überschrieben. Auf einer SSD mit 16 GB dauert das knapp eine Minute, auf einer größeren Platte entsprechend länger, bei einer großen auch Stunden.
	Alles ist geschrieben. Die Anzeige bleibt zehn Sekunden stehen, dann startet die TrutzBox neu.

Bleibt das Wartungssystem bei dauerhaftem Blinken stehen, ist ein Fehler aufgetreten. Welcher, sagt das Muster. „Schnell" heißt etwa fünf Takte je Sekunde, „mittel" gut zwei.

Die drei Leuchtdioden	Takt	Fehler	Mögliche Ursache
● ○ ○	schnell	Netzwerk	Kein Kabel, kein DHCP, keine Namensauflösung
● ● ○	schnell	Beschreibungsdatei	Server erreichbar, Datei fehlt oder ist unlesbar
○ ● ○	mittel	Server	Update-Server antwortet nicht
○ ● ●	schnell	Download	Image ließ sich nicht laden
● ○ ●	mittel	Prüfsumme	Image beschädigt oder unvollständig
○ ○ ●	mittel	Schreiben	Schreiben auf die Systempartition fehlgeschlagen
● ● ●	schnell	Werksreinigung	Datenverzeichnis ließ sich nicht bereinigen
● ● ●	schnell	Gerät	System- oder Datenpartition nicht gefunden
● ● ●	mittel	Bootloader	Bootloader ließ sich nicht umstellen

In jedem dieser Fälle gilt dasselbe: TrutzBox kurz vom Strom trennen und den Vorgang wiederholen. Bleibt es beim selben Muster, gehört es in die Meldung an den Support (Kapitel „Support kontaktieren“).

Ältere TrutzBoxen zeigen im Wartungssystem noch keine Anzeige. Dort bleiben die LEDs während des Vorgangs einfach so, wie sie beim Neustart waren; die TrutzBox arbeitet trotzdem.

Nach dem Neustart in das frische System gilt wieder die gewohnte Anzeige beim Einschalten. Sie steht im folgenden Abschnitt.

Die LEDs vom Einschalten bis zum Setup

Die beiden Tabellen zeigen, was die LEDs nach jedem Einschalten der Reihe nach anzeigen, bis das Setup oder die Verwaltung erreichbar ist. Die Zeiten sind ungefähre Werte. Beim allerersten Start und nach Software-Updates dauern die letzten Schritte länger. Hat jemand die Herzschlag-Leuchte abgeschaltet (Kapitel „Die LEDs an der TrutzBox“), bleibt die Betriebs-LED auch beim Start dunkel.

TrutzBox AMD: drei grüne LEDs an der Front. Die linke zeigt den Start.

Nach dem Einschalten	Die drei Leuchtdioden	Was gerade passiert
sofort		Die linke LED leuchtet dauerhaft. Die TrutzBox startet ihre Hardware.
nach einigen Sekunden		Alle drei LEDs sind für einen Moment dunkel. Das Betriebssystem übernimmt jetzt die LEDs. Das ist kein Fehler.
danach		Die linke LED leuchtet wieder dauerhaft. Das Betriebssystem startet. Ab etwa 40 Sekunden nach dem Einschalten liest die TrutzBox die Taste an der Front. Bis 2 Minuten nach dem Einschalten löst sie dort das Zurücksetzen aus (Tabelle oben).
etwa 1 bis 2 Minuten		Die linke LED blinkt langsam und gleichmäßig. Das Betriebssystem läuft, die Bedienoberfläche startet noch.
etwa 2 bis 3 Minuten		Die linke LED blinkt schnell im Herzschlag-Rhythmus. Die Bedienoberfläche antwortet: Das Setup unter http://trutzbox/setup/ oder die Verwaltung ist erreichbar.

TrutzBox ARM: eine rote LED für den Betrieb und drei grüne LEDs WAN, LAN und WLAN. Die rote LED zeigt den Start wie die linke LED der TrutzBox AMD. Jede grüne LED zeigt die Auslastung des Anschlusses, neben dem sie auf dem Gehäuse steht: dunkel ohne Verbindung, ein seltenes kurzes Aufblitzen in Ruhe, schnelleres Blinken bei mehr Datenverkehr. Im Bild steht die rote LED links.

Nach dem Einschalten	Rote LED, WAN, LAN, WLAN	Was gerade passiert
sofort		Die rote LED geht an, kurz kann sie auch schon blinken. Die grünen LEDs sind dunkel. Die TrutzBox lädt ihr Betriebssystem.
nach wenigen Sekunden		Die rote LED leuchtet dauerhaft. Das Betriebssystem startet. Ab etwa 10 Sekunden nach dem Einschalten liest die TrutzBox die Taste „reset“. Bis 2 Minuten nach dem Einschalten löst sie dort das Zurücksetzen aus (Tabelle oben).
etwa 1 bis 2 Minuten		Die rote LED blinkt langsam und gleichmäßig. Das Betriebssystem läuft, die Bedienoberfläche startet noch. Die grünen LEDs zeigen jetzt ihre Anschlüsse; eine LED ohne Kabel oder ohne verbundenes Gerät bleibt dunkel.
etwa 2 bis 3 Minuten		Die rote LED blinkt schnell im Herzschlag-Rhythmus. Die Bedienoberfläche antwortet: Das Setup unter http://trutzbox/setup/ oder die Verwaltung ist erreichbar.

Was dabei passiert, ist keine oberflächliche Aufräumaktion: Alle Einstellungen und Daten werden gelöscht, auch noch gespeicherte E-Mails. Anschließend wird eine vollständige Kopie der TrutzBox-Software im Auslieferungsstand über den aktiven Bereich gelegt. Das braucht seine Zeit, weshalb Geduld an dieser Stelle die richtige Haltung ist.

Was das Zurücksetzen wirklich überschreibt

Der Systembereich der TrutzBox wird vollständig mit dem frischen Image überschrieben, der Startbereich erneuert, das Datenverzeichnis geleert und sein freier Platz anschließend überschrieben. 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 und neue Schlüssel für den Fernzugang, die TrutzBox heißt wieder `trutzbox`, und das Admin-Passwort vergeben Sie im Setup neu. Spielen Sie im Setup Ihre Sicherung ein, kehren das bisherige Root-Zertifikat, die VPN-Zugänge und der Netzwerkname zurück. Die Rettungspartition bleibt bestehen; auf ihr liegt nichts Persönliches.

Bei hohem Schutzbedarf bleibt eine Einschränkung: Das Überschreiben des freien Platzes ist kein zertifiziertes Löschverfahren. Ein Flash-Speicher verteilt Schreibzugriffe intern, weshalb Reste auf ausgetauschten Blöcken liegen bleiben können. Prüfen Sie deshalb vor einer Weitergabe, wie schutzbedürftig die zuletzt gespeicherten Daten waren. Bei alltäglichen Beständen ist das Zurücksetzen der richtige Weg; bei besonders schutzbedürftigen Daten tauschen Sie besser das Speichermedium (Kapitel „Das Speichermedium tauschen“) oder löschen es mit dem eingebauten Löschbefehl des Laufwerks und spielen danach ein frisches Image auf (Kapitel „Der Ausnahmefall: ein komplettes Image“).

Ihre TrutzMail-Adressen bleiben Ihnen erhalten

Beim Zurücksetzen werden auch alle Benutzer und deren TrutzMail-Adressen auf der TrutzBox gelöscht. Freigegeben werden die Adressen dadurch aber nicht: Die zentrale Verwaltung bei Comidio lässt eine erneute Einrichtung nur zu, wenn sie von einer TrutzBox mit derselben TrutzLegitimation angefordert wird.

So kann niemand eine fremde Adresse übernehmen und sich als jemand anderes ausgeben. In der Benutzerliste erscheinen Ihre früheren Adressen farblich abgesetzt und kehren über **Reaktivieren** zurück (Kapitel „Benutzer, Postfächer, Passwörter“).

17.5 Checkliste vor und nach dem Zurücksetzen

Ein Zurücksetzen läuft entspannter ab, wenn ein paar Dinge vorher erledigt sind. Die folgende Liste hat sich bewährt.

Vorher

- Vollständige Sicherung angelegt, auf den PC geladen und die Passphrase getrennt notiert.
- Die TrutzLegitimation (TrutzKennung und TrutzSchlüssel) griffbereit; ohne sie lässt sich die TrutzBox nicht wieder in Betrieb nehmen.

- Geprüft, dass die Service-Laufzeit Ihrer TrutzKennung noch läuft: unter **Systemeinstellungen → Vertrag und Pakete**, Zeile „Service-Vertrag gültig bis“. Ist sie abgelaufen, kann das Setup nach dem Zurücksetzen keine TrutzMail-Adresse anlegen und kommt über den Schritt „TrutzMail einrichten“ nicht hinaus (Kapitel „Schritt „TrutzMail einrichten"“). Verlängern Sie deshalb vorher.
- Name und Passwort des WLAN der TrutzBox notiert, falls Sie es nutzen; die Sicherung enthält beide nicht.
- Notiert, welche Portweiterleitungen am Internet-Router für VPN und Videokonferenz eingerichtet sind, damit Sie sie hinterher wiedererkennen.
- Mitbenutzer informiert: Während des Vorgangs sind Mail, Chat und der gefilterte Internet-Zugang nicht verfügbar.
- Für eine stabile Verbindung gesorgt: Die TrutzBox lädt das Betriebssystem aus dem Internet nach.

Nachher

- Setup mit der TrutzLegitimation durchlaufen und die Sicherung im Schritt „TrutzBox registrieren" vor dem Registrieren eingespielt.
- Nur wenn Sie ohne anschließende Wiederherstellung neu aufgesetzt haben: auf allen Geräten das alte Root-Zertifikat der TrutzBox gelöscht und das neue importiert (Kapitel „Das Root-Zertifikat installieren“). Ohne diesen Schritt warnen die Browser. Haben Sie eine Sicherung eingespielt, kehrt das bisherige Root-Zertifikat mit zurück und bleibt gültig; auf den Geräten ist dann nichts zu tun.
- Geprüft, ob alle TrutzMail-Adressen wieder da sind; fehlende über **Reaktivieren** zurückholen (Kapitel „Benutzer, Postfächer, Passwörter“).
- Fernzugriff geprüft: Mit der Sicherung kehren die Zugänge für OpenVPN und WireGuard zurück, ebenso die Wahl des Tunnels; die VPN-Profile auf den Geräten gelten weiter. Ohne Sicherung legen Sie die Zugänge neu an (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).
- Das WLAN der TrutzBox unter **Netzwerk → WLAN** mit dem bisherigen Namen und Passwort neu eingerichtet (Kapitel „Das WLAN der TrutzBox“). Dann finden die Geräte es von selbst wieder.
- Nur wenn die TrutzBox ohne Router direkt an der Leitung hängt und der Support dafür eine VLAN-Kennung an LAN-Ext eingerichtet hat: diese vom Support neu setzen lassen. Die Sicherung bringt sie nicht mit.
- Eine Testmail an die eigene Adresse geschickt und den Chat kurz geöffnet.
- Sofort eine frische Sicherung des neuen Zustands angelegt.

17.6 Die TrutzBox weitergeben

Wird die TrutzBox verkauft, verschenkt oder ersetzt, gehört danach das Gerät jemand anderem, Ihre Postfächer, Schlüssel und Verläufe aber nicht. Diese Reihenfolge hat sich bewährt.

- Zuerst eine vollständige Sicherung anlegen und auf den eigenen Rechner laden (Abschnitt „Eine Sicherung anlegen“). Sie enthält Ihre TrutzMail-Konten mit ihren Schlüsseln. Ohne sie sind diese Schlüssel nach dem Zurücksetzen weg, auch Comidio hat keine Kopie.
- Dann die TrutzBox auf den Werkszustand zurücksetzen (Abschnitt „System zurücksetzen (Werksreset)“). Das löscht Einstellungen, Benutzer, E-Mails, Chat-Verläufe, Gerätenamen und das WLAN-Passwort.
- Die TrutzLegitimation behalten und keinesfalls mitgeben, weder das mitgelieferte Blatt noch eine Abschrift. Wer sie hat, kann Ihre TrutzMail-Adressen auf einer anderen TrutzBox neu anlegen und damit Ihre Mail-Identität annehmen. Der neue Besitzer braucht eine eigene TrutzLegitimation von Comidio.
- Auch die Sicherungsdatei und ihre Passphrase bleiben bei Ihnen. Beides zusammen öffnet Ihre Postfächer unabhängig vom Gerät.
- Die Registrierung bei Comidio klären. Die TrutzBox hängt an Ihrer TrutzLegitimation und an Ihrem Konto dort; hinterlegt sind Ihr Name unter mytrutzbox.de und Ihre TrutzMail-Adressen. Der neue Besitzer braucht eine eigene Registrierung, sonst kommt er im Setup nicht durch.
- Auf Ihren eigenen Geräten das Root-Zertifikat dieser TrutzBox entfernen, in Firefox und Thunderbird zusätzlich in deren eigenem Zertifikatsspeicher (Kapitel „Das Root-Zertifikat installieren“). Ebenso die VPN-Profile und die Mail-Konten löschen, die auf diese TrutzBox zeigen.
- Am Internet-Router die Freigaben zurücknehmen, die Sie für diese TrutzBox eingerichtet haben, vor allem die für TrutzVPN und die für die Videokonferenz.
- Ausgegebene Links auf Ihren bisherigen Internet-Namen, etwa Einladungen zu Videokonferenzen, als erledigt betrachten. Nach dem Zurücksetzen führen sie ins Leere.
- Die zurückgesetzte TrutzBox nicht noch einmal selbst einrichten, sondern ausgeschaltet weitergeben. Das Setup gehört dem neuen Besitzer, der es mit seiner eigenen TrutzLegitimation durchläuft.

Ihre TrutzMail-Adressen gehen dabei nicht mit über. Sie bleiben für Ihre TrutzLegitimation reserviert und lassen sich damit auf einer neuen TrutzBox wieder anlegen (Kapitel „Benutzer, Postfächer, Passwörter“). Vor der Entsorgung gilt dieselbe Reihenfolge, nur ohne die letzten beiden Punkte.

Häufige Fragen zum Sichern

Wie oft sollte ich sichern?

Als Faustregel: nach jeder Änderung, die Sie ungern wiederholen würden. Also nach dem Anlegen neuer Benutzer, nach größeren Änderungen an Filtergruppen und in jedem Fall vor einem Zurücksetzen. Wer regelmäßig TrutzMail nutzt, fährt mit einer monatlichen Sicherung gut.

Wo bewahre ich die Sicherungsdatei am besten auf?

Nicht auf der TrutzBox, denn genau die könnte ja ausfallen. Ein Ordner auf dem PC, zusätzlich eine Kopie auf einem USB-Stick oder einer externen Festplatte. Die Datei ist verschlüsselt; ohne

Passphrase kann niemand etwas damit anfangen. Notieren Sie die Passphrase deshalb getrennt von der Datei.

Ich habe die Passphrase vergessen. Kann Comidio helfen?

Nein. Die Passphrase wird nirgends hinterlegt, auch nicht bei Comidio. Eine Sicherung ohne ihre Passphrase ist unbrauchbar. Legen Sie in diesem Fall eine neue Sicherung an, solange die TrutzBox noch läuft, und notieren Sie die Passphrase diesmal sicher.

Passt eine Sicherung auch auf eine andere TrutzBox?

Ja, solange dieselbe TrutzLegitimation verwendet wird. Genau das ist der Weg beim Gerätetausch (Abschnitt „Wiederherstellen: im Betrieb oder im Setup“). Auf einer TrutzBox mit fremder TrutzLegitimation lässt sich die Sicherung dagegen nicht einspielen.

Sind meine E-Mails in der Sicherung enthalten?

Ja, Postfächer und Schlüssel gehören dazu; was genau enthalten ist, steht in Abschnitt „Was in der Sicherung steckt“. Deshalb kann die Datei je nach Postfachgröße auch mehrere hundert Megabyte groß werden.

18 Experten-Zugänge: Webmin, Terminal und SSH

Für den Alltag brauchen Sie die Verwaltungsoberfläche und sonst nichts. Für den Notfall und für erfahrene Administratoren gibt es zwei weitere Wege auf die TrutzBox: die technische Oberfläche Webmin und die Kommandozeile. Beide laufen getrennt von der Verwaltungsoberfläche und helfen deshalb gerade dann, wenn diese einmal nicht lädt. Am besten nutzen Sie sie nur nach Anleitung des Supports.

18.1 Webmin: der Experten-Zugang

Hinter **Systemeinstellungen → Webmin** verbirgt sich eine zweite, technische Verwaltungsoberfläche mit direktem Zugriff auf das Betriebssystem der TrutzBox, erreichbar auch direkt unter `http://trutzbox:10000`. Weil es sich um ein eigenständiges Programm handelt, verlangt Webmin eine eigene Anmeldung. Nach der Anmeldung zeigt Webmin zunächst eine Übersicht der Systeminformationen.

Webmin ist nur aus dem eigenen Netz erreichbar: aus dem Netz der TrutzBox, über TrutzVPN und aus dem lokalen Netz des Routers, dort nur von Geräten mit privater Adresse. Aus dem Internet ist es nicht erreichbar, auch nicht, wenn jemand am Router den Port 10000 freigibt.

Für den normalen Betrieb brauchen Sie Webmin nie. Wertvoll ist es im Notfall, und zwar aus einem bestimmten Grund: Webmin bringt seinen eigenen Web-Server mit und läuft unabhängig von der übrigen TrutzBox-Software. Wenn die gewohnte Oberfläche einmal klemmt, stehen die Chancen deshalb gut, dass Webmin noch antwortet. Der Support kann Sie dort gezielt anleiten, etwa um den Systemstatus als Datei auf Ihren PC zu laden und zur Analyse einzuschicken. Die Menübereiche gliedern sich nach Aufgaben: Webmin selbst, System, TrutzMail, TrutzBase für Firewall und Netzwerk sowie TrutzBrowse.

> **Nur mit Anleitung benutzen**
>
> Webmin richtet sich an erfahrene Linux-Administratoren. Eine Fehlkonfiguration kann die TrutzBox so verstellen, dass nur das Zurücksetzen auf Werkseinstellungen bleibt, mit Datenverlust. Ohne konkreten Anlass und am besten nur nach Anleitung des Supports verwenden.
>
> Das gilt besonders für das Einspielen von Software-Paketen von Hand. Software-Updates kommen ohnehin automatisch (Kapitel „Updates“); ein manueller Eingriff sollte immer mit dem Support abgesprochen sein.

18.2 Die Kommandozeile: Terminal und SSH

Auf der Kommandozeile geben Sie Befehle direkt an das Betriebssystem der TrutzBox, mit vollen Rechten. Im Alltag brauchen Sie sie nie. Wertvoll ist sie im Notfall: Der Support nennt Ihnen einen Befehl, Sie fügen ihn ein, und die TrutzBox führt ihn aus. Dorthin führen zwei Wege, das Terminal im Browser und, für erfahrene Administratoren, SSH. Beide fragen das Admin-Passwort ab.

Das Terminal im Browser

Unter **Systemeinstellungen → Terminal** öffnet sich ein eigenes Fenster. Es fragt zuerst das Admin-Passwort ab, danach arbeiten Sie sofort mit vollen Rechten. Ein eigenes Programm brauchen Sie dafür nicht.

Das Terminal läuft getrennt von der übrigen Verwaltungsoberfläche. Lädt diese einmal nicht, öffnen Sie es direkt unter `https://trutzbox/terminal/`. Erreichbar ist es von denselben Stellen wie die Verwaltungsoberfläche: aus dem Netz der TrutzBox, aus dem lokalen Netz des Internet-Routers und über TrutzVPN, nicht aus dem Internet.

- Bis zu vier Terminals laufen gleichzeitig, jedes in einem eigenen Fenster und jedes mit eigener Abfrage des Admin-Passworts.
- Ein Terminal endet, wenn Sie das Fenster schließen, wenn Sie `exit` eingeben oder nach zwei Stunden ohne Eingabe und ohne neue Ausgabe. Ein Befehl, der dann noch läuft, wird abgebrochen.
- Ab dem sechsten falschen Passwort folgt eine Wartezeit: erst 30 Sekunden, bei weiteren Fehlversuchen fünf und schließlich 30 Minuten.
- Markierten Text kopieren Sie mit Strg+Umschalt+C.

Anmeldung über SSH

Wer ein Programm für SSH benutzt, erreicht dieselbe Kommandozeile auch mit dem Verfahren SSH.

Mit einem Passwort meldet sich dort nur der Benutzer **admin** an, mit demselben Admin-Passwort wie an der Verwaltungsoberfläche, zum Beispiel mit `ssh admin@trutzbox`. Volle Rechte gibt danach das Kommando `sudo -i`. Das Konto root nimmt über SSH kein Passwort an.

Der Angriffsschutz bewacht auch diese Anmeldung: Nach fünf Fehlversuchen innerhalb von 30 Minuten sperrt er die Adresse für eine Stunde, bei Wiederholung immer länger, höchstens eine Woche (Kapitel „Angriffsschutz: Firewall und Wächter“). Von unterwegs führt der Weg zur Kommandozeile über TrutzVPN (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Eine Freigabe für Port 22 am Internet-Router ist nicht nötig und nicht zu empfehlen. Ihr Admin-Passwort schützt auch diesen Zugang, wählen Sie es entsprechend gut.

> **Befehle mit vollen Rechten**
>
> Auf der Kommandozeile gibt es keine Rückfrage und keinen Schutz vor Fehlern, im Terminal ebenso wie über SSH. Ein falscher Befehl kann die TrutzBox so verstellen, dass nur das Zurücksetzen auf Werkseinstellungen bleibt. Geben Sie dort nur Befehle ein, die Sie verstehen oder die der Support Ihnen genannt hat.

19 Was tun, wenn …?

Dieses Kapitel ist nach Symptomen sortiert: Suchen Sie das, was Sie beobachten, und arbeiten Sie die Schritte der Reihe nach ab. In fast allen Fällen hilft schon der erste oder zweite. Zu jedem Symptom steht vorweg, woran es normalerweise liegt, denn wer die Ursache kennt, kommt schneller ans Ziel als jemand, der nur einer Liste folgt.

Immer zuerst: der Betriebszustand

Bevor Sie irgendwo anders suchen, öffnen Sie **Systemeinstellungen → Betriebszustand**. Ist die Ampel grün, liegt die Ursache mit hoher Wahrscheinlichkeit nicht an der TrutzBox selbst. Ist sie gelb oder rot, nennt die betroffene Karte Ursache und Empfehlung im Klartext.

Die Karten kennen vier Zustände: grün für „In Ordnung", gelb für „Auffällig", rot für „Kritisch" und grau. Grau steht für „Ausgeschaltet", also für Funktionen, die Sie selbst abgeschaltet haben, und für „Vom Speicher-Wächter angehalten", also für Dienste, die der Speicher-Wächter gerade angehalten hat (Abschnitt „… die TrutzBox überhaupt nicht mehr reagiert“). Eine graue Karte zieht die Ampel nie auf Gelb oder Rot.

19.1 Die Übersicht: welches Symptom, welcher Abschnitt

Das beobachten Sie	Abschnitt
Gar kein Internet, an einem Gerät oder an allen	17.2
Eine Seite wird blockiert: Sperrseite oder nur ein Verbindungsfehler	17.3
Eine App startet nicht oder bleibt beim Start auf einem weißen Bildschirm stehen	17.3
Eine Seite lädt sehr langsam oder unvollständig	17.4
Der Browser zeigt eine Zertifikatswarnung	17.5
Eine E-Mail kommt nicht an	17.6
Ein Gerät taucht in der Geräteliste nicht auf	17.7
Ein Gerät verbindet sich nicht mit dem TrutzBox-WLAN	17.8
Gäste in der Videokonferenz sehen eine Zertifikatswarnung	17.9
Ein Chat-Kontakt erscheint dauerhaft als nicht erreichbar	17.10
Die Verwaltungsoberfläche lässt sich nicht öffnen	17.11
Die TrutzBox reagiert überhaupt nicht mehr	17.12
Nach einem Software-Update funktioniert etwas nicht mehr	17.13
Der Speicherplatz wird knapp	17.14
Die TrutzBox soll neu gestartet oder zurückgesetzt werden	17.15
Das Passwort für das Admin-Panel ist nicht mehr bekannt	17.16

Das beobachten Sie	Abschnitt
Sie ziehen um oder bekommen einen neuen Internet-Router	17.17

19.2 … kein Internet da ist

Die entscheidende Frage lautet: Betrifft es alle Geräte oder nur eines? Sind alle betroffen, liegt es am Weg nach draußen, also an Kabel, Internet-Router oder Anschluss. Ist nur ein Gerät betroffen, liegt es fast immer an dessen Einstellungen in der TrutzBox, also an einer zu strengen Filtergruppe oder an einer Ausnahmeregel.

1. Prüfen Sie die Kabel: Router-Kabel in **LAN-Ext**, Gerät an **LAN-Int1** oder **LAN-Int2**. Die LEDs an den Buchsen zeigen, ob Kontakt besteht.
2. Prüfen Sie, ob der Internet-Router selbst online ist, etwa mit einem Gerät, das direkt an ihm hängt.
3. Öffnen Sie den Betriebszustand. Eine gelbe oder rote Karte nennt die Ursache im Klartext; Dienste, die auf das Internet angewiesen sind, etwa **Filterlisten** oder **TrutzDynDNS**, melden sich dort zuerst.
4. Laden keine Webseiten, obwohl einzelne Apps oder ein VPN noch funktionieren, fehlt fast immer die Namensauflösung. Dann zeigt der Betriebszustand die Karte **DNS für Geräte** mit Ursache und Abhilfe (Kapitel „Betriebszustand: die Karten im Einzelnen“).
5. Betrifft es nur ein Gerät, schauen Sie im Monitor nach, ob dessen Verbindungen blockiert werden (Kapitel „Monitor und Statistiken“). Häufigste Ursache: eine zu strenge Filtergruppe oder die Einstellung „Nur Ausnahmen erlauben".
6. Prüfen Sie, ob das Gerät eine Adresse aus dem Bereich 192.168.195.50 bis 199 hat. Hat es keine und haben Sie ihm auch keine feste Adresse gegeben (Kapitel „Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen“), hat es die TrutzBox gar nicht erreicht, und Sie sind bei Abschnitt „… ein Gerät nicht auftaucht“ richtig.
7. Hilft nichts: die TrutzBox neu starten, am besten über den entsprechenden Menüpunkt in der Verwaltungsoberfläche. Nur wenn diese nicht mehr erreichbar ist, trennen Sie die TrutzBox vom Strom, warten zehn Sekunden und schließen sie wieder an.

19.3 … eine Seite blockiert wird oder eine App nicht startet

Der Webfilter prüft bei jedem Verbindungsaufbau die Zieladresse gegen die Filterlisten der Filtergruppe, die für dieses Gerät gilt. Passt die Adresse auf eine Liste, entsteht keine Verbindung. Dass eine gewünschte Seite dabei mitgefangen wird, kommt vor, gerade bei Nachrichtenportalen und Shops. Deren Inhalte kommen oft von denselben Servern wie Werbung und unerwünschter Datenverkehr, etwa die Aufzeichnung dessen, was Besucher auf der Seite tun.

Zeigt der Browser die Sperrseite der TrutzBox, nennt sie Ihnen bereits den Grund, also Filterliste oder Regel. Am schnellsten geben Sie die Seite über den Monitor frei: Eintrag suchen, auf das Schild-Symbol klicken, **Freischalten** wählen. Die Adresse landet in der Standard-TrutzContent-WL, der Liste Ihrer Freigaben, und ist sofort wieder erreichbar (Kapitel „Filterlisten verwalten“).

Kennen Sie die Adresse schon, tragen Sie sie alternativ unter **Verwaltung → Eigene Sperren und Ausnahmen** mit **Freischalten** ein (Kapitel „Eigene Sperren und Ausnahmen“).

Erscheint keine Sperrseite, sondern nur ein allgemeiner Verbindungsfehler, ist das bei verschlüsselten Seiten ohne TrutzBrowse der Normalfall: Dort kann die TrutzBox keine eigene Seite einblenden (Kapitel „Die Sperrseite verstehen“). Prüfen Sie im Monitor, ob der Webfilter oder TrutzBrowse blockiert hat. War es TrutzBrowse, schieben Sie den Regler für diese Seite eine Stufe weiter nach rechts, also zu weniger strengem Schutz (Kapitel „Wenn eine Seite nicht richtig funktioniert“).

1. Öffnen Sie den Monitor und suchen Sie den betroffenen Server im gewünschten Zeitraum.
2. Schauen Sie auf das Symbol vorn in der Zeile: Ein grüner Haken heißt durchgelassen, ein rotes Verbotsschild gesperrt. Ein Klick darauf öffnet **Sperren / Freischalten** für diese Adresse; dort lässt sich die Freigabe auch auf einen Teil der Domain eingrenzen.
3. Steht das Gerät auf **TrutzBrowse**, prüfen Sie die gleichnamige Spalte. Sie zeigt die wirksame Slider-Stufe und wie viele der unsichtbaren Folgeaufrufe zurückgehalten wurden.
4. Betrifft es dauerhaft mehrere Seiten derselben Art, passt vermutlich die Filtergruppe des Geräts nicht. Ändern Sie diese lieber einmal richtig, statt viele Einzelausnahmen zu pflegen (Kapitel „Filtergruppen einrichten“).

Wenn eine App nicht startet

Startet eine App nicht oder bleibt sie beim Start auf einem weißen Bildschirm stehen, sperrt der Webfilter oft einen Baustein, den die App zum Start braucht. Zwei solche Bausteine nutzen sehr viele Apps: die Firebase-Kennung, ohne die eine App ihre Starteinstellungen nicht lädt, und die Schnittstelle von RevenueCat für Abos und Käufe. Beide stehen auf Sperrlisten gegen unerwünschten Datenverkehr.

1. Öffnen Sie **Verwaltung → Eigene Sperren und Ausnahmen** und schalten Sie im Bereich **Ausnahmen** den Schalter **App-Grundbausteine durchlassen** ein (Kapitel „Eigene Sperren und Ausnahmen“). Ab Werk ist er aus.
2. Die TrutzBox trägt dann beide Bausteine als Ausnahmen ein. Sie stehen in der Liste darunter mit der Herkunft „Mitgeliefert: App-Grundbausteine". Reine Messdienste bleiben gesperrt.
3. Starten Sie die App neu. Startet sie immer noch nicht, zeigt der Monitor, welcher Server ihr fehlt: Gerät anklicken, gesperrte Server stehen rot. Die eingebaute Hilfe des Monitors führt unter „Eine App oder Webseite funktioniert nicht" Schritt für Schritt zur Freigabe (Kapitel „Die eingebauten Führungen: Hilfe direkt in der Seite“).

19.4 … eine Seite sehr langsam lädt

Wenn eine Seite lädt, aber quälend langsam, hat das selten mit dem Webfilter zu tun; seine Prüfungen kosten im Alltag kaum merklich Zeit. Häufiger sind schlicht viele Daten gleichzeitig unterwegs, eine schlechte Funkverbindung oder eine bewusst eingeschaltete Zusatzfunktion wie TrutzBrowse oder das Tor-Netzwerk.

1. Prüfen Sie, ob es nur ein Gerät betrifft oder alle. Betrifft es alle, liegt es meist an der Leitung und nicht an der TrutzBox.

2. Öffnen Sie den Monitor in der Darstellung **Verbindungen** und wählen Sie den Zeitraum **1m** oder **5m**. Dann zählt nur, was gerade läuft. Wählen Sie bei den Geräten die Sortierung **Daten**: Das Gerät mit den meisten Daten steht oben. Über **Felder anzeigen** haken Sie „Datenmenge im Zeitraum" und „Verlaufskurve mit aktueller Rate" an; dann steht an jedem Gerät, wie viel es überträgt.
3. Klicken Sie das oberste Gerät an und wählen Sie auch bei seinen Servern **Daten**. Oben steht dann der Server, mit dem es die meisten Daten austauscht. Meist findet sich so der Vielfraß, etwa ein laufendes Backup oder ein Videodienst in hoher Qualität. Die eingebaute Hilfe des Monitors zeigt diesen Weg unter „Das Internet ist langsam: Wer überträgt viel?" Schritt für Schritt (Kapitel „Die eingebauten Führungen: Hilfe direkt in der Seite“).
4. Prüfen Sie unter **Verwaltung → Geräte**, ob für dieses Gerät das Tor-Netzwerk eingeschaltet ist. Tor macht die Nutzung spürbar langsamer, und manche Server bereiten damit zusätzliche Schwierigkeiten. Für den Alltag gehört der Schalter aus.
5. Hängt das Gerät im WLAN, prüfen Sie unter **Netzwerk → WLAN** im Bereich **Verbundene WLAN-Geräte** die Signalstärke und die Datenrate. Schlechter Empfang sieht am Gerät genauso aus wie eine langsame Leitung.
6. Prüfen Sie auf der Betriebszustand-Seite die Karte **Arbeitsspeicher**. Ist sie dauerhaft gelb oder rot, kann ein Neustart helfen; die Ursache klärt sonst der Support.

Lädt eine Seite nicht langsam, sondern unvollständig, fehlt also ein Bereich oder reagiert ein Knopf nicht, ist meist TrutzBrowse im Spiel. Kapitel „Wenn eine Seite nicht richtig funktioniert“ beschreibt das Vorgehen.

19.5 … der Browser eine Zertifikatswarnung zeigt

Damit die TrutzBox verschlüsselte Verbindungen für TrutzBrowse öffnen kann, stellt sie den Geräten eigene Zertifikate aus. Das funktioniert nur, wenn das Gerät das TrutzBox-Root-Zertifikat kennt. Fehlt es, ist es veraltet oder wurde es nach einem Zurücksetzen der TrutzBox nicht erneuert, meldet der Browser eine Warnung. Dieselbe Warnung erscheint, wenn ein Mail-Programm verschlüsselt auf den Mail-Server der TrutzBox zugreift, ohne das Zertifikat zu kennen.

1. Achten Sie darauf, wo die Warnung erscheint. Zeigt sie sich bei `https://trutzbox`, im Mail-Programm oder in einer Chat-App, fehlt dem Gerät das Root-Zertifikat der TrutzBox; weiter mit Schritt 2. Erscheint sie beim Besuch einer fremden Webseite, prüfen Sie unter **Verwaltung → Geräte**, ob für dieses Gerät **TrutzBrowse** eingeschaltet ist. Ist es aus, stammt die Warnung nicht von der TrutzBox. Dann stimmt am Server selbst etwas nicht, und Sie sollten die Seite nicht öffnen.
2. Installieren Sie das Root-Zertifikat auf dem Gerät (Kapitel „Das Root-Zertifikat installieren“). Die Datei laden Sie unter **Verwaltung → Allgemeine Einstellungen** über **Root Zertifikat herunterladen** herunter.
3. Wurde die TrutzBox zwischenzeitlich zurückgesetzt, hat sie ein neues Root-Zertifikat erzeugt. Löschen Sie auf dem Gerät zuerst das alte und importieren Sie danach das neue.
4. Beachten Sie, dass manche Browser eigene Zertifikatsspeicher führen und das Zertifikat des Betriebssystems nicht übernehmen. Dann muss es zusätzlich im Browser eingetragen werden.

5. Lässt sich auf dem Gerät kein Zertifikat einrichten, typisch bei Fernsehern, Haustechnik und Gastgeräten, schalten Sie TrutzBrowse für dieses Gerät ab. Webfilter, Firewall und Angriffsschutz bleiben davon unberührt.

19.6 … eine E-Mail nicht ankommt

TrutzMails gehen nicht über einen Mail-Server im Internet, sondern direkt von TrutzBox zu TrutzBox. Das macht sie sicher, hat aber eine Folge: Ist die TrutzBox des Empfängers gerade aus, kann niemand die Mail zwischenlagern. Ihre TrutzBox behält sie und versucht die Zustellung von selbst weiter.

1. Öffnen Sie **E-Mail → Status**. Steht die Mail in der Warteschlange, nennt die Fehlermeldung dort den Grund.
2. Prüfen Sie die fünf Voraussetzungen aus Kapitel „Wenn eine Mail nicht ankommt“, insbesondere ob die Empfänger-TrutzBox eingeschaltet ist; die eigene TrutzBox versucht die Zustellung dann automatisch weiter.
3. Bei einem einzelnen Partner mit Verschlüsselungsproblem: dessen zwischengespeicherten Schlüssel in der Schlüsselverwaltung löschen und erneut senden. Beim nächsten Senden lädt die TrutzBox seinen aktuellen Schlüssel selbsttätig neu.
4. Kommt eine Mail eines TrutzBox-Partners unerwartet unverschlüsselt oder unsigniert an, steckt meist ein veralteter Schlüssel dahinter. Das korrigiert sich in aller Regel von selbst, sobald die TrutzBoxen ihre Schlüssel abgeglichen haben (Kapitel „Schlüssel und Zertifikate“).
5. Bei sehr großen Mails hilft ein Neustart der TrutzBox. Anhänge werden für den Versand in Textzeichen umgewandelt und dabei deutlich größer; ist der Arbeitsspeicher knapp, scheitert der Versand. Der Neustart räumt den Speicher.

19.7 … ein Gerät nicht auftaucht

Die Geräteliste zeigt, was über die TrutzBox läuft. Fehlt ein Gerät dort, läuft sein Verkehr an der TrutzBox vorbei, und dann schützt sie es auch nicht. Der häufigste Fall ist banal: Das Gerät hängt noch im WLAN des Internet-Routers.

1. Prüfen Sie, wo das Gerät wirklich hängt: an **LAN-Int1** oder **LAN-Int2**, im TrutzBox-WLAN oder noch im alten Router-WLAN.
2. Prüfen Sie die Adresse des Geräts. Sie muss aus dem Bereich 192.168.195.50 bis 199 stammen, sofern Sie dem Gerät keine feste Adresse gegeben haben (Kapitel „Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen“). Eine andere Adresse bedeutet: Das Gerät hat sie nicht von der TrutzBox bekommen.
3. Trennen Sie das Gerät kurz vom Netz, beim Kabel durch Aus- und Einstecken, beim WLAN durch Trennen und neu Verbinden. Danach holt es sich eine Adresse von der TrutzBox (Kapitel „Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen“).
4. Bleibt es dabei, schalten Sie das WLAN des Internet-Routers ab. Dann gibt es keinen Weg mehr an der TrutzBox vorbei, und alle Geräte finden von selbst den richtigen.

Kein Grund zur Sorge ist es, wenn ein Eintrag irgendwann aus der Liste verschwindet: Beim Öffnen der Geräte-Seite entfernt die TrutzBox selbsttätig die Einträge, zu denen weder eine MAC-Adresse noch ein Hostname vorliegt. Alles andere bleibt erhalten.

19.8 … ein Gerät sich nicht mit dem TrutzBox-WLAN verbindet

Für ein WLAN, das ein einzelnes Gerät nicht annimmt, gibt es drei typische Gründe: Das Funkmodul ist gerade nach einem eingerichteten Zeitplan ausgeschaltet, das Gerät beherrscht den eingestellten Verschlüsselungsstandard nicht, oder es hat noch das alte Passwort gespeichert.

1. Öffnen Sie **Netzwerk → WLAN** und prüfen Sie, ob **Access-Point verwenden** eingeschaltet ist.
2. Prüfen Sie den Bereich **Zeit-Steuerung**. Ab Werk ist dort kein Zeitplan aktiv; wurde einer eingerichtet, ist das Funkmodul außerhalb der grün hinterlegten Zeiten aus. Ein Einschalten von Hand gilt dabei bis zum nächsten Schaltzeitpunkt des Plans.
3. Prüfen Sie die **Verschlüsselung**. Steht sie auf „Nur WPA3", bleiben ältere Geräte außen vor. „WPA2 + WPA3 (empfohlen)" bedient alte und neue Geräte gleichzeitig.
4. Ist **SSID verstecken** eingeschaltet, erscheint das Netz in keiner Liste. Auf dem Gerät müssen Sie den Namen dann von Hand eintragen.
5. Lassen Sie das Gerät das gespeicherte Netz vergessen und verbinden Sie es neu mit dem Passwort. Gerade nach einer Passwortänderung ist das der eigentliche Grund.
6. Prüfen Sie im Bereich **Verbundene WLAN-Geräte**, ob es kurz auftaucht und wieder verschwindet. Das deutet auf schlechten Empfang hin, nicht auf ein Anmeldeproblem.
7. Sind die Verbindungen allgemein unzuverlässig, hilft der Blick auf die Nachbarnetze im unteren Bereich der Seite. Ist Ihr Kanal stark belegt, wählen Sie einen freieren; bei 2,4 GHz haben sich die Kanäle 1, 6 und 11 bewährt. Prüfen Sie auch, ob der Standort korrekt eingestellt ist, denn er bestimmt, welche Kanäle überhaupt zulässig sind.

19.9 … Gäste in der Videokonferenz eine Zertifikatswarnung sehen

Ihre Gäste kommen über einen öffentlichen Namen auf Ihre TrutzBox. Damit deren Browser diesen Namen ohne Warnung akzeptiert, braucht die TrutzBox ein allgemein anerkanntes Zertifikat für genau diesen Namen. Fehlt es, sieht jeder Gast eine Warnung, obwohl technisch alles funktioniert.

1. Öffnen Sie **Videokonferenz und Chat** und prüfen Sie die Karte **1. Domain-Namen festlegen**. Dort muss TrutzDynDNS eingeschaltet sein, ebenso der Schalter **Zertifikat aktivieren**, mit dem die TrutzBox das kostenlose Zertifikat von Let’s Encrypt holt (Kapitel „Reiter Videokonferenz: einmalig einrichten“). Nutzen Sie stattdessen einen eigenen Namen, braucht er ein öffentlich anerkanntes Zertifikat (Kapitel „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“).
2. Schlägt die Erstellung des Zertifikats fehl, nennt die Fehlermeldung die konkrete Ursache. Meist fehlt die Erreichbarkeit von außen, die für die Prüfung nötig ist.
3. Lassen Sie **Erreichbarkeit prüfen** laufen. Der Selbsttest prüft vier Stationen einzeln: die öffentliche Adresse, das Zertifikat und beide Portfreigaben. Jede meldet ihr Ergebnis in Klartext.

4. Prüfen Sie am Internet-Router die beiden Weiterleitungen: extern **443** auf intern **9082 (TCP)** sowie **9083** auf **9083 (UDP)**.
5. Vergewissern Sie sich, dass Ihre Gäste den Einladungslink mit dem öffentlichen Namen benutzen und nicht die interne Adresse der TrutzBox. Für die interne Adresse gibt es kein öffentlich anerkanntes Zertifikat, und die Warnung wäre die logische Folge.

19.10 … ein Chat-Kontakt dauerhaft als nicht erreichbar erscheint

Der farbige Punkt neben einem Kontakt zeigt dessen Anwesenheit. Nimmt ein Benutzer einen anderen Benutzer derselben TrutzBox als Kontakt auf, gilt das sofort für beide, und der Punkt erscheint gleich. Bei einem Kontakt auf einer anderen TrutzBox erscheint er erst, wenn die Gegenseite die Kontaktaufnahme bestätigt hat; bis dahin zeigt der Web-Chat „Anwesenheit noch nicht freigegeben". Und weil Nachrichten zwischen TrutzBoxen direkt von TrutzBox zu TrutzBox laufen, bedeutet ein grauer Punkt schlicht: Auf der anderen Seite ist gerade niemand angemeldet, oder deren TrutzBox läuft nicht.

1. Prüfen Sie bei einem Kontakt auf einer anderen TrutzBox, ob die Gegenseite die Kontaktaufnahme bestätigt hat. Ohne Bestätigung sehen beide Seiten die Anwesenheit des anderen nicht. Hat die Gegenseite Ihre Anfrage im Web-Chat mit **Ablehnen** beantwortet, ist Ihre Adresse dort gesperrt: Ihre Nachrichten kommen nicht mehr an, bis sie Sie über **Kontakt hinzufügen** aufnimmt.
2. Prüfen Sie die Schreibweise der TrutzMail-Adresse des Kontakts. Ein Tippfehler erzeugt einen Kontakt, den es nicht gibt.
3. Starten Sie auf dem Reiter **TrutzChat** im Bereich **Prüfung** mit dem Knopf **Prüfen** den Chat-Selbsttest. Er prüft in etwa zehn Sekunden den Nachrichtenweg auf Ihrer eigenen TrutzBox und meldet das Ergebnis in Klartext. Beachten Sie dabei, was er nicht prüft: den Chat mit anderen TrutzBoxen, die Erreichbarkeit von unterwegs und die Anmeldung mit Ihren tatsächlichen Konten. Ein erfolgreicher Selbsttest bedeutet also nur, dass der Dienst auf Ihrer TrutzBox grundsätzlich arbeitet.
4. Prüfen Sie auf der Betriebszustand-Seite die Karte **TrutzRTC**. Meldet sie „Läuft, aber gestört", schalten Sie TrutzRTC einmal aus und wieder ein; die Karte nennt diese Empfehlung selbst.
5. Fragen Sie beim Partner nach, ob dessen TrutzBox eingeschaltet ist. Was Sie ihm in der Zwischenzeit geschrieben haben, stellt Ihre TrutzBox nicht später zu: Der Web-Chat markiert solche Nachrichten mit „Nicht zugestellt". Senden Sie sie noch einmal, sobald die TrutzBox des Partners wieder läuft.
6. Benutzen Sie eine Chat-App statt des Browsers, prüfen Sie die Servereinstellung: Der Servername muss `trutzbox` lauten, nicht „comidio.email"; der Port bleibt 5222 (Kapitel „TrutzChat benutzen: im Browser und mit einer Chat-App“). Von unterwegs verbinden Sie sich zuerst über den VPN-Zugang; das gilt auch für den Web-Chat im Browser.

> **Was „Nicht zugestellt" bedeutet**
>
> Erreicht eine Nachricht die TrutzBox des Partners nicht, meldet Ihre TrutzBox das zurück. Im Web-Chat steht an der Nachricht „Nicht zugestellt", und im Gespräch erscheint der Grund. Drei

Gründe gibt es:

„Nicht zugestellt: Die TrutzBox von … ist gerade nicht erreichbar. Sie ist ausgeschaltet oder hat keine Verbindung zum Internet. Die Nachricht bitte später noch einmal senden."

„Nicht zugestellt: Die Adresse … ist zurzeit nicht aktiv. Für sie ist kein gültiger Schlüssel hinterlegt, oder die Service-Laufzeit ihrer TrutzBox ist abgelaufen."

„Nicht zugestellt: Die Adresse … gibt es nicht oder nicht mehr."

Hat der Partner seine TrutzBox neu aufgesetzt, hat er einen neuen Schlüssel. Ihre TrutzBox holt ihn dann selbst und sendet die Nachricht einmal neu; erst wenn auch das scheitert, erscheint die Meldung. Nachrichten an Benutzer Ihrer eigenen TrutzBox betrifft das nicht: Sie warten auf der TrutzBox, bis sich der Empfänger wieder anmeldet.

19.11 … die Verwaltungsoberfläche nicht erreichbar ist

Meist steckt kein Fehler dahinter, sondern die Namensauflösung oder schlicht Ungeduld: Nach einem Neustart brauchen die Dienste einige Minuten, bis die Oberfläche antwortet.

1. Probieren Sie statt `https://trutzbox` die Adresse `http://trutzbox.local`. Unter diesem Namen antwortet die TrutzBox selbst, auch wenn der Router ihren Namen nicht kennt (Kapitel „Das Setup im Browser öffnen“). Das klappt im internen Netz der TrutzBox und im Netz des Routers, nicht über VPN. Nehmen Sie hier http und nicht https: Das Zertifikat der TrutzBox ist auf den Namen trutzbox ausgestellt, bei trutzbox.local würde der Browser deshalb eine Warnung zeigen.
2. Hilft das nicht, geben Sie die Zahlenadresse der TrutzBox ein. Im internen Netz der TrutzBox ist das immer `https://192.168.195.200`; von einem PC im lokalen Netz am Router aus die Adresse, die der Router der TrutzBox gegeben hat (Geräteübersicht des Routers, Kapitel „Das Setup im Browser öffnen“).
3. Prüfen Sie, ob Ihr PC überhaupt mit der TrutzBox verbunden ist: entweder im internen Netz der TrutzBox mit einer Adresse von ihr (192.168.195.50 bis 199) oder im lokalen Netz am selben Router wie die TrutzBox.
4. Warten Sie nach einem Neustart zwei bis drei Minuten; die Dienste brauchen etwas Anlauf. Zeigt der Browser die Seite „Software-Updates werden installiert", spielt die TrutzBox gerade Software-Updates ein. Meist dauert das wenige Minuten, bei einer neuen TrutzBox oder nach längerer Pause bis zu einer halben Stunde. Danach öffnet sich die Oberfläche von selbst, spätestens nach 65 Minuten.
5. Schauen Sie auf die linke LED an der Gerätefront. Blinkt sie schnell im Herzschlag-Rhythmus, antwortet die Oberfläche, und die Ursache liegt auf Ihrem PC. Bleibt sie beim langsamen, gleichmäßigen Blinken stehen, konnte die Oberfläche nicht starten. Ist sie dunkel, obwohl die TrutzBox Strom hat, ist vermutlich die Herzschlag-Leuchte abgeschaltet (Abschnitt „… die TrutzBox überhaupt nicht mehr reagiert“); dann sagt die LED nichts über den Zustand.
6. Als Notzugang für Fortgeschrittene läuft Webmin eigenständig unter `http://trutzbox:10000` weiter (Abschnitt „Webmin: der Experten-Zugang“), am besten

nur nach Anleitung des Supports. Ebenfalls getrennt von der Oberfläche läuft das Terminal im Browser unter `https://trutzbox/terminal/` (Abschnitt „Die Kommandozeile: Terminal und SSH“).

19.12 … die TrutzBox überhaupt nicht mehr reagiert

Die linke LED an der Gerätefront sagt Ihnen zuerst, woran Sie sind. Dauerleuchten heißt: Die TrutzBox startet gerade. Langsames, gleichmäßiges Blinken heißt: Das Betriebssystem läuft, die Oberfläche startet noch. Schnelles Blinken im Herzschlag-Rhythmus heißt: Alles ist bereit. Dunkel ist die LED im Betrieb nur, wenn Sie die Herzschlag-Leuchte abgeschaltet haben: unter **Verwaltung → Allgemeine Einstellungen** in der Karte **LED-Anzeige an der TrutzBox** mit dem Schalter **Herzschlag-Leuchte an** (Kapitel „Die LEDs an der TrutzBox“). Dann bleibt sie auch beim Start dunkel und zeigt keinen der drei Zustände. Ist die Herzschlag-Leuchte an und die LED trotzdem dunkel, fehlt Strom. Bei der TrutzBox ARM übernimmt die rote LED diese Rolle. Die ganze Abfolge vom Einschalten bis zum Setup steht als Tabelle in Kapitel „System zurücksetzen (Werksreset)“.

1. Prüfen Sie Netzteil und Steckdose, wenn keine LED an ist und Sie die Herzschlag-Leuchte nicht abgeschaltet haben.
2. Steht die LED auf Dauerleuchten oder langsamem Blinken, geben Sie der TrutzBox fünf Minuten. Nach Software-Updates dauert dieser Abschnitt länger als sonst.
3. Probieren Sie den Notzugang Webmin unter `http://trutzbox:10000`. Er läuft eigenständig und funktioniert erfahrungsgemäß auch dann noch, wenn die normale Oberfläche klemmt. Dasselbe gilt für das Terminal im Browser unter `https://trutzbox/terminal/` (Abschnitt „Die Kommandozeile: Terminal und SSH“).
4. Starten Sie die TrutzBox neu. Der übliche Weg dafür ist der entsprechende Menüpunkt in der Verwaltungsoberfläche. Antwortet diese nicht mehr, trennen Sie die TrutzBox vom Strom, warten zehn Sekunden und schließen sie wieder an. Ein Neustart ist harmlos und löscht nichts.
5. Bleibt es dabei, wenden Sie sich an den Support (Kapitel „Support kontaktieren“). Kommen Sie noch in Webmin hinein, können Sie den Systemstatus für die Analyse dort selbst herunterladen; der Support sagt Ihnen, wie.

> **Warum die TrutzBox lieber etwas abschaltet, als stehen zu bleiben**
>
> Die TrutzBox überwacht ihren Arbeitsspeicher fortlaufend. Wird er knapp, schaltet der Speicher-Wächter gezielt Dienste ab, zuerst TrutzRTC mit Chat und Videokonferenz, danach TrutzMail. Das ist kein Fehler, sondern Absicht: Lieber fällt vorübergehend eine Zusatzfunktion aus, als dass die ganze TrutzBox einfriert und damit auch der Internet-Zugang steht. Auf der Betriebszustand-Seite steht die Karte des Dienstes dann grau auf „Vom Speicher-Wächter angehalten". Ist wieder genug Speicher frei, startet der Wächter den Dienst von selbst. Muss er innerhalb eines Tages ein zweites Mal eingreifen, bleibt der Dienst aus, bis Sie ihn wieder einschalten: TrutzRTC auf der Seite Videokonferenz und Chat, TrutzMail auf der Übersicht.

19.13 … nach einem Software-Update etwas nicht mehr funktioniert

Software-Updates werden vor der Auslieferung getestet, auch die Pakete des Betriebssystems (Kapitel „Software-Paket-Updates“). Trotzdem kann eine Neuerung eine Einstellung anders auslegen als zuvor. Meist steckt dann kein Fehler dahinter, sondern eine bewusste Änderung, die im Forum beschrieben ist.

1. Öffnen Sie den Betriebszustand und dort die Karte **Software-Updates**. Unter „Letzter Update-Lauf" und „Ergebnis" sehen Sie, ob der letzte Lauf abgeschlossen wurde, unter „Zuletzt Pakete eingespielt", wann zuletzt etwas dazukam. Blieb ein Lauf stehen, nennt „Stehen geblieben bei" das Paket. Einen solchen Lauf holt die TrutzBox in der kommenden Nacht oder beim nächsten Start von selbst nach. Bleibt die Karte länger als zwei Tage gelb, senden Sie den Support-Bericht.
2. Sehen Sie sich auch die übrigen Karten an. Eine gelbe oder rote Karte nennt Ursache und Empfehlung im Klartext, oft mit einem konkreten Handlungsvorschlag.
3. Sieht die Oberfläche seit dem Software-Update seltsam aus, laden Sie die Seite im Browser neu. Ein Fenster, das schon vorher offen war, zeigt sonst noch den alten Stand der Oberfläche. Meist lädt es sich von selbst neu, sobald dabei keine Eingabe verloren geht; bis dahin erscheint der Hinweis „Die Oberfläche der TrutzBox wurde aktualisiert" mit dem Knopf **Neu laden**.
4. Sehen Sie im TrutzBox-Forum unter forum.trutzbox.de im Bereich „TrutzBox-Updates" nach, was das Software-Update geändert hat.
5. Starten Sie die TrutzBox einmal neu. Manche Dienste übernehmen eine Änderung erst beim Start vollständig.
6. Betrifft es Chat oder Videokonferenz, schalten Sie TrutzRTC einmal aus und wieder ein.
7. Prüfen Sie unter **Systemeinstellungen → Vertrag und Pakete**, ob bei den Paketen die Spalten **Installierte Version** und **Version im Kanal Stabil** übereinstimmen. Der Schalter **Nur Unterschiede** zeigt nur die abweichenden Pakete. Weichen sie ab, ist das Software-Update vielleicht noch nicht vollständig angekommen.
8. Bleibt es unklar, senden Sie den Support-Bericht an Comidio und beschreiben Sie, was seit dem Software-Update anders ist (Kapitel „Support kontaktieren“).

19.14 … der Speicherplatz knapp wird

Die TrutzBox legt eine Menge ab: Protokolle, Monitor-Daten, Postfächer, Chat-Verläufe und Anhänge. Das meiste räumt sie selbst wieder auf. Knapp wird es vor allem, wenn ausnahmsweise eine ausführliche Fehlerprotokollierung eingeschaltet blieb, oder wenn sich über die Jahre alte Bestandteile angesammelt haben.

1. Öffnen Sie den Betriebszustand und tippen Sie auf die Karte **SSD-Gesundheit**. Über **Größte Platzfresser finden** spürt die TrutzBox die speicherintensivsten Daten selbst auf; der zugehörige Dialog räumt auf Wunsch auch alte Systemstände ab.
2. Prüfen Sie unter **Systemeinstellungen → System-Logs** die **Debug Einstellungen**. Eine ausführliche Protokollierung schreibt sehr viel und sollte nur kurzzeitig und mit Bedacht eingeschaltet sein. Über **Alle Logdateien löschen** räumen Sie die Protokolle ab.

3. Prüfen Sie auf dem Reiter **TrutzChat** den Platzbedarf der Gesprächsverläufe. Dort lässt sich die Aufbewahrungsdauer verkürzen, und **Alle Verläufe löschen** räumt gesammelt ab. Anhänge entfernt die TrutzBox ohnehin nach 30 Tagen von selbst.
4. Verwechseln Sie Speicherplatz nicht mit Arbeitsspeicher. Die Karte **Arbeitsspeicher** betrifft den Speicher der laufenden Programme, also Hauptspeicher (RAM) und Auslagerung (Swap); dort hilft ein Neustart, auf der SSD hilft er nicht.
5. Zeigt **SSD-Details anzeigen** auffällige Selbstdiagnose-Werte, deutet das auf einen alternden Datenträger hin. Legen Sie dann zuerst eine Sicherung an (Kapitel „Sichern, Wiederherstellen und Zurücksetzen“) und melden Sie sich beim Support.

Haben Sie die SSD gegen eine größere getauscht, oder läuft die TrutzBox auf eigener Hardware oder in einer virtuellen Maschine mit größerer Platte, nutzt sie den zusätzlichen Platz erst nach einem Zurücksetzen (Kapitel „System zurücksetzen (Werksreset)“) oder nach dem Aufspielen mit dem Tank-Stick ab V80 (Kapitel „Der Ausnahmefall: ein komplettes Image“). Beim ersten Start danach vergrößert sie ihren Datenbereich selbst bis zum Ende der Platte, höchstens bis 2 TB. Mit älteren Images bleibt der Datenbereich bei rund 5,4 GB. Denken Sie vor dem Zurücksetzen an eine Sicherung (Kapitel „Eine Sicherung anlegen“).

19.15 … die TrutzBox neu gestartet oder zurückgesetzt werden soll

Einen Neustart lösen Sie normalerweise über den entsprechenden Menüpunkt im Admin-Panel aus. Nur wenn die Oberfläche nicht mehr antwortet, trennen Sie die TrutzBox kurz vom Strom. Der Neustart ist harmlos und löscht nichts; er hilft bei hartnäckigen Hängern, nach ungewöhnlich großen Mails und immer dann, wenn der Arbeitsspeicher voll gelaufen ist.

Neustart und Ausschalten finden Sie im Ein-Aus-Symbol rechts oben in der Kopfzeile der Verwaltungsoberfläche. Es öffnet das Menü **Energie** mit den drei Einträgen **Abmelden**, **Neustarten** und **Herunterfahren**. Zum Ausschalten nehmen Sie immer **Herunterfahren** und ziehen erst danach den Stecker: Die TrutzBox schreibt dabei ihre laufenden Daten sauber zu Ende. Wie oft ihr das nicht gelungen ist, zählt die Karte **SSD-Gesundheit** unter *Unsaubere Abschaltungen* mit (Kapitel „Betriebszustand: die Karten im Einzelnen“).

Nach **Neustarten** zeigt die Oberfläche die Warteseite „Die TrutzBox wird neu gestartet". Das dauert rund drei Minuten; ist die TrutzBox wieder bereit, lädt die Seite von selbst neu. Nach **Herunterfahren** erscheint „Die TrutzBox wird ausgeschaltet" mit dem Hinweis „Diese Seite können Sie schließen."

Das vollständige Zurücksetzen auf den Werkszustand beschreibt Kapitel „System zurücksetzen (Werksreset)“. Denken Sie unbedingt vorher an eine Sicherung: Ohne sie sind Postfächer und Schlüssel verloren. Denken Sie außerdem an das Root-Zertifikat: Bauen Sie die TrutzBox ohne Wiederherstellung neu auf, erzeugt sie ein neues, das auf allen Geräten das alte ersetzen muss (Kapitel „Das Root-Zertifikat installieren“). Spielen Sie danach Ihre Sicherung ein, kehrt das bisherige Zertifikat zurück und bleibt gültig.

> **Zurücksetzen ist der letzte Schritt, nicht der erste**
>
> Ein Werksreset löst kaum ein Problem, das nicht auch anders zu lösen wäre, kostet aber Zeit und im schlimmsten Fall Daten. Bevor Sie ihn erwägen, wenden Sie sich an den Support. Der Support-

Bericht aus dem Betriebszustand zeigt in aller Regel, woran es wirklich liegt.

19.16 … das Passwort für das Admin-Panel nicht mehr bekannt ist

Hier ist Klartext angebracht: Es gibt keinen Ausweg außer dem Zurücksetzen auf den Werkszustand. Das Admin-Passwort liegt ausschließlich auf Ihrer TrutzBox und ist für niemanden lesbar. Es gibt keine Funktion „Passwort vergessen", keine Rücksetz-Mail und keine Hintertür, und auch Comidio kann es nicht neu setzen. Das ist Absicht: Wer das Passwort zurücksetzen könnte, käme an Ihre Post und Ihre Schlüssel. Auch der Notzugang Webmin hilft nicht, denn er prüft dieselbe Anmeldung.

1. Suchen Sie zuerst gründlich: Viele notieren das Passwort bei der Einrichtung im Passwortspeicher des Browsers oder im Passwort-Programm des Telefons.
2. Probieren Sie es ohne Hast weiter. Nach mehreren Fehlversuchen bremst die TrutzBox die Anmeldung absichtlich aus und nennt Ihnen die Wartezeit; danach ist die Anmeldung wieder möglich.
3. Führt das nicht zum Ziel, bleibt nur das Zurücksetzen auf den Werkszustand nach Kapitel „System zurücksetzen (Werksreset)“. Dabei gehen alle Daten auf der TrutzBox verloren. Ohne Anmeldung lösen Sie den Vorgang mit der Taste am Gehäuse aus: Schalten Sie die TrutzBox ein, halten Sie die Taste innerhalb der ersten 2 Minuten 3 Sekunden lang gedrückt, bis die LEDs dauerhaft leuchten, und lassen Sie dann los. Wo diese Taste sitzt und was die LEDs dabei anzeigen, steht in Kapitel „System zurücksetzen (Werksreset)“.
4. Richten Sie die TrutzBox danach mit Ihrer TrutzLegitimation neu ein und vergeben Sie ein neues Admin-Passwort (Kapitel „TrutzBox einrichten (Setup)“).

Was eine Sicherung hier leistet, und was nicht

Eine Sicherung enthält auch das Admin-Passwort. Spielen Sie sie nach dem Zurücksetzen ein, kehrt damit genau das Passwort zurück, an das Sie sich nicht erinnern. Bei dieser einen Störung ist die Sicherung also kein Rettungsanker für den Zugang, wohl aber für Ihre Postfächer und Schlüssel.

Die Lehre daraus zieht man am besten vorher: Notieren Sie das Admin-Passwort bei der Einrichtung an einem sicheren Ort, getrennt von der TrutzBox, so wie Sie es mit der Passphrase Ihrer Sicherung ohnehin tun sollten.

19.17 … Sie umziehen oder einen neuen Internet-Router bekommen

Die TrutzBox nimmt beides gelassen. Sie hängt am Router, nicht am Anschluss, und alles Wesentliche liegt auf der TrutzBox selbst. Ihre TrutzMail-Adressen, Schlüssel und Einstellungen wandern deshalb mit, ohne dass jemand etwas beantragen müsste. Aufpassen muss man nur an drei Stellen: an der Portfreigabe im neuen Router, an der Erreichbarkeit von außen und beim WLAN.

1. Legen Sie vor dem Abbau eine Sicherung an und laden Sie sie auf Ihren PC (Kapitel „Eine Sicherung anlegen“). Das kostet zwei Minuten und erspart im Ernstfall alles Weitere.

2. Notieren Sie sich, welche Portfreigaben im alten Router eingerichtet waren, also insbesondere die Freigabe für TrutzVPN (Kapitel „Schritt 2: Portweiterleitung am Internet-Router“), eine etwaige IPv6-Freigabe (Kapitel „VPN auch über IPv6 anbieten“) und, falls genutzt, die für die Videokonferenz (Kapitel „Reiter Videokonferenz: einmalig einrichten“).
3. Bauen Sie am neuen Ort wie gehabt auf: Router-Kabel in **LAN-Ext**, Geräte an **LAN-Int1** und **LAN-Int2** (Kapitel „Die Anschlüsse“). Am inneren Netz ändert sich nichts, auch die Adressen der Geräte bleiben gleich.
4. Richten Sie die notierten Portfreigaben im neuen Router erneut ein. Sie sind der einzige Teil der Einrichtung, der im Router und nicht auf der TrutzBox liegt, und gehen beim Routerwechsel deshalb verloren.
5. Prüfen Sie anschließend unter **Netzwerk → Fernzugriff** die Erreichbarkeit. Der Name Ihrer TrutzBox unter mytrutzbox.de bleibt unverändert; die TrutzBox meldet die neue Adresse von selbst dorthin. Kommt trotz richtiger Freigabe von außen nichts an, lässt der neue Anschluss vermutlich nichts oder nur IPv6 herein (Abschnitt „Welcher Anschluss ist von außen erreichbar?“).
6. Starten Sie zum Schluss die angeschlossenen Geräte einmal neu und schalten Sie, falls gewünscht, auch im neuen Router das WLAN ab (Kapitel „Mehr Geräte anschließen: der Switch“).

Ein Wechsel des Internet-Anbieters ändert daran nichts Grundsätzliches. Neu sein können allerdings zwei Dinge: ein Anschluss, der von außen nur IPv6 oder gar nichts hereinlässt (Abschnitt „Welcher Anschluss ist von außen erreichbar?“), und ein Router mit anderer Bedienung, für den Sie die Portfreigabe in dessen Anleitung nachschlagen müssen. Der Support hilft weiter, wenn der Fernzugriff nach dem Wechsel nicht wieder anspringt.

20 Support kontaktieren

Kommen Sie mit Kapitel „Was tun, wenn …?“ nicht weiter, hilft Comidio gerne. Je genauer Ihre Angaben, desto schneller die Lösung. Dieses Kapitel zeigt, welche Unterlagen die TrutzBox selbst zusammenstellt, was Sie in eigenen Worten dazugeben sollten und über welche Wege Sie Comidio erreichen. Es sagt außerdem klar, was Comidio bewusst nicht tut, denn auch das gehört zum Verständnis.

20.1 Zuerst: die Selbstdiagnose der TrutzBox

Die Seite **Systemeinstellungen → Betriebszustand** ist als schnelle Selbstdiagnose gedacht. Statt Protokolle zu durchsuchen, lesen Sie dort in Klartext, ob Hardware, Speicher und Dienste in Ordnung sind. Ganz oben steht die Ampel für den Gesamtzustand, daneben die Verfügbarkeit der letzten 30 Tage und die Laufzeit seit dem letzten Neustart.

- **Jetzt prüfen:** stößt eine sofortige Überprüfung an, statt auf den nächsten Durchlauf zu warten.
- **Ampel auf Grün stellen:** ein Schalter, der nur erscheint, wenn die Ampel nicht grün steht. Damit quittieren Sie die gemeldeten Punkte, die Sie zur Kenntnis genommen haben (Kapitel „Betriebszustand: die Ampel lesen“).
- **Bericht an Support:** stellt die relevanten Informationen für eine Anfrage zusammen.

Sehr oft erledigt sich eine Anfrage hier schon: Eine gelbe oder rote Karte nennt nicht nur, was nicht stimmt, sondern auch, was zu tun ist. Erst wenn diese Empfehlung nicht weiterhilft, lohnt der Weg zum Support.

20.2 Was in den Support-Bericht gehört

Menüpfad: Systemeinstellungen → Betriebszustand → Bericht an Support



Abbildung 20-1: Das Fenster „Bericht an den Support senden": Der Bericht beginnt mit dem Vertragsblock und der Zeile für Ihr Anliegen, darunter folgen die technischen Angaben. Sie sehen den vollständigen Text, bevor irgendetwas Ihre TrutzBox verlässt. (© 2026 Comidio GmbH)

Den technischen Teil erledigt die TrutzBox für Sie. In vier Schritten ist die Anfrage fertig:

1. Öffnen Sie **Systemeinstellungen → Betriebszustand** und klicken Sie auf **Bericht an Support**. Es öffnet sich das Fenster **Bericht an den Support senden**, in dem der fertige Bericht als Klartext steht.
2. Lesen Sie ihn durch. Der Bericht ist kein verschlossener Umschlag: Was darin steht, sehen Sie vorher.
3. Wählen Sie, wie es weitergehen soll: **E-Mail-Programm öffnen** übergibt den Bericht an Ihr Mail-Programm, **Bericht kopieren** legt den Text in die Zwischenablage, und **Schließen** beendet das Fenster, ohne etwas zu senden.
4. Mit **E-Mail-Programm öffnen** öffnet sich Ihr Mail-Programm mit vorbereitetem Text und bereits eingetragener Empfängeradresse support@trutzbox.de. Schreiben Sie Ihre

Beschreibung unter die Zeile „Bitte beschreiben Sie hier Ihr Anliegen:" und schicken Sie die Nachricht ab. Von selbst verschickt die TrutzBox nichts.

Öffnet sich kein Mail-Programm, meldet das Fenster das und bietet **Als Datei speichern** an; die Datei hängen Sie dann an eine E-Mail an support@trutzbox.de. Schneidet Ihr Mail-Programm den langen Text ab, kopieren Sie den Bericht mit **Bericht kopieren** und fügen ihn von Hand in die E-Mail ein. Ist der Service-Vertrag abgelaufen, erstellt die TrutzBox keinen Bericht; das Fenster bittet dann darum, den Vertrag zu verlängern.

Der Bericht beginnt mit dem Block „VERTRAG": Ihre TrutzKennung, seit wann der Vertrag läuft und bis wann er gilt, mit den verbleibenden Tagen. Danach folgt die Zeile „Bitte beschreiben Sie hier Ihr Anliegen:" mit Platz für Ihre Worte. Darunter stehen die technischen Angaben: Image-Version und Update-Kanal, die Hardware samt Hauptspeicher (RAM) und SSD-Größe, der Gesamtzustand und die Zustände der einzelnen Karten, wie sie die Betriebszustand-Seite ermittelt, die installierten Pakete und die letzten Ereignisse. Genau das sind die Angaben, nach denen der Support sonst zuerst fragen müsste.

Der Abschnitt „Speicher und Abstürze" zeigt, wie es um den Arbeitsspeicher stand. Die Liste „Größte Speicherverbraucher" nennt dort die Dienste, die am meisten Hauptspeicher belegen, jeweils mit dem Teil, der in der Auslagerung (Swap) liegt. Damit sieht der Support, wer den Speicher hält, wenn die Karte Arbeitsspeicher gelb oder rot war. Laufen Fernzugriff oder Videokonferenz, steht im Bericht außerdem der Block „Erreichbarkeit von außen" mit dem Ergebnis der letzten Prüfung je Dienst und Anschluss, dem TrutzDynDNS-Namen und den Adressen Ihres Anschlusses (Kapitel „Netzwerk-Übersicht: außen und innen“). Damit sieht der Support auf einen Blick, ob eine Freigabe am Internet-Router fehlt.

Ergänzen Sie dazu in eigenen Worten:

- Was genau haben Sie beobachtet, und was hatten Sie erwartet? Möglichst konkret, also lieber „die Anmeldung bei dieser einen Seite bricht ab" als „das Internet funktioniert nicht".
- Seit wann tritt es auf, und hat sich davor etwas geändert (neues Gerät, neue Einstellung, Umzug, Wechsel des Internet-Anbieters)?
- Betrifft es alle Geräte oder nur eines? Und tritt es immer auf oder nur manchmal?
- Welche Schritte aus Kapitel „Was tun, wenn …?“ haben Sie schon versucht, und was ist dabei passiert?
- Den genauen Wortlaut einer Fehlermeldung, falls eine erscheint. Ein Bildschirmfoto hilft ebenfalls.

> **Ein Fall, eine Nachricht**
>
> Beschreiben Sie in einer Anfrage nur ein Problem. Zwei unabhängige Beobachtungen in derselben Nachricht kosten meist mehr Zeit als zwei getrennte Anfragen, weil Rückfragen zum einen die Klärung des anderen aufhalten.

20.3 Protokolldateien herunterladen

Bei tiefer liegenden Fragen bittet der Support Sie zusätzlich um die Protokolldateien. Sie finden sie unter **Systemeinstellungen → System-Logs**. Die Schaltfläche **Alle Logdateien herunterladen**

packt sämtliche Protokolle in ein ZIP-Archiv, das Sie als Anhang mitsenden können. Daneben lassen sich die laufenden Protokolle der fünf wichtigsten Dienste live mitlesen: Proxy-Server, TrutzMail, TrutzMeeting, Web-Server und Paketmanager.

Dieselbe Seite zeigt außerdem die internen Systemmails, die das Betriebssystem der TrutzBox über bestimmte Vorgänge verschickt. Diese Mails hält die TrutzBox nur kurze Zeit vor und löscht sie danach selbsttätig.

> **Ausführliche Protokollierung nur kurz einschalten**
>
> Im Bereich **Debug Einstellungen** lässt sich die Protokollierung des Webfilters bis ins Detail hochdrehen. Der Support bittet gelegentlich darum, um einen schwer fassbaren Fehler einzukreisen. Schalten Sie sie danach unbedingt wieder aus: Auf dieser Stufe schreibt die TrutzBox sehr große Datenmengen, und der Datenträger kann volllaufen. Im Normalbetrieb steht die Einstellung auf der sparsamsten Stufe, und dabei sollte es bleiben.

Kommen Sie an die normale Oberfläche nicht mehr heran, gibt es einen zweiten Weg. In Webmin (Abschnitt „Webmin: der Experten-Zugang“) lässt sich auf Anleitung des Supports ein Systemstatus der TrutzBox abrufen und als Datei auf Ihren PC laden. Diese Datei können Sie, gegebenenfalls zusammen mit Protokolldateien, an Comidio senden. Nehmen Sie diesen Weg am besten nur nach Anleitung des Supports. Für eine Reparatur kann der Support Ihnen auch einen Befehl nennen, den Sie im Terminal im Browser eingeben (Abschnitt „Die Kommandozeile: Terminal und SSH“).

20.4 Wege zum Support

- **E-Mail:** die allgemeine Support-Adresse lautet support@trutzbox.de. Der übliche Weg, und der einzige, bei dem Sie Bericht und Protokolle gleich anhängen können. Verschicken Sie den Support-Bericht aus der Oberfläche heraus, brauchen Sie keine Adresse einzutragen: Die TrutzBox setzt sie selbst ein.
- **Forum:** forum.trutzbox.de mit dem Bereich „TrutzBox-Updates" und Antworten auf häufige Fragen. Oft steht die Antwort dort schon.
- **Telefon:** Ob Ihr Vertrag telefonische Unterstützung umfasst, und unter welcher Rufnummer, steht in Ihrer Auftragsbestätigung.

Auch vermutete Schwachstellen, ungewöhnliches Verhalten und allgemeine Sicherheitsfragen gehen an dieselbe Adresse oder ins Forum. Comidio bewertet solche Meldungen, entwickelt eine Korrektur und liefert sie mit den nächtlichen Software-Updates an alle TrutzBoxen aus; bei besonders kritischen Fällen auch außerhalb des Tagesrhythmus (Kapitel „Ankündigungen, Fragen und Meldungen“).

20.5 Das Forum sinnvoll nutzen

Das TrutzBox-Forum ist mehr als eine Fragestunde. Im Bereich „TrutzBox-Updates" beschreibt Comidio, was jedes Software-Update ändert und verbessert. Wer dort gelegentlich nachsieht, versteht Änderungen an der Oberfläche, ohne nachfragen zu müssen. Daneben stehen Antworten

auf häufige Fragen, und bei einer eigenen Frage lohnt zuerst die Suche: Vieles ist bereits beantwortet.

Bedenken Sie beim Schreiben im Forum, dass es öffentlich ist. Der Support-Bericht enthält Angaben zu Ihrer TrutzBox, die dort nicht hingehören. Solche Unterlagen schicken Sie besser per E-Mail an den Support.

20.6 Was Comidio nicht kann und nicht tut

Einen dauerhaften Fernwartungszugang von außen gibt es bewusst nicht. Niemand bei Comidio kann sich auf Ihre TrutzBox schalten, weder mit noch ohne Ihr Wissen. Das ist eine bewusste Entscheidung: Ein solcher Zugang wäre eine Tür, die immer offensteht, und damit genau die Art von Angriffsfläche, die die TrutzBox vermeiden soll.

Der Vollständigkeit halber: Prüft Ihre TrutzBox, ob sie von außen erreichbar ist, bittet sie einen Server von Comidio um Testpakete an ihre eigene Adresse (Kapitel „Netzwerk-Übersicht: außen und innen“). Ein Zugang ist das nicht. Der Server wird nur auf Bitte Ihrer TrutzBox tätig, meldet sich nirgends an und liest nichts.

Die Folge für den Alltag: Die Diagnose läuft über den Support-Bericht und die Protokolldateien, die Sie selbst übermitteln. Sie entscheiden also jedes Mal aufs Neue, was Ihre TrutzBox verlässt. Der Support arbeitet dafür mit gezielten Anleitungen, die Sie an Ihrer TrutzBox ausführen. Das kostet gelegentlich einen Nachrichtenwechsel mehr und ist den Gewinn an Kontrolle wert.

Zwei weitere Punkte gehören zur ehrlichen Erwartung: Comidio kennt Ihre Zugangsdaten nicht und kann sie nicht zurücksetzen; und die Passphrase Ihrer Sicherungsdatei kann auch Comidio nicht wiederherstellen (Kapitel „Was in der Sicherung steckt“). Verlorene Passwörter und Passphrasen sind verloren. Was in diesem Fall noch bleibt, beschreibt Kapitel „… das Passwort für das Admin-Panel nicht mehr bekannt ist“.

20.7 Hardware-Defekt und Tausch des Boot-Mediums

Geht die Hardware kaputt, ist das weniger dramatisch, als es klingt. Alle Schlüssel, mit denen sich Ihre TrutzBox und Ihre TrutzMail-Konten ausweisen, liegen ausschließlich als Software auf dem Boot-Medium. Es lässt sich deshalb in eine andere TrutzBox-Hardware einsetzen und unverändert in Betrieb nehmen. Ihre Identität wandert mit dem Medium, nicht mit dem Gehäuse.

Auch das interne Speichermedium selbst lässt sich bei einem Defekt austauschen. Ihre TrutzMail-Adressen hängen an Ihrer TrutzLegitimation, nicht an einem bestimmten Bauteil. Mit ihr reaktivieren Sie die Adressen auf dem neuen Medium (Kapitel „Adressen anlegen, löschen und reaktivieren“), und Ihre Mail-Partner erkennen Sie darunter wieder als dieselbe Person. Comidio erfährt dabei nicht mehr über Sie als vorher.

Nach einem Tausch des Speichermediums ist die TrutzBox zunächst leer und braucht ein frisches System. Das Zurücksetzen aus der Oberfläche scheidet dafür aus, denn auf dem neuen Medium gibt es noch keine Oberfläche. Das System spielen Sie deshalb mit dem Tank-Stick auf. Das können Sie komplett selbst erledigen; die Schritt-für-Schritt-Anleitung samt Bedeutung der LEDs steht in Kapitel „Der Ausnahmefall: ein komplettes Image“.

1. Melden Sie den Defekt beim Support und beschreiben Sie, was die LEDs an der Gerätefront anzeigen (Kapitel „… die TrutzBox überhaupt nicht mehr reagiert“).
2. Halten Sie Ihre Sicherungsdatei und deren Passphrase bereit sowie Ihre TrutzLegitimation.
3. Setzen Sie das neue System nach Anleitung auf und durchlaufen Sie das Setup erneut mit Ihrer TrutzLegitimation (Kapitel „TrutzBox einrichten (Setup)“).
4. Spielen Sie im Setup-Schritt „TrutzBox registrieren" über „Backup laden" Ihre Sicherung ein, bevor Sie registrieren (Kapitel „Wiederherstellen: im Betrieb oder im Setup“). Postfächer, Schlüssel und Einstellungen kehren damit zurück.
5. Nur wenn Sie keine Sicherung einspielen konnten: Erneuern Sie auf allen Geräten das TrutzBox-Root-Zertifikat (Kapitel „Das Root-Zertifikat installieren“). Mit Sicherung kehrt das bisherige Zertifikat zurück, und auf den Geräten ist nichts zu tun.

Ohne Sicherung sind Postfächer und Schlüssel verloren

Ihre Postfächer und die geheimen Schlüssel Ihrer TrutzMail-Konten gibt es nur einmal, und zwar auf Ihrer TrutzBox. Ohne Sicherung reaktivieren Sie Ihre TrutzMail-Adressen nach einem Hardware-Defekt zwar mit Ihrer TrutzLegitimation, aber mit leeren Postfächern und neuen Schlüsseln. Die TrutzBoxen Ihrer Partner holen den neuen Schlüssel selbst; PGP-Partner ohne TrutzBox brauchen dagegen Ihren neuen öffentlichen Schlüssel (Kapitel „Schlüssel und Zertifikate“). Legen Sie eine Sicherung an, solange die TrutzBox noch läuft, und bewahren Sie sie außerhalb der TrutzBox auf (Kapitel „Eine Sicherung anlegen“).

20.8 Das Speichermedium tauschen

Das interne Speichermedium der TrutzBox ist eine SSD-Karte, die in einer Halterung auf der Hauptplatine sitzt. Sie lässt sich mit einem Schraubendreher und etwas Ruhe selbst tauschen, etwa wenn die Karte defekt ist oder mehr Platz gebraucht wird. Der Ablauf entspricht der Einbauanleitung, die Comidio schon für die früheren TrutzBoxen herausgegeben hat.

Zwei Dinge vorweg

Statische Ladung: Eine SSD-Karte nimmt Schaden, wenn sie sich beim Anfassen entlädt. Berühren Sie deshalb erst ein geerdetes Metallteil, etwa einen Heizkörper, oder wenigstens mit beiden Händen das TrutzBox-Gehäuse, bevor Sie die neue Karte aus ihrer Tüte nehmen.

Stromlos arbeiten: Fahren Sie die TrutzBox vorher über das Energie-Menü der Oberfläche herunter (Kapitel „… die TrutzBox neu gestartet oder zurückgesetzt werden soll“) und ziehen Sie danach alle Kabel ab, auch das Netzteil. Am geöffneten Gerät wird nicht gearbeitet, solange Strom anliegt.

1. Die TrutzBox über **Energie → Herunterfahren** ausschalten, dann vom Strom trennen und alle übrigen Kabel abziehen.
2. Statische Ladung ableiten, dann die vier Gehäuseschrauben lösen und den Gehäusedeckel abziehen.

3. Die alte SSD-Karte lösen: Beide Sicherungsfedern vorsichtig nach hinten drücken, zur Gehäuserückseite hin. Die Karte hebt sich dabei leicht an.
4. Die gelöste Karte schräg nach oben aus der Halterung ziehen. Nicht verkanten und nicht mit Gewalt arbeiten.
5. Die neue Karte schräg nach unten ansetzen und mit sanftem Druck in die Halterung einführen.
6. Die Karte auf der freien Seite mit Gefühl nach unten drücken, bis sie hörbar in beide Sicherungsfedern einrastet.
7. Den Gehäusedeckel wieder aufschieben und die vier Schrauben eindrehen.
8. Kabel und Strom wieder anschließen.

Die TrutzBox ist nach dem Tausch leer und braucht ein frisches System. Das spielen Sie mit dem Tank-Stick auf (Kapitel „Der Ausnahmefall: ein komplettes Image“), danach durchlaufen Sie das Setup mit Ihrer TrutzLegitimation und spielen im Schritt „TrutzBox registrieren" über „Backup laden" Ihre Sicherung ein, bevor Sie registrieren (Kapitel „Wiederherstellen: im Betrieb oder im Setup“). Ihre TrutzMail-Adressen kehren damit zurück, denn sie hängen an Ihrer TrutzLegitimation und nicht an der getauschten Karte.

Mehr Platz bringt eine größere Karte, wenn Sie sie mit dem Tank-Stick ab V80 betanken oder die TrutzBox danach einmal zurücksetzen (Kapitel „System zurücksetzen (Werksreset)“). Beim ersten Start danach vergrößert die TrutzBox ihren Datenbereich selbst bis zum Ende der Karte. Betanken Sie die Karte mit einem älteren Image, bleibt der Datenbereich bis zum ersten Zurücksetzen bei rund 5,4 GB. Beachten Sie außerdem: Ein Zurücksetzen dauert auf einer größeren Karte deutlich länger.

> **Wenn Sie das nicht selbst machen möchten**
>
> Der Tausch ist keine Pflichtübung. Melden Sie sich beim Support (Abschnitt „Wege zum Support“), beschreiben Sie den Fehler und was die LEDs anzeigen; Comidio nennt Ihnen dann die passende Karte oder übernimmt den Tausch. Solange die TrutzBox noch läuft, legen Sie vorher unbedingt eine Sicherung an.

21 Das Root-Zertifikat installieren

Für den Grundschutz durch die TrutzBox brauchen Sie dieses Kapitel nicht: Der Webfilter TrutzContent arbeitet auf jedem Gerät, ohne dass dort irgendetwas installiert werden muss. Zwei Dinge verlangen aber ein zusätzliches Stück Vorbereitung, und zwar das **Root-Zertifikat** der TrutzBox. Dieses Kapitel erklärt, wann es gebraucht wird, warum, und wie Sie es auf Ihren Geräten installieren.

21.1 Wann Sie das Root-Zertifikat brauchen

Es gibt genau zwei Anlässe:

- **TrutzBrowse (Kapitel „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“):** Diese Zusatzfunktion entfernt identifizierende Merkmale aus dem Datenverkehr. Dafür muss die TrutzBox verschlüsselte Seiten kurz öffnen, prüfen und neu verschlüsseln. Ohne installiertes Root-Zertifikat zeigt der Browser dann bei jeder verschlüsselten Seite eine Warnung. Für Geräte mit eingeschaltetem TrutzBrowse ist das Zertifikat also Pflicht.
- **Programme, die sich mit der TrutzBox verbinden:** Ihr Mail-Programm holt Post vom Mail-Server der TrutzBox (Kapitel „TrutzMail: sichere E-Mail“), ein Chat-Programm meldet sich am Chat-Server an (Kapitel „TrutzChat und Videokonferenz“), und der Browser öffnet die Verwaltungsoberfläche unter `https://trutzbox`. In all diesen Fällen weist sich die TrutzBox mit einem Zertifikat aus, das sie selbst ausgestellt hat. Damit das Programm ihr glaubt, muss es das Root-Zertifikat kennen.

Nicht gebraucht wird es für den normalen Webfilter. TrutzContent prüft nur, *ob* eine Adresse aufgerufen werden darf, und muss dafür nicht in die übertragenen Daten hineinschauen. Verschlüsselte Verbindungen reicht die TrutzBox in diesem Fall unangetastet durch, samt dem Originalzertifikat der besuchten Seite. Deshalb schützt die TrutzBox auch Geräte, auf denen sich gar kein Zertifikat installieren lässt.

> **Für Neugierige: Was ein Root-Zertifikat eigentlich ist**
>
> Jede verschlüsselte Verbindung im Internet beruht auf Vertrauen: Ihr Browser glaubt einer Webseite nur dann, wenn deren Zertifikat von einer Stelle beglaubigt wurde, die er kennt. Diese obersten Beglaubigungsstellen heißen Root-Zertifikate, und ein paar Dutzend davon bringt jedes Betriebssystem ab Werk mit.
>
> Ihre TrutzBox ist eine solche Stelle, allerdings eine ganz private: Sie steht bei Ihnen zuhause oder in der Firma, ihr geheimer Schlüssel verlässt die TrutzBox nie, und beglaubigt wird damit ausschließlich, was Ihre eigene TrutzBox prüft. Das Root-Zertifikat zu installieren heißt also: Ihrem eigenen Gerät zu sagen, dass es Ihrer eigenen TrutzBox vertrauen darf.

21.2 Das Root-Zertifikat herunterladen

Menüpfad: Verwaltung → Allgemeine Einstellungen

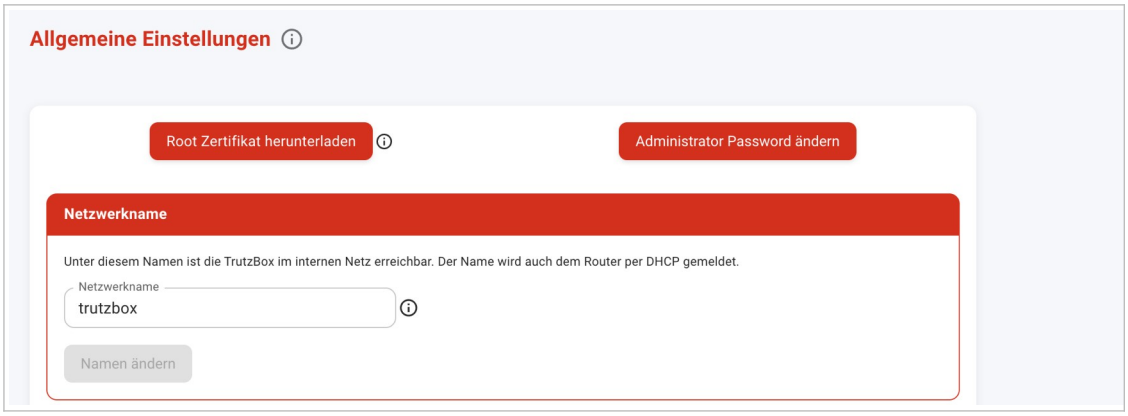


Abbildung 21-1: Oben links „Root Zertifikat herunterladen", daneben „Administrator Password ändern", darunter die Karte „Netzwerkname". (© 2026 Comidio GmbH)

1. Öffnen Sie im Admin-Panel **Verwaltung → Allgemeine Einstellungen**.
2. Klicken Sie auf **Root Zertifikat herunterladen**. Sie erhalten eine kleine Datei mit der Endung `.cer`.
3. Bringen Sie die Datei auf das Gerät, auf dem Sie sie brauchen. Am einfachsten laden Sie sie gleich am Zielgerät herunter, und zwar ohne Anmeldung am Admin-Panel: Öffnen Sie dort im Browser die Adresse `http://trutzbox/api/system/certificate`. Das funktioniert von jedem Gerät im internen Netz.

21.3 Installieren auf den gängigen Systemen

Jedes Betriebssystem führt eine Liste vertrauenswürdiger Stellen, und dort wird das Root-Zertifikat der TrutzBox eingetragen. Der Ablauf ist überall derselbe: Datei öffnen, in den Zertifikatsspeicher aufnehmen, Vertrauen bestätigen. Die genauen Bezeichnungen und Klickwege ändern sich allerdings mit jeder Systemversion. Dieses Handbuch nennt deshalb nur den Weg im Groben und verweist für die tagesaktuellen Schritte auf den jeweiligen Hersteller.

System	Der Weg im Groben	Aktuelle Anleitung
Windows	Zertifikat öffnen und unter „Vertrauenswürdige Stammzertifizierungsstellen" importieren. Das Werkzeug dafür heißt „Benutzerzertifikate verwalten" und ist über die Suche im Startmenü zu finden.	support.microsoft.com
Android	Auf die heruntergeladene Datei tippen, einen Namen vergeben (etwa „TrutzBox") und als Verwendungszweck „VPN und Apps" wählen.	support.google.com/android
macOS	Doppelklick öffnet die Schlüsselbundverwaltung. Das Zertifikat in den Schlüsselbund „System" legen, dort öffnen und das Vertrauen auf „Immer vertrauen" stellen.	support.apple.com
iPhone und iPad	Die Datei wird als Profil geladen und in den Einstellungen installiert. Danach ist in einem zweiten Schritt das volle	support.apple.com

System	Der Weg im Groben	Aktuelle Anleitung
	Vertrauen für das Zertifikat einzuschalten.	

Auf iPhone und iPad sind es zwei Schritte

Nach dem Installieren des Profils ist das Zertifikat zwar vorhanden, aber noch nicht wirksam. Erst das Einschalten des vollen Vertrauens in den Zertifikatseinstellungen macht es gültig. Dieser zweite Schritt wird häufig übersehen und ist die mit Abstand häufigste Ursache dafür, dass es auf einem Apple-Gerät nicht funktioniert.

21.4 Programme mit eigenem Zertifikatsspeicher

Die meisten Programme benutzen den Zertifikatsspeicher des Betriebssystems; für sie genügt der Import aus dem vorigen Abschnitt. Die Software von Mozilla verwaltet ihre Zertifikate dagegen selbst: Der Browser **Firefox** und das Mail-Programm **Thunderbird** brauchen das Root-Zertifikat zusätzlich in ihren eigenen Einstellungen, sonst warnen sie weiterhin.

	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	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).																							

Abbildung 21-2: Welche Programme den Zertifikatsspeicher des Systems nutzen und welche einen eigenen führen. (© 2026 Comidio GmbH)

In beiden Programmen führt der Weg über die Einstellungen zum Bereich **Datenschutz & Sicherheit** und dort zur Zertifikatsverwaltung; importiert wird unter den Zertifizierungsstellen, mit dem Häkchen für das Identifizieren von Webseiten. Die aktuelle Anleitung steht unter support.mozilla.org.

21.5 Wenn sich kein Zertifikat installieren lässt

Auf vielen Geräten gibt es schlicht keine Möglichkeit, ein eigenes Zertifikat zu hinterlegen: Fernseher, Kameras, Thermostate, Spielkonsolen. Auch auf Geräten von Gästen möchte man in der Regel nicht eingreifen. Das ist kein Problem, es hat nur eine Konsequenz:

- **Schalten Sie TrutzBrowse für diese Geräte aus** (Kapitel „TrutzBrowse je Gerät einschalten“). Sonst schlagen deren verschlüsselte Verbindungen fehl.
- **Alles andere wirkt weiter:** Der Webfilter TrutzContent, die Firewall, der Angriffsschutz und die Erfassung im Monitor arbeiten unabhängig vom Zertifikat. Gerade bei Fernsehern und Haustechnik ist der Filter nach Adressen ohnehin das wirksamere Mittel.

Wird die TrutzBox im halböffentlichen Betrieb eingesetzt, etwa in einem Seniorenheim oder einer Pension mit vielen fremden Geräten, achten Sie darauf, dass unter **Verwaltung → Geräte** in der Zeile **Standard für neu erkannte Geräte:** der Schalter **TrutzBrowse** aus bleibt. So ist er ab Werk eingestellt (Kapitel „Neue Geräte erscheinen automatisch“).

21.6 Nach einem Zurücksetzen der TrutzBox

Wird die TrutzBox auf den Werkszustand zurückgesetzt (Kapitel „System zurücksetzen (Werksreset)“) und ohne eingespielte Sicherung neu eingerichtet, erzeugt sie ein neues Root-Zertifikat. Das alte wird damit ungültig. Löschen Sie es auf allen Geräten aus dem Zertifikatsspeicher und importieren Sie anschließend das neue, sonst zeigen Browser und Mail-Programme Warnungen an. Denken Sie dabei auch an Firefox und Thunderbird mit ihren eigenen Speichern.

Häufige Fragen zum Root-Zertifikat

Ist es gefährlich, ein eigenes Root-Zertifikat zu installieren?

Es ist ein Vertrauensvorschuss, und zwar an ein Gerät, das Ihnen selbst gehört und bei Ihnen steht. Der geheime Schlüssel dazu verlässt die TrutzBox nie. Anders als bei einem Dienst im Internet können Sie hier genau sehen, wem Sie vertrauen: sich selbst.

Muss ich es auf jedem Gerät installieren?

Nur auf denen, für die einer der beiden Anlässe aus Abschnitt „Wann Sie das Root-Zertifikat brauchen“ zutrifft. Ein Fernseher, der einfach nur gefiltert ins Internet soll, braucht es nicht.

Der Browser warnt trotz installiertem Zertifikat. Woran liegt das?

Meist am eigenen Zertifikatsspeicher: Firefox und Thunderbird brauchen den Import in ihren eigenen Einstellungen. Auf iPhone und iPad fehlt oft der zweite Schritt, das Einschalten des vollen Vertrauens. Und nach einem Zurücksetzen der TrutzBox liegt schlicht das alte Zertifikat auf dem Gerät.

22 Mail-Programme für TrutzMail einrichten

Dieses Kapitel zeigt für die gebräuchlichen Mail-Programme, wie Sie ein TrutzMail-Konto anlegen. Die Angaben sind in jedem Programm dieselben. Sie stehen im ersten Abschnitt, die Abschnitte danach nennen je Programm den Weg dorthin. Was TrutzMail ist und wie Sie eine Adresse anlegen, steht in Kapitel „TrutzMail: sichere E-Mail“.

22.1 Die Angaben für jedes Mail-Programm

Diese fünf Angaben verlangt jedes Mail-Programm:

Angabe	Wert
Benutzername	die TrutzMail-Adresse
Passwort	das Passwort des TrutzMail-Accounts
Server für Eingang und Ausgang	der Name Ihrer TrutzBox, ab Werk trutzbox
Eingang	IMAP, Port 993, SSL/TLS
Ausgang	SMTP, Port 587, STARTTLS

Dieselben Angaben zeigt die TrutzBox selbst, mit ihrem tatsächlichen Namen: Öffnen Sie im Admin-Panel **Verwaltung → Benutzer** und klicken Sie auf das „i" hinter der TrutzMail-Adresse des Benutzers.

Ob Sie die Angaben eintragen müssen, hängt vom Mail-Programm ab:

- **Thunderbird** (am Computer und auf Android) findet die Angaben zu einer TrutzMail-Adresse selbst. Sie geben nur Name, Adresse und Passwort ein.
- **Apple Mail, Outlook und die Mail-Apps der Android-Hersteller** finden die Angaben nicht selbst. Dort tragen Sie die Werte aus der Tabelle von Hand ein.

Zwei Voraussetzungen gelten für jedes Programm:

- **Das Gerät vertraut dem Root-Zertifikat der TrutzBox.** Das Mail-Programm verbindet sich direkt mit der TrutzBox und prüft dabei ihr Zertifikat. Fehlt das Root-Zertifikat, meldet das Programm eine Zertifikatswarnung oder verweigert die Verbindung. Wie Sie es installieren, steht in Kapitel „Das Root-Zertifikat installieren“.
- **Das Gerät erreicht die TrutzBox unter ihrem Namen.** Der Name gilt im Netz der TrutzBox, im lokalen Netz am Internet-Router und unterwegs über TrutzVPN (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Ohne VPN ist das Postfach von unterwegs nicht erreichbar.

> **Bezeichnungen wechseln mit der Programmversion**
>
> Die Hersteller benennen Menüs und Schaltflächen von Version zu Version um. Die folgenden Abschnitte nennen deshalb den Weg im Groben. Entscheidend sind die fünf Angaben aus der Tabelle: Wo immer das Programm danach fragt, tragen Sie diese Werte ein.

22.2 Thunderbird einrichten

Thunderbird führt einen eigenen Zertifikatsspeicher. Importieren Sie das Root-Zertifikat deshalb zuerst in Thunderbird selbst (Abschnitt „Programme mit eigenem Zertifikatsspeicher“).

Der kurze Weg: Thunderbird fragt die Einstellungen für eine TrutzMail-Adresse selbst ab.

1. Ein neues E-Mail-Konto anlegen.
2. Ihren Namen, die TrutzMail-Adresse und das Passwort eintragen und fortfahren.
3. Thunderbird zeigt die gefundenen Einstellungen: IMAP und SMTP mit dem Server `trutzbox`. Mit **Fertig** übernehmen.

Von Hand: Findet Thunderbird nichts oder trägt Ihre TrutzBox einen eigenen Namen, wählen Sie im selben Fenster die manuelle Einrichtung:

1. Bei Posteingang das Protokoll IMAP wählen, als Server den Namen Ihrer TrutzBox eintragen, Port 993, Verbindungssicherheit SSL/TLS, Authentifizierung „Passwort, normal".
2. Bei Postausgang denselben Server eintragen, Port 587, Verbindungssicherheit STARTTLS, Authentifizierung „Passwort, normal".
3. Als Benutzernamen an beiden Stellen die TrutzMail-Adresse eintragen.
4. Die Einstellungen prüfen lassen und mit **Fertig** übernehmen.

22.3 Apple Mail auf dem Mac einrichten

1. In Mail einen Account hinzufügen und als Art „Anderer Mail-Account" wählen.
2. Ihren Namen, die TrutzMail-Adresse und das Passwort eintragen und anmelden.
3. Mail meldet, dass es den Account nicht überprüfen kann, und zeigt weitere Felder. Als Benutzernamen die TrutzMail-Adresse eintragen, als Accounttyp IMAP wählen.
4. Als Server für eintreffende und für ausgehende E-Mails jeweils den Namen Ihrer TrutzBox eintragen und anmelden.

Die Ports wählt Mail selbst. Fragt das Programm danach, gelten die Werte aus der Tabelle.

22.4 Mail auf iPhone und iPad einrichten

1. In den Einstellungen des Geräts bei Mail einen Account hinzufügen und „Andere" wählen, dann „Mail-Account hinzufügen".
2. Ihren Namen, die TrutzMail-Adresse und das Passwort eintragen und weitergehen.
3. IMAP wählen. Beim Server für eintreffende E-Mails und beim Server für ausgehende E-Mails jeweils als Hostname den Namen Ihrer TrutzBox, als Benutzernamen die TrutzMail-Adresse und das Passwort eintragen.
4. Weitergehen und sichern.

> **Erst das Root-Zertifikat, in zwei Schritten**
>
> Auf iPhone und iPad ist das Root-Zertifikat erst wirksam, wenn nach dem Installieren des Profils auch das volle Vertrauen eingeschaltet ist (Abschnitt „Installieren auf den gängigen Systemen“).

Fehlt dieser zweite Schritt, lässt sich der Account nicht überprüfen.

22.5 Mail-App auf Android einrichten

Auf Android-Geräten ist je nach Hersteller eine andere Mail-App vorinstalliert. Der Ablauf ist in allen ähnlich:

1. In der Mail-App ein Konto hinzufügen und als Art „Sonstige" oder „Andere" wählen.
2. Die TrutzMail-Adresse eintragen und als Kontotyp IMAP wählen.
3. Das Passwort eintragen.
4. Beim Eingangsserver den Namen Ihrer TrutzBox eintragen, Port 993, Sicherheitstyp SSL/TLS. Benutzername ist die TrutzMail-Adresse.
5. Beim Ausgangsserver denselben Namen eintragen, Port 587, Sicherheitstyp STARTTLS. Anmeldung erforderlich, mit derselben Adresse und demselben Passwort.

Thunderbird gibt es auch für Android. Es fragt die Einstellungen für eine TrutzMail-Adresse selbst ab, wie im Abschnitt „Thunderbird einrichten“ beschrieben.

22.6 Outlook einrichten

Nur das klassische Outlook verwenden

Das neue Outlook für Windows und die Outlook-App für Telefon und Tablet holen die Post nicht selbst ab. Das übernehmen Server von Microsoft, und dort wird auch das Passwort hinterlegt. Diese Server erreichen Ihre TrutzBox nicht, und Ihr Passwort läge außerhalb Ihrer TrutzBox. Verwenden Sie für TrutzMail das klassische Outlook oder ein anderes Mail-Programm.

Im klassischen Outlook richten Sie das Konto von Hand ein:

1. Ein Konto hinzufügen und die TrutzMail-Adresse eintragen.
2. Die erweiterten Optionen öffnen, die manuelle Einrichtung wählen und fortfahren.
3. Als Kontotyp IMAP wählen.
4. Bei eingehender E-Mail den Namen Ihrer TrutzBox eintragen, Port 993, Verschlüsselung SSL/TLS.
5. Bei ausgehender E-Mail denselben Namen eintragen, Port 587, Verschlüsselung STARTTLS.
6. Das Passwort eintragen und verbinden.

22.7 Wenn das Mail-Programm keine Verbindung bekommt

- **Zertifikatswarnung, Identität des Servers nicht überprüfbar:** Dem Gerät fehlt das Root-Zertifikat der TrutzBox, oder das Vertrauen ist nicht eingeschaltet (Kapitel „Das Root-Zertifikat installieren“).

- **Server nicht gefunden:** Das Gerät erreicht die TrutzBox unter diesem Namen nicht. Vergleichen Sie den Namen mit der Anzeige hinter dem „i" unter **Verwaltung → Benutzer**. Unterwegs verbinden Sie zuerst TrutzVPN.
- **Anmeldung abgelehnt:** Benutzername ist die vollständige TrutzMail-Adresse. Das Passwort ist das des Benutzers, nicht das des Admin-Panels.

23 Chat-Programme für TrutzChat einrichten

Dieses Kapitel zeigt, wie Sie TrutzChat statt im Browser in einem Chat-Programm benutzen. TrutzChat spricht den offenen Chat-Standard XMPP, den viele Programme auf allen Systemen beherrschen. Was TrutzChat kann und wie der Web-Chat funktioniert, steht in Kapitel „TrutzChat und Videokonferenz“.

23.1 Die Angaben für jedes Chat-Programm

Diese Angaben verlangt jedes Chat-Programm:

Angabe	Wert
Konto-Kennung (Jabber-ID)	die TrutzMail-Adresse
Passwort	das Passwort des TrutzMail-Accounts
Server	der Name Ihrer TrutzBox, ab Werk trutzbox
Port	5222, die Vorgabe der Programme

Zwei Voraussetzungen gelten für jedes Programm:

- **Das Gerät erreicht die TrutzBox unter ihrem Namen.** Das gilt im Netz der TrutzBox und unterwegs über TrutzVPN (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“). Aus dem Internet nimmt die TrutzBox Chat-Programme nicht an, eine Freigabe am Router ist nicht vorgesehen.
- **Das Gerät vertraut dem Root-Zertifikat der TrutzBox.** Das Programm verbindet sich verschlüsselt mit der TrutzBox und prüft dabei ihr Zertifikat (Kapitel „Das Root-Zertifikat installieren“).

> **Der Server steht oft in den erweiterten Einstellungen**
> Viele Programme leiten den Server aus der Adresse ab und versuchen es dann bei „comidio.email“. Das ist für TrutzChat falsch. Suchen Sie beim Anlegen des Kontos nach einem Feld wie „Server“, „Hostname“ oder „Verbindungsserver“, oft hinter „Erweitert“ oder „Erweiterte Einstellungen“, und tragen Sie dort den Namen Ihrer TrutzBox ein.

23.2 Empfohlene Chat-Programme

Comidio empfiehlt je Betriebssystem diese Programme. Eine vollständige Übersicht weiterer XMPP-Programme führt die Wikipedia unter de.wikipedia.org/wiki/Liste_von_XMPP-Clients.

System	Empfohlene Programme
Windows und Linux	Gajim
macOS	BeagleIM, Monal
iPhone und iPad	Monal, Siskin IM
Android	Conversations

23.3 Ein Chat-Programm einrichten

Der Ablauf ist in allen Programmen ähnlich:

1. Das Programm installieren und darin ein neues Konto anlegen. Wählen Sie dabei ein vorhandenes Konto, nicht die Registrierung eines neuen.
2. Als Konto-Kennung die TrutzMail-Adresse und als Passwort das Passwort des TrutzMail-Accounts eintragen.
3. Den Server prüfen und auf den Namen Ihrer TrutzBox stellen. Den Port 5222 unverändert lassen.
4. Verbinden. Danach einen Kontakt über dessen TrutzMail-Adresse hinzufügen.

In einem Programm lassen sich auch mehrere TrutzMail-Adressen gleichzeitig einrichten. Unterwegs verbinden Sie zuerst TrutzVPN, danach arbeitet das Programm mit demselben Servernamen wie im Netz der TrutzBox.

23.4 Wenn das Chat-Programm keine Verbindung bekommt

- **Zertifikatswarnung:** Dem Gerät fehlt das Root-Zertifikat der TrutzBox (Kapitel „Das Root-Zertifikat installieren“).
- **Server nicht gefunden oder Zeitüberschreitung:** Im Feld für den Server steht noch „comidio.email“, oder das Gerät ist nicht im Netz der TrutzBox. Unterwegs verbinden Sie zuerst TrutzVPN.
- **Anmeldung abgelehnt:** Konto-Kennung ist die vollständige TrutzMail-Adresse. Das Passwort ist das des Benutzers, nicht das des Admin-Panels.

24 VPN-Apps für TrutzVPN einrichten

Dieses Kapitel zeigt je Betriebssystem, wie Sie einen Zugang für TrutzVPN auf ein Gerät bringen. Wie Sie TrutzVPN auf der TrutzBox einrichten und einen Zugang anlegen, steht in Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“.

Welche App Sie brauchen, hängt vom Tunnel ab, der auf Ihrer TrutzBox läuft. Das zeigt Karte 2 auf der Seite **Netzwerk → Fernzugriff**:

- **WireGuard** (die Vorgabe): die WireGuard-App und je Gerät ein Zugang, als Bildcode oder als Datei mit der Endung `.conf`.
- **OpenVPN:** ein OpenVPN-Programm und je Benutzer ein Profil mit der Endung `.ovpn`.

> **Bezeichnungen wechseln mit der App-Version**
> Die Apps ändern sich mit jeder Version ein wenig. Die folgenden Abschnitte nennen deshalb den Weg im Groben. Maßgeblich sind die Anleitungen der Hersteller, für WireGuard unter wireguard.com/install.

24.1 WireGuard unter Windows

Die App **WireGuard für Windows** von wireguard.com, kostenlos unter wireguard.com/install. Sie liest keinen Bildcode.

1. Die App installieren und öffnen.
2. *„Tunnel aus Datei importieren"* wählen und die `.conf`-Datei öffnen.
3. Die Verbindung mit *„Aktivieren"* neben dem Tunnelnamen starten.

24.2 WireGuard unter macOS

WireGuard aus dem Mac App Store. Auch sie liest keinen Bildcode.

1. Die App installieren und öffnen.
2. *„Tunnel aus Datei importieren"* wählen und die `.conf`-Datei öffnen.
3. Beim ersten Einschalten fragt macOS einmalig, ob die App VPN-Verbindungen einrichten darf. Das bestätigen Sie mit Ihrem Anmeldekennwort.

24.3 WireGuard auf iPhone und iPad

WireGuard aus dem App Store.

1. In der App auf *„Hinzufügen"* tippen und *„Aus QR-Code erstellen"* wählen.
2. Den Bildcode von der Fernzugriff-Seite abfotografieren.
3. Beim ersten Verbinden fragt das Gerät einmalig, ob die App VPN-Konfigurationen hinzufügen darf. Das bestätigen Sie.

24.4 WireGuard auf Android

WireGuard aus dem Play Store.

1. In der App auf das Pluszeichen tippen und *„Aus QR-Code scannen"* wählen.
2. Den Bildcode einlesen. Wer lieber die Datei nimmt, kopiert sie auf das Gerät und wählt *„Aus Datei oder Archiv importieren"*.
3. Beim ersten Start fragt Android einmalig um Erlaubnis für die VPN-Verbindung. Das bestätigen Sie.

24.5 WireGuard unter Linux

WireGuard steckt im Linux-Kern; es fehlen nur die Werkzeuge, unter Debian und Ubuntu das Paket `wireguard`.

1. Die `.conf`-Datei als `/etc/wireguard/trutzbox.conf` ablegen.
2. Mit `wg-quick up trutzbox` einschalten, mit `wg-quick down trutzbox` wieder aus.

Der NetworkManager kann die Datei ebenfalls importieren.

24.6 Geräte mit OpenVPN einrichten

Läuft auf Ihrer TrutzBox OpenVPN, brauchen Sie ein VPN-Programm, das OpenVPN-Profile versteht. Das Vorgehen ist überall gleich: Programm installieren, die `.ovpn`-Datei importieren, Verbindung einschalten. Bewährt haben sich:

- **Windows: OpenVPN Connect** vom OpenVPN-Hersteller, kostenlos unter openvpn.net/client. Nach der Installation genügt ein Doppelklick auf die `.ovpn`-Datei oder deren Import über „Upload File". Die Verbindung starten Sie über den Schalter neben dem Profilnamen. Anleitungen: openvpn.net/connect-docs.
- **macOS:** das freie Programm **Tunnelblick** (tunnelblick.net). Dort ziehen Sie die Profildatei einfach auf das Programmsymbol. Alternativ funktioniert auch hier OpenVPN Connect.
- **iPhone und iPad: OpenVPN Connect** aus dem App Store. Übertragen Sie die Profildatei per AirDrop oder über die Dateien-App, tippen Sie sie an und wählen Sie „In OpenVPN öffnen". Beim ersten Verbinden fragt das Gerät einmalig, ob die App VPN-Konfigurationen hinzufügen darf. Das bestätigen Sie.
- **Android: OpenVPN Connect** aus dem Play Store. Kopieren Sie die Profildatei auf das Gerät (USB-Kabel oder Dateien-App), öffnen Sie die App und importieren Sie die Datei über „Upload File". Auch Android fragt beim ersten Start einmalig um Erlaubnis für die VPN-Verbindung.
- **Linux:** Der NetworkManager importiert die Profildatei direkt.

> **Andere VPN-Programme?**
>
> Jedes Programm, das den OpenVPN-Standard beherrscht, funktioniert. Eine Übersicht weiterer Programme: de.wikipedia.org/wiki/OpenVPN. Die in Windows, iOS und Android fest eingebauten VPN-Funktionen unterstützen OpenVPN dagegen nicht; deshalb braucht es das zusätzliche Programm.

24.7 Wenn die VPN-App keine Verbindung bekommt

- **Die App bleibt beim Verbinden hängen und zeigt keinen Fehler:** Das ist bei WireGuard der Normalfall, wenn die Anfrage nicht bis zur TrutzBox kommt. Prüfen Sie die Erreichbarkeit auf der Fernzugriff-Seite (Abschnitt „Wenn es nicht klappt“).
- **Verbindung klappt nur unterwegs nicht:** Testen Sie über Mobilfunk bei ausgeschaltetem WLAN. Im eigenen Netz sagt ein Test nichts über den Weg von außen.
- **Zwei Geräte stören sich gegenseitig:** Derselbe WireGuard-Zugang steckt auf zwei Geräten. Legen Sie je Gerät einen eigenen Zugang an (Abschnitt „Schritt 5: Zugänge für die WireGuard-App anlegen“).

25 Den Proxy-Mode am Gerät einrichten

Dieses Kapitel zeigt je Betriebssystem, wo Sie die TrutzBox als Proxy eintragen. Was der Proxy-Mode ist, wann er sich eignet und was er nicht leistet, steht in Abschnitt „Weg 2: Gerät im Proxy-Mode betreiben“.

25.1 Die Angaben für jedes Gerät

Sie haben zwei Möglichkeiten. Die erste ist empfohlen:

Möglichkeit	Was Sie eintragen
Automatische Proxy-Konfiguration (empfohlen)	die Adresse http://trutzbox/api/proxy/pac
Proxy von Hand	Server trutzbox, Port 8081, für HTTP und für HTTPS

- **Im Betriebssystem eintragen, nicht im Browser.** Dann gilt der Proxy für alle Programme des Geräts.
- **Auf Smartphone und Tablet gilt der Eintrag nur für ein WLAN.** Sie nehmen ihn beim WLAN des Internet-Routers vor. Im Mobilfunk und in fremden WLANs gilt er nicht. Für unterwegs ist deshalb TrutzVPN der richtige Weg (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

> **Bezeichnungen wechseln mit der Version**
> Die Hersteller benennen Menüs von Version zu Version um. Die folgenden Abschnitte nennen deshalb den Weg im Groben. Entscheidend sind die Angaben aus der Tabelle.

25.2 Proxy unter Windows

1. Öffnen Sie **Einstellungen** → **Netzwerk und Internet** → **Proxy**.
2. Unter **Automatische Proxyeinrichtung** bei **Setupskript verwenden** auf **Einrichten** klicken, den Schalter einschalten und als Skriptadresse `http://trutzbox/api/proxy/pac` eintragen. Speichern.

Von Hand: Unter **Manuelle Proxyeinrichtung** bei **Proxyserver verwenden** auf **Einrichten** klicken, den Schalter einschalten, Adresse `trutzbox` und Port `8081` eintragen und speichern.

25.3 Proxy unter macOS

1. Öffnen Sie **Systemeinstellungen** → **Netzwerk** und wählen Sie die Verbindung, über die der Mac ins Internet geht, etwa WLAN oder Ethernet.
2. Klicken Sie auf **Details** und dann auf **Proxies**.
3. **Automatische Proxy-Konfiguration** einschalten und als URL `http://trutzbox/api/proxy/pac` eintragen. Mit **OK** übernehmen.

Von Hand: Statt der automatischen Konfiguration **Web-Proxy (HTTP)** und **Sicherer Web-Proxy (HTTPS)** einschalten und bei beiden Server `trutzbox` und Port `8081` eintragen.

25.4 Proxy auf iPhone und iPad

1. Öffnen Sie **Einstellungen** → **WLAN** und tippen Sie neben dem WLAN des Internet-Routers auf das „i“.
2. Ganz unten **Proxy konfigurieren** öffnen und **Automatisch** wählen.
3. Als URL `http://trutzbox/api/proxy/pac` eintragen und **Sichern**.

Von Hand: **Manuell** wählen, Server `trutzbox` und Port `8081` eintragen.

25.5 Proxy auf Android

Je nach Hersteller heißen die Menüs etwas anders. Der Ablauf ist ähnlich:

1. Öffnen Sie in den Einstellungen die WLAN-Liste und dort die Einstellungen des WLANs Ihres Internet-Routers, meist über das Zahnrad oder durch langes Tippen.
2. Die erweiterten Optionen öffnen und bei **Proxy** den Eintrag **Automatisch** oder **Proxy Auto-Config** wählen.
3. Als PAC-Adresse `http://trutzbox/api/proxy/pac` eintragen und speichern.

Von Hand: Bei **Proxy** den Eintrag **Manuell** wählen, Hostname `trutzbox` und Port `8081` eintragen.

25.6 Proxy unter Linux

Auf einem Linux-Rechner mit der Oberfläche GNOME:

1. Öffnen Sie **Einstellungen** → **Netzwerk** → **Netzwerk-Proxy**.
2. **Automatisch** wählen und als Konfigurations-URL `http://trutzbox/api/proxy/pac` eintragen.

Von Hand: **Manuell** wählen und beim HTTP-Proxy und beim HTTPS-Proxy `trutzbox` mit Port `8081` eintragen. Andere Oberflächen haben eine ähnliche Einstellung in ihren Netzwerk-Einstellungen.

25.7 Firefox

Firefox kann eine eigene Proxy-Einstellung haben. Damit er den Eintrag des Betriebssystems übernimmt, öffnen Sie in Firefox **Einstellungen** → **Allgemein** → **Verbindungs-Einstellungen** und wählen *„Die Proxy-Einstellungen des Systems verwenden"*. Tragen Sie den Proxy nur in Firefox ein, ist allein Firefox geschützt.

25.8 Prüfen, ob der Proxy-Mode wirkt

- Rufen Sie auf dem Gerät eine Internet-Seite auf. Unter **Verwaltung** → **Geräte** steht das Gerät danach in der Spalte **Verbindung** als „Proxy (extern)".
- Bleibt es bei „Nicht verbunden (extern)", prüfen Sie den Eintrag am Gerät auf Tippfehler und ob er beim richtigen WLAN oder bei der richtigen Verbindung steht.

26 Ports und Freigaben am Internet-Router

Dieses Kapitel fasst zusammen, welche Ports die TrutzBox benutzt, welche davon am Internet-Router freigegeben werden und wie das in einer FRITZ!Box aussieht. Ein **Port** ist die Nummer, unter der ein Dienst auf einem Gerät erreichbar ist. Eine **Freigabe** (auch Portweiterleitung) sagt dem Router, dass er Verbindungen aus dem Internet auf diesem Port an die TrutzBox weiterreichen soll.

26.1 Welche Ports die TrutzBox braucht

Freigaben am Internet-Router. Nur diese Ports gehören am Router freigegeben, und nur für die Dienste, die Sie nutzen:

Wofür	Protokoll	Port außen	Port an der TrutzBox	Abschnitt
TrutzVPN von unterwegs	UDP	1194	1194	„Schritt 2: Portweiterleitung am Internet-Router“
Videokonferenz über IPv4	TCP	443	9082	„Reiter Videokonferenz: einmalig einrichten“
Videokonferenz über IPv6	TCP	443	443	„Die IPv6-Freigabe in einer FRITZ!Box“
Videokonferenz, Bild und Ton	UDP	9083	9083	„Reiter Videokonferenz: einmalig einrichten“

Nicht freigeben. Diese Ports benutzt die TrutzBox nur im eigenen Netz und über TrutzVPN. Am Router werden sie nicht freigegeben:

Port	Wofür
TCP 80 und 443	Admin-Panel, Webmail, Web-Chat
TCP 993	Mail-Programme, Eingang (IMAP)
TCP 587	Mail-Programme, Ausgang (SMTP)
TCP 5222	Chat-Programme (XMPP)
TCP 8081	Proxy-Mode
TCP 10000	Webmin
TCP 22	Kommandozeile (SSH)

Nicht sperren. Die TrutzBox fragt Namen im Internet verschlüsselt über **TCP 853** ab. Das ist keine Freigabe, sondern eine Verbindung von innen nach außen. Sperrt der Router sie, weicht die TrutzBox auf unverschlüsselte Abfragen aus und meldet das (Abschnitt „Betriebszustand: die Karten im Einzelnen“).

26.2 Beispiel: die Freigaben in einer FRITZ!Box

In einer FRITZ!Box legen Sie alle Freigaben für die TrutzBox auf einer Seite an. So gehen Sie vor:

1. Öffnen Sie in der Benutzeroberfläche der FRITZ!Box **Internet**, dann **Freigaben** und den Reiter **Portfreigaben**.
2. Klicken Sie auf **Gerät für Freigaben hinzufügen** und wählen Sie unter **Gerät** die TrutzBox aus.
3. Klicken Sie auf **Neue Freigabe**. Im Fenster **Freigabe anlegen** wählen Sie **Portfreigabe** und unter **Anwendung** den Eintrag **Andere Anwendung**.
4. Tragen Sie eine **Bezeichnung** ein, etwa „TrutzVPN“, und die Werte aus einer Zeile der Tabelle unten. Wählen Sie unten den **Internetzugriff** wie in der letzten Spalte angegeben. Bestätigen Sie mit **OK**.
5. Wiederholen Sie die Schritte 3 und 4 für jede weitere Zeile, die Sie brauchen. Sichern Sie zum Schluss mit **Übernehmen**.

Wofür	Protokoll	Port an Gerät	Port extern gewünscht	Internetzugriff
TrutzVPN von unterwegs	UDP	1194	1194	über IPv4 und IPv6
Videokonferenz	TCP	9082	443	über IPv4
Videokonferenz	UDP	9083	9083	über IPv4 und IPv6

Menüpfad: FRITZ!Box: Internet → Freigaben → Portfreigaben

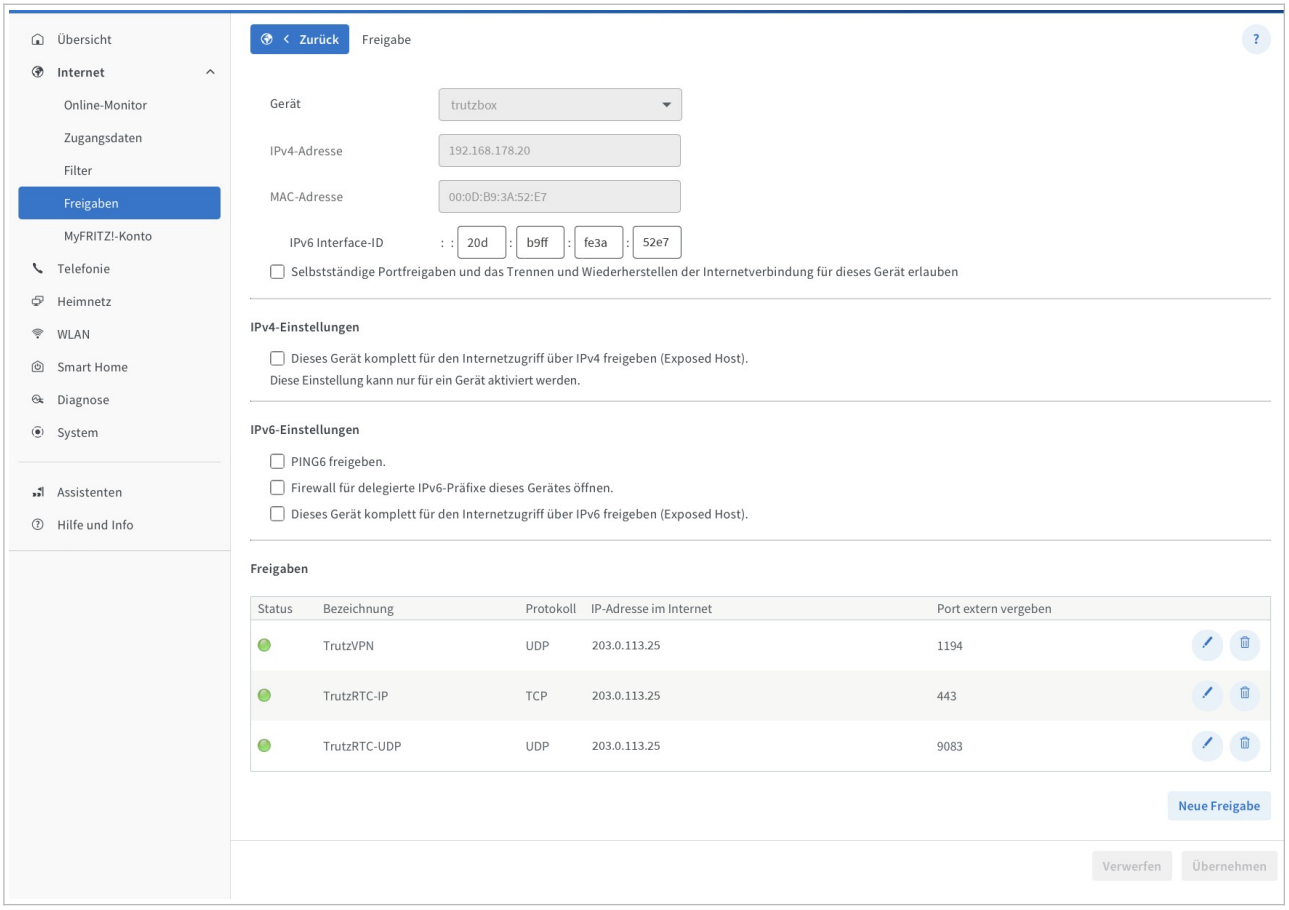


Abbildung 26-1: Die Seite einer FRITZ!Box mit den drei fertigen Freigaben für die TrutzBox. Die Spalte „Port extern vergeben“ zeigt den Port, den die FRITZ!Box nach außen öffnet. (© 2026 Comidio GmbH)

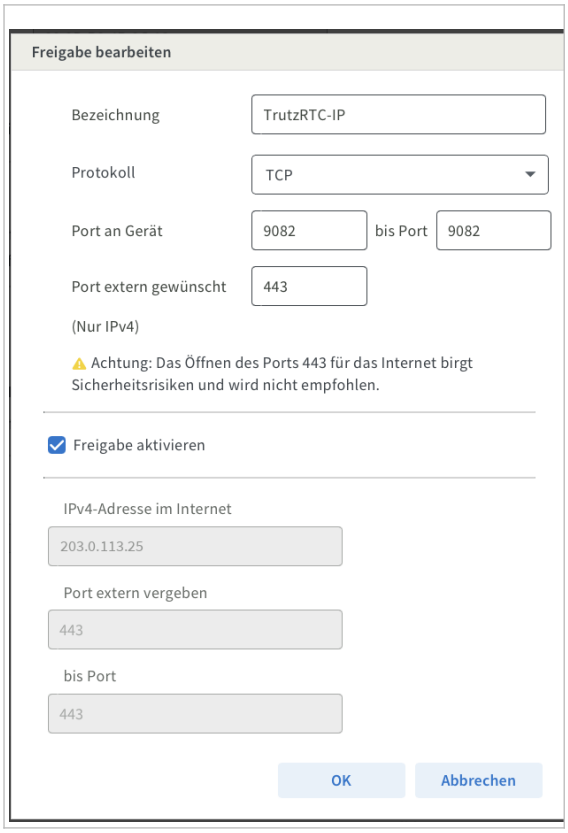


Abbildung 26-2: Die Freigabe für die Videokonferenz geöffnet: außen Port 443, an der TrutzBox Port 9082. (© 2026 Comidio GmbH)

Zwei verschiedene Zahlen bei Port 443

Bei der Freigabe für die Videokonferenz kommt die Verbindung von außen auf Port **443** an, die FRITZ!Box reicht sie an Port **9082** der TrutzBox weiter. Deshalb stehen in **Port an Gerät** und **Port extern gewünscht** verschiedene Zahlen. Die Warnung der FRITZ!Box zu Port 443 können Sie bestätigen, diese Freigabe braucht die Videokonferenz.

Diese Freigabe gilt nur **über IPv4**, weil die FRITZ!Box nur dort einen Port auf einen anderen umsetzt. Über IPv6 braucht die Videokonferenz eine eigene Freigabe auf TCP 443 ohne Umsetzung (Abschnitt „Die IPv6-Freigabe in einer FRITZ!Box“).

Ist der gewünschte Port schon vergeben, nimmt die FRITZ!Box einen anderen und zeigt ihn in der Spalte **Port extern vergeben**. Steht dort eine andere Zahl als gewünscht, ist der Port an Ihrem Anschluss bereits belegt, etwa durch eine zweite TrutzBox (Abschnitt „Einen eigenen Namen statt des TrutzDynDNS-Namens verwenden“).

26.3 Die IPv6-Freigabe in einer FRITZ!Box

Unter IPv6 gibt es keine Weiterleitung auf eine andere Adresse. Der Router öffnet den Port direkt für die IPv6-Adresse der TrutzBox und fragt dafür ihre **Interface-ID** ab. Den Wert finden Sie unter **Netzwerk → Fernzugriff** im Domain-Bereich als **IPv6-Interface-ID (für Freigaben am Router)**. Wozu Sie die IPv6-Freigabe brauchen, steht in Abschnitt „VPN auch über IPv6 anbieten“. Die Schritte gelten für FRITZ!OS 7.5 und neuer; ältere Versionen führen zum selben Ziel, nur heißen die Menüpunkte 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, nehmen Sie den Eintrag mit der Adresse, die im lokalen Netz zur TrutzBox gehört.
3. Im Feld **IPv6 Interface-ID** den Wert von der TrutzBox eintragen. Die FRITZ!Box schlägt oft selbst eine Kennung vor; überschreiben Sie diese mit dem Wert von der TrutzBox, sonst zeigt die Freigabe ins Leere.
4. **Neue Freigabe** anklicken, **Portfreigabe** und unter **Anwendung** den Eintrag **Andere Anwendung** wählen und eintragen: Protokoll **UDP**, Port **1194** für TrutzVPN. Unten **Internetzugriff über IPv6** wählen. Haben Sie die Freigabe schon mit **Internetzugriff über IPv4 und IPv6** angelegt, gilt sie bereits auch für IPv6, sobald die Interface-ID stimmt.
5. Mit **OK** und **Übernehmen** sichern.

Für die Videokonferenz, auch für Anrufe aus dem Chat, legen Sie auf demselben Weg eine Freigabe TCP 443 über IPv6 an, mit 443 auch bei Port an Gerät, also ohne Umsetzung auf 9082. Die Freigabe UDP 9083 ist schon dabei, wenn Sie sie mit IPv4 und IPv6 angelegt haben, sonst legen Sie sie hier ebenso an. Der Chat selbst braucht keine Freigabe.

- Der grüne Punkt neben der Freigabe sagt nur, dass die Regel aktiv ist, nicht, dass die TrutzBox von außen antwortet. Das zeigt erst ein Versuch unterwegs.
- Hängt eine zweite TrutzBox am selben Router, bekommt sie eine eigene Freigabe mit ihrer eigenen Interface-ID. Beide dürfen denselben Port benutzen, weil es bei IPv6 keine Umsetzung auf eine gemeinsame Adresse gibt.

26.4 Anleitungen der Router-Hersteller

Andere Router führen zum selben Ziel, nur heißen die Menüs anders. Die Hersteller ändern ihre Oberflächen laufend; die aktuelle Anleitung finden Sie auf ihren Hilfeseiten:

Router	Suchen Sie nach …	Hilfeseite
FRITZ!Box	„Portfreigabe einrichten"	fritz.com/service
Telekom Speedport	„Portweiterleitung Speedport"	telekom.de/hilfe
Vodafone Station	„Portfreigabe Vodafone Station"	vodafone.de/hilfe
O2 HomeBox	„Portfreigabe HomeBox"	hilfe.o2online.de
Ubiquiti UniFi	„Port Forwarding"	help.ui.com

27 Sicherheit, Entsorgung und Kontakt

Dieses Kapitel bündelt die Angaben, die man selten braucht und dann sofort finden möchte: Sicherheitshinweise zum Gerät, was beim Entsorgen zu beachten ist, und wie Sie Comidio erreichen.

27.1 Sicherheitshinweise

Die TrutzBox ist ein Gerät für den Dauerbetrieb in Wohn- und Büroräumen. Beachten Sie die folgenden Punkte, damit das gefahrlos bleibt:

- **Nur das mitgelieferte Netzteil verwenden.** Andere Netzteile können eine andere Spannung liefern und das Gerät beschädigen. Ist das Netzteil defekt, fordern Sie Ersatz beim Support an.
- **Beschädigte Kabel nicht weiterverwenden.** Ein Netzkabel mit gequetschter oder aufgescheuerter Isolierung gehört ausgetauscht, nicht geklebt.
- **Für Luft sorgen.** Die TrutzBox gibt ihre Wärme über das Gehäuse ab. Stellen Sie sie nicht in einen geschlossenen Schrank, decken Sie sie nicht mit Papier oder Textilien ab und stapeln Sie keine warmen Geräte darauf (Kapitel „Aufstellort, Belüftung und Dauerbetrieb“).
- **Trocken aufstellen.** Das Gerät ist nicht gegen Spritzwasser geschützt. Küchentheke neben der Spüle, Fensterbank und Badezimmer sind ungeeignet.
- **Nicht in direkter Sonne oder neben der Heizung betreiben.** Dauerhafte Hitze verkürzt die Lebensdauer der Bauteile; die aktuelle Temperatur zeigt der Betriebszustand.
- **Gehäuse geschlossen lassen.** Im Inneren gibt es nichts zu warten. Ein Öffnen ist nur für den Einbau eines WLAN-Moduls oder den Tausch des Speichermediums vorgesehen und sollte in Absprache mit dem Support erfolgen; trennen Sie die TrutzBox dabei zuerst vom Strom.
- **Vor Gewitter schützen.** Wie bei allen Netzwerkgeräten empfiehlt sich ein Überspannungsschutz in der Steckdosenleiste.

Beim Ausschalten nichts erzwingen

Fahren Sie die TrutzBox im Normalfall über die Verwaltungsoberfläche herunter, statt einfach den Stecker zu ziehen. Die TrutzBox schreibt dabei laufende Vorgänge sauber zu Ende. Reagiert die Oberfläche nicht mehr, ist das Trennen vom Strom trotzdem erlaubt und in aller Regel folgenlos; die TrutzBox ist darauf ausgelegt.

27.2 Entsorgung

Elektro- und Elektronikaltgeräte gehören nicht in den Hausmüll. Das Symbol der durchgestrichenen Mülltonne auf dem Gerät weist darauf hin. Geben Sie die TrutzBox am Ende ihrer Nutzungsdauer bei einer kommunalen Sammelstelle für Elektroaltgeräte ab oder senden Sie sie an Comidio zurück; der Support nennt Ihnen den Weg. Das mitgelieferte Netzteil und die Kabel gehören ebenfalls dorthin.

Vor dem Weitergeben oder Entsorgen zurücksetzen

Auf der TrutzBox liegen Ihre Postfächer, Ihre Schlüssel und Ihre Einstellungen. Setzen Sie die TrutzBox deshalb vor jedem Besitzerwechsel und vor der Entsorgung auf den Werkszustand zurück (Kapitel „System zurücksetzen (Werksreset)“). Legen Sie vorher eine Sicherung an, falls Sie die Daten auf einer anderen TrutzBox weiterverwenden möchten. Was sonst noch dazugehört, vor allem der Umgang mit Ihrer TrutzLegitimation, steht in Abschnitt „Die TrutzBox weitergeben“.

27.3 Gewährleistung und Ersatzteile

Für die TrutzBox gelten die gesetzlichen Gewährleistungsfristen. Weil ein Sicherheitsgerät ohne Aktualisierungen wertlos wäre, liefert Comidio Software-Updates über die gesamte vereinbarte Dauer aus; die gesetzliche Grundlage dafür steht in Kapitel „Voraussetzung: ein gültiger Service-Vertrag“.

Ist die Hardware defekt, bedeutet das nicht den Verlust Ihrer Identität: Ihre TrutzMail-Adressen hängen an Ihrer TrutzLegitimation, nicht am Gehäuse. Das Vorgehen beim Hardware-Defekt beschreibt Kapitel „Hardware-Defekt und Tausch des Boot-Mediums“. Ersatznetzteile, Netzwerkkabel und das WLAN-Modul erhalten Sie über den Support.

27.4 Datenschutz in eigener Sache

Die TrutzBox ist ein Datenschutzgerät, und sie hält sich selbst daran. Alle Aufzeichnungen, also Monitor-Daten, Statistiken, Protokolle, Postfächer und Chat-Verläufe, entstehen und bleiben auf Ihrer TrutzBox. Comidio hat darauf keinen Zugriff und keinen Fernwartungszugang (Kapitel „Was Comidio nicht kann und nicht tut“).

Nach außen gehen nur die Daten, die für den Betrieb nötig sind, etwa die Anfragen an den Update-Server, die Registrierung Ihrer TrutzLegitimation, die Meldung Ihrer aktuellen Internet-Adresse an TrutzDynDNS, die Bitte um Testpakete, mit denen die TrutzBox ihre Erreichbarkeit von außen prüft (Kapitel „Netzwerk-Übersicht: außen und innen“), und die verschlüsselten Namensanfragen an den gewählten DNS-Anbieter. Alle Comidio-Dienste laufen auf eigener Infrastruktur in Deutschland. Was genau in einem Support-Bericht steht, sehen Sie vollständig, bevor Sie ihn absenden (Kapitel „Was in den Support-Bericht gehört“).

27.5 Hersteller und Kontakt

Angabe	Wert
Hersteller	Comidio GmbH, Eichendorffweg 2, 65343 Eltville am Rhein, Deutschland
Internet	www.trutzbox.de
Support	support@trutzbox.de
Forum	forum.trutzbox.de
Ihre Kundennummer	die TrutzKennung vom Beileger, ebenfalls sichtbar unter Systemeinstellungen → Vertrag und Pakete
Version dieser	Systemeinstellungen → Vertrag und Pakete nennt Image-Version, Hardware

Angabe	Wert
TrutzBox	und alle Paketstände

Halten Sie bei jeder Anfrage Ihre TrutzKennung bereit und legen Sie nach Möglichkeit den Support-Bericht bei. Das erspart in aller Regel die erste Rückfrage. Rechtliche Hinweise und Lizenzangaben zur eingesetzten quelloffenen Software finden Sie außerdem in der Oberfläche unter **Systemeinstellungen → Rechtliche Hinweise**.

Glossar: wichtige Begriffe erklärt

Hier finden Sie die Begriffe, die in diesem Handbuch vorkommen, in Kurzform erklärt. Die Verweise in Klammern führen zur ausführlichen Beschreibung.

Admin-Panel Die Verwaltungsoberfläche der TrutzBox im Browser, erreichbar unter https://trutzbox. Anmeldung mit dem Benutzernamen „admin".

Angriffsschutz Die Abwehr der TrutzBox gegen Zugriffe aus dem Internet: Eine Firewall lässt nur erlaubte Verbindungen herein, ein Wächter sperrt zusätzlich Absender, die es wiederholt versuchen (Kapitel „Angriffsschutz: Firewall und Wächter“).

Anruf aus dem Chat Ein Anruf, den Sie im Web-Chat direkt aus einem Gespräch starten, mit „Videoanruf starten" oder „Anruf ohne Bild starten". Die TrutzBox legt dafür einen Raum der Videokonferenz an, schickt die Einladung ins Gespräch und öffnet die Konferenz ohne zweite Anmeldung. Die Knöpfe erscheinen nur, wenn die TrutzBox Konferenzen unter einem öffentlichen Namen anbietet, etwa über TrutzDynDNS (Kapitel „TrutzChat benutzen: im Browser und mit einer Chat-App“).

App-Grundbausteine Zwei Dienste, ohne die viele Apps nicht starten, obwohl Sperrlisten sie führen: die Firebase-Kennung, mit der eine App ihre Starteinstellungen lädt, und die Schnittstelle von RevenueCat für Abos und Käufe. Der Schalter „App-Grundbausteine durchlassen" trägt beide als Ausnahmen ein; ab Werk ist er aus. Reine Messdienste bleiben gesperrt (Kapitel „Eigene Sperren und Ausnahmen“ und „… eine Seite blockiert wird oder eine App nicht startet“).

Arbeitsspeicher Der Speicher, mit dem die laufenden Programme der TrutzBox arbeiten. Er besteht aus dem Hauptspeicher (RAM) und der Auslagerung (Swap). Die Übersicht zeigt ihn in der Karte „Arbeitsspeicher (RAM und Swap)", der Betriebszustand in der Karte „Arbeitsspeicher" (Kapitel „Die Startseite lesen“ und „Betriebszustand: die Karten im Einzelnen“).

Auslagerung (Swap) Der zweite Teil des Arbeitsspeichers. Hierhin legt die TrutzBox Daten, die gerade nicht gebraucht werden, sobald der Hauptspeicher voll ist. Die Auslagerung liegt nicht auf der SSD, sondern gepackt im Hauptspeicher selbst. Eng wird es erst, wenn Hauptspeicher und Auslagerung beide fast voll sind (Kapitel „Betriebszustand: die Karten im Einzelnen“).

Betriebszustand Die Gesundheitsseite der TrutzBox mit einer Ampel für den Gesamtzustand und Karten für die einzelnen Bereiche (Kapitel „Betriebszustand: die Ampel lesen“).

Blacklist Eine Sperrliste: Was darin steht, wird blockiert. Das Gegenstück zur Whitelist (Kapitel „Filterlisten verwalten“).

DHCP Verfahren, mit dem ein Gerät beim Anschließen automatisch seine Netzwerk-Adresse erhält. Im internen Netz vergibt die TrutzBox die Adressen.

DNS Die Namensauflösung des Internets: Sie übersetzt Namen wie „beispiel.de" in die Zahlenadressen, mit denen Geräte tatsächlich arbeiten. Die TrutzBox verschlüsselt diese Anfragen (Kapitel „DNS-Schutz und verschlüsselte Namensauflösung“).

DNS-Rebind-Schutz Eine Schutzfunktion vieler Router, etwa der FRITZ!Box: Sie nennt Geräten im eigenen Netz keine Namen, die auf Adressen in diesem Netz zeigen. Für den Namen der TrutzBox braucht es dort manchmal eine Ausnahme (Abschnitt „TrutzDynDNS nur mit IPv6“).

DoH und DoT Zwei Verfahren, die DNS-Anfragen verschlüsseln, damit unterwegs niemand mitlesen kann, welche Seiten aufgerufen werden. Die TrutzBox verschlüsselt ihre eigene Weiterleitung mit DoT; fremde

verschlüsselte Namensdienste, die Geräte an ihr vorbei nutzen wollen, fängt sie auf Wunsch ab (Kapitel „DNS-Schutz und verschlüsselte Namensauflösung“).

DS-Lite Anschlussart mancher Anbieter ohne eigene öffentliche IPv4-Adresse. Von außen ist die TrutzBox dort nur über IPv6 erreichbar. TrutzVPN funktioniert dann über IPv6: mit einer IPv6-Freigabe am Router und dem Schalter „TrutzDynDNS nur mit IPv6", den die TrutzBox meist selbst setzt; bei OpenVPN zusätzlich mit dem Schalter „VPN auch über IPv6 anbieten" (Abschnitte „Welcher Anschluss ist von außen erreichbar?“ und „TrutzDynDNS nur mit IPv6“).

Eigene Sperren und Ausnahmen Die Seite unter Verwaltung, auf der Sie eigene Sperren und Freigaben für Webfilter und Firewall an einem Ort anlegen, suchen und löschen. Dort stehen auch mitgelieferte Ausnahmen, die sich mit einem Schalter abschalten lassen, etwa „Werbeblocker-Blocker erlauben" und „App-Grundbausteine durchlassen" (Kapitel „Eigene Sperren und Ausnahmen“).

Felder anzeigen Ein Knopf im Monitor. Damit wählen Sie, welche Angaben an Servern und Geräten stehen, etwa Land, Organisation, Datenmenge im Zeitraum oder eine Verlaufskurve mit der aktuellen Rate. Die Auswahl bleibt im Browser gespeichert (Kapitel „Der Aufbau: Geräte, TrutzBox, Internet“ und „… eine Seite sehr langsam lädt“).

Fernzugriff Der Zugang zur eigenen TrutzBox und ihrem Netz von unterwegs, etwa im Büro, im Hotel oder im Café, über TrutzVPN (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

Filtergruppe Ein Filterprofil, das mehrere Filterlisten bündelt. Jedes Gerät bekommt genau eine Filtergruppe zugewiesen (Kapitel „Filtergruppen zuordnen“ und „Filtergruppen einrichten“).

Filterliste Ein Verzeichnis von Internet-Adressen zu einem Thema, etwa Werbung oder Dienste, die aufzeichnen, was man im Internet tut. Die Adressen darin werden gesperrt oder erlaubt (Kapitel „Filterlisten verwalten“).

Firewall Die Schutzschicht, die unerwünschte Verbindungen auf Netzwerkebene abwehrt, unabhängig davon, welches Programm sie aufbaut.

Hauptspeicher (RAM) Der eingebaute schnelle Speicher, in dem die laufenden Programme der TrutzBox arbeiten. Sein Inhalt geht beim Ausschalten verloren. Ein fast voller Hauptspeicher ist kein Engpass, solange die Auslagerung noch Platz hat (Kapitel „Die Startseite lesen“).

IMAP, POP3 und SMTP Die drei gebräuchlichen Verfahren, mit denen ein Mail-Programm Post abholt (IMAP, POP3) und versendet (SMTP). Bei der Einrichtung von TrutzMail wählt das Programm sie meist von selbst (Kapitel „Ein Mail-Programm einrichten“).

Interface-ID Die hintere Hälfte einer IPv6-Adresse. Die TrutzBox bildet sie aus ihrer Hardware-Adresse, deshalb bleibt sie gleich, auch wenn der Anbieter den vorderen Teil wechselt. Sie wird am Router für die IPv6-Freigabe eingetragen (Kapitel „VPN auch über IPv6 anbieten“).

Internes TrutzBox-Netzwerk Weg 1, ein Gerät mit der TrutzBox zu verbinden: Das Gerät hängt per Kabel oder über das TrutzBox-WLAN hinter der TrutzBox, sein gesamter Verkehr läuft automatisch durch sie. Der empfohlene Weg (Kapitel „Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen“).

IP-Adresse Die Zahlenadresse eines Geräts im Netz. Im internen TrutzBox-Netz beginnen sie mit 192.168.195.

IPv4 und IPv6 Die beiden Adressarten des Internets. IPv4 ist die ältere mit kurzen Adressen aus vier Zahlen, IPv6 die neuere mit deutlich längeren Adressen. Viele Anschlüsse haben beide, manche nur eine eigene IPv6-Adresse (DS-Lite). TrutzVPN nutzt ab Werk IPv4, auf Wunsch unterwegs auch IPv6 (Kapitel „VPN auch über IPv6 anbieten“).

Kontaktanfrage Im Web-Chat eine Nachricht von einer Adresse, die noch nicht zu Ihren Kontakten gehört. Der Chat hält sie zurück und fragt, ob Sie die Adresse aufnehmen. „Ablehnen" sperrt die Adresse, bis Sie sie über „Kontakt hinzufügen" aufnehmen. Nimmt ein Benutzer einen anderen Benutzer derselben TrutzBox auf, gilt der Kontakt sofort für beide (Kapitel „TrutzChat benutzen: im Browser und mit einer Chat-App“).

LAN-Ext Der Anschluss der TrutzBox zum Internet-Router, also die unsichere Außenseite.

LAN-Int1, LAN-Int2 Die Anschlüsse der TrutzBox für das geschützte interne Netzwerk.

Lesebestätigung Die Rückmeldung „Gelesen" an einer gesendeten Chat-Nachricht. Mit dem Schalter „Lesebestätigungen senden" im Web-Chat lässt sie sich abschalten. Dann verschickt der Chat keine, und die Lesebestätigungen der anderen bleiben ebenfalls verborgen; die Meldung „Zugestellt" bleibt (Kapitel „TrutzChat benutzen: im Browser und mit einer Chat-App“).

Let’s Encrypt Eine gemeinnützige Stelle, die kostenlose, allgemein anerkannte Zertifikate für Internet-Adressen ausstellt. Die TrutzBox holt sich darüber auf Wunsch ein Zertifikat, damit Gäste in der Videokonferenz keine Warnung sehen (Kapitel „Reiter Videokonferenz: einmalig einrichten“).

MAC-Adresse Die vom Hersteller vergebene Hardware-Kennung einer Netzwerk-Schnittstelle. Daran erkennt die TrutzBox ein Gerät wieder. Neuere Smartphones und Notebooks können aus Datenschutzgründen zufällige Adressen verwenden; dann ist die Wiedererkennung nicht mehr eindeutig (Kapitel „Neue Geräte erscheinen automatisch“).

mDNS Ein offener Standard, mit dem sich Geräte im eigenen Netz selbst bekannt machen, ohne dass der Router ihren Namen kennen muss; bei Apple heißt er „Bonjour". Die TrutzBox ist darüber zusätzlich unter trutzbox.local erreichbar, im internen Netz und im Netz des Routers, nicht über VPN (Kapitel „Das Setup im Browser öffnen“).

Metadaten Die Begleitdaten einer Nachricht: wer schreibt wem, wann, wie oft. Bei TrutzMail zwischen TrutzBoxen bleiben auch sie verborgen.

Mobilfunk-Router Ein Router für LTE oder 5G statt eines Festnetz-Anschlusses. Von außen ist eine TrutzBox dahinter meist nicht erreichbar, weder über IPv4 noch über IPv6 (Abschnitt „Welcher Anschluss ist von außen erreichbar?“).

Monitor Die Live-Ansicht aller Verbindungen im Netz, mit den drei Darstellungen Liste, Verbindungen und Blasendiagramm (Kapitel „Monitor und Statistiken“).

NTP Der Zeitdienst des Internets, über den Geräte ihre Uhr stellen. Die TrutzBox kann diese Anfragen selbst beantworten, damit Geräte dafür nicht nach außen funken müssen (Kapitel „Weitere Einstellungen je Gerät“).

OpenVPN Ein bewährtes Verfahren für den VPN-Tunnel. Die TrutzBox bietet es neben WireGuard an; es läuft immer nur einer der beiden Tunnel (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

Passphrase Ein längeres Passwort aus mehreren Wörtern, mit dem die Datensicherung verschlüsselt wird. Anders als ein vergessenes Kennwort lässt sie sich von niemandem zurücksetzen: Ohne Passphrase ist die Sicherung unbrauchbar (Kapitel „Eine Sicherung anlegen“).

PGP Ein offener Standard zur Verschlüsselung von E-Mail. Die TrutzBox nutzt ihn für Partner ohne eigene TrutzBox (Kapitel „Weg B einrichten: Postfach beim Anbieter verbinden“).

Port-Scan Das planmäßige Abklopfen vieler Ports einer Adresse, also der nummerierten Zugänge, über die ein Rechner seine Dienste anbietet. Wer das tut, sucht nach einem offenen Dienst, durch den er eindringen kann. Die Firewall der TrutzBox wehrt solche Versuche aus dem Internet ab, und der

Angriffsschutz sperrt Absender, die es wiederholt versuchen (Kapitel „Angriffsschutz: Firewall und Wächter“).

Portweiterleitung Eine Regel im Internet-Router, die Anfragen aus dem Internet an ein bestimmtes Gerät im Netz weiterreicht. Für den VPN-Zugang nötig (Kapitel „Schritt 2: Portweiterleitung am Internet-Router“).

Proxy Ein Vermittler im Datenstrom. Die TrutzBox arbeitet als Proxy und kann Verbindungen dadurch inhaltlich prüfen und filtern.

Proxy-Mode Weg 2, ein Gerät mit der TrutzBox zu verbinden: Das Gerät bleibt im Netz des Routers und bekommt die TrutzBox nur als Proxy eingetragen. Proxy-Port 8081 oder automatische Konfiguration (Kapitel „Weg 2: Gerät im Proxy-Mode betreiben“).

QUIC Ein modernes Übertragungsprotokoll, das an klassischen Filtern vorbeiläuft. Die TrutzBox kann es deshalb gezielt sperren.

Reserve Was vom Arbeitsspeicher noch verfügbar ist: der freie Hauptspeicher plus der nutzbare Teil der freien Auslagerung. Liegt die Reserve unter 11 Prozent des Hauptspeichers, warnt die Karte Arbeitsspeicher; unter 5 Prozent greift der Speicher-Wächter ein (Kapitel „Betriebszustand: die Karten im Einzelnen“).

Root-Zertifikat Die Datei, mit der ein Gerät der TrutzBox vertraut. Nötig für TrutzBrowse und für Programme, die sich mit der TrutzBox verbinden, nicht für den normalen Webfilter (Kapitel „Das Root-Zertifikat installieren“).

Security-Slider Der Regler mit zehn Stufen, mit dem der Anonymisierungsgrad von TrutzBrowse eingestellt wird. Stufe 1 gibt die höchste, Stufe 10 die geringste Anonymität (Kapitel „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“).

Service-Laufzeit Die Laufzeit Ihres Service-Vertrags mit Comidio. Ist sie abgelaufen, lassen sich keine TrutzMail-Adressen mehr anlegen oder reaktivieren, und der Bericht an den Support lässt sich nicht erstellen. Nach der Verlängerung ist beides wieder möglich (Kapitel „Adressen anlegen, löschen und reaktivieren“ und „Voraussetzung: ein gültiger Service-Vertrag“).

Software-Updates (Karte) Die Karte im Betriebszustand, die zeigt, ob die TrutzBox ihre Software-Updates einspielt: den letzten Update-Lauf mit Ergebnis, wann zuletzt Pakete eingespielt wurden und wann der nächste Lauf ansteht. Gelb wird sie, wenn ein Lauf nicht fertig wurde. Sind angebotene Pakete seit über einer Woche nicht eingespielt oder war der Update-Server so lange nicht erreichbar, wird sie gelb und nach zwei Wochen rot. Gezählt wird nur die Zeit, in der die TrutzBox eingeschaltet ist (Kapitel „Betriebszustand: die Karten im Einzelnen“ und „… nach einem Software-Update etwas nicht mehr funktioniert“).

Speicher-Wächter Die Überwachung des Arbeitsspeichers. Wird die Reserve knapp, hält sie gezielt Dienste an, zuerst TrutzRTC und danach TrutzMail, damit die TrutzBox nicht einfriert, und startet sie wieder, sobald genug frei ist (Kapitel „Betriebszustand: die Karten im Einzelnen“).

Speicherverlauf Ein Fenster mit drei Diagrammen für Hauptspeicher (RAM), Auslagerung (Swap) und Webfilter, wahlweise über 1 Stunde, 24 Stunden, 7 Tage oder 30 Tage. Es öffnet sich mit einem Klick auf das Diagramm der Karte „Arbeitsspeicher (RAM und Swap)" auf der Übersicht (Kapitel „Die Startseite lesen“).

Sperrseite Die Seite, die die TrutzBox anstelle einer blockierten Webseite anzeigt, mit Angabe des Grundes (Kapitel „Die Sperrseite verstehen“).

SSH Das Verfahren für den verschlüsselten Zugang zur Kommandozeile der TrutzBox, gedacht für erfahrene Administratoren. Mit einem Passwort meldet sich dort nur der Benutzer „admin" an (Abschnitt „Die Kommandozeile: Terminal und SSH“).

SSID Der Name eines Funknetzes, also das, was auf dem Smartphone in der WLAN-Liste erscheint (Kapitel „Das WLAN der TrutzBox“).

Switch Ein Verteiler mit mehreren Netzwerkbuchsen. Er erweitert die internen Anschlüsse der TrutzBox; alles daran bleibt geschützt (Kapitel „Mehr Geräte anschließen: der Switch“).

Tank-Stick Ein USB-Stick mit einem kompletten Image, der die Platte des Rechners überschreibt, von dem er startet. Ab V80 betankt er jede gewöhnliche PC-Hardware (x86) und jede virtuelle Maschine ohne Rückfrage, nur die APU1 nicht (Kapitel „Der Ausnahmefall: ein komplettes Image“).

Terminal Die Kommandozeile der TrutzBox in einem Browser-Fenster, mit vollen Rechten und geschützt durch das Admin-Passwort. Gedacht für den Notfall und für Befehle, die der Support nennt (Abschnitt „Die Kommandozeile: Terminal und SSH“).

Tor Ein weltweites Netz freiwilliger Vermittlungsstellen, das Verbindungen über mehrere Zwischenstationen führt, sodass sich Absender und Ziel nicht mehr zusammenbringen lassen. Die TrutzBox nutzt es für die verdeckte Zustellung von TrutzMail und Chat-Nachrichten zwischen TrutzBoxen und, auf Wunsch, für einzelne Geräte (Schalter Tor-Netzwerk verwenden, Kapitel „Weitere Einstellungen je Gerät“).

Transparent Die Verbindungsart von Geräten im internen TrutzBox-Netzwerk: Ihr Verkehr läuft durch die TrutzBox, ohne dass am Gerät etwas eingestellt werden müsste (Kapitel „Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen“).

TrutzBase Der Sicherheitsteil der TrutzBox: Firewall, Angriffserkennung und VPN-Server.

TrutzBrowse Die Anonymisierungsfunktion, die identifizierende Merkmale aus dem Datenverkehr entfernt (Kapitel „TrutzBrowse: zusätzlicher Schutz für Browser und Apps“).

TrutzBurg-Icon Das kleine Burg-Symbol, das TrutzBrowse in aufgerufene Seiten einblendet, ab Werk oben rechts. Ein Klick darauf öffnet das TrutzBurg-Menü, in dem sich der Security-Slider für die gerade besuchte Seite verstellen lässt (Kapitel „Das TrutzBurg-Menü im Browser“).

TrutzChat Der Nachrichtendienst der TrutzBox auf Basis des offenen XMPP-Standards (Kapitel „TrutzChat und Videokonferenz“).

TrutzContent Der Webfilter der TrutzBox, der anhand von Filtergruppen über jeden Zugriff entscheidet (Kapitel „Webfilter und Jugendschutz (TrutzContent)“).

TrutzDynDNS Der Dienst von Comidio, der Ihrer TrutzBox einen festen Namen unter mytrutzbox.de gibt, auch wenn die IP-Adresse wechselt. Nötig, wenn die TrutzBox von außen erreichbar sein soll (Kapitel „TrutzDynDNS: Ihre TrutzBox aus dem Internet erreichbar machen“).

TrutzKennung Ihre Kundennummer bei Comidio, nur aus Ziffern. Zusammen mit dem TrutzSchlüssel für die Registrierung nötig.

TrutzLegitimation TrutzKennung und TrutzSchlüssel zusammen: der Nachweis, dass diese TrutzBox Ihnen gehört.

TrutzMail Die E-Mail-Funktion der TrutzBox mit automatischer Verschlüsselung; Adressen enden auf @comidio.email (Kapitel „TrutzMail: sichere E-Mail“).

TrutzMeeting Der Videokonferenz-Dienst auf der eigenen TrutzBox; Gäste brauchen nur einen Browser und einen Link (Kapitel „Reiter Videokonferenz: einmalig einrichten“).

TrutzRTC Der gemeinsame Unterbau von TrutzChat und TrutzMeeting auf Ihrer TrutzBox. Er gehört zur Business-Ausstattung und erscheint als eigene Karte auf der Betriebszustand-Seite (Kapitel „TrutzChat und Videokonferenz“).

TrutzSchlüssel Der 16-stellige Schlüssel im Format XXXX-XXXX-XXXX-XXXX vom Beileger, für die Registrierung der TrutzBox.

VLAN-Kennung Eine Nummer, mit der ein Internet-Anbieter auf seiner Leitung verschiedene Dienste auseinanderhält. Gebraucht wird sie an LAN-Ext nur, wenn die TrutzBox ohne Router direkt an der Leitung hängt. In der Oberfläche lässt sie sich nicht setzen; eingerichtet wird sie in diesem Fall vom Support, und die Sicherung nimmt sie nicht mit (Kapitel „Netzwerk-Übersicht: außen und innen“ und „Was in der Sicherung steckt“).

VPN Ein verschlüsselter Tunnel durch das Internet. Er verbindet Geräte unterwegs mit der TrutzBox und ihrem Netz. Die TrutzBox bietet ihn über OpenVPN oder WireGuard an (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

Wartungssystem Ein kleines eigenes System auf der Rettungspartition der TrutzBox. Es führt das Zurücksetzen auf den Werkszustand aus und zeigt dabei mit den LEDs, wie weit es ist (Kapitel „System zurücksetzen (Werksreset)“).

Webmin Die technische Zweit-Oberfläche der TrutzBox für erfahrene Administratoren und den Notfall (Abschnitt „Webmin: der Experten-Zugang“).

Werksreset Das Zurücksetzen der TrutzBox auf den Auslieferungszustand: Alle Daten werden gelöscht, das Betriebssystem neu aufgespielt. Ausgelöst über die Verwaltung oder ohne Anmeldung über die Taste am Gehäuse. Dafür die Taste in den ersten 2 Minuten nach dem Einschalten 3 Sekunden halten, bis die LEDs dauerhaft leuchten, dann loslassen (Kapitel „System zurücksetzen (Werksreset)“).

Whitelist Eine Ausnahmeliste: Was darin steht, ist erlaubt, auch wenn andere Filter es sperren würden.

WireGuard Ein schlankes, modernes Verfahren für den VPN-Tunnel. Die TrutzBox bietet es neben OpenVPN an; es läuft immer nur einer der beiden Tunnel. Bei WireGuard bekommt jedes Gerät einen eigenen Zugang, auch mehrere unter demselben Benutzerkonto (Kapitel „TrutzBox unterwegs nutzen (TrutzVPN)“).

WPA2 und WPA3 Die beiden gebräuchlichen Verschlüsselungsverfahren für WLAN. WPA3 ist das neuere und sicherere, WPA2 versteht auch ältere Geräte (Kapitel „Das WLAN der TrutzBox“).

XMPP Der offene Standard hinter TrutzChat, den viele Chat-Programme auf allen Systemen unterstützen.

Stichwortverzeichnis

5

5 GHz (WLAN) 170

A

Absenderadresse (Postausgang) 108
Access-Point verwenden 168
Ad-Shield (Werbeblocker-Blocker) 99
admin (Benutzerkonto) 29, 67
Admin-Panel 32, 42
Alias (Absenderadresse) 108
Alle löschen (Ausnahmen) 83
Altersgruppen 77
Ampel 48
Ampel auf Grün stellen 48
Android 222, 233
Android (Mail-App) 228
Angezeigte IPs blockieren 96
Angriffsschutz 173
Angriffsversuche von außen 116
Anleitungen zum Anklicken 7, 22, 74, 87, 103, 135, 173
Anmeldename (Mail-Anbieter) 108
Anonymisierung 155
Anruf aus dem Chat 129
Anschlussarten (Internet) 117
Anschlüsse 17, 22
App startet nicht 203
App-Grundbausteine 83, 203
Apple Mail 227
APU1 184
Arbeitsspeicher 42, 50, 211
Aufbewahrungsdauer (Chat) 127
Aufzeichnung (Videokonferenz) 126
Auslagerung (Swap) 42, 50
Ausnahmen (Whitelist) 78, 82
Automatische Proxy-Konfiguration 37, 235

B

Backup 27, 189
Beim Anbieter (behalten, abgleichen, löschen) 108
Benutzer anlegen 30, 68
Benutzer ohne TrutzMail-Adresse 67
Bericht an Support 48, 216
Besitzerwechsel 197
Betriebszustand 48
Blasendiagramm 92
Blockierte IPs 173
Bonjour 24
Bootloader 190

C

Chat 129
Chat-Programme 230
Checkliste Zurücksetzen 196
Comidio-Server erkennen diese TrutzBox nicht 68

D

Datenbereich (wächst beim ersten Start) 186, 191
Datenvolumen 98
Details (Erreichbarkeit von außen) 167
DHCP 25
Dienst-Symbole (Monitor) 89
DNS für Geräte (Karte) 50, 203
DNS-Rebind-Schutz 120
DNS-Umgehungsschutz 171
DNS, verschlüsseltes 171
DS-Lite 117, 119, 148
Dual-Stack 141

E

E-Mail 103
E-Mail-Austausch mit normalen Adressen 108
Eigene Sperren und Ausnahmen 83, 203
Eigener Domain-Name 120
Eigener Name (Karte) 50
Erreichbar, nur über IPv4 166
Erreichbarkeit prüfen 141, 150
Erreichbarkeit von außen 143, 166, 217, 219
Erweiterte Ansicht (Geräte) 58
Export (CSV, Monitor) 92

F

Felder anzeigen (Monitor) 89, 204
Fernzugriff 135
Feste IP-Adresse 25
Filtergruppen 60, 76
Filterliste, Größengrenze 80
Filterlisten 78
Filterlisten importieren 80
Firewall 173
Firewall-Ausnahme 83, 173
FRITZ!Box 238, 240
Führungen (Monitor-Hilfe) 87

G

Gajim, Monal, Conversations (Chat) 230
Gast-Konto (Weg C) 103, 105
Geräte benennen 59
Geräte verwalten 58
Geräteübersicht des Routers 24, 209
Glossar 245
Größere SSD 211, 220

Größte Speicherverbraucher 50, 216
Gruppen (Chat) 132

H

Handschlag (WireGuard) 141
Hauptspeicher (RAM) 42, 50
Herunterfahren 212
Herzschlag-Leuchte 19, 194, 210
Hilfe & Führungen (Monitor) 87
Hilfe im Monitor 87

I

Ignorierliste (Angriffsschutz) 83
Interface-ID (IPv6) 148, 167, 240
Interner Datenverkehr (Monitor) 89
Internet-Anschluss (Karte) 50
Internet-Router 22, 139
Internetzugang (Schalter) 61, 62
IP-Blockliste 173, 181
iPhone und iPad 222, 232, 233
IPv6 141, 148
IPv6 für die TrutzBox anfordern 165
IPv6-Freigabe 124, 148
IPv6-Präfix 119

J

Jugendschutz 74, 77

K

Kommandozeile (SSH) 174, 201
Kommandozeile (Terminal im Browser) 200
Kontaktanfrage (Chat) 129, 208

L

LAN-Ext 17, 22
LAN-Int1 / LAN-Int2 17, 36
LED-Anzeige an der TrutzBox 19
LEDs 19, 185, 193, 194, 209, 210
Lesebestätigung (Chat) 129
Let’s Encrypt 120, 124, 207
Letzte 60 Minuten 42, 98
Lieferumfang 16
Liste (Monitor) 92
Live-Update (Monitor) 96

M

macOS 222, 232, 233
Mail abholen (Postfach beim Anbieter) 108
Mail-Programm einrichten 105, 226
mDNS 24
Mehrere TrutzBoxen an einem Router 120, 148
Metadaten 103
Mobilfunk-Router (LTE, 5G) 117
Monitor 89

N

Nachweis (Mail aufbewahren) 108
Netzwerk-Anschlüsse (Monitor) 89, 92
Netzwerkname 25
Neu laden (Oberfläche aktualisiert) 72
Neustart 42, 212
Nicht verbunden (extern) 37, 60
Nicht zugestellt (Chat) 129, 208
Notzugang 200, 209
„Nur Ausnahmen erlauben" 82

O

Online-Monitor (FRITZ!Box) 118
OpenVPN 135, 150
Original beim Anbieter 108
Outlook 228
.ovpn-Datei 150

P

Passwort ändern 69
Passwortregel 29, 69
PGP 108
Port 1194 139, 237
Port 443 124, 238
Port an Gerät 238
Port von außen für VPN 120
Port-Scan 96, 173
Ports (Übersicht) 237
Portweiterleitung 139, 237
Private Adressen (Monitor) 90, 102
Proxy-Mode 37, 235

Q

Quellpakete 32
QUIC 82, 173

R

Reaktivieren (TrutzMail-Adresse) 30, 113
Rechtliche Hinweise 42, 182, 243
Registrierung 27
Reiter (Geräte) 62
Reserve (Arbeitsspeicher) 50
Rettungspartition 190
Richtiger Name 70
root (Konto) 201
Root-Zertifikat 222
Router hinter Router 117

S

Schlüsselverwaltung 110
Security-Slider 158, 161

Seitenanalyse 96, 99
Service-Laufzeit abgelaufen 30, 68, 71, 113, 196
Service-Vertrag 182
Setup 23
Sicherung 188
Software-Updates (Karte) 50, 56, 182, 211
Software-Updates im Setup 26, 180
Speicher-Wächter 50, 210
Speichermedium tauschen 219, 220
Speicherverlauf 42
Sperren / Freischalten (Monitor) 96
Sperrseite 82
SSD tauschen 219, 220
SSH (Kommandozeile) 174, 201
Stammzertifikat 222
Standard für neu erkannte Geräte 58
Standard-Filterlisten 78
Standard-Gateway 37
Startseite 42
Statistiken 98
Support 216, 218
Support-Bericht 216
Systemgrenzen 50

T

Tank-Stick (Image aufspielen) 183, 185
Taste am Gehäuse 192, 213
Terminal (im Browser) 200, 210
Testpakete (Erreichbarkeit) 167
Thunderbird (Mail-Programm) 227
Transparent (intern) 60
TrutzBox ARM (LEDs) 20, 194
trutzbox.local 23, 41, 191, 209
TrutzBrowse 155, 161
TrutzBurg-Icon 160
TrutzChat 129
TrutzContent 74
TrutzDynDNS 116
TrutzDynDNS nur mit IPv6 119, 167
TrutzKennung 27
TrutzLegitimation 16, 219
TrutzMail 30, 103
TrutzSchlüssel 27
Tunnel wählen (OpenVPN oder WireGuard) 140
Tunnelblick 233

U

Unsaubere Abschaltungen 50
Updates 179
USB-Stick (Image aufspielen) 183, 185

V

Verbindungen (Monitor) 89
Verlaufskurve (Monitor) 89
Videodokumentation (trutzbox.de) 7
Videokonferenz 124, 126
Virtuelle Maschine 166, 185, 191
VLAN (LAN-Ext) 165, 189
VLAN-Kennung 164, 188
VPN 135
VPN über IPv6 148
VPN-Geräte im Monitor 90
VPN-Profil 148, 150

W

Wächter (Angriffsschutz) 173
Warteseite Software-Updates 26, 72, 180, 209
Wartungssystem 191
Webfilter 74
Webmail 105
Webmin 200
Werbeblocker-Blocker erlauben 83, 99
Werbeblocker-Sperre 82, 99
Werksreset 190
Windows 222, 232, 233
WireGuard 135, 140, 143
WireGuard-App 232
WireGuard-Zugang 70, 143
WLAN 168

X

XMPP 129, 230

Z

Zeitraum (Monitor) 96
Zertifikat 222
Zertifikatswarnung 205, 207
Zurücksetzen 190