TrutzBox Handbuch

Privatsphäre und Sicherheit, zuhause und in der Firma

Gilt für die TrutzBox EVO (64 Bit) ab Betriebssystem 2.5.0, Abbild V78

Ausgabe September 2026

Comidio GmbH · Eichendorffweg 2 · 65343 Eltville

Inhaltsverzeichnis

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 Kapitelnummer. Wenn Sie Ihre TrutzBox gerade erst ausgepackt haben, beginnen Sie mit Teil B: Kapitel 3 führt durch die Einrichtung, Kapitel 4 bringt Ihre Geräte unter den Schutz der Box.

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 „Kapitel 7" führen zum genannten Kapitel; 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 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 Box 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 Box es leistet. Wer gleich loslegen möchte, kann direkt zu Kapitel 3 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 Box 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 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 Tracker von Google 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, Sprachassistenten, Thermostate, Kameras. Viele dieser Geräte funken nach Hause, 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 Box 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 Box Kinder vor ungeeigneten Inhalten und alle vor Trackern und Schadsoftware. 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

Tracking 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. Sprachassistenten 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 Werbe- und Tracking-Server 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 Tracker angewiesen, sodass neue Tracker 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 Tracker auf der Seite arbeiten unverändert weiter.
- **Eine sichere E-Mail-Anwendung** schützt die E-Mail, aber weder das Surfen noch die übrigen Geräte im Haus.
- **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 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 Tracking-Daten 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 9). Erst beide Richtungen zusammen ergeben einen vollständigen Schutz. Deshalb bringt die Box 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
Kommerzielle Daten-Tracker	Verfolgen Ihr Surfverhalten über Werbe- und Analysedienste hinweg	TrutzBrowse und die Filterlisten (Kapitel 8 und 13)
Datenhändler	Kaufen, verknüpfen und verkaufen Profile aus vielen Quellen	TrutzBrowse, Filterlisten (Kapitel 8 und 13)
Geheimdienste und staatliche Autoritäten	Lesen unverschlüsselte Kommunikation mit	TrutzMail, TrutzChat und Videokonferenz mit durchgehender Verschlüsselung, alles auf Ihrer eigenen Box (Kapitel 10 und 11)
Internet-Kriminelle	Erpressungstrojaner, Phishing, Kontenübernahme	Firewall, Angriffsschutz und Webfilter (Kapitel 8 und 14)
Staatlich unterstützte Angreifer	Gezielte, lang laufende Angriffe auf Netzwerke	Firewall und Angriffsschutz mit Protokollierung (Kapitel 14)
Geräte mit zweifelhafter Datenpolitik	Fernseher, Assistenten und andere Geräte senden ungefragt Daten an Hersteller	Filtergruppen je Gerät und der Monitor, der alles sichtbar macht (Kapitel 6 und 9)

Etwas ausführlicher gesagt:

Kommerzielle Daten-Tracker sind Werbeplattformen und Analysedienste, die das Verhalten von Nutzern auf Webseiten und in Apps verfolgen, 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, Sprachassistenten und Apps mit aggressiven Tracking-Praktiken.

1.7 Die Funktionen im Überblick

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

TrutzContent, der Webfilter (Kapitel 8): 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 13): entfernt beim Surfen identifizierende Merkmale aus dem Datenverkehr, damit Tracker aus Browser und Gerät keinen wiedererkennbaren „Fingerabdruck" bilden können. Wie stark, bestimmen Sie mit dem Security-Slider: neun feste Stufen von L1 bis L9, dazu die Sonderstellung L10, auf Wunsch je Gerät und je Webseite.

TrutzMail, die sichere E-Mail (Kapitel 10): verschlüsselt E-Mails automatisch von Ende zu Ende, samt der sonst überall anfallenden Metadaten (wer schreibt wem wann). Die Schlüsselverwaltung übernimmt die Box; Sie schreiben einfach E-Mails wie bisher.

TrutzChat und TrutzMeeting (Kapitel 11): Nachrichten und Videokonferenzen, die vollständig auf Ihrer eigenen Box 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 Box diese Ausstattung mitbringt, sehen Sie am schnellsten unter **Systemeinstellungen → Vertrag und Pakete**. Dort steht, was Ihr Servicevertrag 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 5.3).

TrutzBase, Firewall und Angriffsschutz (Kapitel 14): 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 12): nimmt den Schutz mit auf Reisen. Ein verschlüsselter Tunnel verbindet Smartphone oder Laptop unterwegs mit Ihrer TrutzBox, als wären Sie vor Ort.

Der Monitor (Kapitel 9): 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 Box; nichts davon verlässt Ihr Haus.

> **Für Neugierige: Warum kein einfacher DNS-Filter?**
> Viele Werbeblocker-Boxen 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 Tracking-Bausteine einer sonst erlaubten Seite, 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 Box 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 4.

> **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 3 (Einrichtung), dann Kapitel 4 (Geräte anschließen). Damit läuft der Grundschutz.
Kinder oder Jugendliche schützen	Kapitel 6 (Geräte zuordnen) und Kapitel 8 (Filtergruppen und Jugendschutz).
Wissen, was die Geräte im Haus eigentlich tun	Kapitel 9 (Monitor). Besonders aufschlussreich bei Fernsehern und Haustechnik.
Sicher E-Mails schreiben	Kapitel 10 (TrutzMail), dazu Kapitel 7 für weitere Postfächer.
Unterwegs geschützt sein	Kapitel 12 (TrutzVPN).
Etwas funktioniert nicht	Kapitel 17 (Was tun, wenn) und bei Bedarf Kapitel 18 (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 3); 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 Box 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 2.5.
- **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 Box 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 Box später einmal neu eingerichtet werden muss. 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 Box 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 15.7); 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 Box 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 12).

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 14.2).

> **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 Box 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 Box

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 Box gesund sind, sehen Sie nicht an den LEDs, sondern auf der Seite **Betriebszustand** der Verwaltungsoberfläche (Kapitel 5.2).

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

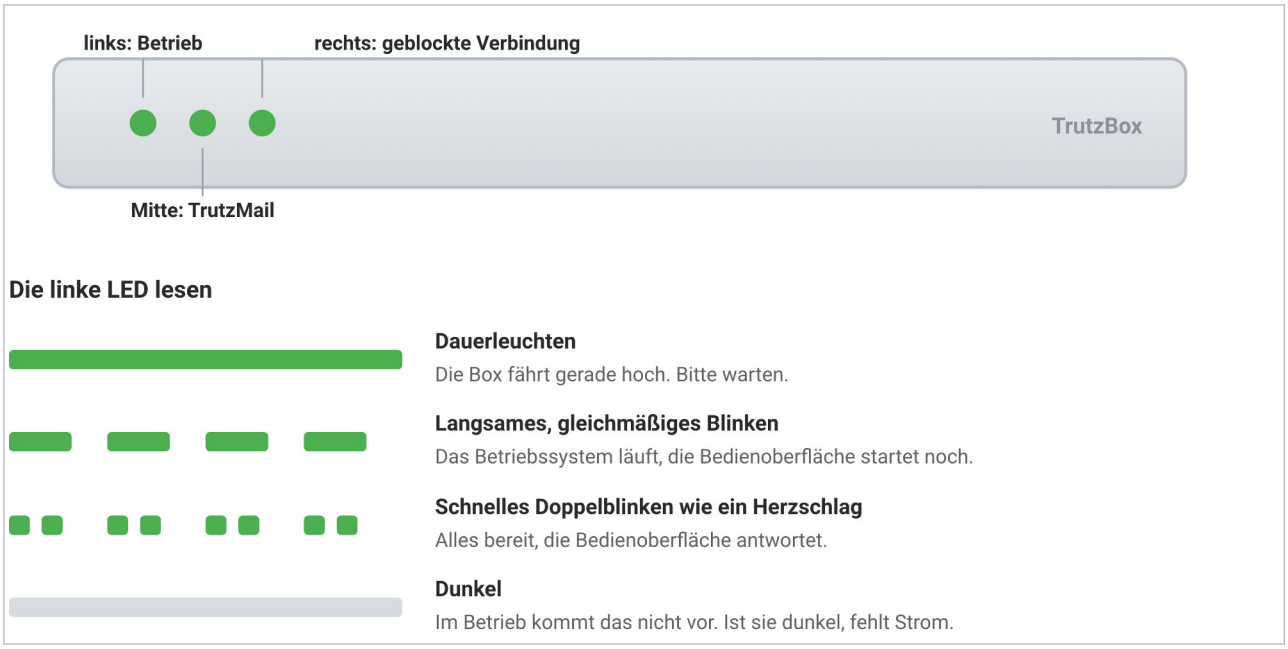


Abbildung 2-3: Die drei LEDs an der Gerätefront und die Blinkmuster der linken LED. (© 2026 Comidio GmbH)

- **Die linke LED** zeigt den Betriebszustand. Beim Start leuchtet sie zunächst dauerhaft (die Box 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** im Abschnitt **LED-Anzeige an der Box**. 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 im Haus normal gearbeitet wird, hat den besten Eindruck davon, was die Box leistet.

Direkt nach dem Einstecken braucht die Box einen Moment zum Starten. Beim allerersten Start und nach Updates kann diese Phase mehrere Minuten dauern. Danach geht es weiter mit der 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 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 Box auf eine feste, ebene Fläche, am besten direkt neben den Internet-Router. Kurze Wege sparen Kabel und Fehlerquellen.
- Lassen Sie ringsum etwas Luft. Die Box 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 Box angestoßen werden kann.
- Sorgen Sie für eine dauerhaft belegte Steckdose. Wer die Box an eine schaltbare Steckdosenleiste hängt, schaltet sie versehentlich mit ab.

Die Betriebstemperatur beobachtet die Box 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 Box startet danach von selbst wieder. Geben Sie ihr anschließend einen Moment, bevor Sie die Oberfläche aufrufen; nach einem Update kann der Start mehrere Minuten in Anspruch nehmen.

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 Box.

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 6).

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 17.8 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 Box an Ihren Internet-Router an und durchlaufen anschließend das Einrichtungsprogramm, das Setup. Es führt Sie in acht Schritten von der ersten Verbindung bis zur fertig eingerichteten Box. 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 Box allein; Sie können nebenher etwas anderes tun.

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 Box von einem PC oder Laptop, der ohnehin schon in Ihrem Heimnetz am Router hängt; ob per Kabel oder WLAN, spielt keine Rolle. Ihre Geräte schließen Sie erst nach dem Setup an die Innenseite der Box an.

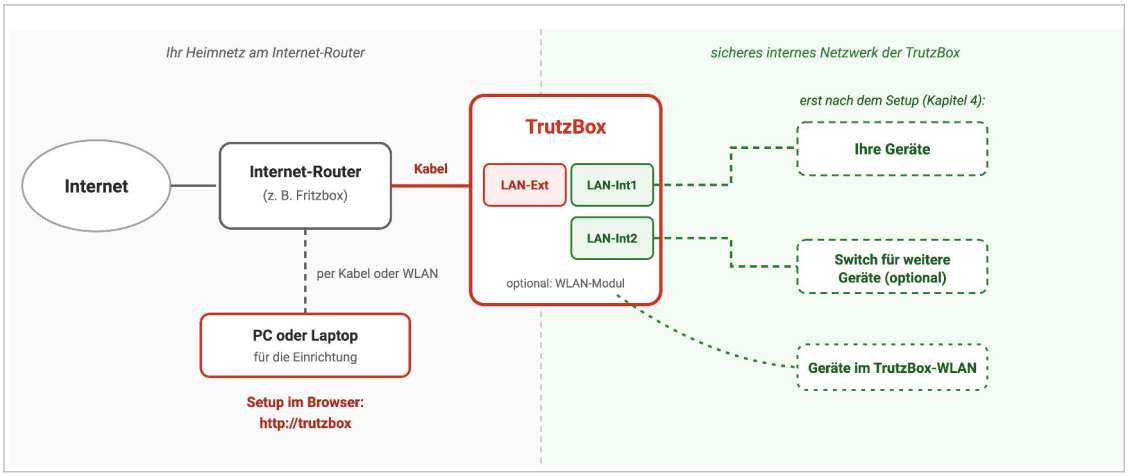


Abbildung 3-1: So wird die TrutzBox angeschlossen: ein Kabel vom Router zu LAN-Ext. Eingerichtet wird sie von einem PC in Ihrem Heimnetz; Ihre Geräte kommen erst danach an LAN-Int1, LAN-Int2 oder ins TrutzBox-WLAN. (© 2026 Comidio GmbH)

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 Box 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 Box hindurch. Nur so kann sie Tracker blockieren, Filter durchsetzen und Angriffe abwehren. 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 Heimnetz einen Browser und geben Sie in die Adresszeile ein:

```
http://trutzbox
```

Die Box meldet sich mit dem Setup-Assistenten. Deutet der Browser den Namen als Suchbegriff oder findet er die Box 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 Fritzbox steht die Liste unter **Heimnetz → Netzwerk**.

Falls zuerst ein Wartebildschirm erscheint

Direkt nach dem ersten Start prüft die Box, ob es neue Updates gibt. Dann sehen Sie die Meldung *„Aktualisierung im Hintergrund läuft"*. Lassen Sie das Fenster einfach geöffnet. Die Einrichtung wird automatisch fortgesetzt, sobald der Vorgang abgeschlossen ist.

Links im Setup sehen Sie die acht Stationen der Einrichtung. Der fett hervorgehobene Eintrag zeigt immer, wo Sie gerade stehen. Mit **Weiter** und **Zurück** bewegen Sie sich zwischen den Schritten.

3.3 Schritt „Willkommen"

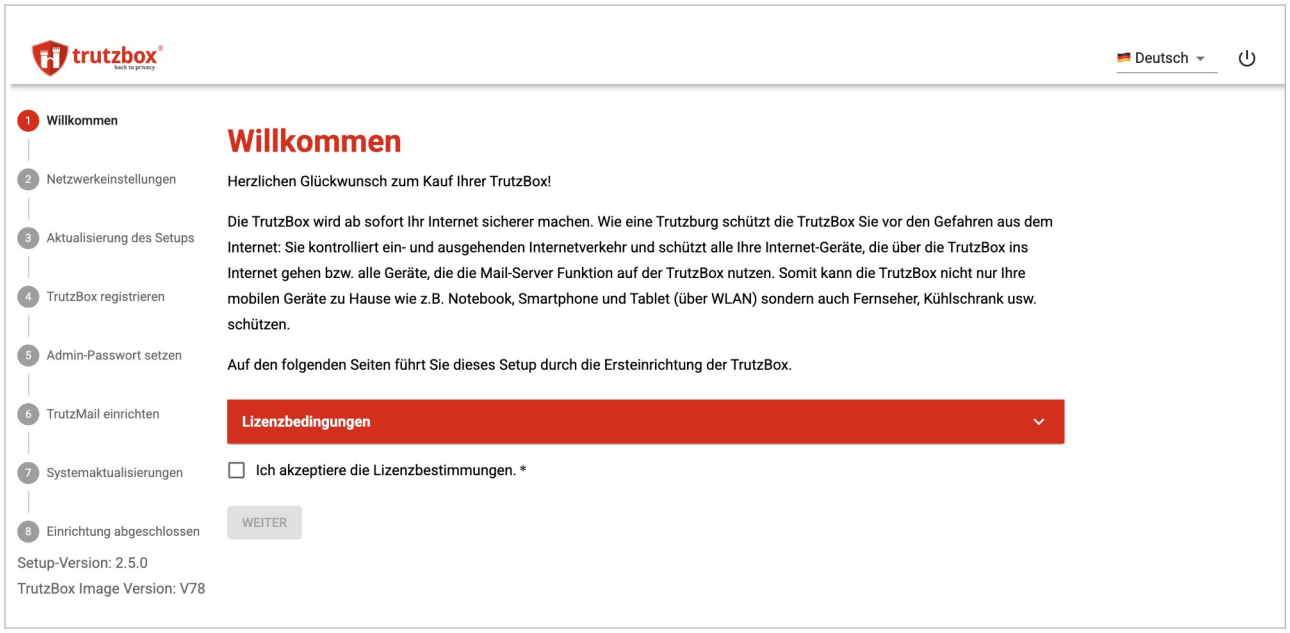


Abbildung 3-2: Der erste Schritt: Lizenzbestimmungen lesen und akzeptieren. (© 2026 Comidio GmbH)

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"

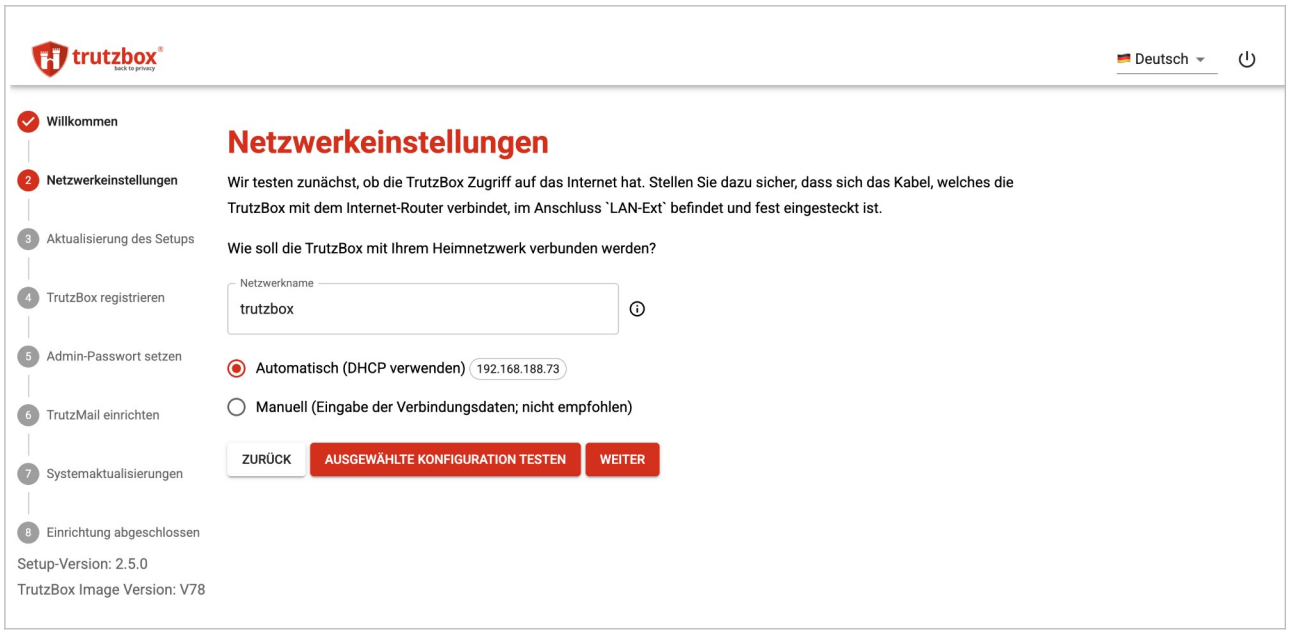


Abbildung 3-3: Der Verbindungstest ist gelungen: Die Box hat Zugriff auf das Internet. (© 2026 Comidio GmbH)

Jetzt prüft die Box, ob sie über Ihren Router ins Internet kommt. Belassen Sie die Auswahl auf **Automatisch (DHCP verwenden)**. Das ist für praktisch alle Netzwerke richtig. Klicken Sie dann auf **Ausgewählte Konfiguration Testen**.

Erscheint die grüne Meldung *„Die Verbindung wurde erfolgreich hergestellt."*, klicken Sie auf **Weiter**.

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 Box nicht mehr erreichbar ist. Die Box testet die neue Konfiguration deshalb erst und stellt bei einem Fehlschlag die vorherige Einstellung automatisch wieder her.

> **Wenn der Test fehlschlägt**
>
> Meldet die Box *„Der Verbindungsaufbau ist fehlgeschlagen"*, 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 den Test einfach wiederholen.

3.5 Schritt „Aktualisierung des Setups" und Sicherung einspielen

Bevor es weitergeht, bringt sich das Einrichtungsprogramm selbst auf den neuesten Stand. Sie können den Fortschritt beobachten; sobald *„Das Setup-Paket ist auf dem neusten Stand"* erscheint, geht es mit **Weiter** voran. Wie lange das dauert, hängt von Ihrer Internet-Geschwindigkeit ab. Meist sind es nur wenige Minuten.

Sicherung einspielen (Backup laden): Ersetzen Sie eine bestehende TrutzBox oder richten Sie Ihre Box nach einem Zurücksetzen neu ein? Dann können Sie in diesem Schritt über die Schaltfläche **Backup laden** eine vorhandene Sicherungsdatei einspielen. Die Box übernimmt daraus den kompletten gesicherten Zustand, also Benutzer, Postfächer und Einstellungen. Ist die Wiederherstellung gelungen, führt **Weiter** 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 16.

3.6 Schritt „TrutzBox registrieren"

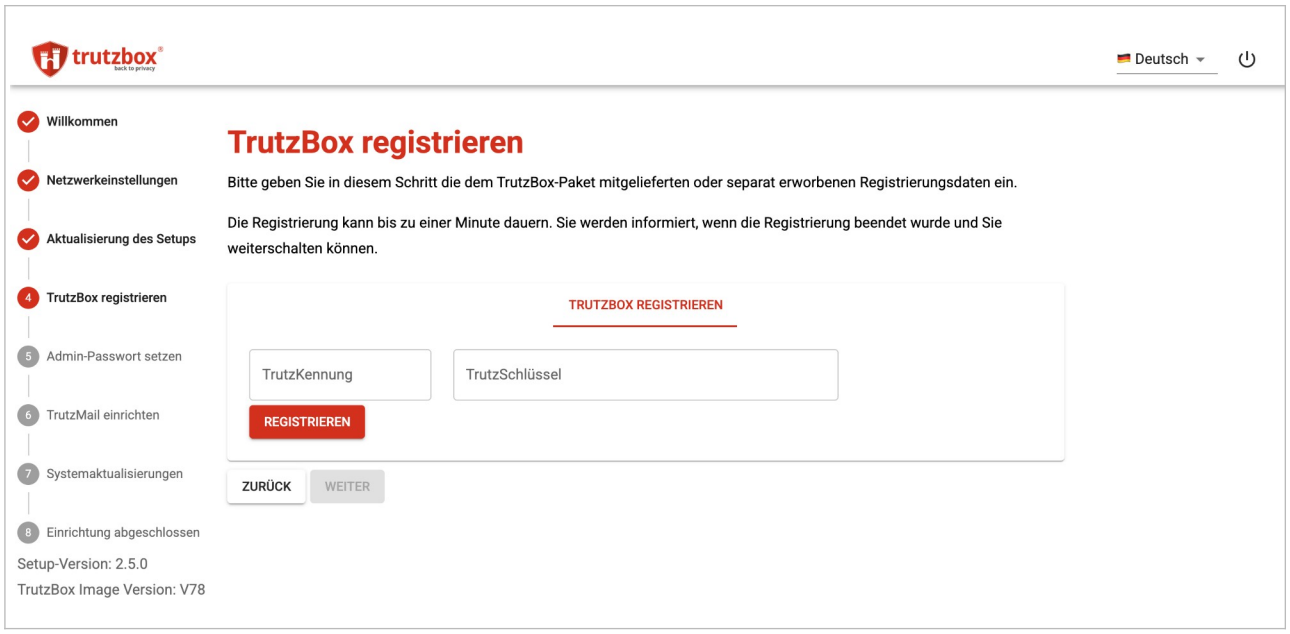


Abbildung 3-4: Registrierung mit TrutzKennung und TrutzSchlüssel vom Beileger. (© 2026 Comidio GmbH)

Mit der Registrierung wird Ihre Box bei Comidio freigeschaltet. Dabei entstehen auch die Zertifikate, mit denen sich Ihre Box 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.

> **Fehlermeldung bei der Registrierung?**
>
> Schon beim Eintippen prüft die Box 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 Box darunter den Grund: Hat der Registrierungsserver die Anmeldung abgelehnt, stimmen TrutzKennung und TrutzSchlüssel nicht zusammen; ist er nicht erreichbar, fehlt der Box der Internet-Zugang (zurück zum Schritt Netzwerkeinstellungen). Bleibt der Fehler bestehen, hilft der Comidio-Support (Kapitel 18) weiter.

3.7 Schritt „Admin-Passwort setzen"

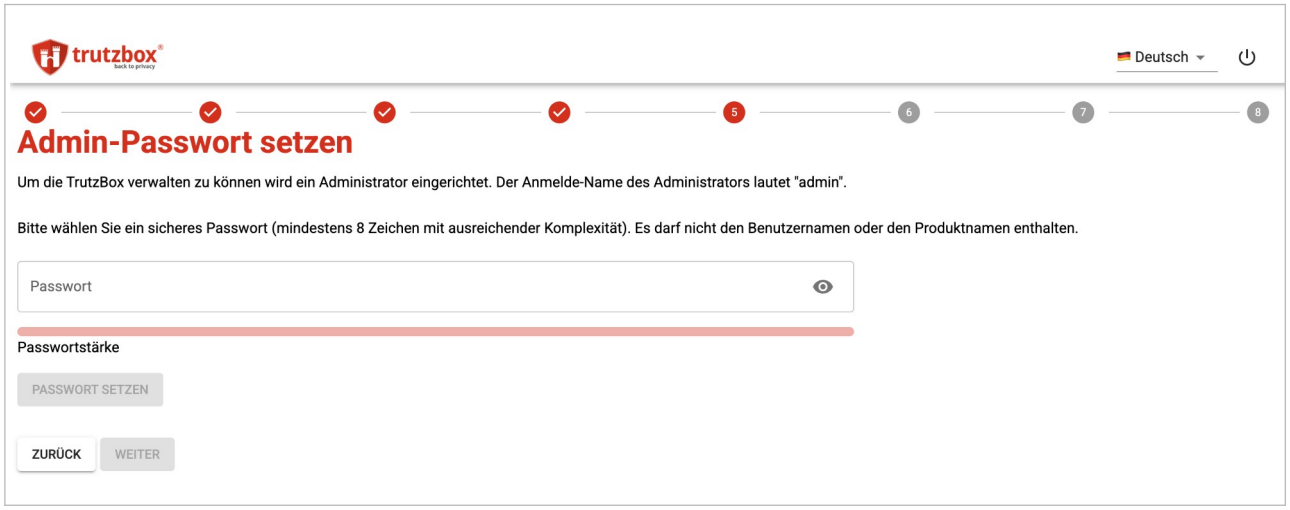


Abbildung 3-5: Das Passwort für den Verwalter-Zugang „admin" festlegen. (© 2026 Comidio GmbH)

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, es darf weder „admin" noch „trutzbox" noch „comidio" enthalten, und es muss eine Komplexitätsprüfung bestehen, also verschiedene Zeichenarten mischen. Der Balken *Passwortstärke* zeigt Ihnen sofort, 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"

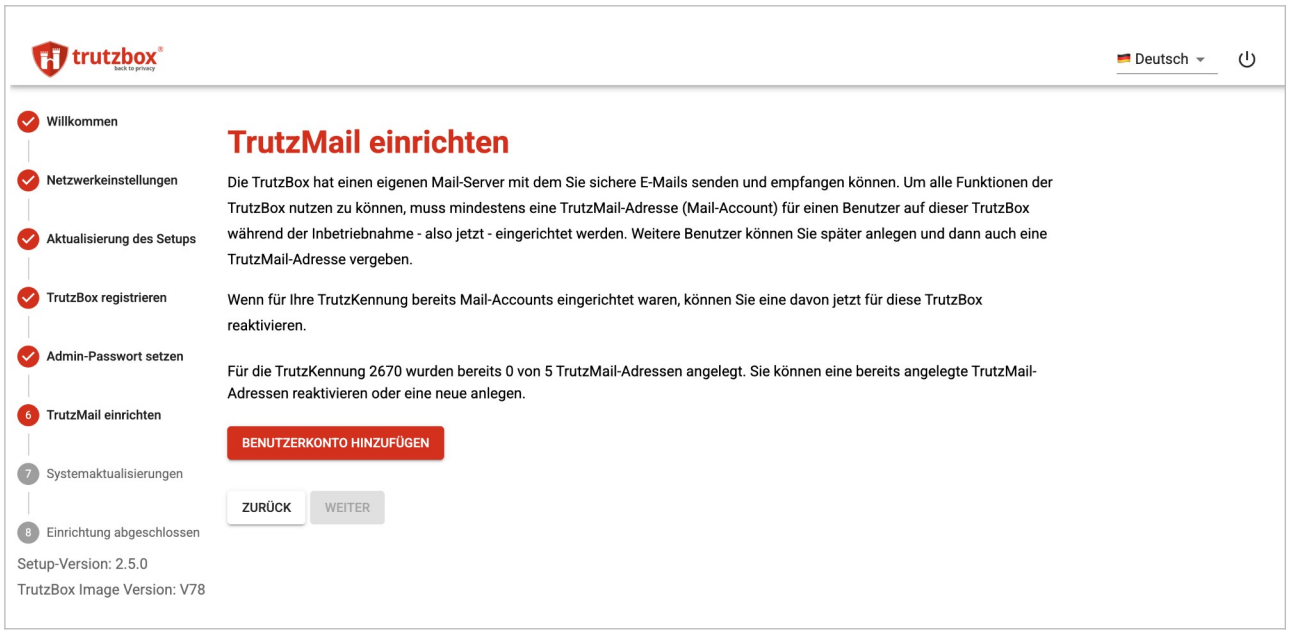


Abbildung 3-6: Die erste TrutzMail-Adresse anlegen, hier im Dialog „Neuen Benutzer + TrutzMail hinzufügen". (© 2026 Comidio GmbH)

Die TrutzBox bringt einen eigenen Mail-Server mit, über den Sie später verschlüsselte E-Mails senden und empfangen. Damit alle Funktionen der Box nutzbar sind, muss jetzt mindestens eine **TrutzMail-Adresse** angelegt werden.

1. Klicken Sie auf **Benutzerkonto hinzufügen**.
2. Tragen Sie unter **Richtiger Name** den Namen ein, der bei Empfängern angezeigt wird, zum Beispiel „Anna Muster".
3. Wählen Sie den **Anmelde-Namen**. Er wird zugleich der vordere Teil der Mail-Adresse; die Endung `@comidio.email` ergänzt die Box automatisch.
4. Vergeben Sie ein Passwort für dieses Postfach (mindestens 6 Zeichen) und klicken Sie auf **Hinzufügen**.

Die Untergrenze von 6 Zeichen gilt nur hier im Setup. Legen Sie später im Admin-Panel weitere Postfächer an, verlangt die Oberfläche dort mindestens 8 Zeichen (Kapitel 7). Wählen Sie deshalb am besten gleich ein Passwort, das der strengeren Regel genügt.

Die neue Adresse erscheint danach unter *Aktivierte Benutzer*, und die Box bestätigt: *„Soeben wurde folgende TrutzMail-Adresse eingerichtet."* Weitere Postfächer für Familie oder Kollegen legen Sie später bequem im Admin-Bereich an (Kapitel 7).

Hatten Sie schon einmal eine TrutzBox mit dieser TrutzKennung im Einsatz, zeigt der Schritt zusätzlich *Reaktivierbare Benutzer*. Vorhandene Adressen übernehmen Sie dann einfach mit **Aktivieren**.

3.9 Schritt „Systemaktualisierungen"

Jetzt prüft die Box ein letztes Mal, ob alle installierten Programme auf dem neuesten Stand sind. In aller Regel ist das nach wenigen Sekunden erledigt, denn die Box hat bereits beim Starten alle

verfügbaren Updates eingespielt. Nur wenn währenddessen etwas Neues erschienen ist, dauert es etwas länger. Sobald *„Die TrutzBox ist auf dem neusten Stand"* erscheint, klicken Sie auf **Weiter**.

3.10 Schritt „Einrichtung abgeschlossen"

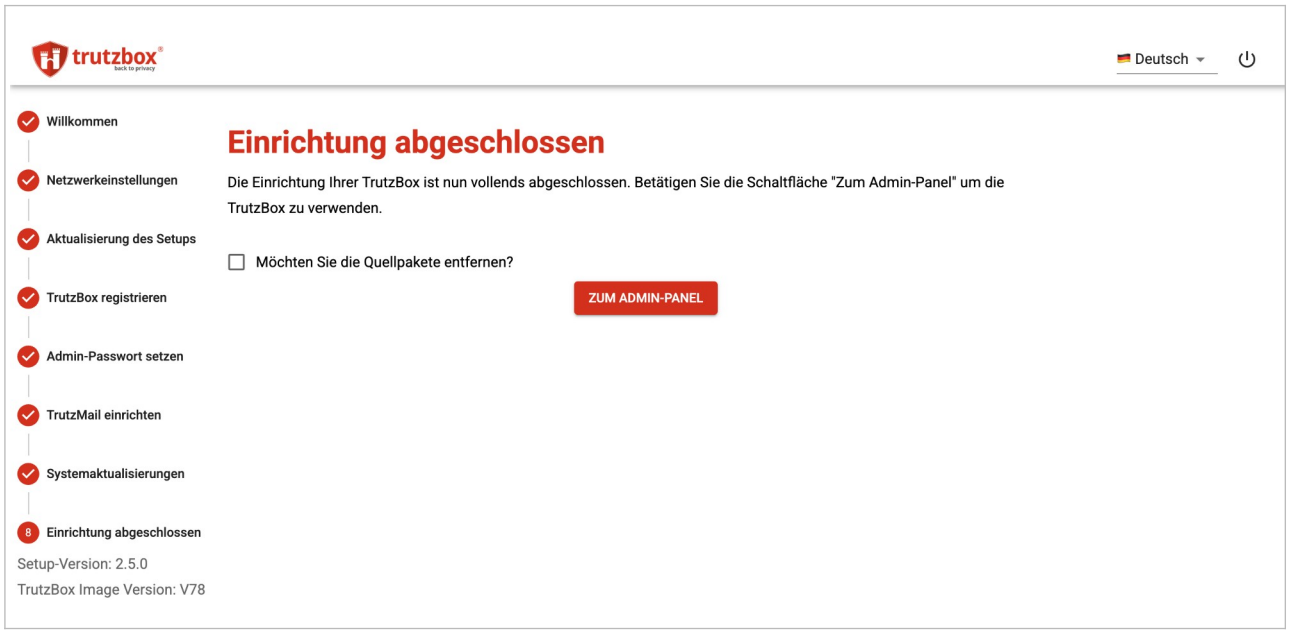


Abbildung 3-7: Geschafft: Mit „Zum Admin-Panel" geht es in die Verwaltungsoberfläche. (© 2026 Comidio GmbH)

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 Box 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?"* können Sie gesetzt lassen: Es löscht lediglich Installationsdateien, die nach der Einrichtung nicht mehr gebraucht werden, und schafft Platz.

3.11 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 das geht, ob per Kabel, über das TrutzBox-WLAN oder im Proxy-Mode, zeigt ausführlich das folgende Kapitel 4 „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 Schritt 3.7 an.
- **Geräte anschließen:** Verbinden Sie Ihre Geräte nach und nach mit der TrutzBox (Kapitel 4).
- **Geräte benennen und einordnen:** Geben Sie den Geräten anschließend sprechende Namen und ordnen Sie sie Filtergruppen zu (Kapitel 6).

Was Sie im Admin-Panel nach der Anmeldung erwartet, also die Startseite mit ihren Kacheln und die Ampel für den Betriebszustand, erklärt Kapitel 5. Es lohnt sich, dort einmal in Ruhe hineinzusehen, bevor Sie mit dem Einordnen der Geräte beginnen.

3.12 Der Ablauf auf einen Blick

Schritt	Was passiert	Dauer
Anschließen	Kabel vom Router in LAN-Ext, Netzteil einstecken; eingerichtet wird vom PC im Heimnetz	wenige Minuten
Willkommen	Lizenzbedingungen bestätigen	kurz
Netzwerkeinstellungen	Verbindungstest zum Internet	kurz
Aktualisierung des Setups	Einrichtungsprogramm aktualisiert sich; wahlweise Sicherung einspielen	wenige Minuten
TrutzBox registrieren	TrutzKennung und TrutzSchlüssel eingeben	laut Oberfläche bis zu einer Minute
Admin-Passwort setzen	Passwort für den Verwalterzugang festlegen	kurz
TrutzMail einrichten	Erste TrutzMail-Adresse anlegen oder reaktivieren	kurz
Systemaktualisierungen	Prüfung, ob noch Aktualisierungen offen sind	meist wenige Sekunden
Einrichtung abgeschlossen	Weiter ins Admin-Panel; danach die Geräte anschließen (Kapitel 4)	kurz

Häufige Fragen zur Einrichtung

Muss ich die TrutzBox nach dem Setup neu starten?

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

Kann ich das Setup abbrechen und später fortsetzen?

Ja. Die Box merkt sich den erreichten Schritt. Rufen Sie einfach wieder `http://trutzbox` auf, und das Setup macht dort weiter, wo Sie aufgehört haben. Über das Menü rechts oben lässt sich die Box auch jederzeit sauber ausschalten.

Ich möchte die Einrichtung komplett neu beginnen. Geht das?

Das geht erst, 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. Der Vorgang dauert je nach Modell und Internet-Geschwindigkeit etwa 5 bis 25 Minuten. Mehr dazu in Kapitel 16. 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 3 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 Box: Computer, Smartphones, Tablets, Fernseher und Haustechnik, zuhause genauso wie im Büro.

> **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 19.

4.1 Drei Wege zur TrutzBox

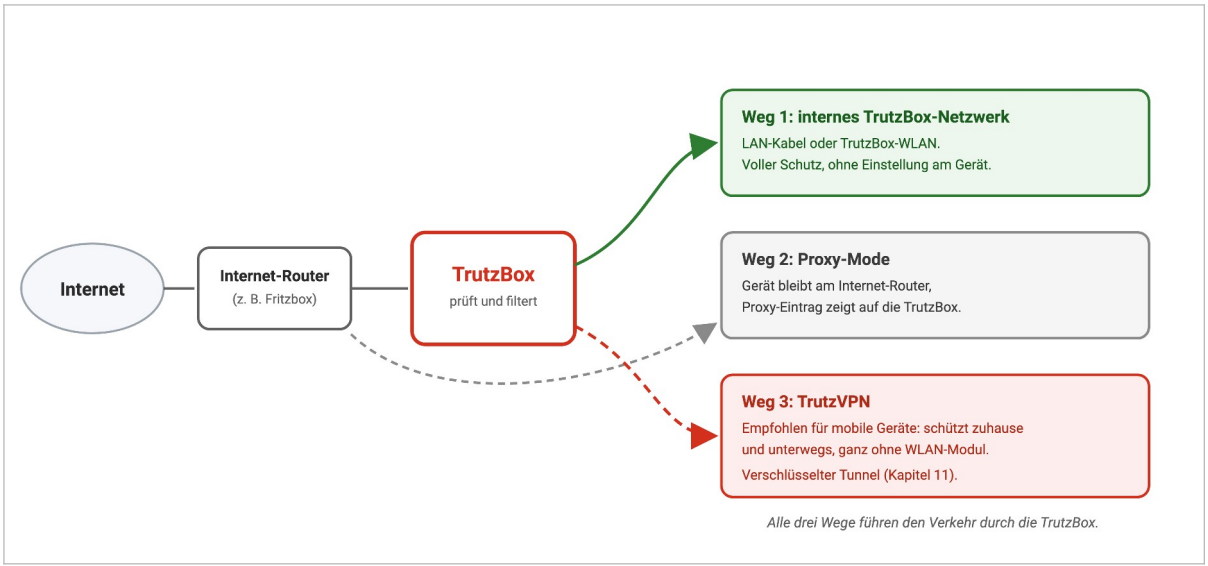


Abbildung 4-1: Drei Wege, ein Gerät mit der TrutzBox zu verbinden: internes Netzwerk, Proxy-Mode und TrutzVPN. (© 2026 Comidio GmbH)

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

- **Weg 1, das interne TrutzBox-Netzwerk (empfohlen für alles, was im Haus 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 Box, 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 zuhause und unterwegs gleichermaßen, und die TrutzBox braucht dafür kein eingebautes WLAN-Modul. Kapitel 12 beschreibt die Einrichtung.

4.2 Weg 1: Gerät ans interne TrutzBox-Netzwerk hängen

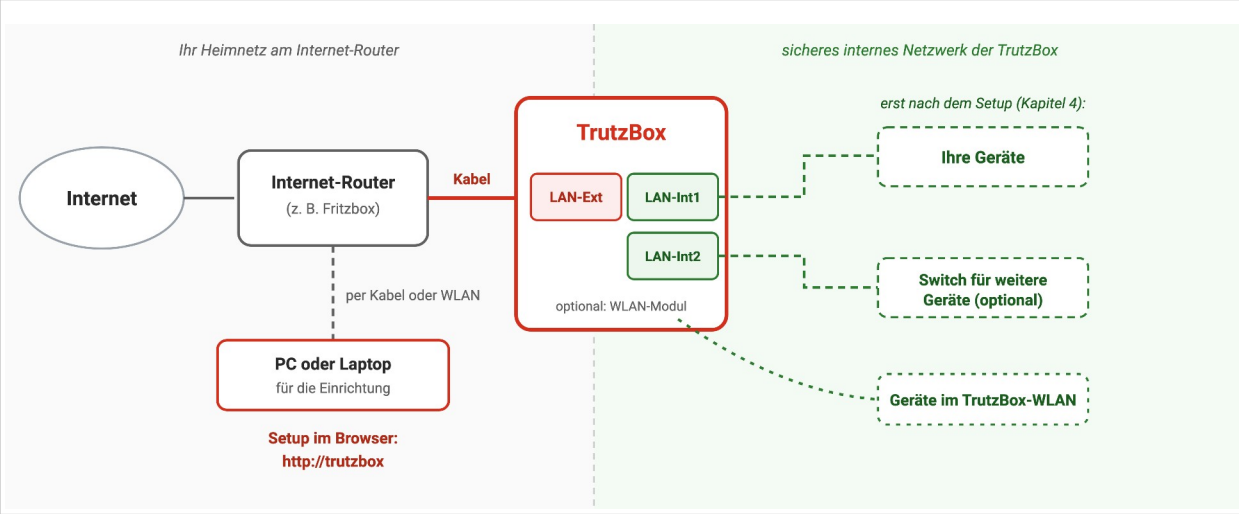


Abbildung 4-2: Das interne Netzwerk der TrutzBox: alles rechts der Box ist geschützt. (© 2026 Comidio GmbH)

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 14.2). 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 mit dem Verbindungstyp „Transparent". Geben Sie ihm dort gleich einen sprechenden Namen (Kapitel 6).

Das Gerät bezieht seine Adresse automatisch aus dem internen Bereich der Box. 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 Box im Vorbeigehen auf ihren eigenen Filter um; nur was an die Box 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 Box 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 Box 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 Box 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.

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 Box einmal nicht erreichbar sein, geht das Gerät direkt weiter, 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.

Das Gerät taucht anschließend unter **Verwaltung → Geräte** mit dem Verbindungstyp „Proxy" auf, im Monitor erscheint es 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 Box vorbei, ebenso Programme, die einen eingetragenen Proxy bewusst ignorieren.

4.4 Weg 3: TrutzVPN für mobile Geräte

Smartphones und Tablets wechseln ständig das Netz: zuhause 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 12 Schritt für Schritt.

4.5 Welcher Weg für welches Gerät?

Gerät	Empfohlener Weg
PC, Laptop im Haus	Weg 1, per Kabel oder TrutzBox-WLAN
Smartphone, Tablet	Weg 3 (TrutzVPN), dann ist das Gerät zuhause und unterwegs geschützt
Geräte von Kindern	Weg 1, weil sich nur dieser Weg am Gerät nicht abschalten lässt

Gerät	Empfohlener Weg
Fernseher, Streaming-Box, Spielkonsole	Weg 1
Haustechnik, Kameras, Thermostate	Weg 1, dazu eine enge Filtergruppe (Kapitel 8)
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 13) oder wenn ein Mail- oder Chat-Programm auf dem Gerät sich mit der TrutzBox verbinden soll (Kapitel 10 und 11), kommt das Root-Zertifikat ins Spiel, und dafür gibt es Kapitel 19.

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 Box laufen (Kapitel 9).

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 17.7 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 Box 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 Heimnetz am Internet-Router. 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 seinen normalen Gang geht.

5.1 Die Startseite lesen

Menüpfad: Übersicht

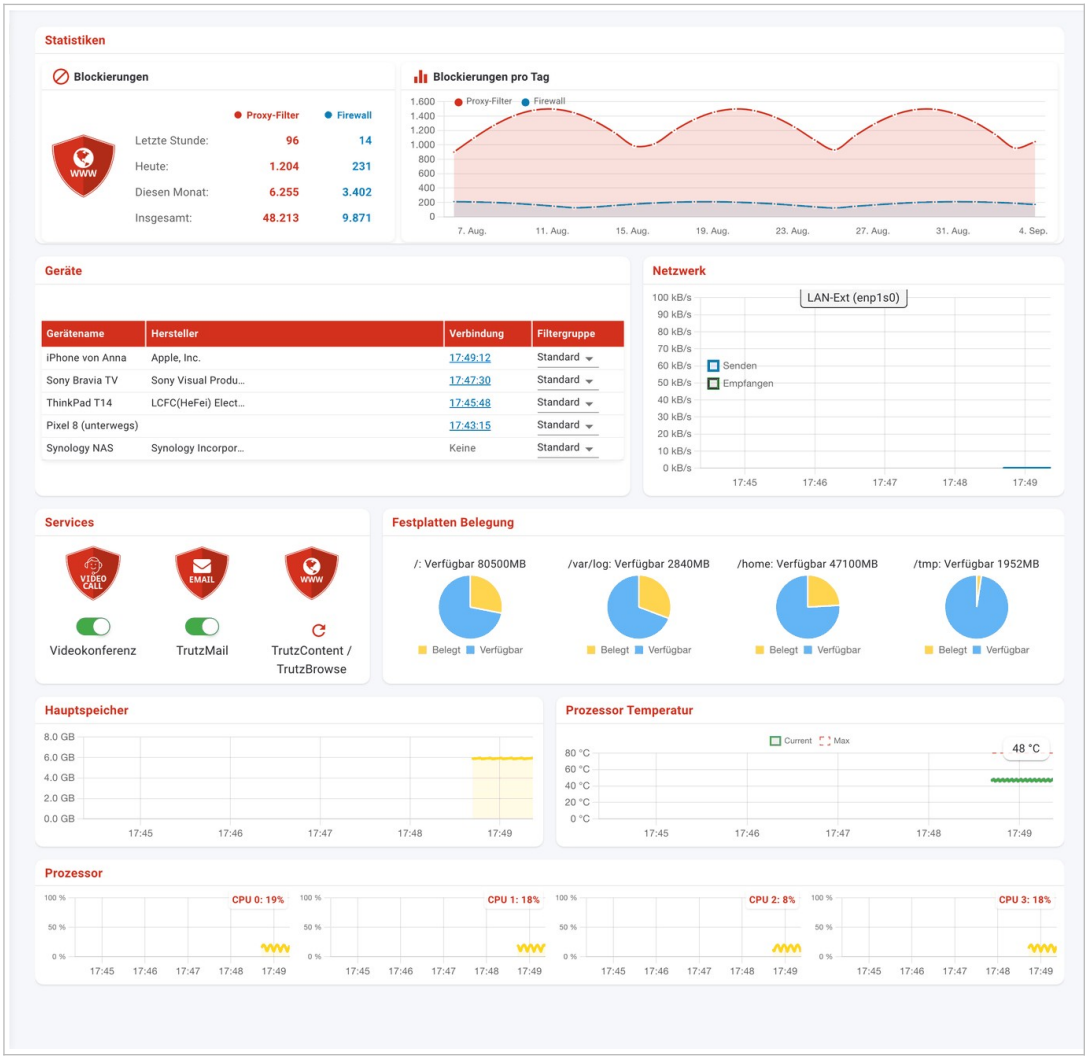


Abbildung 5-1: Die Startseite fasst das Wichtigste zusammen: Blockierungen, Geräte, Netzwerk und Auslastung der Box. (© 2026 Comidio GmbH)

Nach der Anmeldung begrüßt Sie eine Seite aus Kacheln; 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 Box heute blockiert? Ein Klick auf eine Kachel führt jeweils zur ausführlichen Seite, die Blockierungs-Zahl etwa öffnet die passende Ansicht im Monitor.

Die einzelnen Kacheln im Überblick:

- **Statistiken:** oben links die Anzahl der geblockten Verbindungen, aufgeschlüsselt nach der letzten Stunde, heute, diesem Monat und insgesamt. Daneben zeigt ein Zeitdiagramm die geblockten Verbindungen pro Tag. Diese Zahlen sind der schnellste Beleg dafür, dass die Box tatsächlich arbeitet. Sie erscheinen allerdings erst, wenn die Statistik eingeschaltet ist; ab Werk ist sie ausgeschaltet, und wie Sie sie einschalten, steht in Kapitel 9.7.
- **Geräte:** alle mit der TrutzBox verbundenen Geräte mit den Spalten Gerätename, Hersteller, Letzte Proxy-Verbindung, Filtergruppe und Verbindung. Ein Klick auf die Verbindungszeit öffnet das Verbindungsprotokoll genau dieses Geräts im Monitor. Die vollständige Liste mit allen Einstellmöglichkeiten finden Sie in Kapitel 6.
- **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 das Haus verlässt oder hereinkommt.
- **Services:** drei Symbole für **TrutzMeeting** (Videokonferenz), **TrutzMail** und **TrutzContent** mit **TrutzBrowse**. Ein rotes Symbol bedeutet aktiv, ein graues inaktiv. Ein Klick auf das Symbol von TrutzMeeting oder TrutzMail schaltet den Dienst ein oder aus; das Symbol für TrutzContent und TrutzBrowse startet den Webfilter dagegen 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.
- **Hauptspeicher:** ein Zeitdiagramm der Arbeitsspeicher-Auslastung. Die farbige Linie markiert den aktuell belegten Speicher, die Achse den maximal verfügbaren.
- **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 2.4).
- **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 Box geordnet herunter beziehungsweise starten sie neu.

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

Das Menü ist in vier Bereiche gegliedert. 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 Kacheln	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 → 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
Netzwerk → Netzwerkdienste	Verschlüsselte Namensauflösung und Zeitserver	14.3
Netzwerk → WLAN	Eigenes Funknetz der Box	14.2
Netzwerk → Fernzugriff	TrutzVPN einrichten und prüfen	12
Systemeinstellungen → Betriebszustand	Ampel, Karten, Verlauf, Support-Bericht	5.2, 18
Systemeinstellungen → Vertrag und Pakete	Servicevertrag, Kontingent, Hardware, Versionen	15, 7.5
Systemeinstellungen → Sichern und Wiederherstellen	Sicherung anlegen, einspielen, zurücksetzen	16
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, sofern die Statistik eingeschaltet ist. Die Kachel **Geräte** sagt, ob ein Gerät auftaucht, das dort nicht hingehört. Alles Weitere ist Hintergrundinformation.

5.2 Betriebszustand: die Ampel lesen

Menüpfad: Systemeinstellungen → Betriebszustand

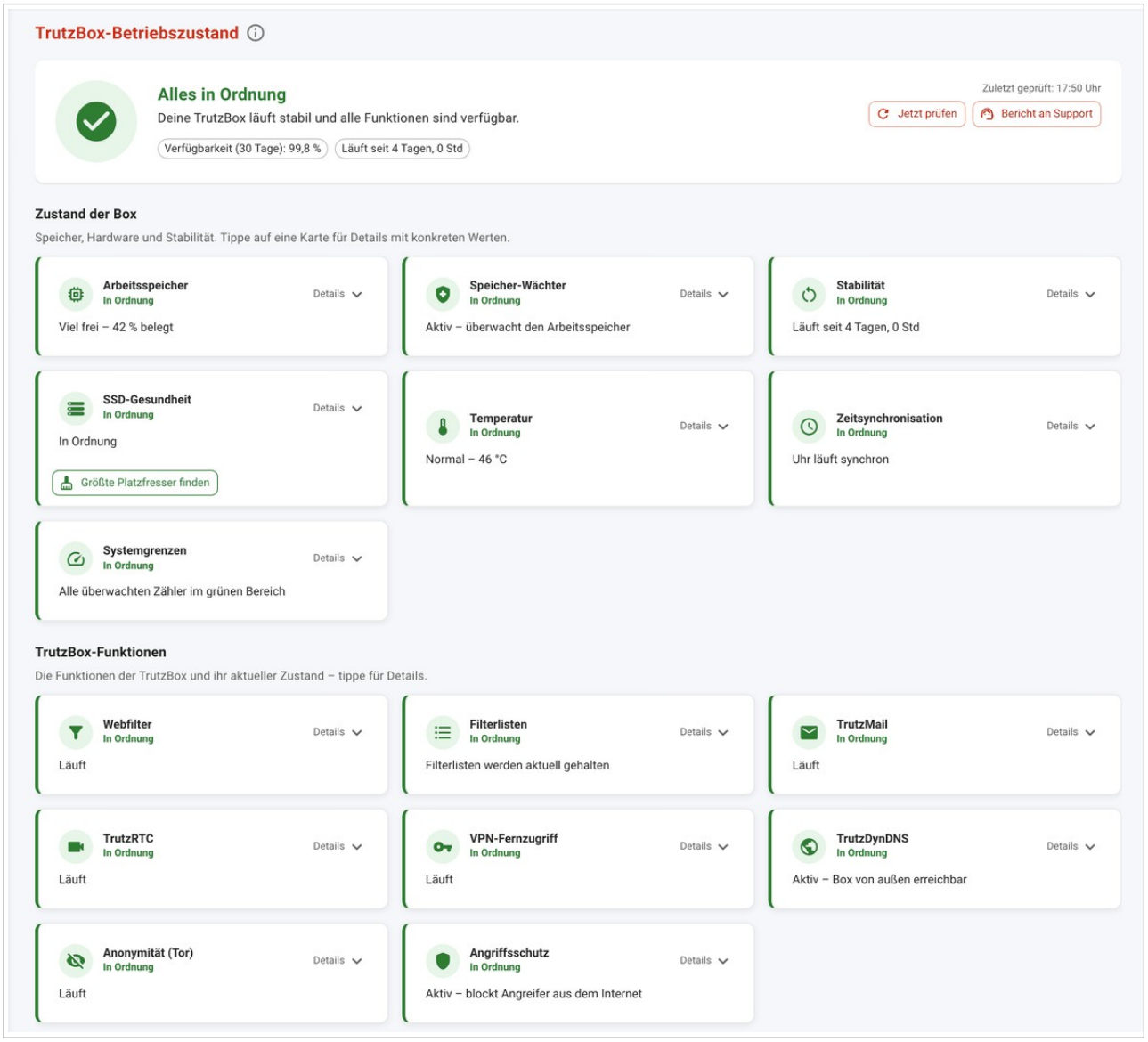


Abbildung 5-2: Der Betriebszustand: eine Ampel für den Gesamtzustand, darunter die einzelnen Bereiche. (© 2026 Comidio GmbH)

Die Seite **Systemeinstellungen → Betriebszustand** ist die Gesundheitsanzeige Ihrer Box. 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. Ganz oben steht eine einzige Ampel für den Gesamtzustand:

- **Grün:** Alles in Ordnung. Sie müssen nichts tun.
- **Gelb:** Auffällig. Etwas verdient einen Blick, der Schutz läuft aber weiter, zum Beispiel wenn bereitstehende Filterlisten länger nicht installiert wurden.
- **Rot:** Kritisch. Ein Bereich braucht Ihre Aufmerksamkeit; die betroffene Karte darunter nennt Ursache und Abhilfe in Klartext.
- **Neutral:** 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.

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.

Drei Schaltflächen gehören zur Ampel:

- **Jetzt prüfen:** stößt die Prüfung sofort neu an, ohne auf den nächsten Turnus zu warten.
- **Ampel zurücksetzen:** quittiert Hinweise, die Sie zur Kenntnis genommen haben, sodass die Anzeige wieder von vorn beginnt.
- **Bericht an Support:** stellt alle für eine Anfrage relevanten Angaben zusammen.

> **Der kürzeste Weg zum Support**
>
> Auf dieser Seite sitzt auch die Schaltfläche **Bericht an Support**: Sie sammelt alle relevanten Angaben ein und lässt sie ansehen, kopieren, als Datei sichern oder an Ihr Mailprogramm übergeben. Beim letzten Weg öffnet sich lediglich eine vorbereitete Nachricht; abgeschickt wird sie erst, wenn Sie es selbst tun. Die Oberfläche weist eigens darauf hin. Mehr dazu in Kapitel 18.

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 „TrutzRTC aus- und wieder einschalten".

Zustand der Box 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	Die aktuelle Auslastung des Arbeitsspeichers. Die Details schlüsseln

Karte	Was sie zeigt
	zusätzlich den Speicherbedarf von Webfilter und Web-Server einzeln auf und nennen die Schwelle, ab welcher der Speicher-Wächter eingreift.
Speicher-Wächter	Überwacht den Arbeitsspeicher und hält bei Knappheit gezielt zuerst TrutzRTC und danach TrutzMail an, damit die Box 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. 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.
Temperatur	Die aktuelle Betriebstemperatur der Hardware.
Zeitsynchronisation	Ob die Uhr der Box mit vertrauenswürdigen Zeitservern abgeglichen ist. Eine falsche Uhrzeit stört verschlüsselte Verbindungen und Updates. Direkt nach einem Neustart steht hier für einige Minuten „Synchronisierung läuft".
Systemgrenzen	Betriebsmittel, die knapp werden können, ohne dass Prozessor oder Arbeitsspeicher auffällig aussehen. Der nächste Abschnitt erklärt die Kachel 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 wie viele 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 Box unter einem festen Namen von außen erreichbar ist.
- **Anonymität (Tor):** die Anbindung an das Tor-Netzwerk.
- **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.

Wie viel hinter einer einzelnen Karte stecken kann, zeigt das Beispiel **Filterlisten**: Aufgeklappt nennt sie Stand und Installationszeitpunkt der Listen, die Paketversion, die Zahl der blockierten Adressen und der aktiven Filter sowie 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

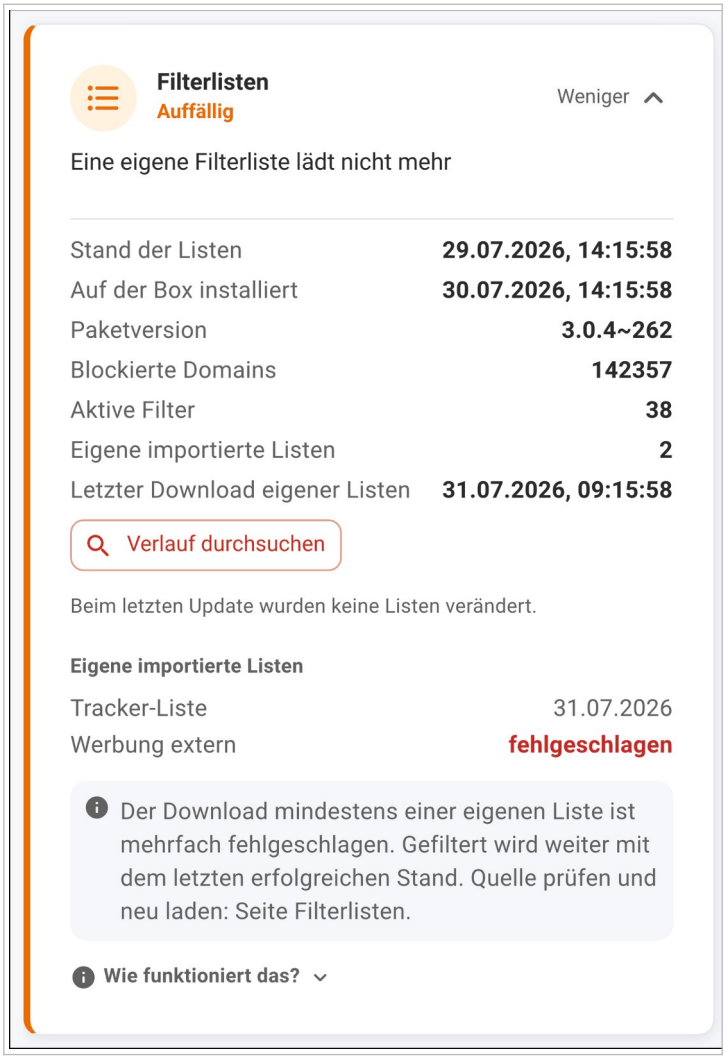


Abbildung 5-3: Eine aufgeklappte Karte am Beispiel der Filterlisten: Stand, Version und die eigenen importierten Listen. (© 2026 Comidio GmbH)

Die Kachel Systemgrenzen

Eine Karte fällt aus der Reihe, weil sie Dinge misst, die man sonst nirgends sieht. Manche Betriebsmittel einer Box 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 Box 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 Kachel **Systemgrenzen**.

Ein kleiner Hintergrund-Dienst misst alle fünf Minuten und immer nur dann, wenn die Box gerade nichts Wichtigeres zu tun hat; ausbremsen kann er sie deshalb nicht. Aufgeklappt zeigt die Kachel jeden überwachten Wert samt seiner Warnschwelle, etwa *2 % (1443 von 65536), Warnung ab 80 %*. Überwacht werden unter anderem die geöffneten Dateien je Dienst, die Verbindungstabelle der Firewall, Paket-Wiederholungen und Empfangspuffer des Netzwerks, Fehler und verworfene Pakete der Netzwerkkarten, ein Anschluss, der nur noch mit 10 Mbit oder im Halbduplex-Betrieb aushandelt, die Antwortzeit der SSD, das laufende Zurückholen ausgelagerter Daten, die

Reaktionszeit von Webfilter und Web-Server, die Auslastung einzelner Prozessorkerne, Adress-Konflikte zwischen zwei Geräten und das Wachstum der Protokolldateien.

Überschreitet ein Wert seine Schwelle, färbt sich die Kachel 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 Kachel meldet, sie schaltet nichts ab. Bleibt sie über Tage gelb oder wird die Box spürbar langsam, gehört ihr Text in den Support-Bericht (Kapitel 18.2). 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

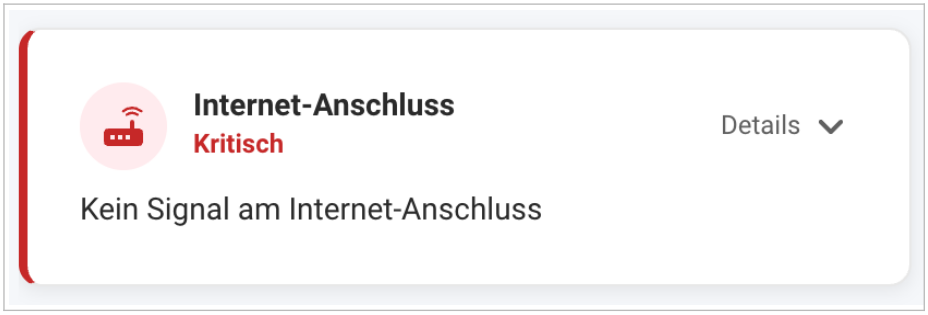


Abbildung 5-4: Die Karte erscheint erst im Störungsfall, hier mit gezogenem Netzwerkkabel. (© 2026 Comidio GmbH)

Aufgeklappt nennt sie den benutzten Anschluss der Box, die ausgehandelte Geschwindigkeit, die Adresse der Box 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 Box 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 Box diese Karten als Folge des fehlenden Anschlusses. Zu tun ist dann nur eines: die Leitung zum Router prüfen (Kapitel 17.2).

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 14.3). Die Box löst dazu einen Testnamen auf zwei Wegen auf: über ihre Adresse im Heimnetz, so wie Ihre Geräte fragen, und über sich selbst, so wie sie für Updates und Mail fragt. Solange beide Wege antworten, bleibt die Karte ausgeblendet.

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 Box 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 Box bekommen keine Namen aufgelöst, die Box 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 Box selbst löst keine Namen auf (orange)	Die Geräte haben Internet, aber Updates, TrutzDynDNS und der Mailversand der Box scheitern.	Wie oben: die verschlüsselte Weiterleitung aus- und wieder einschalten.
Keine Namensauflösung, weder für Geräte noch für die Box (rot)	Meist fehlt der Internet-Anschluss, oder der Router antwortet nicht.	Zuerst die Leitung zum Router prüfen (Kapitel 17.2).
Verschlüsselung zum DNS-Anbieter nicht möglich, Auflösung unverschlüsselt (orange)	Die Box erreicht ihren DNS-Anbieter 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 vier Stunden erneut. Filter und Sperren arbeiten unverändert.	Port 853 im Router freigeben. Geht das nicht, 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 geht das schon länger so?

Der Verlauf der letzten 30 Tage ist eine Zeile mit einem Feld pro Tag. Die Farbe steht für den Tagesstatus: grün für *„In Ordnung"*, orange 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 Box 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 Box übrigens keine spürbare Leistung; sie können die Seite so oft öffnen, wie Sie möchten.

Menüpfad: Systemeinstellungen → Betriebszustand → Verlauf

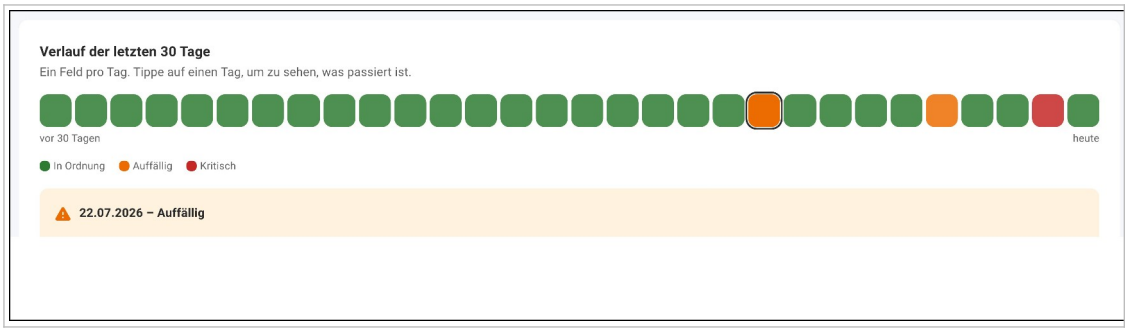


Abbildung 5-5: Der Verlauf der letzten 30 Tage: ein Feld pro Tag, die Farbe zeigt den Tageszustand. (© 2026 Comidio GmbH)

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"* (orange): Die nächtliche Installation hat noch nicht stattgefunden oder wurde verpasst. Löst sich in der Regel in der folgenden Nacht von selbst.
- *„Unverschlüsselt"* bei der DNS-Anzeige: Das verschlüsselte DNS ließ sich im Moment nicht nutzen; die Box versucht es alle vier Stunden erneut (Kapitel 14.3).
- Karten mit dem Zustand *„Läuft, aber gestört"* nennen immer eine konkrete Empfehlung. Erst wenn die nicht hilft, ist der Support dran (Kapitel 18).

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

Meldung	Was dahintersteckt	Was zu tun ist
Filterlisten veraltet (orange)	Der Update-Server bietet neuere Filterlisten an, die die Box seit über zwei Tagen nicht übernommen hat. Die Karte nennt dazu die verfügbare Version und seit wann die Box 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.
DNS unverschlüsselt	Die verschlüsselte Namensauflösung war im Moment der Prüfung nicht nutzbar, etwa weil der Anbieter kurzzeitig nicht antwortete. Die Namensauflösung selbst funktioniert weiter, nur eben unverschlüsselt.	Nichts. Die Box versucht es alle vier Stunden erneut. Hält der Zustand an, hilft Kapitel 14.3 weiter.
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 Box gezielt	Nichts. Ist wieder genug Speicher frei, startet der

Meldung	Was dahintersteckt	Was zu tun ist
	zuerst TrutzRTC und danach TrutzMail an. Der Webfilter und damit der Schutz bleiben davon unberührt.	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.

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

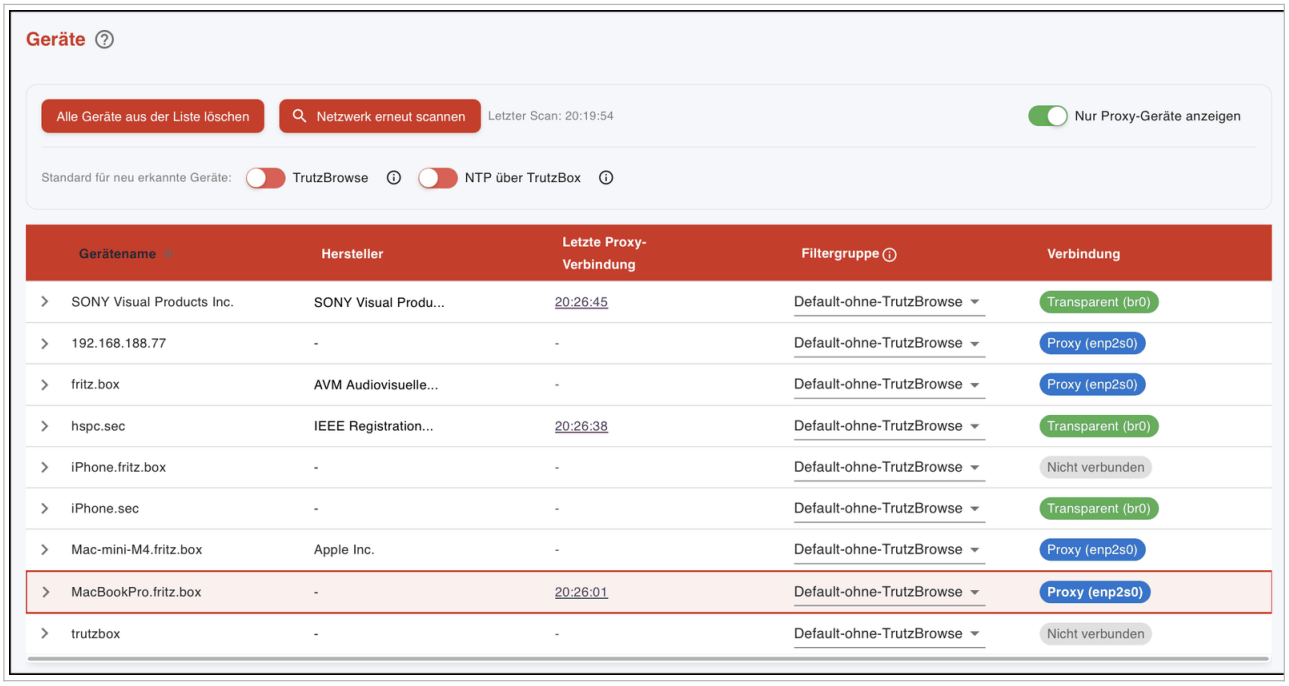


Abbildung 6-1: Die Geräte-Seite: Gerätename, Hersteller, Filtergruppe und Verbindungsart je Gerät. (© 2026 Comidio GmbH)

Sobald ein Gerät zum ersten Mal Verkehr durch die Box 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 Box 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 6.5). **Nur Proxy-Geräte anzeigen** ist in Abschnitt 6.4 erklärt. Die Schaltfläche **Alle Geräte aus der Liste löschen** räumt die Liste komplett; die Geräte tauchen beim nächsten Verkehr einfach wieder auf, verlieren aber ihre Einstellungen. Für einzelne Karteileichen ist das Löschen im jeweiligen Gerät der bessere Weg (Abschnitt 6.8).

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 8. 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 Box, 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 blockiert Werbung, Tracker, 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 6.6.

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 Box Hostname, Hersteller oder IP-Adresse, in dieser Reihenfolge.
Hersteller	Der aus der Hardware-Adresse ermittelte Gerätehersteller. Bei zufällig vergebenen Adressen weist die TrutzBox darauf hin, dass keine eindeutige Zuordnung möglich ist.
Letzte Proxy-Verbindung	Wann das Gerät zuletzt über die Box im Internet war. Sind

Spalte	Bedeutung
	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" für den Anschluss über das interne Netz (Kabel, WLAN oder VPN), „Proxy" für ein Gerät, das über den äußeren Anschluss per Proxy-Eintrag kommt, und „Nicht verbunden" für ein früher bekanntes, gerade abwesendes Gerät.

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 vier 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.

> **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.

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 6.8).

6.7 Weitere Einstellungen je Gerät

Ein Klick auf den Pfeil links vor dem Gerätenamen klappt die Detail-Einstellungen auf. Sie sind auf zwei Karteikarten verteilt: **Proxy** für Filterung und Anonymisierung, **Netzwerk** für Anschluss und Zugang. Bei reinen Netzwerkgeräten, die den Proxy nicht nutzen, ist nur die Karteikarte Netzwerk gefüllt; die Oberfläche weist darauf hin.

Menüpfad: Verwaltung → Geräte → Gerät aufklappen → Proxy

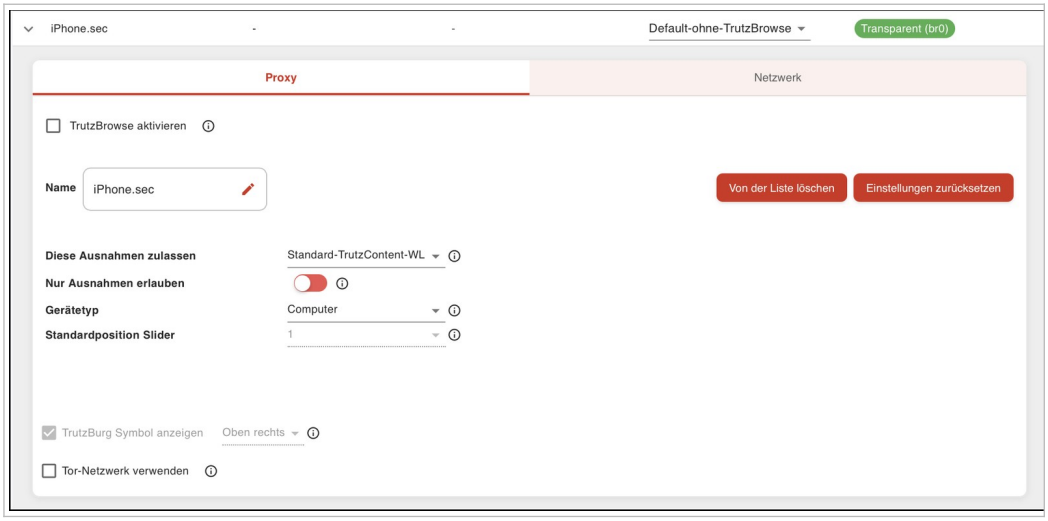


Abbildung 6-2: Die Karteikarte Proxy: TrutzBrowse, Ausnahmelisten, Gerätetyp und die TrutzBurg, dazu Löschen und Zurücksetzen. (© 2026 Comidio GmbH)

Auf der Karteikarte **Proxy** finden Sie:

- **TrutzBrowse aktivieren:** schaltet die Anonymisierung für dieses Gerät ein; die **Standardposition Slider** daneben legt die Grundeinstellung des Security-Sliders fest (Kapitel 13). Für Geräte ohne installierbares Zertifikat bleibt der Schalter aus.
- **Name:** der von Ihnen vergebene Gerätename (Abschnitt 6.2).
- **Diese Ausnahmen zulassen** und **Nur Ausnahmen erlauben**: die beiden Whitelist-Einstellungen aus Abschnitt 6.3. 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 Box 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 kleine TrutzBurg-Zeichen ein, über das sich der Security-Slider direkt im Browser verstellen lässt; daneben wählen Sie die Bildschirmecke (Kapitel 13.5).
- **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 17.4, 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

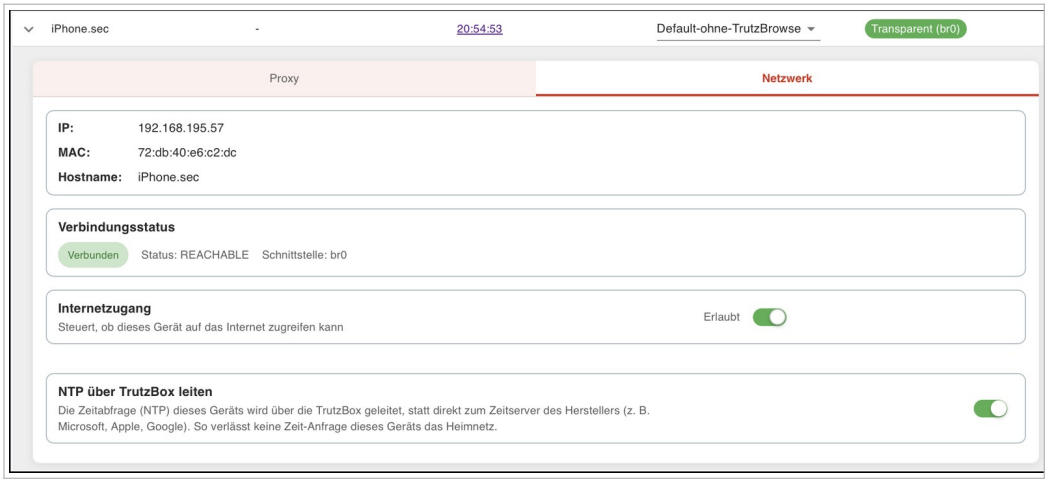


Abbildung 6-3: Die Karteikarte Netzwerk: Adressen, Verbindungsstatus, Internetzugang und die NTP-Umleitung. (© 2026 Comidio GmbH)

Auf der Karteikarte **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 6.6).
- **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 Box 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:** entfernt alle über den Proxy konfigurierten Geräte samt ihren gespeicherten Einstellungen. Geräte, die die TrutzBox im Netz selbst erkannt hat, bleiben in der Liste sichtbar; die Box liest sie anschließend neu ein.

Was „Alle Geräte löschen" wirklich entfernt

Der Dialog sagt es deutlich: Entfernt werden ausschließlich die proxy-konfigurierten Geräte. Deren Namen, Filtergruppen-Zuordnungen und Proxy-Einstellungen sind danach weg und müssen neu vergeben werden. Die netzwerk-erkannten Geräte verschwinden dagegen nicht aus der Liste. 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 Box 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 Box. 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 17 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. Geht das?

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 10), für TrutzChat und Videokonferenzen (Kapitel 11), für den VPN-Fernzugriff (Kapitel 12) und für personenbezogene Filtergruppen (Kapitel 8). 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 Box von selbst und verwaltet sie auf der Geräte-Seite (Kapitel 6). Ein Benutzerkonto steht für eine Person, unabhängig davon, an welchem Gerät sie gerade sitzt. Deshalb lohnt sich ein Konto auch dann, wenn jemand gar keine Mail-Adresse braucht: Nur so bekommt diese Person ihre eigenen Filtereinstellungen mit, egal ob sie am Laptop oder am Tablet arbeitet.

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 Box.
- **Benutzer ohne TrutzMail-Adresse:** beliebig viele. Praktisch, um einzelnen Personen eigene Filtergruppen zu geben, unabhängig vom benutzten Gerät. In der Liste erkennen Sie sie daran, dass keine E-Mail-Adresse angezeigt wird.
- **Benutzer mit TrutzMail-Adresse:** nötig für TrutzMail, Chat, das Eröffnen von Videokonferenzräumen und den VPN-Zugang. Die Zahl solcher Adressen begrenzt Ihr Servicepaket; jede Adresse ist weltweit eindeutig.

Chat und Videokonferenz gehören zu TrutzRTC und stehen nur in der Business-Version der TrutzBox zur Verfügung (Kapitel 11). Auf einer Box ohne diese Ausstattung dienen die Konten also den übrigen Zwecken: TrutzMail, VPN-Fernzugriff und personenbezogene Filtergruppen.

Konten mit TrutzMail-Adresse können aktiv oder deaktiviert sein. Läuft Ihr Servicevertrag ab, wird das zugehörige Mail-Zertifikat nicht mehr erneuert; eingehende TrutzMails werden von den Boxen der Gegenseite dann nicht mehr angenommen. 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

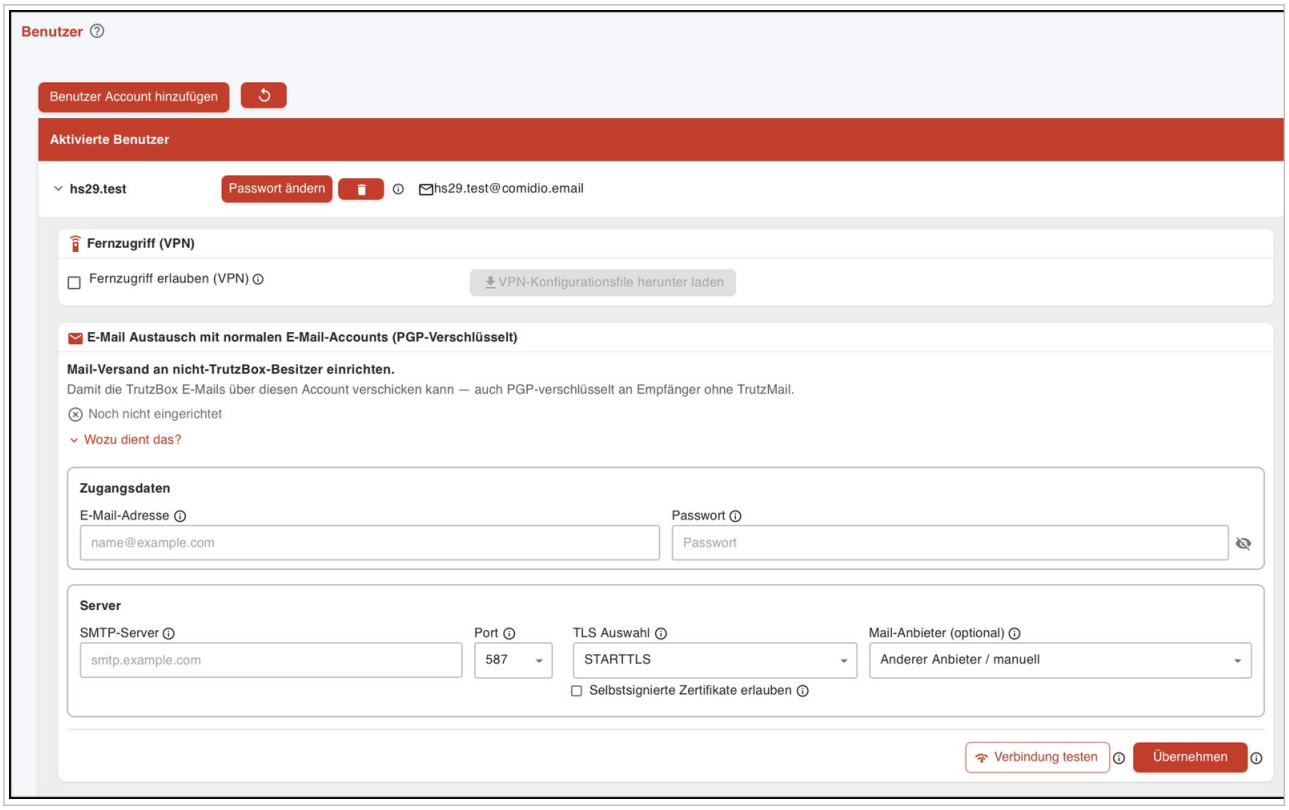


Abbildung 7-1: Die Benutzerliste: aktivierte Konten oben, früher angelegte Adressen darunter zum Reaktivieren. (© 2026 Comidio GmbH)

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 Box.
3. Vergeben Sie ein Passwort (mindestens 8 Zeichen, der Balken zeigt die Stärke) und speichern Sie.

Setzen Sie das Häkchen für die TrutzMail-Adresse, prüft die Box im selben Moment bei Comidio nach, ob der gewünschte Name noch frei ist und ob Ihr Vertrag noch eine freie Adresse hergibt. 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.

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. Die Box verlangt mindestens 8 Zeichen und prüft zusätzlich eine Mindeststärke; ein Balken zeigt Ihnen beim Tippen, wie gut das gewählte Passwort abschneidet. Ein Passwort, das die Prüfung nicht besteht, wird nicht angenommen.

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 achten Sie auf den Stärkebalken. Speichern Sie erst, wenn er nicht mehr im roten Bereich steht.
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 Box, und niemand kann es zurücksetzen, auch Comidio nicht (Kapitel 17.16). Wählen Sie ein langes, einprägsames Passwort (die Merkhilfe aus Kapitel 3.7 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 an, wertet der Angriffsschutz das nach zehn Fehlversuchen als Angriff und sperrt die Internet-Adresse, von der es kommt, für sechs Stunden (Kapitel 14.4). 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:

- **Fernzugriff erlauben (VPN):** schaltet den VPN-Zugang für diesen Benutzer frei. Ist er aktiv, erscheint darunter eine Schaltfläche, mit der Sie die persönliche VPN-Konfigurationsdatei für das Mobilgerät herunterladen (Kapitel 12.6). Jeder Benutzer bekommt seine eigene Datei; geben Sie sie nicht weiter.
- **E-Mail Austausch mit normalen E-Mail-Accounts (PGP-Verschlüsselt):** hier trägt der Benutzer den Postausgangsserver eines bestehenden gewöhnlichen Mail-Kontos ein. Die Box braucht ihn, um PGP-verschlüsselte Post an Partner ohne TrutzBox zu versenden (Kapitel 10.5). Zum Empfangen ist dieser Eintrag nicht nötig.

- **Selbstsignierte Zertifikate erlauben:** lässt für diesen Benutzer Verbindungen zu Servern zu, die kein anerkanntes Zertifikat vorweisen. Bleibt im Normalfall ausgeschaltet und wird nur gesetzt, wenn ein bestimmter Server im eigenen Netz es erfordert.

Diese Einstellungen sind der Grund, warum sich in Kapitel 10 und Kapitel 12 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 Box. 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 Box 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 Box oder nach einem Hardwaretausch (Kapitel 16).

1. Öffnen Sie **Verwaltung → Benutzer** und suchen Sie den Abschnitt **Reaktivierbare Benutzer**.
2. Klicken Sie bei der gewünschten Adresse auf **Reaktivieren**. Die Box 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 Kommunikationspartner merken vom Schlüsselwechsel nichts: Deren Boxen bemerken ihn selbst und holen den neuen Schlüssel beim nächsten Briefwechsel nach.

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 Box, die Laufzeit des Servicevertrags und den gebuchten Umfang, also ob Fernzugriff und Videokonferenz freigeschaltet sind. Das Kontingent hängt am Servicepaket 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 Servicevertrags laufen nicht über die Box, 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. Die Box selbst arbeitet weiter, sie erhält dann aber keine 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 Box 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 Update nachsehen wollen, ob alles wieder läuft. Die Sitzungskennung ist dabei zusätzlich abgesichert.

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 Box 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 Box offen, und sie überdauert auch das Schließen des Browserfensters.

Häufige Fragen zu Benutzern

Braucht jede Person im Haushalt ein eigenes Konto?

Nötig ist es nicht. Für den reinen Internet-Schutz genügt es, die Geräte einzuordnen (Kapitel 6). Ein eigenes Konto lohnt sich, sobald jemand ein TrutzMail-Postfach, den Chat oder den VPN-Zugang braucht, oder wenn die Filtereinstellungen einer Person auf allen ihren Geräten gleich sein sollen.

Kann ich einen Benutzernamen später umbenennen?

Den Anzeigenamen ja, 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 16).

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; 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 14.4).

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, und blockiert Werbung, Tracker, Schadseiten 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 3) und die zu schützenden Geräte sind angeschlossen (Kapitel 4).

• 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 „Tracker", „Werbung" oder „Gewalt". Ausgeliefert wird die TrutzBox mit weit über hundert 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 über die täglichen Updates 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** (und auf Wunsch Benutzer) bekommen je genau eine Filtergruppe zugewiesen. Ab da gilt: Dieses Gerät darf nur, was seine Gruppe erlaubt.

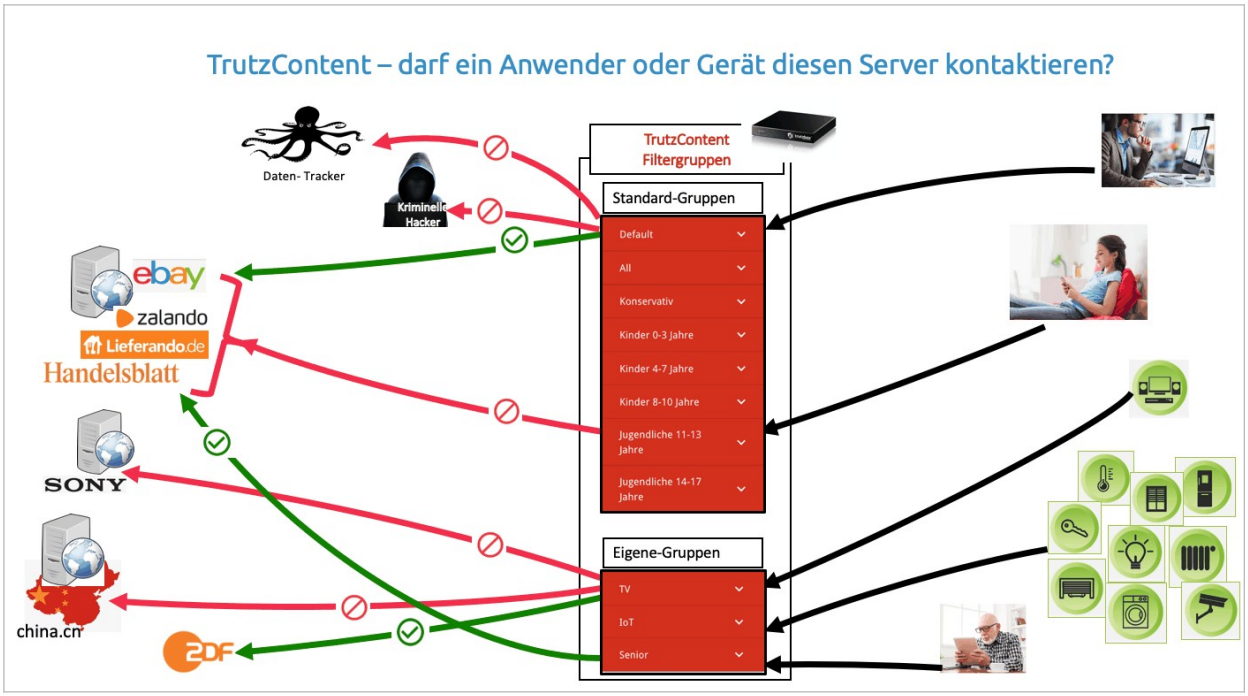


Abbildung 8-1: Das Prinzip: Jedes Gerät gehört zu einer Filtergruppe, und die Gruppe entscheidet, welche Server erreichbar sind. (© 2026 Comidio GmbH)

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 6.3).

Wichtig für den Jugendschutz: Die Einstellungen kann nur der Administrator ändern. Wer am Gerät sitzt, kann die Filterung an der Box 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.

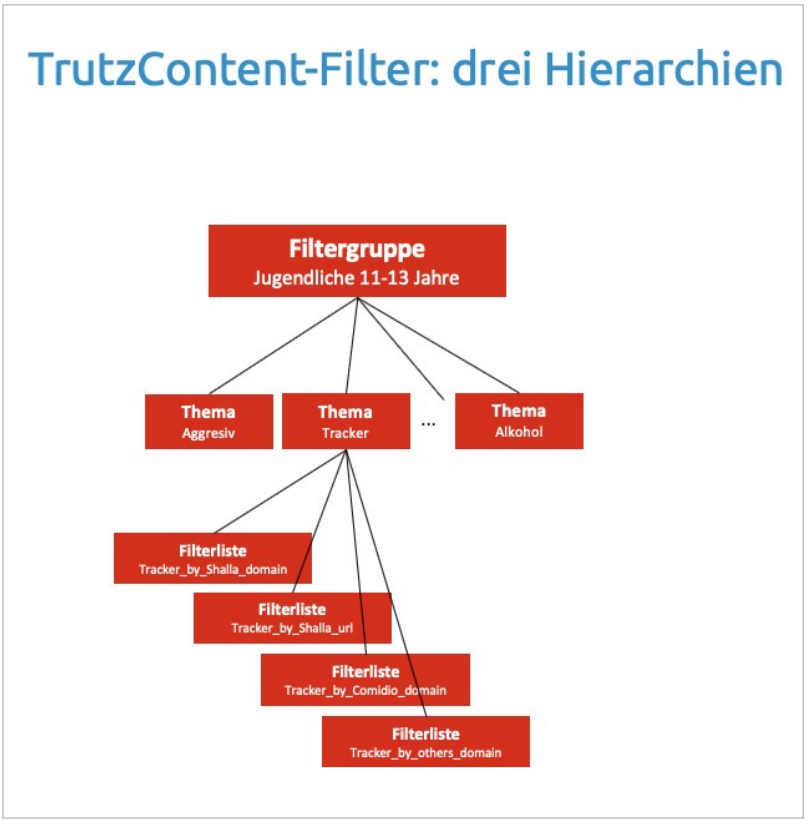


Abbildung 8-2: Die drei Ebenen im Detail: Eine Filtergruppe enthält Themen, ein Thema enthält einzelne Filterlisten. (© 2026 Comidio GmbH)

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

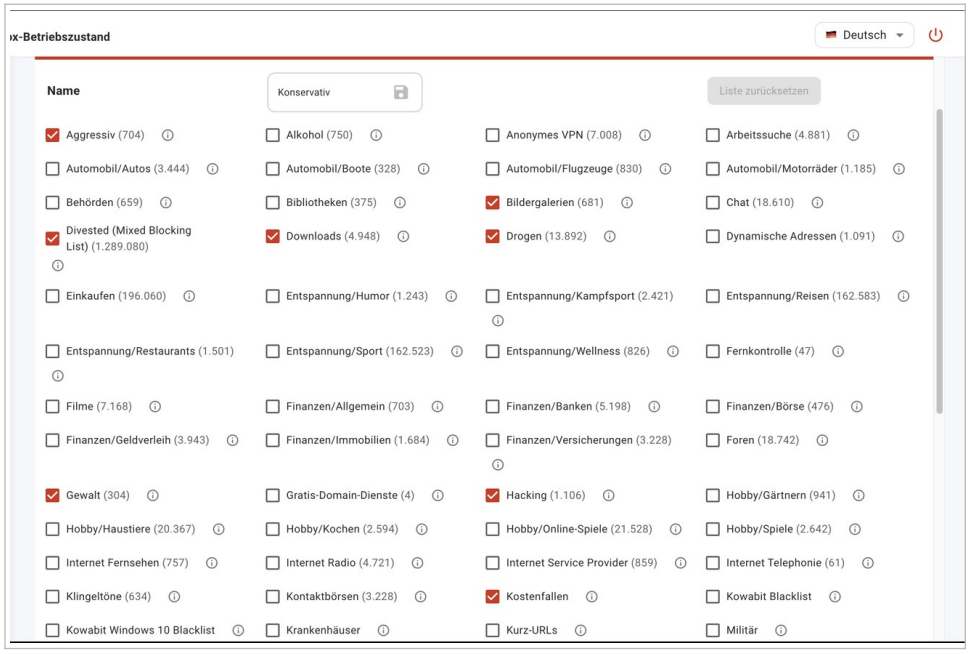


Abbildung 8-3: Die Filtergruppen-Seite: Pro Gruppe wird per Häkchen festgelegt, welche Themengebiete blockiert werden. (© 2026 Comidio GmbH)

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" 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 Filterlisten verwalten

Die einzelnen Filterlisten finden Sie unter **Verwaltung → Filterlisten**. Die von Comidio mitgelieferten Listen können Sie ansehen und durchsuchen, aber nicht verändern; sie werden bei den täglichen Updates automatisch angepasst. Eigene Listen legen Sie daneben an und pflegen sie selbst.

Menüpfad: Verwaltung → Filterlisten

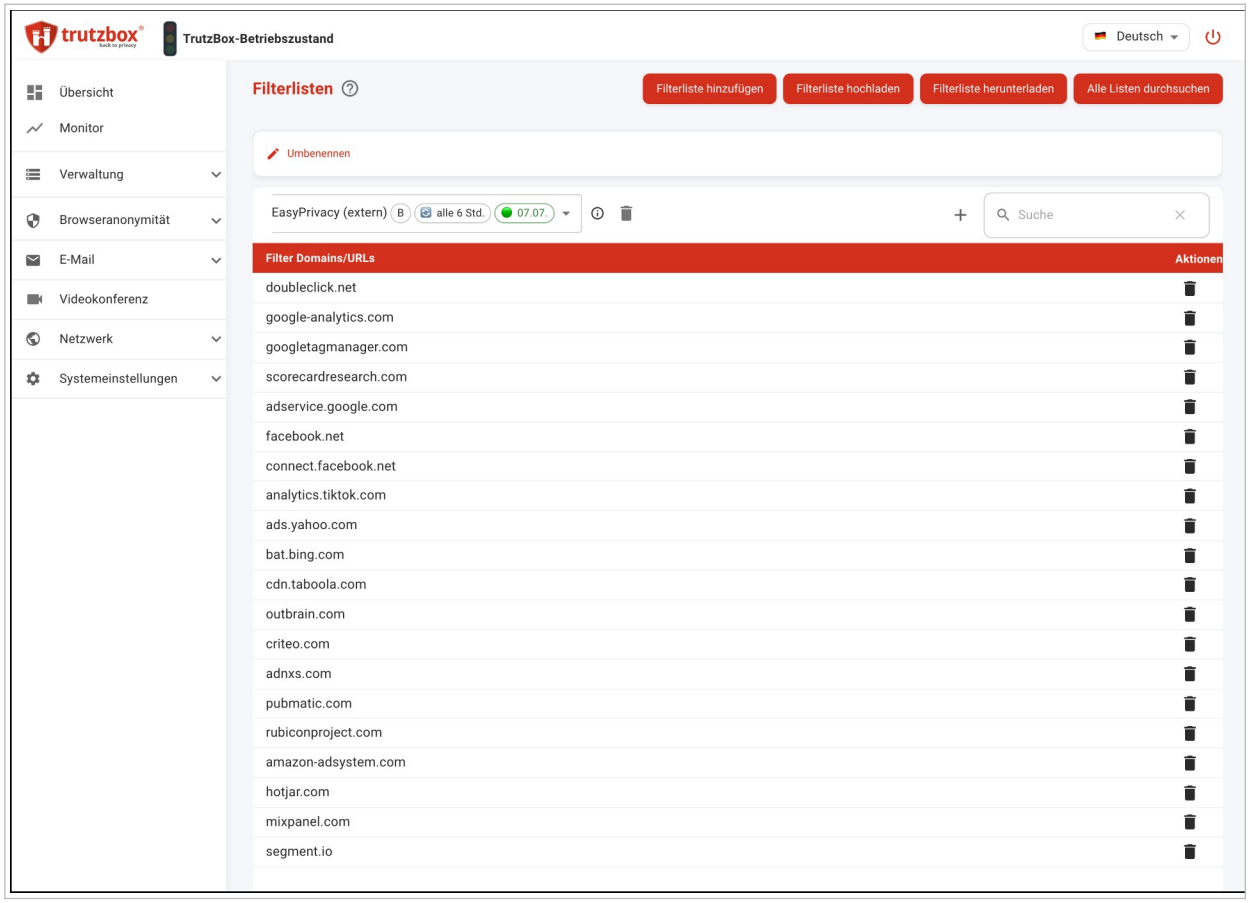


Abbildung 8-4: Die Filterlisten-Seite mit einer importierten Liste: Rhythmus, Status der letzten Aktualisierung und die enthaltenen Adressen. (© 2026 Comidio GmbH)

Beim Eintragen eigener Adressen gilt: nur den Domain-Namen eintragen, also zum Beispiel `facebook.com`, ohne „http" oder „www" davor. Die Box 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. Zeigt die Box einen impliziten Zugriff auf einen Server (etwa einen Tracker im Hintergrund einer Seite), sperren Sie ihn mit einem Klick, und die Adresse landet in dieser Liste.
Standard-TrutzContent-BL	Sperrliste des Webfilters, gilt für alle Geräte. Ein Klick auf einen angezeigten Zugriff übernimmt die Adresse hierher und sperrt sie.
Standard-TrutzContent-WL	Ausnahmeliste (Whitelist), bei allen Geräten und Benutzern aktiv. Blockiert die Box 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

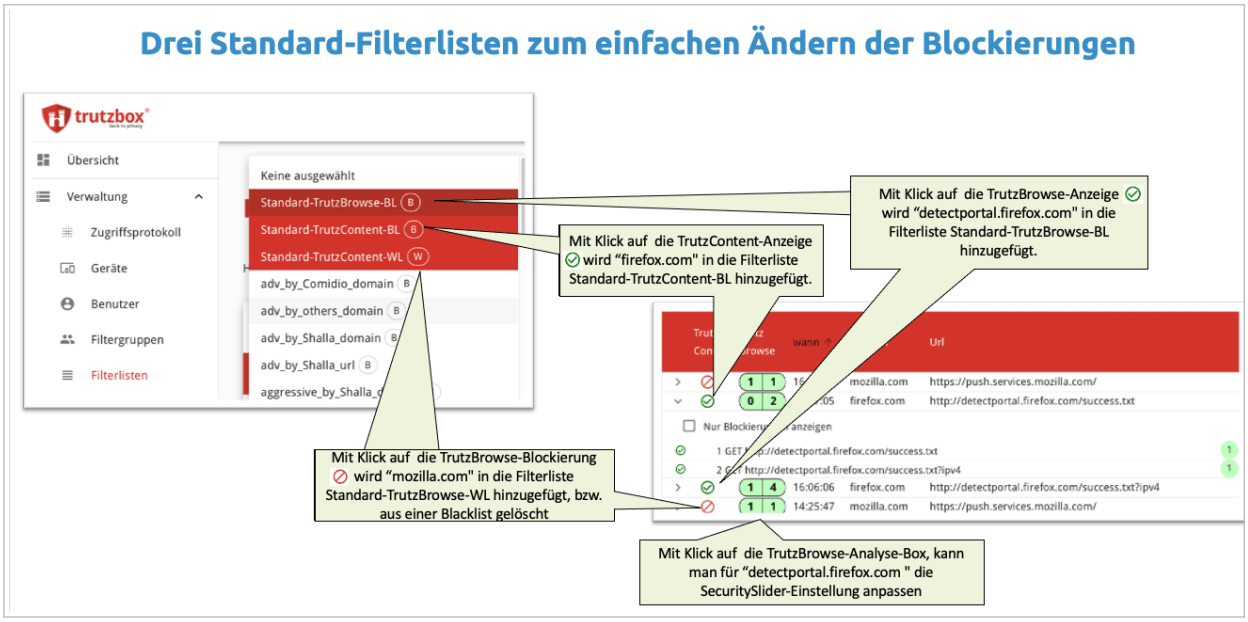


Abbildung 8-5: Sperren und Freigeben mit einem Klick: Aus der Monitor-Liste heraus wandern Adressen direkt in die passende Standard-Liste. (© 2026 Comidio GmbH)

Am bequemsten füllen sich diese Listen direkt aus dem **Monitor** (Kapitel 9): Dort klicken Sie beim betreffenden Eintrag einfach auf das TrutzContent- oder TrutzBrowse-Symbol, und die Adresse wird gesperrt beziehungsweise freigegeben, ohne dass Sie die Filterlisten-Seite überhaupt öffnen müssen.

8.4 Filterlisten aus dem Internet laden und automatisch aktualisieren

Im Internet pflegen Freiwillige seit Jahren hervorragende öffentliche Sperrlisten gegen Werbung und Tracker. Solche Listen übernehmen Sie direkt in Ihre TrutzBox, samt automatischer Aktualisierung. Ein Assistent führt in drei Schritten durch den Import:

Menüpfad: Verwaltung → Filterlisten → Filterliste hinzufügen

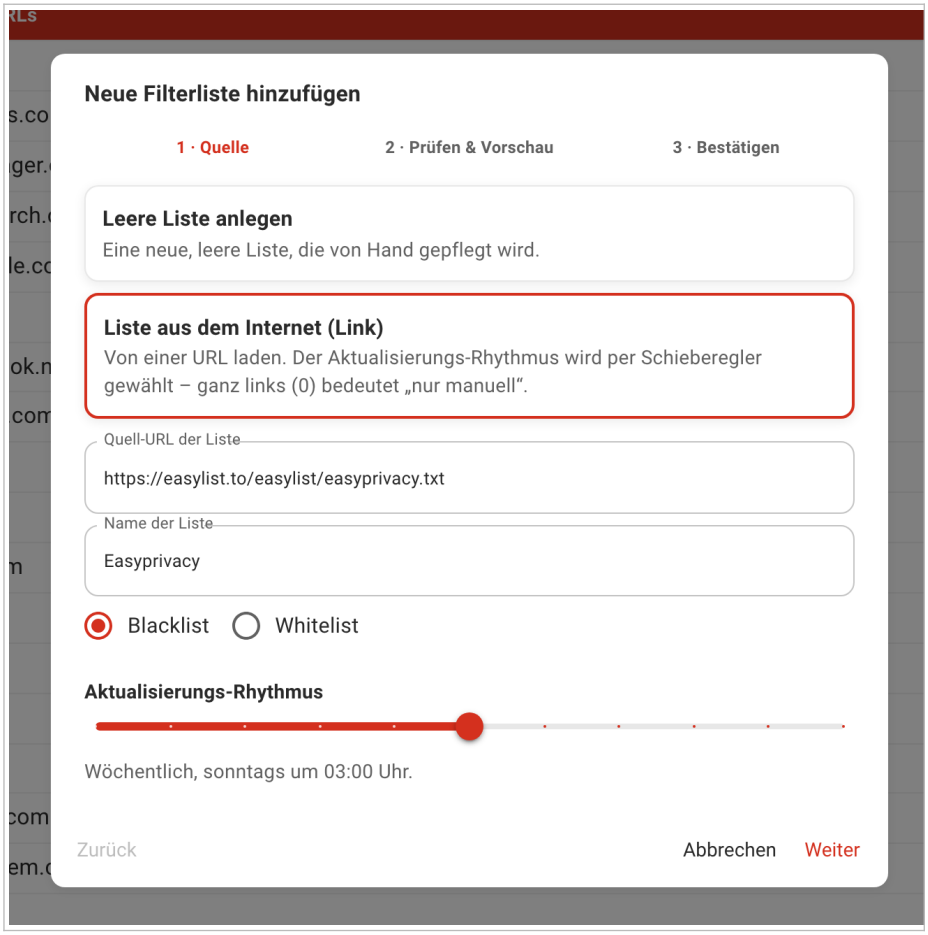


Abbildung 8-6: Der Assistent „Neue Filterliste hinzufügen", Schritt 1: Quell-Adresse, Name, Listenart und Aktualisierungs-Rhythmus. (© 2026 Comidio GmbH)

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 Box die Liste und zeigt, was erkannt wurde. Alle gängigen Listenformate erkennt die Box 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 Updates laufen nachts ab 3 Uhr; schlägt eines fehl, bleibt einfach die letzte funktionierende Fassung 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 Box 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 http/https-Quellen bis 50 MB.

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 Box zeigt jeden Treffer samt Liste, in der er steht. Das ist der schnellste Weg, wenn eine Seite blockiert wird und Sie den Grund suchen.

8.5 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 Box ab Werk netzweit.

8.6 Die Sperrseite verstehen

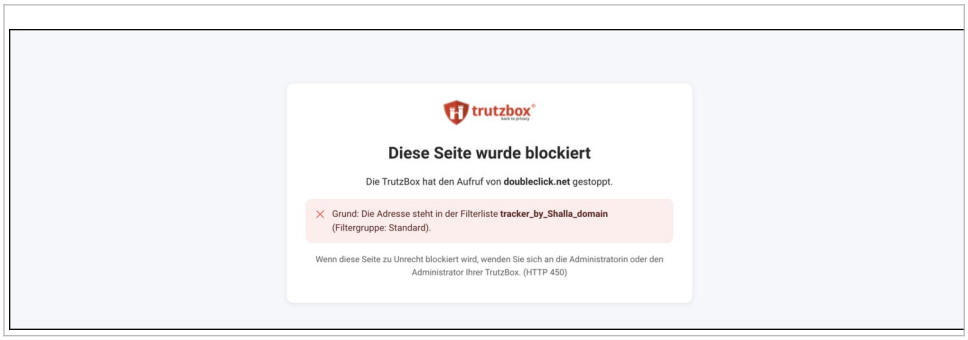


Abbildung 8-7: Die Sperrseite der TrutzBox nennt die blockierte Adresse, die Filterliste und die Filtergruppe. (© 2026 Comidio GmbH)

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 Box 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 Box 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 Box 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 9).

8.7 Ein Vorschlag für den Anfang

Wer neu einsteigt, fährt mit dieser Aufteilung erfahrungsgemäß gut:

Gerätegruppe	Filtergruppe	Warum
Erwachsene: PC, Laptop, Telefon	Standard	Blockiert Werbung, Tracker, 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 melden besonders viel nach Hause. Werbe- und Trackerthemen konsequent sperren, den Rest beobachten.
Haustechnik: Thermostate, Kameras, Steckdosen	Eigene Gruppe „IoT", auf Wunsch „Nur	Solche Geräte brauchen meist nur eine Handvoll Server. Alles andere zu sperren

Gerätegruppe	Filtergruppe	Warum
	Ausnahmen erlauben"	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 höheren Stufen funktionieren manche Seiten erst nach Nachjustieren des Sliders. Was sie leistet und für wen sie sich eignet, steht in Kapitel 13.

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.

Häufige Fragen zum Webfilter

Eine Seite wird zu Unrecht blockiert. Was tun?

Am schnellsten über den Monitor: Eintrag suchen, auf das Filter-Symbol klicken, freigeben. Die Adresse landet in der Standard-TrutzContent-WL und ist sofort wieder erreichbar. Alternativ tragen Sie die Adresse von Hand in eine Whitelist ein.

Kann mein Kind die Filterung umgehen?

Nicht über die Einstellungen: Die liegen auf der Box, 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 Box ab, und das QUIC-Protokoll ist ab Werk im gesamten Netz gesperrt. Offen bleibt, was an der Box vorbeiführt, etwa die mobilen Daten eines Smartphones oder das WLAN des Routers. Deshalb gehört ein Kindergerät ins interne Netz der Box, und das Router-WLAN sollte für Kinder tabu sein (Kapitel 4).

Verlangsamen die Filterlisten das Internet?

Im Alltag nicht merklich. Die Prüfung läuft in Echtzeit im Arbeitsspeicher der Box. Was zusätzliche Listen tatsächlich kosten, ist Arbeitsspeicher; deshalb nennt die Box beim Einschalten sehr großer Listen den Bedarf und warnt, bevor es knapp wird.

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 14.2). Und der Internetzugang eines einzelnen Geräts lässt sich auf der Geräte-Seite jederzeit von Hand entziehen und später wieder freigeben (Kapitel 6.6). 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 Box. 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 9.4), fragt die Box zu den gerade angezeigten Server-Adressen die öffentlichen Registrierungsdienste ab; Angaben über Ihre Geräte gehen dabei nicht hinaus.

> **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 Info-Symbol („i"); beim ersten Aufruf pulsiert ein blauer Ring darum. Ein Klick öffnet **Hilfe & Führungen**: eine Themenliste in fünf Abschnitten („Erste Schritte", „Geräte untersuchen", „Internet-Ziele untersuchen", „Sperren und freigeben", „Übersicht behalten") mit sechzehn geführten Touren.

Jede Tour läuft 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. Beenden lässt sich eine Tour jederzeit mit dem Schließkreuz oder der Esc-Taste. Da die Touren auf die tatsächlichen Bedienelemente zeigen, bleiben sie auch nach Oberflächen-Updates aktuell. Dieses Kapitel gibt Ihnen das Grundverständnis; die Feinheiten zeigt Ihnen die Box am lebenden Objekt selbst.

Menüpfad: Monitor

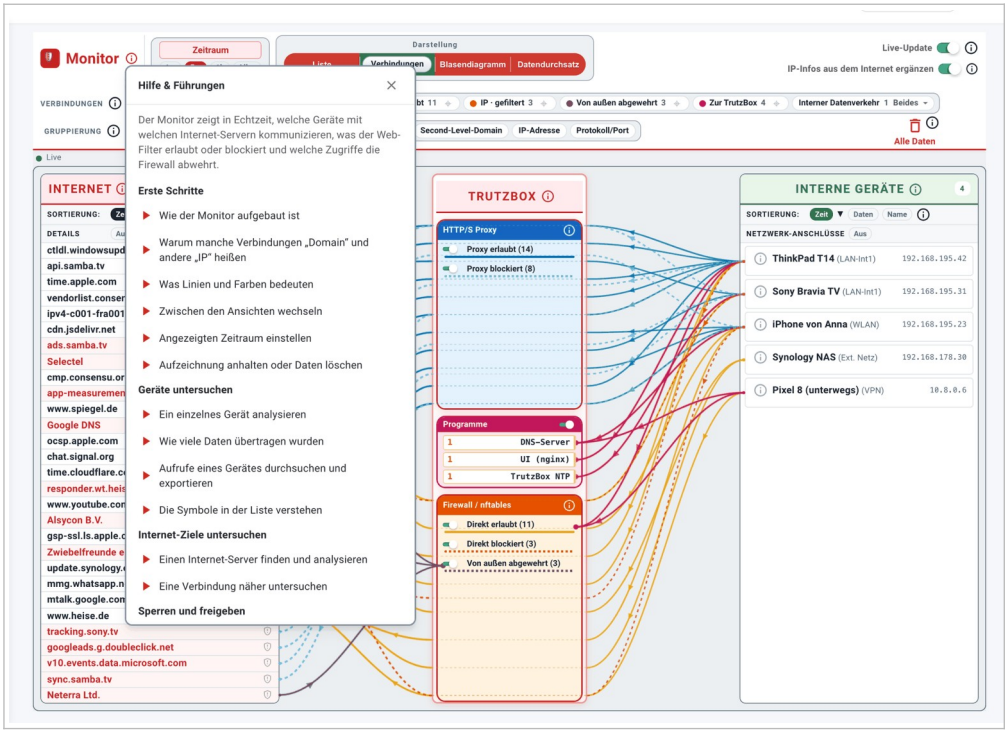


Abbildung 9-1: Eine geführte Tour im Monitor: Die Seite wird abgedunkelt, die Sprechblase erklärt das markierte Element. (© 2026 Comidio GmbH)

9.2 Der Aufbau: Geräte, TrutzBox, Internet

Menüpfad: Monitor → Verbindungen

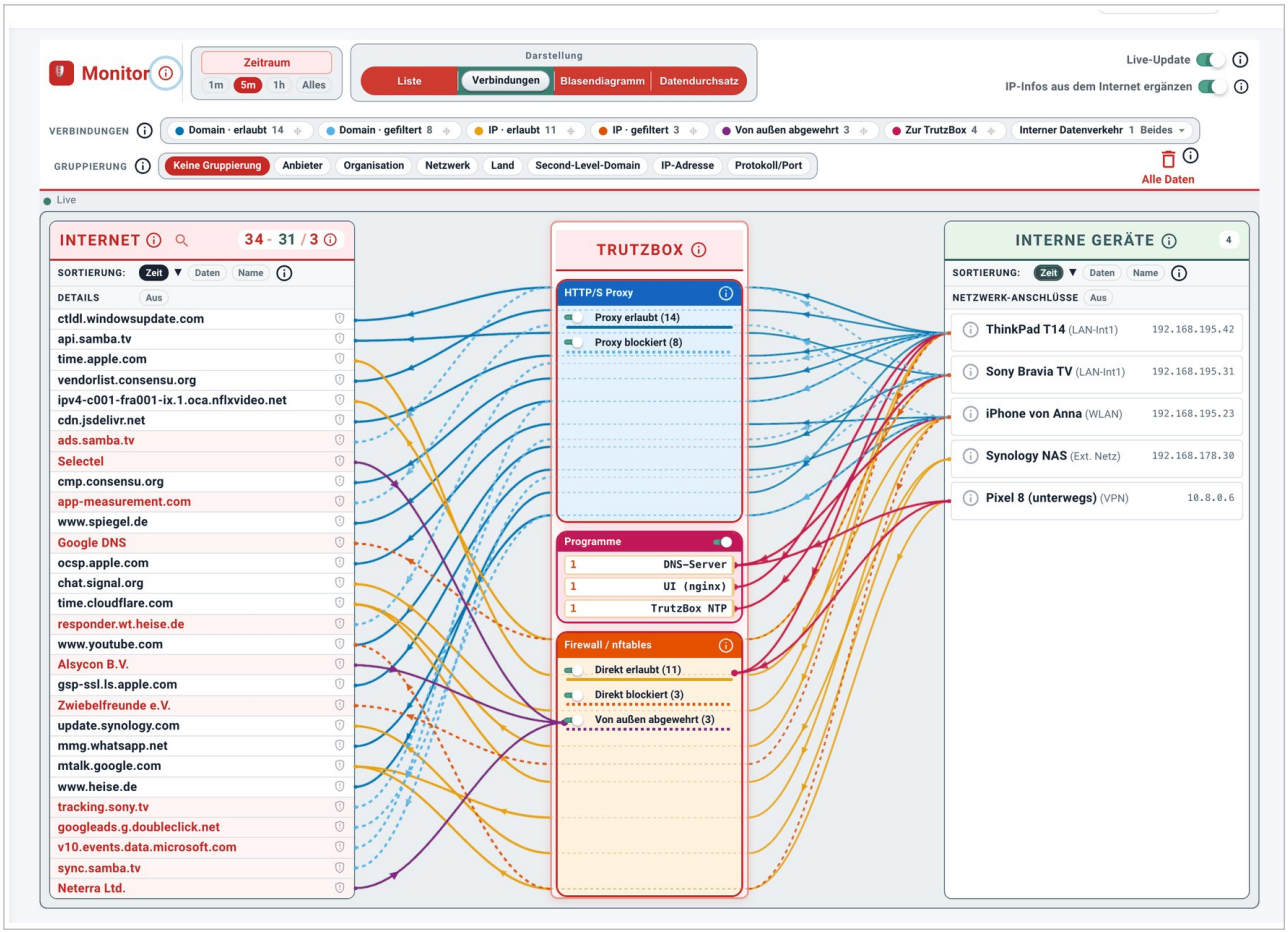


Abbildung 9-2: Die Darstellung „Verbindungen": rechts die eigenen Geräte, in der Mitte die TrutzBox, links die Ziele im Internet. (© 2026 Comidio GmbH)

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

- Rechts die **Geräte im eigenen Netz**, gruppiert nach Anschluss: das LAN getrennt nach Anschlussbuchse („LAN-Int1", „LAN-Int2"), dazu WLAN und VPN-Tunnel. Die Zahl hinter dem Gruppennamen sagt, wie viele Geräte im gewählten Zeitraum aktiv waren. 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.
- 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.

Warum heißen manche Verbindungen „Domain" und andere „IP"? Über den Proxy laufen die Verbindungen, bei denen die Box den Namen der Gegenstelle kennt; nur dort kann nach Domain gefiltert werden. Alles andere, etwa verschlüsselte Apps und Spielkonsolen, geht direkt durch die Firewall, und dort ist nur die IP-Adresse sichtbar. Die Chip-Zeile Verbindungen unterscheidet entsprechend sieben Arten: „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 Box selbst und „Interner Datenverkehr" zwischen zwei eigenen Geräten.

Linien und Farben: Jede Linie ist eine Verbindung. Durchgezogen heißt durchgelassen, gestrichelt heißt blockiert; die Liniendicke entspricht der Datenmenge. Die Farbe sagt, welchen Weg die Verbindung genommen hat: Blau steht für den Weg über den Proxy, 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 Updates. Die Zahlen über der Internet-Spalte fassen zusammen: Gesamtzahl, davon durchgelassen (grün) und blockiert (rot).

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

9.3 Die vier Darstellungen

Derselbe Datenbestand lässt sich über den Umschalter **Darstellung** auf vier Arten ansehen; 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

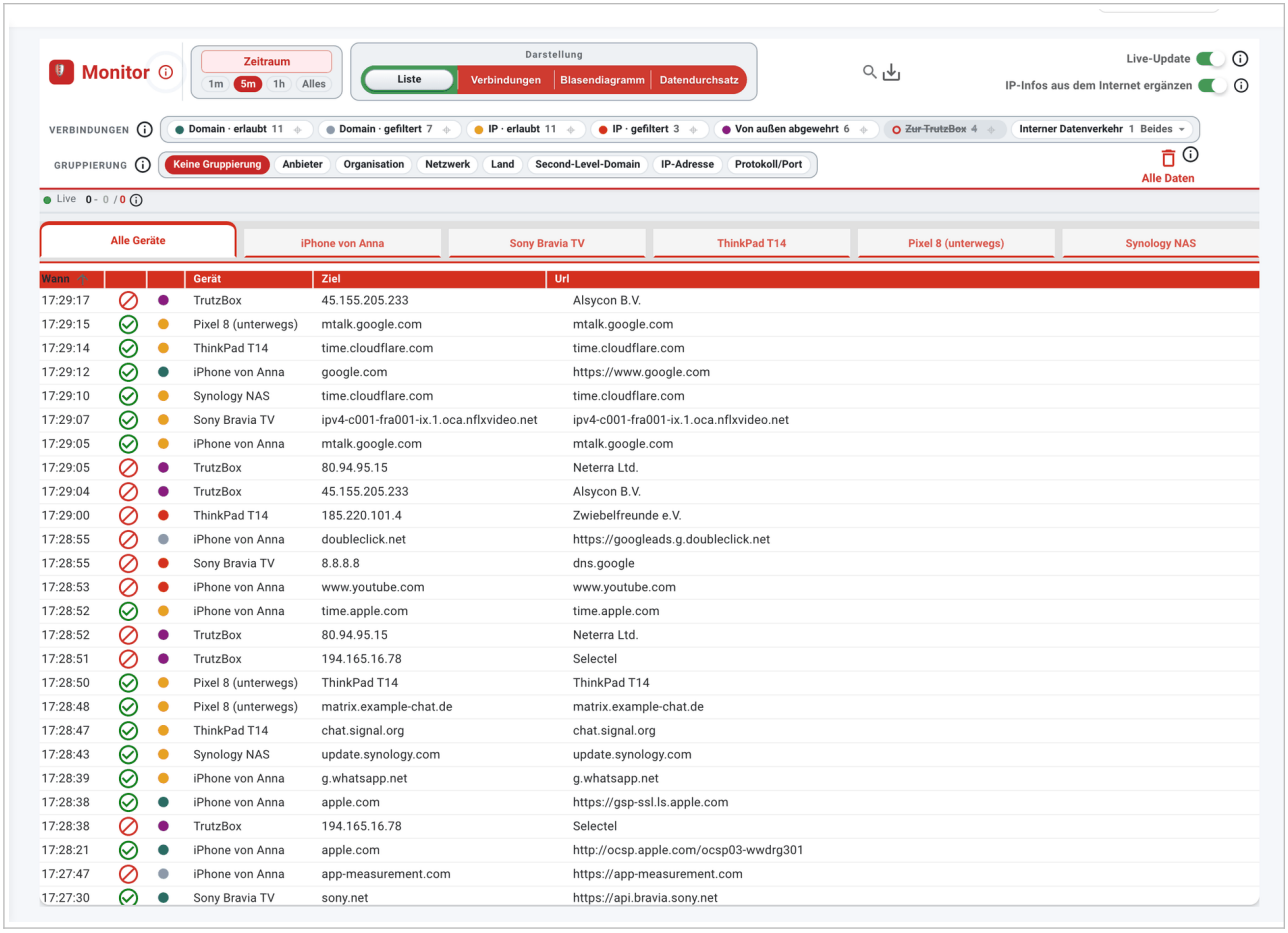


Abbildung 9-4: Die Darstellung „Liste": jeder Zugriff eine Zeile mit dem Ergebnis des Webfilters; hier für ein Gerät ohne TrutzBrowse. (© 2026 Comidio GmbH)

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

- Rechts oben sitzen **Suche** und der **CSV-Export**, mit dem sich das Protokoll zur Auswertung herunterladen lässt.
- Ein Klick auf eine **freie Stelle der Kopfzeile** öffnet das Menü **Spalten anzeigen**: Dort schalten Sie Zusatzspalten wie Land, Anbieter, Organisation, IP-Adresse oder Seitentitel hinzu. Die Auswahl merkt sich die Box.
- Ein Klick auf einen **Spaltenkopf** sortiert; voreingestellt sind die neuesten Einträge oben.
- Ein Klick auf die **Uhrzeit** einer Zeile öffnet die Einzelheiten der Verbindung samt der Regel, die gegriffen hat; ein Klick auf das **Ziel** die Einzelheiten des Servers, samt Sperren und Freigeben.

Wie die Liste aussieht, hängt davon ab, ob für das gewählte Gerät TrutzBrowse eingeschaltet ist. Ohne TrutzBrowse zeigt jede Zeile das Ergebnis des Webfilters TrutzContent. Mit TrutzBrowse kommt die Spalte **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 13.8). Alle weiteren Einzelheiten der Listen-Darstellung beschreibt das TrutzBox-Kompendium.

Menüpfad: Monitor → Liste

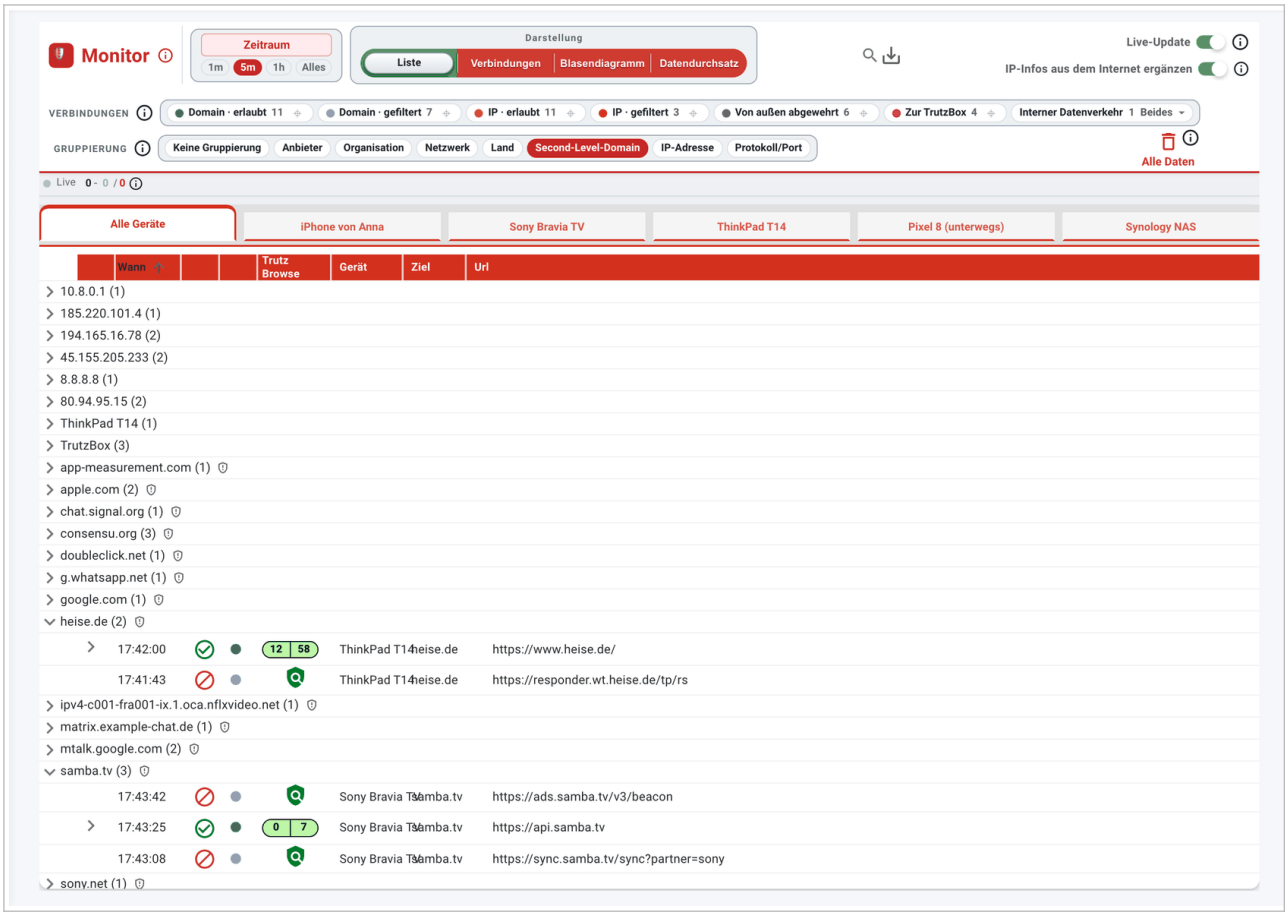


Abbildung 9-5: Dieselbe Liste für ein Gerät mit TrutzBrowse: zusätzlich die Spalte mit Slider-Stufe und dem Zahlenpaar der Hintergrund-Zugriffe. (© 2026 Comidio GmbH)

Verbindungen: das Bild zum Verstehen und Eingreifen

Das Spaltenbild aus Abschnitt 9.2 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 geht mit den Einträgen der Karte **Programme** für den Verkehr der Box selbst.
- Ein Klick auf eine **Linie** heftet die Kurzinfo zu genau dieser Verbindung an.
- Ein Klick auf die **grüne Zahl** über der Internet-Spalte öffnet einen Dialog, der alle gerade angezeigten, noch nicht gesperrten Server auf einen Schlag sperrt. Das ist der schnellste Weg, einem geschwätzigen Gerät sämtliche Kontakte zu untersagen; vorher mit den Schaltern und der Suche eingrenzen.
- Über die **Lupe** in der Internet-Spalte filtern Sie nach Namen; die Sortierung je Spalte wechselt zwischen Zeit, Daten und Name.

Blasendiagramm: Ausreißer entdecken

Menüpfad: Monitor → Blasendiagramm

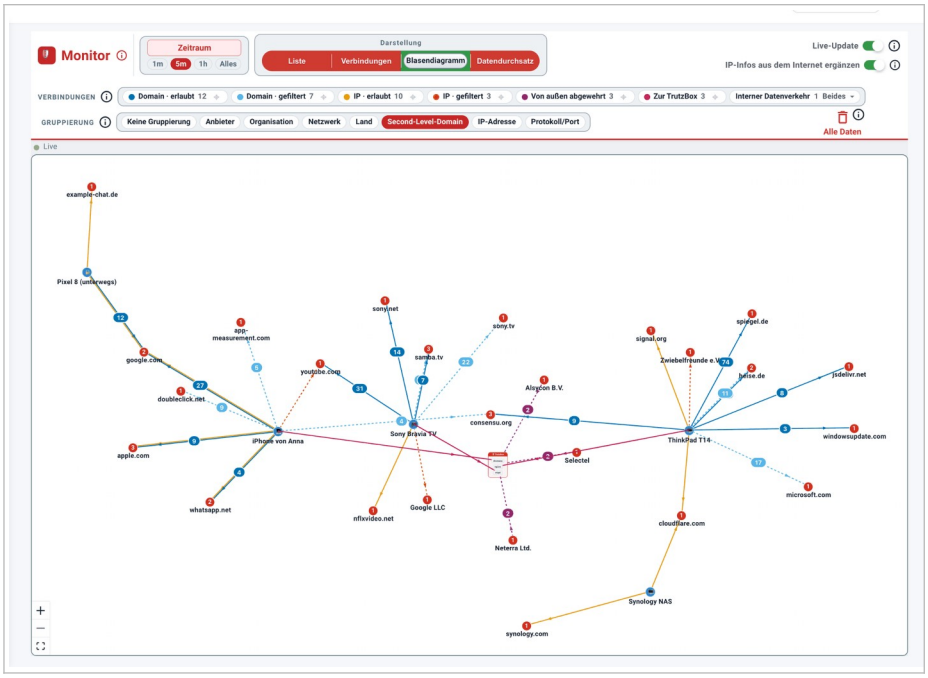


Abbildung 9-6: Das Blasendiagramm: jedes Gerät und jeder Server ein Kreis. Ausreißer fallen hier sofort auf. (© 2026 Comidio GmbH)

Jedes Gerät und jeder Server ist ein Kreis, die Zahl daran nennt die Verbindungen. 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.
- 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.

Datendurchsatz: wer wie viel überträgt

Menüpfad: Monitor → Datendurchsatz

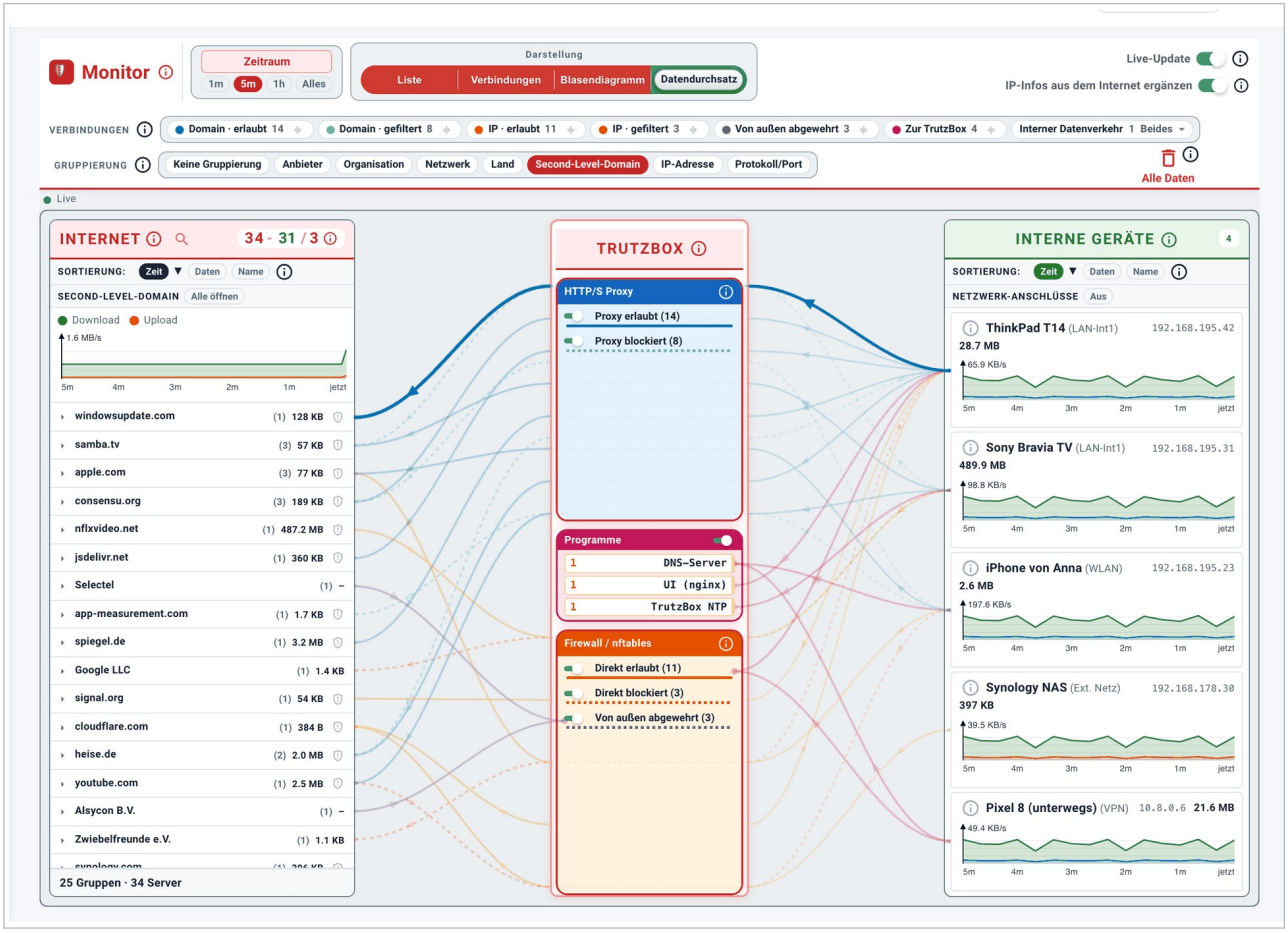


Abbildung 9-7: Datendurchsatz mit ausgeschalteten Netzwerk-Anschlüssen: alle Geräte in einer Liste, je mit eigener Durchsatzkurve. (© 2026 Comidio GmbH)

Diese Darstellung rückt die Datenmengen in den Vordergrund: Zu jedem Server und jedem Gerät gehört eine kleine Durchsatzkurve, getrennt nach Herunterladen und Hochladen, dazu die übertragene Menge. Mit der Sortierung **Daten** stehen die größten Verbraucher oben; so ist die Frage „Wer verbraucht gerade mein Volumen?" in Sekunden beantwortet.

Der Schalter **Netzwerk-Anschlüsse** in der Geräte-Spalte bestimmt die Gliederung. Ausgeschaltet stehen alle Geräte in einer Liste, der Anschluss steht in Klammern hinter dem Namen. Eingeschaltet bekommt jeder Anschluss (WLAN, LAN, externes Netz, VPN) eine eigene aufklappbare Karte mit Gesamtmenge und eigener Durchsatzkurve, und die Geräte gruppieren sich darunter. Das beantwortet eine Frage, die sonst schwer zu greifen ist: Wie viel läuft eigentlich über das Funknetz, wie viel über Kabel?

Menüpfad: Monitor → Datendurchsatz

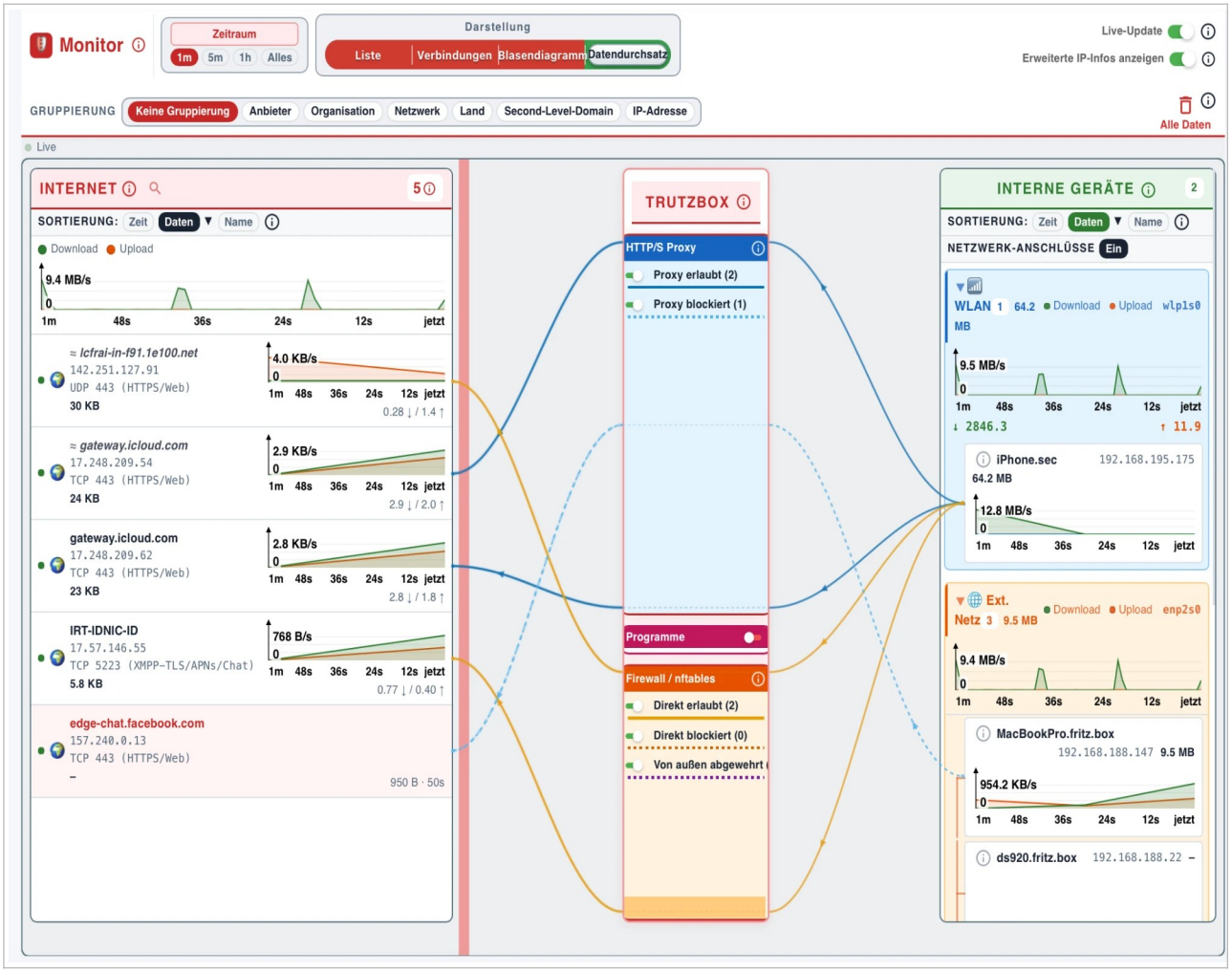


Abbildung 9-8: Netzwerk-Anschlüsse eingeschaltet: je Anschluss eine Karte mit eigener Kurve, die Geräte darunter gruppiert. (© 2026 Comidio GmbH)

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 Box die Daten überhaupt aufhebt: Aus, 10 Minuten, 1 Stunde, 6 Stunden oder 24 Stunden, danach wird automatisch gelöscht. Weiter zurückschauen als die Speicherdauer geht naturgemäß nicht.

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 Box 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.

Live-Update hält das Bild an, ohne die Aufzeichnung zu stoppen. **IP-Infos aus dem Internet ergänzen** blendet Land, Anbieter und Organisation zu jeder Gegenstelle ein; dazu fragt die Box 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 Box 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?".
- **Sperren und freigeben:** In den Details eines Servers sperren oder erlauben Sie ihn mit einem Klick, wahlweise die ganze Domain oder nur eine Adresse. Die Änderung landet in den Standard-Filterlisten (Kapitel 8.3) und wirkt sofort für alle Geräte. Die grüne Zahl über der Internet-Spalte kann sogar alle gerade angezeigten Gegenstellen eines Geräts auf einmal sperren, mit Nachfrage und Auswahlliste.
- **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, keine Portscan-Erkennung. Die eigentliche Erkennung von Scannern sitzt beim Angriffsschutz (Kapitel 14.4) und speist dieses Abzeichen nicht.

Die drei Zahlen neben Internet

In der Verbindungs-Darstellung stehen 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 einen Dialog, der alle gerade angezeigten, noch nicht gesperrten Server in einem Schritt sperrt. Grenzen Sie das Bild vorher mit den Schaltern, der Suche oder dem Geräte-Fokus auf das Gewünschte ein, dann ist das der schnellste Weg, einem Gerät eine ganze Gruppe unerwünschter Kontakte zu untersagen.

> **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?" Gerätekarte anklicken, Zeitraum auf „1h" stellen und die Liste durchsehen. Sie sehen jeden Server, den das Gerät kontaktiert hat, wie oft und mit welcher Datenmenge. 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?" Darstellung **Datendurchsatz** wählen und nach „Daten" sortieren. Ganz oben stehen die größten Verbraucher, aufgeschlüsselt nach Gerät und Gegenstelle. Meist ist es Video, gelegentlich aber auch ein Gerät, das im Hintergrund unbemerkt Daten überträgt.

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 die letzte Stunde, heute, diesen Monat und insgesamt sowie einem Diagramm „Blockierungen pro Tag".

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 einschalten

Ab Werk zeichnet die Box keine Statistik auf, und deshalb bleiben die Zahlen auf der Startseite zunächst leer. Zwei Klicks ändern das:

1. Öffnen Sie **Verwaltung → Statistiken**.
2. Schalten Sie **Statistiken speichern** ein. Ab diesem Moment zählt die Box mit; die ersten Zahlen erscheinen nach wenigen Minuten, das Tagesdiagramm füllt sich über die nächsten Tage.

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

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 im Monitor auf den Eintrag der betreffenden Gegenstelle.
2. Klicken Sie im geöffneten Eintrag auf das Symbol für TrutzContent. Die Adresse wandert damit in die Liste *Standard-TrutzContent-BL* und ist ab sofort gesperrt (Kapitel 8.3).

3. Umgekehrt geht es genauso: Wurde etwas zu Unrecht blockiert, gibt derselbe Weg die Adresse wieder frei; sie landet dann in der Ausnahmeliste *Standard-TrutzContent-WL*.

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. Solche Seiten nutzen dafür einen 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

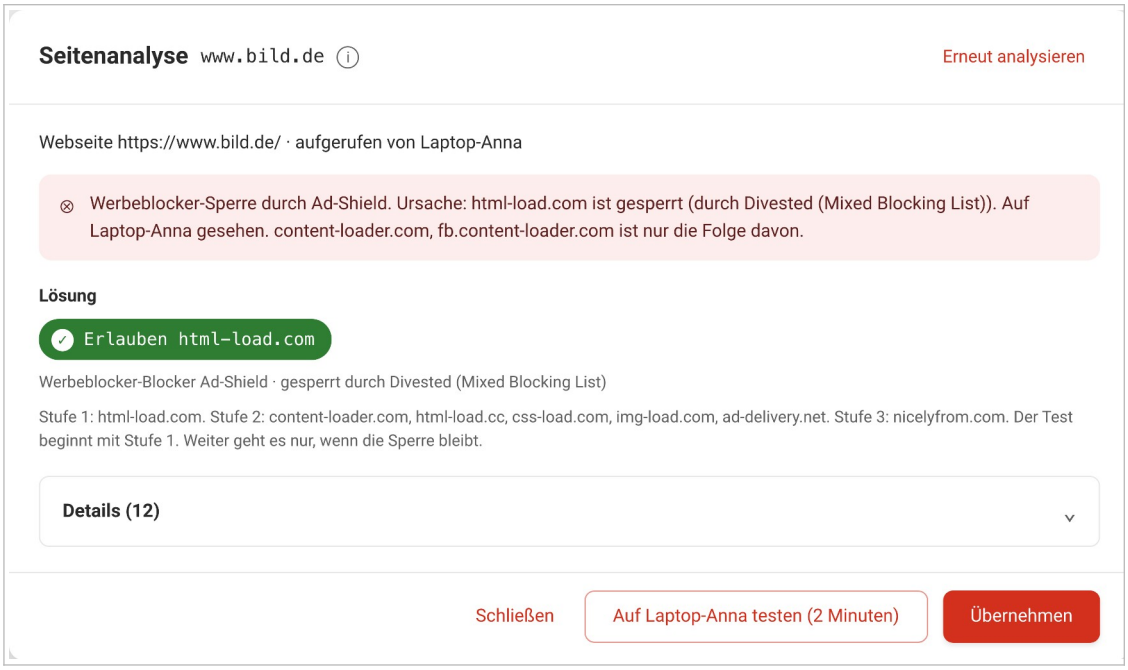


Abbildung 9-9: Die Seitenanalyse: oben das Ergebnis in einem Satz, darunter die Lösung, alles Weitere unter „Details". (© 2026 Comidio GmbH)

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, zum Beispiel: „Werbeblocker-Sperre durch Ad-Shield. Ursache: html-load.com ist gesperrt. Auf Laptop-Anna gesehen." 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 Box in Stufen bereit und nennt sie unter der Lösung: „Stufe 1: html-load.com. Stufe 2: content-loader.com, … Stufe 3: nicelyfrom.com."

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 geht: Behalten**. Die Box trägt genau diese Freigabe ein, nicht mehr.
3. Bleibt die Sperrseite: Klicken Sie **Sperre bleibt: Stufe 2**. Die Box 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 8.3) mit der Herkunft „Seitenanalyse: bild.de" und lassen sich dort jederzeit wieder löschen.

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 Box zählt nur, was zur Seite gehört. Was das Gerät nebenbei anfragt, etwa die Netzprüfung eines Smartphones, steht als „Hintergrundverkehr" nur unter Details.

Dazu kommen Hinweise, die keine Freigabe brauchen, aber gut zu wissen sind: Tracking über die eigene Domain der Seite, getarnte Tracker, Fingerprinting, 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 Box 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 Box zeigt den Zustand ihrer Listen, und der stimmt.

Die Seitenanalyse findet kein Gerät.

Die Box weiß nur von Aufrufen, die über sie gelaufen sind, und merkt sie sich so lange wie die Speicherdauer des Monitors (Kapitel 9.4), ab Werk eine Stunde. Rufen Sie die Seite auf dem Gerät auf und starten Sie die Analyse danach. Ohne Gerät fehlt der Test; „Übernehmen" geht trotzdem.

Sieht Comidio, was der Monitor aufzeichnet?

Nein. Alle Daten entstehen und bleiben auf Ihrer Box. Nur wenn Sie den Schalter „IP-Infos aus dem Internet ergänzen" einschalten, fragt die Box 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 Box?

Ein Teil der Erfassung läuft dauerhaft, auch ohne geöffnete Monitor-Ansicht (Abschnitt 9.4). Die Box 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 Box 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 Box entstehen und dort bleiben, kann Comidio verschlüsselte Post zwischen TrutzBoxen weder lesen noch herausgeben.

Die Box gehört eingeschaltet

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

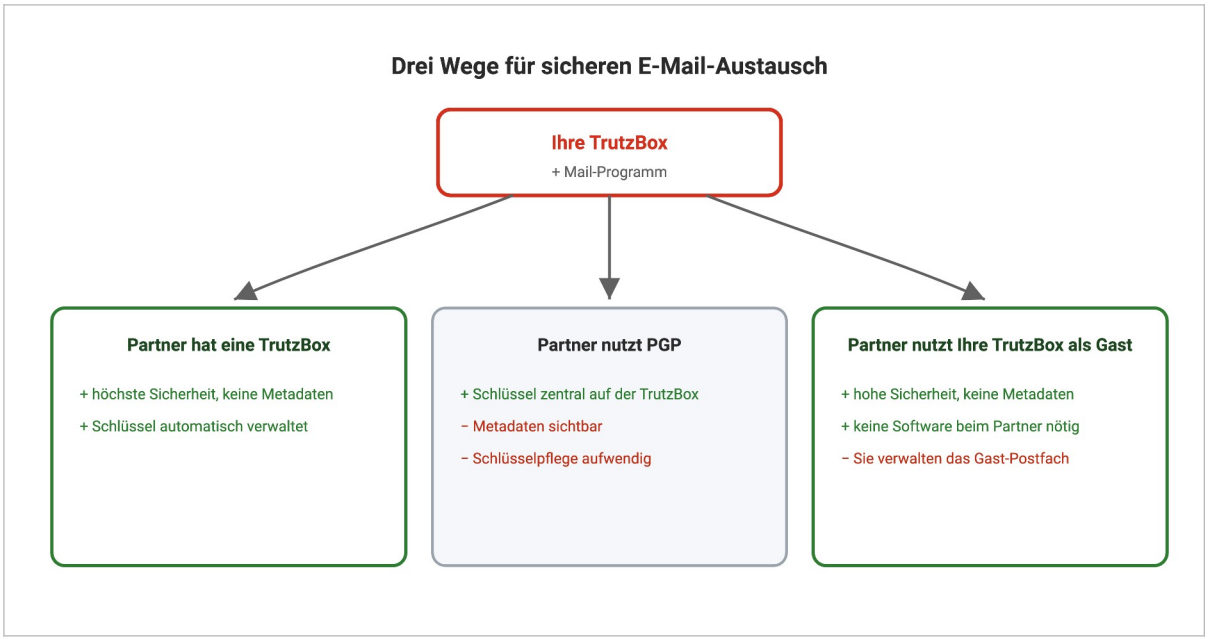


Abbildung 10-1: Drei Wege, je nach Gegenstelle: Partner mit TrutzBox, Partner mit PGP, Partner als Gast auf Ihrer TrutzBox. (© 2026 Comidio GmbH)

Weg A, der Partner hat eine eigene TrutzBox: der Königsweg. Beide schreiben mit ihrem normalen Mail-Programm, und die Boxen 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 Boxen 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: beglaubigt 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 Box. Ab diesem Moment verschlüsselt die Box 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 Box an (Kapitel 7). 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 Box, ohne

Metadaten nach außen. Dafür verwalten Sie das Konto, und der Partner muss dem Betreiber der Box, 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 Box an und nennen ihm Adresse und Passwort. Er ruft das Webmail im Browser auf und schreibt los; von unterwegs geht er dafür über den VPN-Zugang (Kapitel 12). 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 Box	ja	ja, alles bleibt auf Ihrer Box	keiner, Sie verwalten das Konto

Und der Empfang von ganz normaler, unverschlüsselter E-Mail? Der funktioniert weiterhin: Ein Comidio-Gateway nimmt Post aus dem freien Internet an Ihre @comidio.email-Adresse entgegen und reicht sie verschlüsselt an Ihre Box weiter. Nach außen verhält sich dieses Gateway wie ein ganz gewöhnlicher Mail-Server, nach innen wie eine TrutzBox. Nur in eine Richtung ist die Box konsequent streng: *Unverschlüsselt senden kann sie grundsätzlich nicht.* Wer es versucht, bekommt eine Fehlermeldung zurück. Auch das Gateway leitet aus Sicherheitsgründen nichts von Ihrer Box an gewöhnliche Adressen weiter. Für Alltagspost an beliebige Empfänger behalten Sie deshalb einfach Ihre bisherige Mail-Adresse parallel; 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 12). Technisch steckt dahinter Roundcube, ein weit verbreiteter quelloffener Web-Mailer, der auf der Box 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. Sie legen darin einfach ein zusätzliches Konto an; besondere Erweiterungen braucht es nicht, denn alle Verschlüsselung passiert auf der Box:

1. Neues Konto anlegen mit Ihrer TrutzMail-Adresse als Adresse und Benutzername.
2. Als Server für Eingang (IMAP) und Ausgang (SMTP) jeweils `trutzbox` eintragen, mit verschlüsselter Verbindung. Die automatische Erkennung der Mail-Programme trifft die Ports in der Regel von selbst. Falls das Programm nachfragt: Für den Eingang ist Port 993 richtig, für den Ausgang 465 oder 587, jeweils mit Verschlüsselung.
3. Testmail an die eigene Adresse schicken. Kommt sie an, ist alles richtig.

Die beiden Servernamen erledigen zwei verschiedene Aufgaben, die auf der Box 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 Box, 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.

Auf dem Smartphone

Auf Telefon und Tablet gilt dasselbe: In der Mail-App ein weiteres Konto anlegen, als Adresse und Benutzernamen die TrutzMail-Adresse eintragen, als Eingangs- und Ausgangsserver jeweils `trutzbox`. Das funktioniert mit den mitgelieferten Apps von Android und iOS ebenso wie mit anderen Mail-Programmen.

Zwei Dinge sind dabei zu beachten. Erstens erreicht das Telefon den Namen `trutzbox` nur, solange es im internen TrutzBox-Netzwerk ist, also im TrutzBox-WLAN. Unterwegs brauchen Sie dafür TrutzVPN (Kapitel 12); ist die VPN-Verbindung aufgebaut, funktioniert das Konto genau wie zuhause. Zweitens verbindet sich die Mail-App direkt mit der Box, und deshalb muss das Gerät der Box vertrauen: Auf dem Telefon gehört also das Root-Zertifikat installiert (Kapitel 19). Ohne es meldet die App eine Zertifikatswarnung oder verweigert die Verbindung ganz.

> **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 Boxen. Bei ungewöhnlich großen Sendungen lässt sich deshalb kaum vorhersagen, ob sie durchgehen. Hakt es, hilft meist ein Neustart der Box, weil der Arbeitsspeicher dabei geleert wird.

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

Abbildung 10-2: Die Kennzeichnung im Posteingang: [SE] von Box zu Box, [UE] mit PGP, [UU] gewöhnliche Internet-Post. (© 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 (beglaubigt), **U** für unsigniert. Der zweite die Übertragung: **E** für verschlüsselt (encrypted), **U** für unverschlüsselt.

Kennzeichen	Bedeutung
[SE]	Signiert und verschlüsselt: eine echte TrutzMail von Box zu Box. Absender beglaubigt, Inhalt und Metadaten geschützt.
[UE]	Verschlüsselt, aber Absender nicht beglaubigt: typisch für PGP-Post von Partnern ohne TrutzBox.
[UU]	Unverschlüsselt und unsigniert: gewöhnliche Internet-Post. 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 Box die Prüfung nicht durchführen.

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 10.6). Werbe- und Massenpost aus dem freien Internet 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. Gewöhnliche Post aus dem freien Internet erreicht Ihre TrutzMail-Adresse über das Comidio-Gateway und trägt immer die Kennzeichnung [UU]; daran erkennen Sie sie sofort und können sie im Mail-Programm auch automatisch in einen

eigenen Ordner sortieren lassen. In der Praxis kommt wenig Werbemüll an, weil eine TrutzMail-Adresse nicht in den Adresslisten der Massenversender steht. Geben Sie sie deshalb nur gezielt weiter und nutzen Sie für Anmeldungen bei Shops und Newslettern weiter Ihre bisherige Adresse.

Auch eine Größenbegrenzung für Ihr Postfach gibt es nicht. Die Grenze setzt allein der freie Platz auf der Box, und wie viel das ist, zeigt die Startseite (Kapitel 5.1).

10.5 Weg B einrichten: PGP mit Partnern ohne TrutzBox

1. Besorgen Sie sich den öffentlichen PGP-Schlüssel des Partners (er kann ihn Ihnen einfach mailen) und hinterlegen Sie ihn unter **E-Mail → Schlüsselverwaltung** über **Schlüssel hinzufügen**, aus einer Datei oder direkt aus der Zwischenablage. Ohne hinterlegten Schlüssel kann die Box an diesen Empfänger nicht senden.
2. Für den Versand nach draußen braucht die Box zusätzlich einen Postausgangsserver: Tragen Sie in den Benutzer-Einstellungen (**Verwaltung → Benutzer**) den SMTP-Server eines bestehenden Mail-Kontos ein. Die Box erkennt Server, Port und Verschlüsselung meist automatisch anhand der Adresse; mit **Verbindung testen** und **Test-Mail senden** prüfen Sie die Angaben sofort. Viele Anbieter verlangen dafür ein sogenanntes App-Passwort.
3. Ihren eigenen öffentlichen Schlüssel geben Sie dem Partner mit: In der Schlüsselverwaltung lässt er sich per Klick auf Ihr Konto herunterladen.

Warum dieser Umweg über ein zweites Konto nötig ist: Das Comidio-Gateway nimmt Post aus dem Internet für Sie an, gibt aber aus Sicherheitsgründen nichts von Ihrer Box nach draußen weiter. Für den Weg hinaus braucht die Box deshalb einen eigenen Ausgang, und das ist der Postausgangsserver eines gewöhnlichen Mail-Kontos, das Sie ohnehin schon haben.

Die Prüfung im zweiten Schritt läuft in Etappen ab und benennt einen Fehler dort, wo er auftritt: bei der Namensauflösung, beim Verbindungsaufbau oder bei der Anmeldung. Scheitert es an der Anmeldung, obwohl das Passwort stimmt, ist fast immer das App-Passwort die Lösung. Eine einmal eingerichtete Konfiguration lässt sich an derselben Stelle auch wieder löschen.

Beachten Sie die Richtungen getrennt: Zum **Senden** an eine gewöhnliche Adresse braucht die Box den öffentlichen Schlüssel des Empfängers und den Postausgangsserver. Zum **Empfangen** von PGP-Post braucht es beides nicht; nötig ist dann nur, dass der Absender Ihren öffentlichen Schlüssel kennt. Verschlüsselt eintreffende Post entschlüsselt die Box in jedem Fall automatisch und legt sie lesbar ins Postfach.

Menüpfad: E-Mail → Schlüsselverwaltung

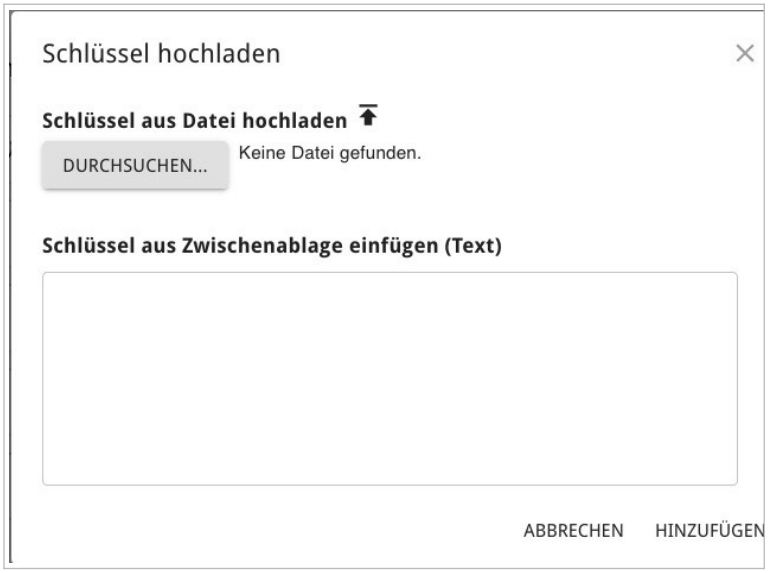


Abbildung 10-3: Den Schlüssel eines Partners hinzufügen: als Datei hochladen oder als Text einfügen. (© 2026 Comidio GmbH)

10.6 Schlüssel und Zertifikate

Menüpfad: E-Mail → Schlüsselverwaltung

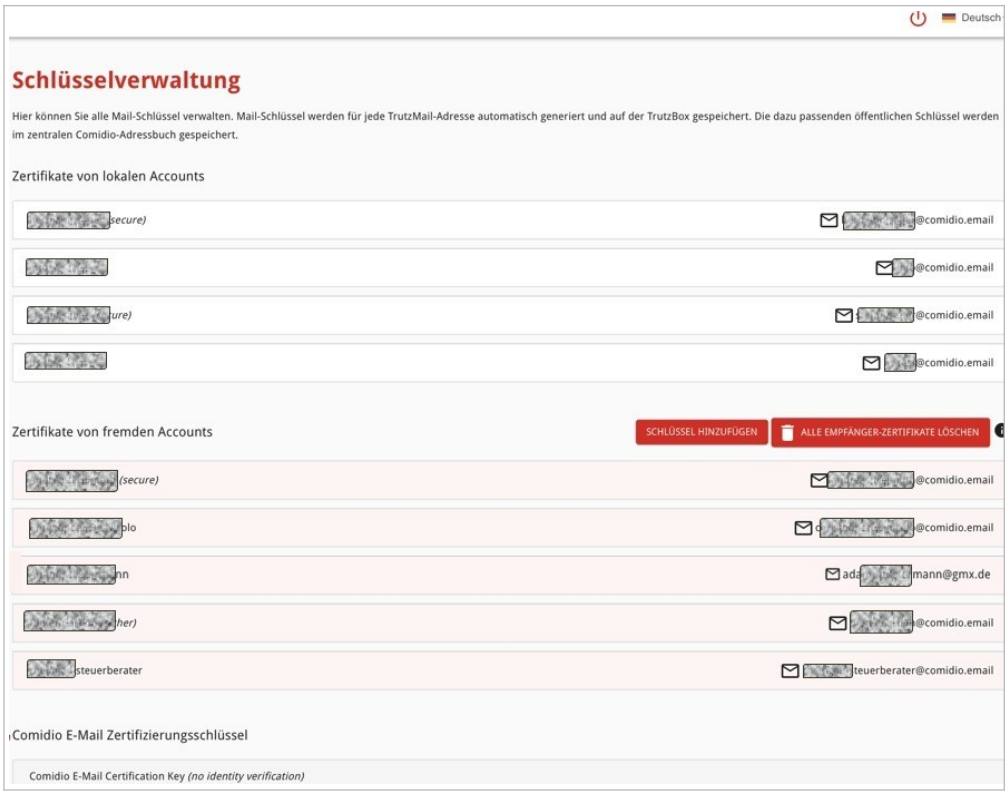


Abbildung 10-4: Die Schlüsselverwaltung: eigene Schlüssel oben, zwischengespeicherte fremde darunter, zuletzt der Comidio-Zertifizierungsschlüssel. (© 2026 Comidio GmbH)

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-Box 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 Box. 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 Box die Signaturen eingehender TrutzMails prüft.

Einmal täglich gleicht die Box zusätzlich ab, ob eines der gespeicherten fremden Zertifikate inzwischen ungültig geworden ist, etwa weil eine Box 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 Box 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 Box merkt das von selbst. Verschlüsselt sie noch an den alten Schlüssel, schickt die Gegenseite automatisch eine Korrektur-Notiz, und Ihre Box 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 Boxen 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 16): 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 Box 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 Box 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-Box in eine Zeitüberschreitung gelaufen ist; das heißt schlicht, dass die Box der Gegenseite gerade nicht erreichbar war. In diesem Fall ist nichts zu tun, Ihre Box 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-Box ist eingeschaltet und online. Ist sie es vorübergehend nicht, wiederholt Ihre Box die Zustellung selbsttätig.
- Ihr eigenes TrutzMail-Zertifikat ist gültig. Nach Ablauf des Servicevertrags 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-Box 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 7). Setzen Sie dort beim Anlegen das Häkchen **Als TrutzMail-Adresse registrieren**, prüft die Box zwei Dinge bei Comidio nach, bevor sie die Adresse einrichtet: ob der gewünschte Name überhaupt noch frei ist, denn TrutzMail-Adressen sind weltweit eindeutig, und ob Ihr Servicevertrag noch eine freie Adresse im Kontingent hat.

Erst wenn beides passt, erzeugt die Box das Schlüsselpaar und das zugehörige Mail-Zertifikat. Der geheime Teil verlässt die Box 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 Boxen 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 Box. In der Benutzerliste erscheint sie farblich abgesetzt unter **Reaktivierbare Benutzer** und kehrt über **Reaktivieren** mit einem Klick zurück.

> **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 16). Ihre Kommunikationspartner merken vom Schlüsselwechsel nichts: Ihre Boxen bemerken ihn selbst und holen den neuen Schlüssel beim nächsten Briefwechsel automatisch nach.

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 Servicevertrags 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 Boxen sprechen direkt miteinander.

Den Schlüssel einer Gegenstelle holt Ihre Box nur beim allerersten Kontakt aus dem Adressbuch und behält ihn danach. Auch der tägliche Abgleich über gesperrte Zertifikate läuft ausschließlich über Prüfwerte, nicht über Klartext-Adressen. Comidio betreibt darüber hinaus nur noch das Gateway, das gewöhnliche Post aus dem Internet an Ihre Adresse annimmt und verschlüsselt an Ihre Box weiterreicht. Alles andere, von der Verschlüsselung über die Zustellung bis zur Ablage, geschieht auf Ihrer eigenen Box.

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 dagegen alles, 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 Boxen. Hakt es bei einer ungewöhnlich großen Mail, hilft ein Neustart der Box. Der Dateiversand über TrutzChat (Kapitel 11) ist oft der bequemere Weg, allerdings nur bis 25 MB je Datei.

Kann Comidio meine Mails lesen?

Ihre verschlüsselte Post nicht: Comidio betreibt nur das Adressbuch mit den öffentlichen Schlüsseln und das Empfangs-Gateway, die geheimen Schlüssel und Ihre Postfächer liegen ausschließlich auf Ihrer Box. Für gewöhnliche, unverschlüsselte Post aus dem Internet gilt dasselbe wie für jede E-Mail: Sie ist offen unterwegs, bis das Comidio-Gateway sie verschlüsselt an Ihre Box weiterreicht. Deshalb trägt sie auch das Kennzeichen [UU].

Was passiert, wenn mein Servicevertrag ausläuft?

Das TrutzMail-Zertifikat wird dann nicht mehr erneuert. Empfänger-Boxen nehmen Ihre Mails danach nicht mehr an, und die Warteschlange weist auf das ungültige eigene Zertifikat hin. Die übrigen Schutzfunktionen der Box arbeiten weiter.

Muss ich meine Mails selbst sichern?

Die Sicherung unter **Systemeinstellungen → Sichern und Wiederherstellen** nimmt die Postfächer samt geheimer Schlüssel mit (Kapitel 16). Ohne sie sind die Schlüssel nach einem Zurücksetzen unwiederbringlich verloren, denn niemand sonst hat eine Kopie davon.

11 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 Box; 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 Box 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 7); damit meldet man sich an Chat und Videokonferenz an.
- Für Teilnehmer von außerhalb: ein TrutzDynDNS-Name samt Portfreigaben am Router (unten beschrieben). Im eigenen Netz und zwischen TrutzBoxen ist beides nicht nötig.
- Für eine Videokonferenz braucht nur der Einladende eine TrutzMail-Adresse. Alle anderen Teilnehmer kommen ohne Konto und ohne eigene TrutzBox aus.

11.1 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 Karteikarten: **Videokonferenz** für den Konferenz-Server und **TrutzChat** für den Nachrichtendienst. Dieses Kapitel folgt genau dieser Aufteilung: zuerst die Karteikarte Videokonferenz, danach die Karteikarte TrutzChat, zum Schluss die Benutzung im Alltag.

Menüpfad: Videokonferenz und Chat

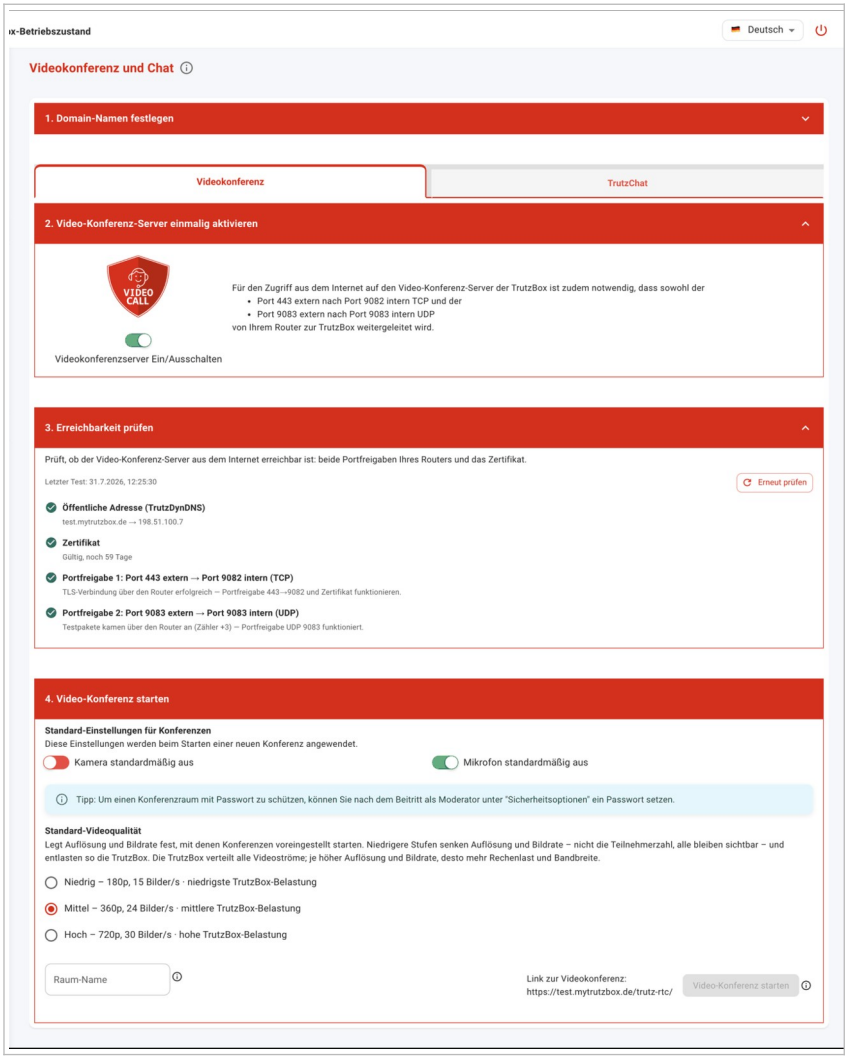


Abbildung 11-1: Die Seite Videokonferenz und Chat: oben der gemeinsame Schritt, darunter die beiden Karteikarten. (© 2026 Comidio GmbH)

Wenn der Server von außen nicht erreichbar ist

Meldet die Prüfung auf dieser Seite, dass Ihre Box von außen nicht erreichbar ist, liegt das fast nie an Chat oder Konferenz selbst, sondern an der Erreichbarkeit Ihres Internet-Anschlusses: fehlende Portfreigabe am Router oder ein Anschluss ohne eigene öffentliche IPv4-Adresse (DS-Lite). Beides behandelt ausführlich das Fernzugriff-Kapitel, insbesondere Kapitel 12.4 zur Erreichbarkeitsprüfung und Kapitel 12.9, wenn es nicht klappt. Die dortigen Schritte gelten für die Videokonferenz genauso.

11.2 Karteikarte Videokonferenz: einmalig einrichten

Menüpfad: Videokonferenz und Chat

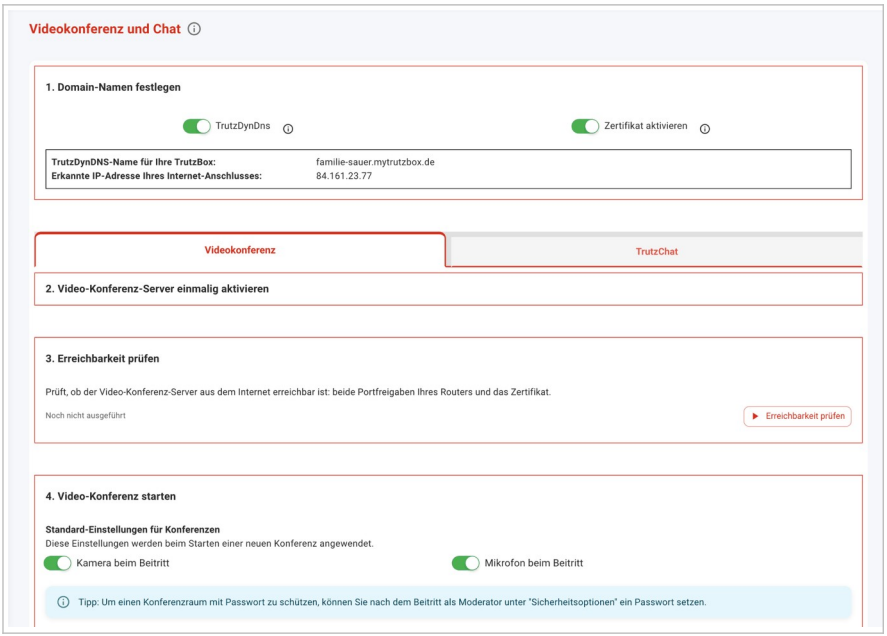


Abbildung 11-2: Die Karteikarte Videokonferenz führt in nummerierten Schritten durch die Einrichtung. (© 2026 Comidio GmbH)

Die Videokonferenz braucht einmalig vier Schritte auf der Karteikarte **Videokonferenz**; die Seite führt der Reihe nach hindurch:

1. **Domain-Namen festlegen:** TrutzDynDNS einschalten (wie beim Fernzugriff, Kapitel 12.2) und zusätzlich das kostenlose LetsEncrypt-Zertifikat aktivieren. Ohne dieses Zertifikat sehen Ihre Gäste Browserwarnungen. Schlägt die Ausstellung fehl, nennt die Fehlermeldung die konkrete Ursache.
2. **Video-Konferenz-Server einmalig aktivieren** und am Internet-Router zwei Portweiterleitungen einrichten: extern **443** auf intern **9082 (TCP)** und **9083 auf 9083 (UDP)**. Das Vorgehen am Router ist dasselbe wie in Kapitel 12.3 beschrieben.
3. **Erreichbarkeit prüfen:** Der Selbsttest prüft in vier Stationen die öffentliche Adresse, das Zertifikat und beide Portfreigaben und meldet das Ergebnis jeweils im Klartext, etwa dass die Verbindung über den Router gelungen ist oder dass eine Freigabe fehlt.
4. **Video-Konferenz starten:** Raumnamen eingeben (ohne Sonderzeichen) und los. Der Einladungslink hat die Form `https://ihrname.mytrutzbox.de/trutz-rtc/raumname`. Hier legen Sie auch fest, ob Kamera und Mikrofon in neuen Konferenzen zunächst an oder aus sind.

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://ihrname.mytrutzbox.de:4443/trutz-rtc/raumname`. Verfügt Ihr Anschluss über IPv6, ist der Konferenz-Server zusätzlich direkt über die globale IPv6-Adresse der Box erreichbar, ohne Portweiterleitung; dafür genügt am Router eine IPv6-Freigabe für die Box auf 443 (TCP) und 9083 (UDP), ohne Umleitung auf 9082. Wie eine IPv6-Freigabe angelegt wird, zeigt Kapitel 12.11.

Das Zertifikat nicht ständig neu anfordern

LetsEncrypt 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.

11.3 Konferenzen im Alltag

Einen Raum eröffnen kann nur, wer sich mit einer TrutzMail-Adresse Ihrer Box 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.

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.

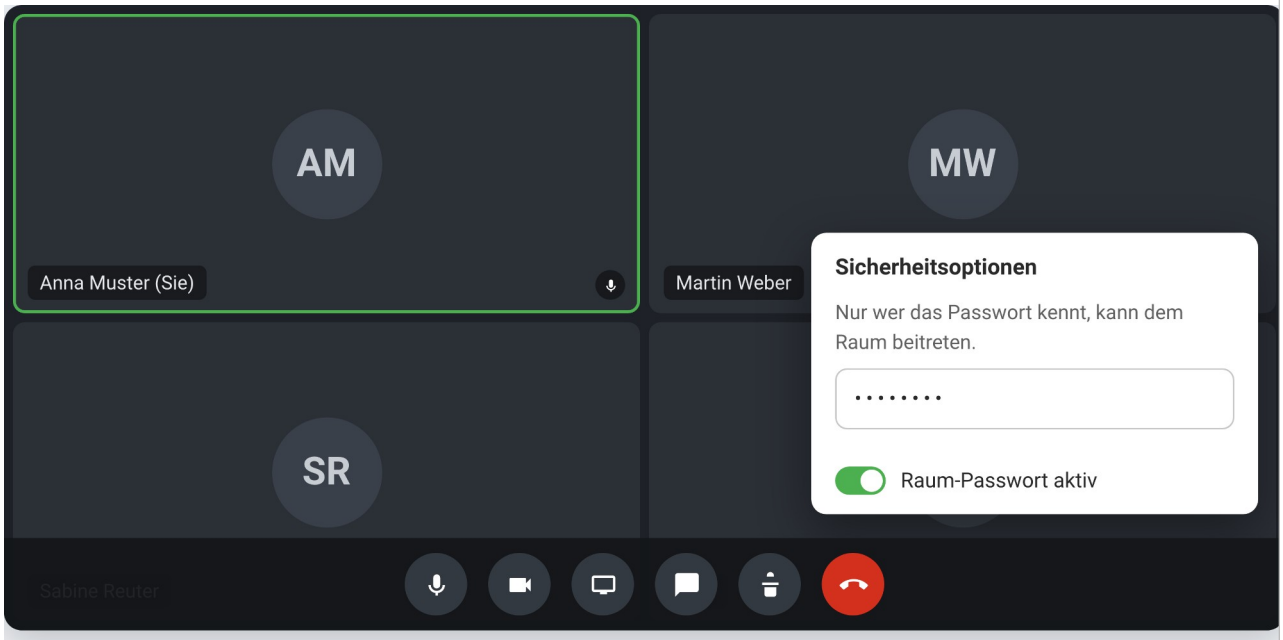


Abbildung 11-3: Das Konferenzfenster mit Bedienleiste und geöffneten Sicherheitsoptionen für das Raum-Passwort. (© 2026 Comidio GmbH)

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 danach beitritt, wird danach gefragt. Geben Sie Link und Passwort möglichst auf getrennten Wegen weiter, damit nicht beides in derselben Nachricht steht.

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 Box 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 Box 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.

11.4 Karteikarte TrutzChat: Selbsttest, Aufbewahrung, Gruppen

Für Verwaltung und Aufräumen gibt es auf der Seite **Videokonferenz und Chat** die Karteikarte **TrutzChat**. Sie nennt oben die beiden Zugangsadressen, im eigenen Netz und von unterwegs, und weist ausdrücklich darauf hin: Im eigenen Netz und zwischen TrutzBoxen kommt TrutzChat ohne TrutzDynDNS aus. Der öffentliche Name wird nur für den direkten Zugriff von unterwegs gebraucht.

Der Chat-Selbsttest

Der **Chat-Selbsttest** prüft auf Knopfdruck den kompletten Nachrichtenweg auf der Box: 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 Box selbst, und der Support hat sofort einen Anhaltspunkt.

Ein bestandener Test sagt allerdings nur, dass der Nachrichtenweg auf Ihrer Box arbeitet. Ausdrücklich nicht geprüft werden drei Dinge: der Chat mit Teilnehmern auf anderen TrutzBoxen, der über das Tor-Netzwerk läuft, die Erreichbarkeit von unterwegs mit Portfreigaben und TrutzDynDNS 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

Unter **Verwaltung** legen Sie fest, wie viele Tage Chat-Verläufe aufbewahrt werden. Die Änderung wird mit dem nächsten Start des Chat-Dienstes wirksam; Älteres löscht die Box danach selbsttätig. Die Frist gilt für Einzelgespräche und Gruppen gleichermaßen. Anhänge räumt die Box 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 Box 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.

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

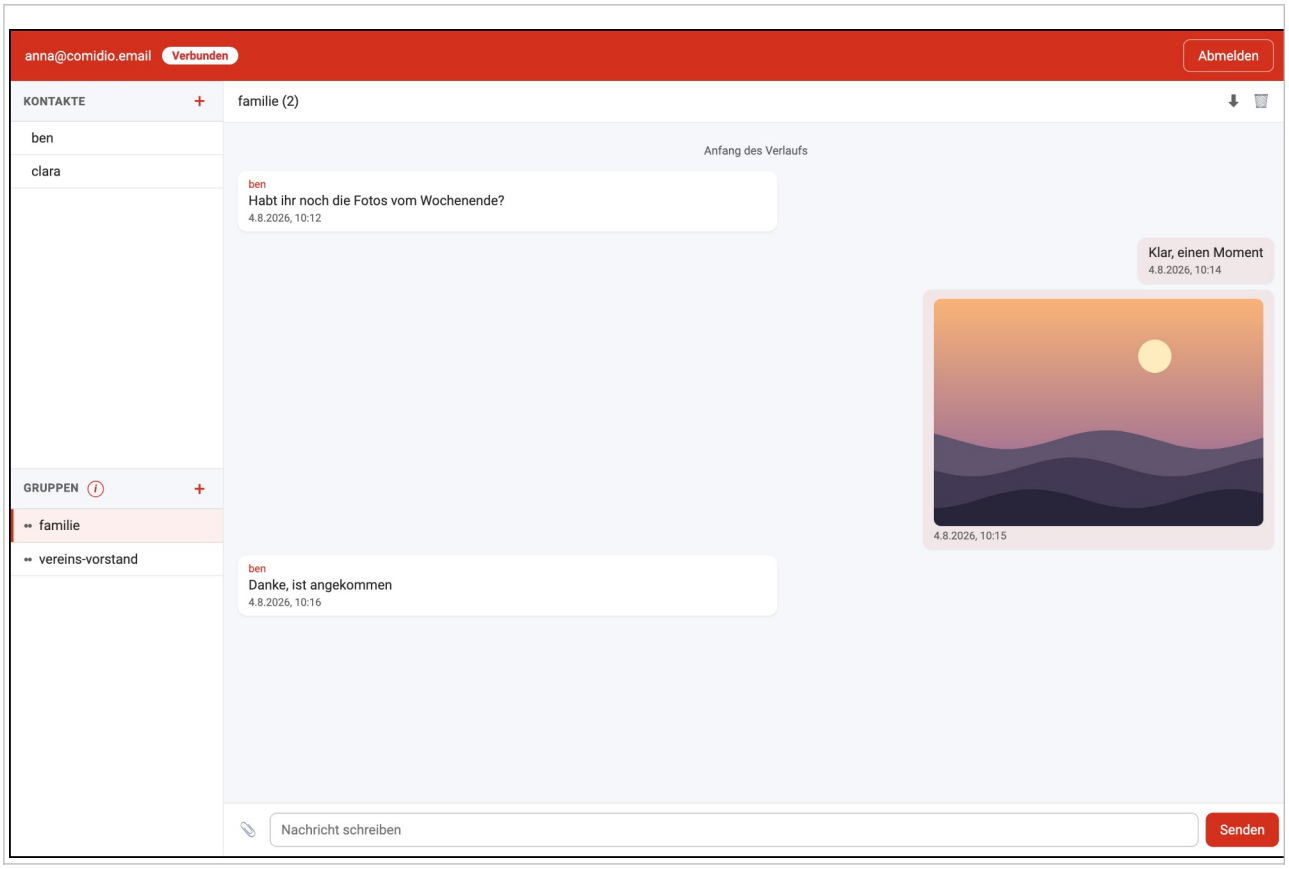


Abbildung 11-4: TrutzChat im Browser: links Kontakte und Gruppen, rechts das Gespräch mit Bildern und Dateien. (© 2026 Comidio GmbH)

Der eingebaute Web-Chat ist der einfachste Einstieg: Im eigenen Netz öffnen Sie `https://trutzbox/chat/`, von unterwegs die gleiche Adresse mit Ihrem TrutzDynDNS-Namen, und melden sich mit TrutzMail-Adresse und Passwort an. Kontakte fügen Sie über deren TrutzMail-Adresse hinzu; die Gegenseite bestätigt einmal, danach zeigt ein farbiger Punkt die Erreichbarkeit.

Dateien und Bilder wandern per Büroklammer oder einfach mit der Maus ins Fenster. Bilder erscheinen als Vorschau direkt im Gespräch, andere Dateien als anklickbarer Verweis; die Gegenseite lädt einen Anhang erst dann von Ihrer Box, wenn sie ihn öffnet. Nach 30 Tagen räumt die Box Anhänge selbsttätig ab.

Der Gesprächsverlauf kommt aus dem Archiv Ihrer Box, 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 Box 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 Box; 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.

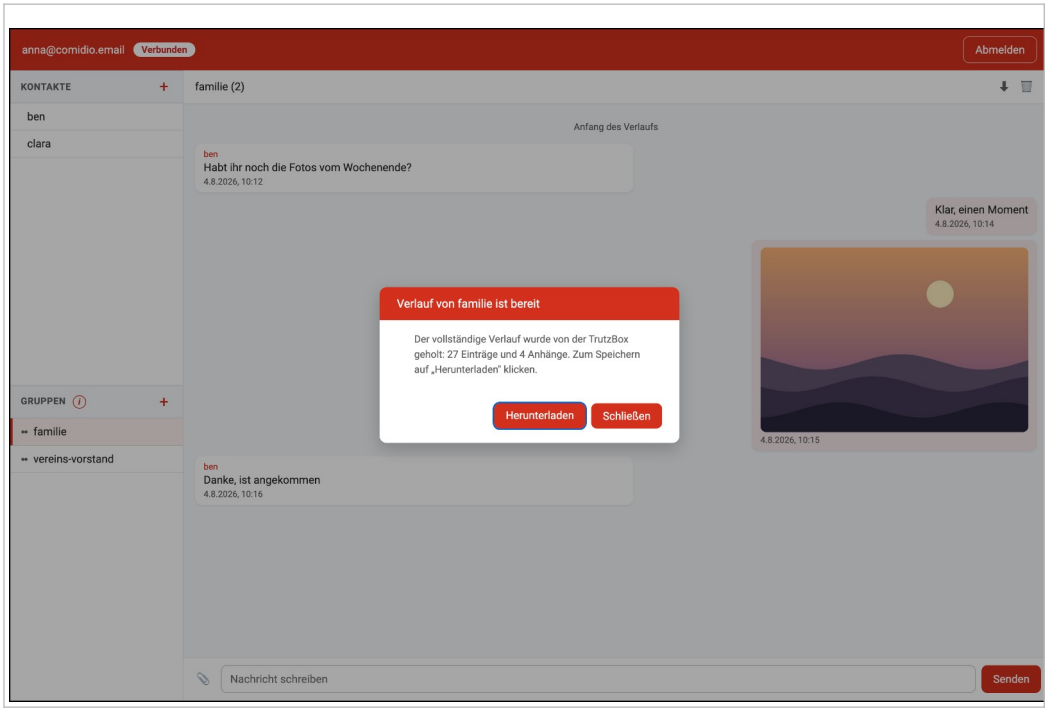


Abbildung 11-5: Verlauf sichern oder löschen: Der Gesprächsverlauf liegt auf Ihrer Box, nicht im Browser. (© 2026 Comidio GmbH)

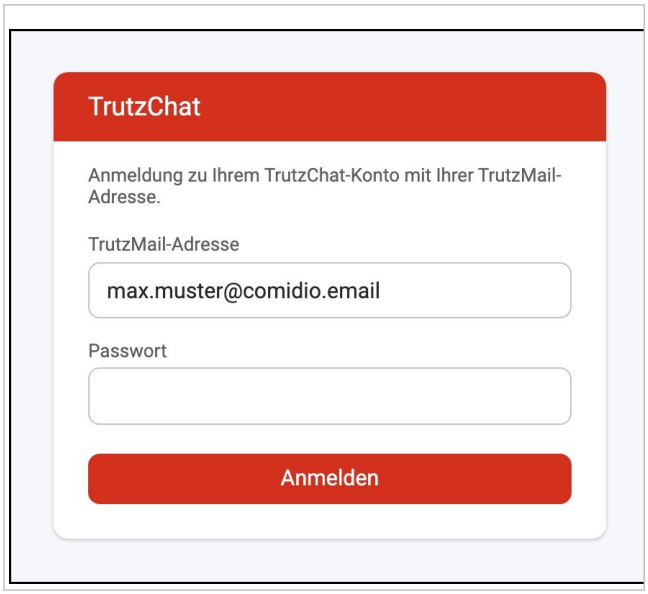


Abbildung 11-6: Die Anmeldung am Web-Chat mit TrutzMail-Adresse und Passwort. (© 2026 Comidio GmbH)

Eine Chat-App einrichten

Lieber eine App? TrutzChat spricht den offenen Chat-Standard XMPP, den viele Programme auf allen Systemen beherrschen. Die Einrichtung dauert eine Minute:

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

1. Installieren Sie das Programm und legen Sie darin ein neues Konto an.
2. Tragen Sie als Konto-Kennung Ihre **TrutzMail-Adresse** ein und als Passwort Ihr TrutzMail-Passwort.
3. Prüfen Sie den **Servernamen**. Viele Apps leiten ihn aus der Adresse ab und tragen dann „comidio.email" ein; richtig ist im eigenen Netz `trutzbox`. Der Standard-Port 5222 bleibt unverändert.
4. Verbinden und einen Kontakt über dessen TrutzMail-Adresse hinzufügen. In einem Programm lassen sich auch mehrere TrutzMail-Adressen gleichzeitig einrichten.

Für unterwegs empfiehlt Comidio ausdrücklich den Weg über den VPN-Zugang (Kapitel 12): Ist die VPN-Verbindung aufgebaut, funktioniert die App mit dem Servernamen `trutzbox` genau wie zuhause. Eine Freigabe des Chat-Ports am Router ist nicht vorgesehen: Chat-Programme nimmt die Box nur aus dem eigenen Netz und über den VPN-Zugang an.

Welche Ports der Zugang von unterwegs braucht

Den Web-Chat erreichen Sie von unterwegs über **443/TCP**, also über dieselbe Portfreigabe am Router, die auch die Videokonferenz braucht. Chat-Programme sprechen dagegen über Port **5222/TCP**, und den nimmt die Box nur aus dem eigenen Netz und über den VPN-Zugang an; am Router wird er nicht freigegeben. Im eigenen Netz und zwischen TrutzBoxen ist gar keine Freigabe nötig.

Alternativ erreichen Sie den Chat über den Fernzugriff per VPN (Kapitel 12). Dieser Weg kommt ohne zusätzliche Freigabe am Router aus, weil der Chat vollständig innerhalb der VPN-Verbindung läuft.

11.6 Kontakte und Gruppen

Menüpfad: Videokonferenz und Chat → TrutzChat

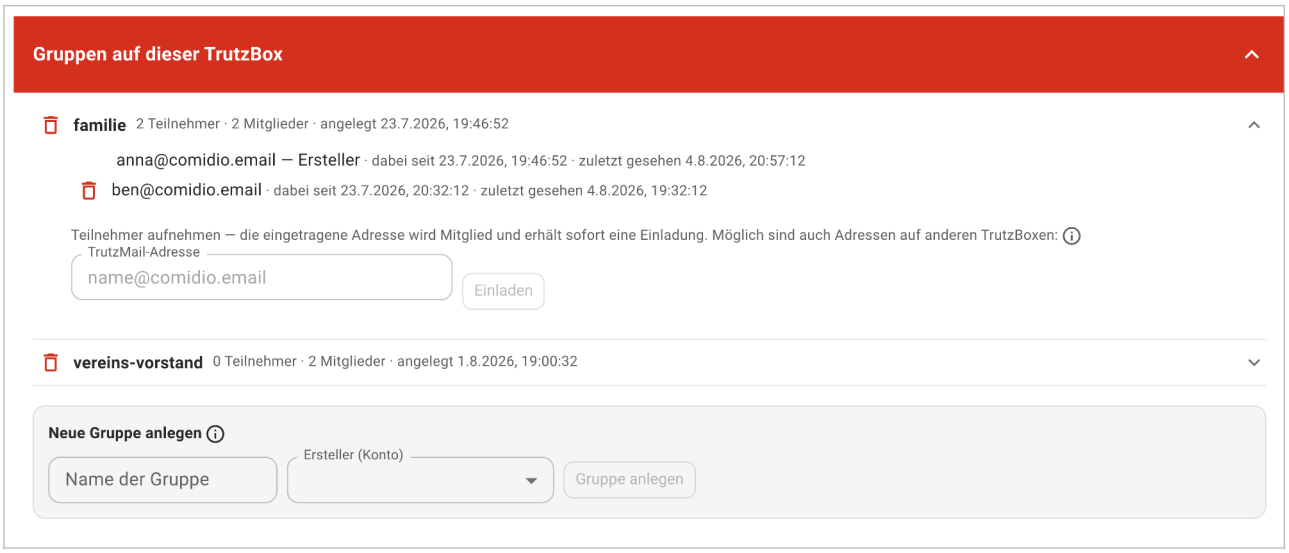


Abbildung 11-7: Gruppenverwaltung: Gruppen anlegen, Mitglieder aufnehmen und Verläufe im Blick behalten. (© 2026 Comidio GmbH)

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 Boxen der Teilnehmer verbinden sich dann verschlüsselt untereinander. Über das Stift-Symbol einer Gruppe sehen Sie, wer gerade in der Gruppe ist (Ersteller und Abwesende sind gekennzeichnet), laden weitere Teilnehmer ein oder entfernen sie. 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 Box, 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 11.4).

11.7 Was im Hintergrund für Sicherheit sorgt

Bei Nachrichten zwischen zwei TrutzBoxen greifen drei Schutzschichten ineinander. Die Nachricht selbst ist verschlüsselt, die Verbindung zwischen den Boxen 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 Boxen ist nicht im Spiel.

Adressiert wird dabei immer die TrutzMail-Adresse, und beim Verbindungsaufbau prüft die Box 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 Box 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 Box und nimmt zu keinem anderen Server im Internet Verbindung auf. Die Browser der Teilnehmer sprechen ausschließlich mit Ihrer Box, 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 Box zu Box, 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 Portfreigabe, Zertifikatsprobleme und Router-Eigenheiten. Zertifikatswarnungen bei Gästen deuten auf ein fehlendes LetsEncrypt-Zertifikat. 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 weder TrutzDynDNS noch Portfreigaben. Nur wer von unterwegs direkt auf den Web-Chat will, geht über den VPN-Zugang oder den TrutzDynDNS-Namen.

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.

12 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 3) und Sie kennen das Admin-Passwort.

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

• Ihr Internet-Anschluss hat eine eigene öffentliche IPv4-Adresse (IPv4 und IPv6 sind die beiden Adressarten des Internets, siehe Glossar). Fehlt sie, wie bei DS-Lite, geht TrutzVPN nur über IPv6, siehe Abschnitt 12.11.

• 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.

12.1 So funktioniert TrutzVPN

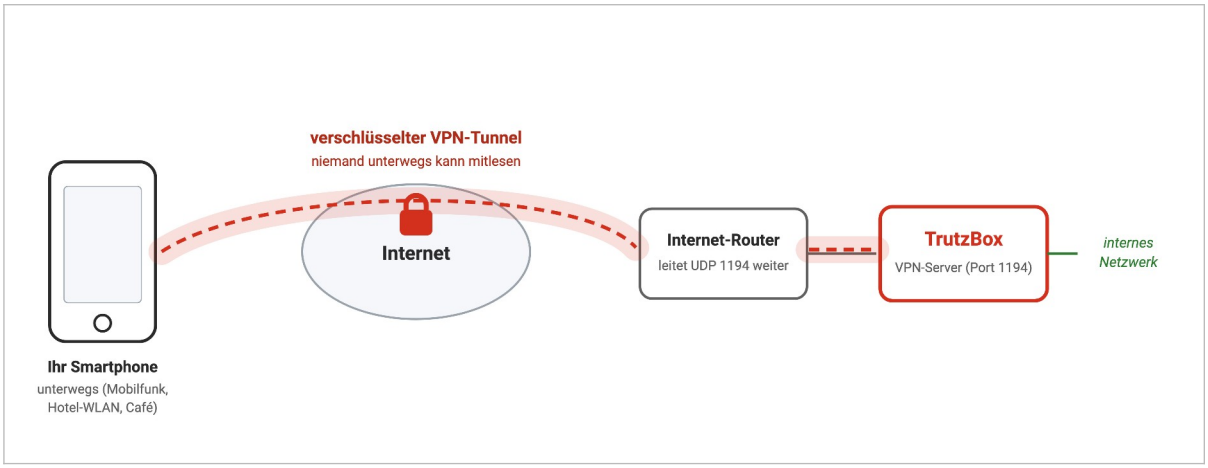


Abbildung 12-1: Der VPN-Tunnel: vom Smartphone unterwegs verschlüsselt durch das Internet bis zur TrutzBox. (© 2026 Comidio GmbH)

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. Alles auf der TrutzBox erledigen Sie an einer einzigen Stelle: **Netzwerk → Fernzugriff**. Die Seite ist dort in drei

nummerierte Karten gegliedert: Karte **1. Domain-Namen festlegen** (Abschnitt 12.2), Karte **2. Erreichbarkeit prüfen** (Abschnitt 12.4) und Karte **3. VPN-Server einrichten** (Abschnitt 12.5). Die Portweiterleitung aus Abschnitt 12.3 liegt dazwischen und hat bewusst keine eigene Karte, denn sie wird nicht auf der Box, sondern am Internet-Router eingerichtet.

> **Für Neugierige: Die Technik dahinter**
>
> TrutzVPN basiert auf **OpenVPN**, einem seit Jahrzehnten bewährten offenen Standard. Der Server läuft auf der TrutzBox und ist über den UDP-Port 1194 erreichbar. Jeder Zugang wird mit einem eigenen Zertifikat abgesichert; 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.

12.2 Schritt 1: Domain-Name festlegen (TrutzDynDNS)

Ihr Gerät muss Ihre TrutzBox im Internet finden können. Die IP-Adresse Ihres Anschlusses wechselt aber immer wieder. Deshalb bekommt Ihre Box einen festen Namen, der automatisch immer auf die aktuelle Adresse zeigt. Diesen Dienst stellt Comidio kostenlos unter dem Namen **TrutzDynDNS** bereit.

Menüpfad: Netzwerk → Fernzugriff

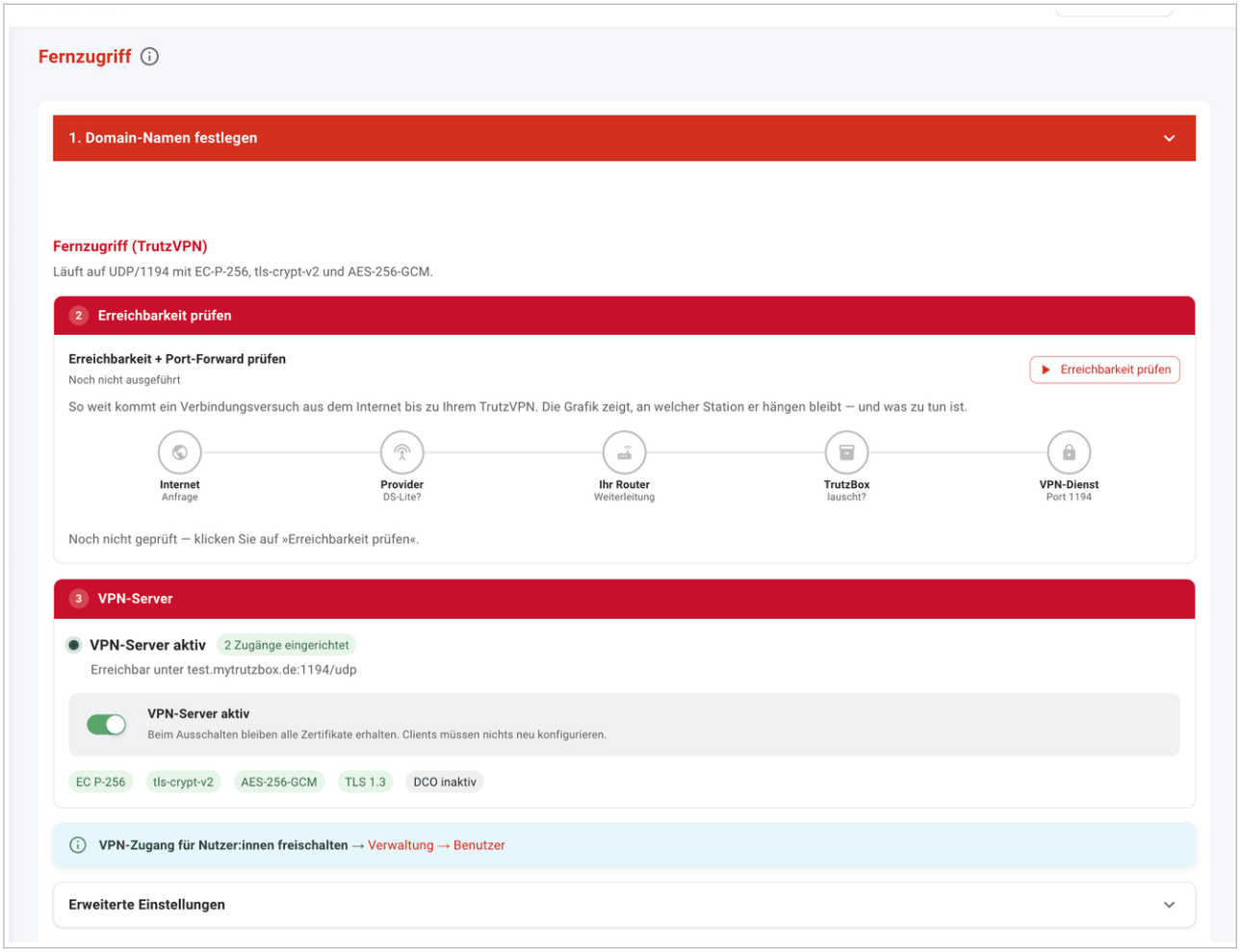


Abbildung 12-2: Die Seite Netzwerk → Fernzugriff mit den drei Schritten: Domain-Namen festlegen, Erreichbarkeit prüfen, VPN-Server. (© 2026 Comidio GmbH)

1. Öffnen Sie im Admin-Panel **Netzwerk → Fernzugriff**.
2. Schalten Sie in Karte **1. Domain-Namen festlegen** den Schalter **TrutzDynDns** ein.
3. Notieren Sie sich den angezeigten Namen, etwa `a1b2c3d4e5.mytrutzbox.de`. Unter diesem Namen ist Ihre Box künftig von außen erreichbar.

> **Was speichert Comidio dabei?**
> Nur Ihre jeweils aktuelle IP-Adresse, verknüpft mit Ihrem Domain-Namen, und das jeweils nur bis zur nächsten Aktualisierung, ohne Verlauf. Schalten Sie TrutzDynDNS ab, endet die Speicherung.

12.3 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.

Wie die Einrichtung genau aussieht, unterscheidet sich von Router zu Router, und die Hersteller ändern ihre Oberflächen laufend. Deshalb beschreiben wir hier nur das Prinzip. Die stets aktuelle Klick-Anleitung für Ihr Modell finden Sie über die Hilfeseiten des Herstellers (Tabelle unten). Im Grundsatz sind es immer dieselben fünf Angaben:

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.

Aktuelle Anleitungen der Router-Hersteller:

Router	Suchen Sie nach …	Hilfeseite
AVM Fritzbox	„Portfreigabe einrichten"	avm.de/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

IPv6-Freigabe und mehrere TrutzBoxen

Wollen Sie TrutzVPN auch über IPv6 anbieten, kommt am Router eine zweite Regel hinzu, die IPv6-Freigabe (Abschnitt 12.11). 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 Box ist von außen nur über IPv6 erreichbar, ebenfalls Abschnitt 12.11.

12.4 Schritt 3: Erreichbarkeit prüfen

Ob Domain-Name und Portweiterleitung stimmen, prüft die TrutzBox selbst. Klicken Sie im Schritt **2. Erreichbarkeit prüfen** auf die gleichnamige Schaltfläche. Die Box schickt sich daraufhin über das Internet ein Testpaket und zeigt den Weg als Kette mit fünf Stationen:

Menüpfad: Netzwerk → Fernzugriff

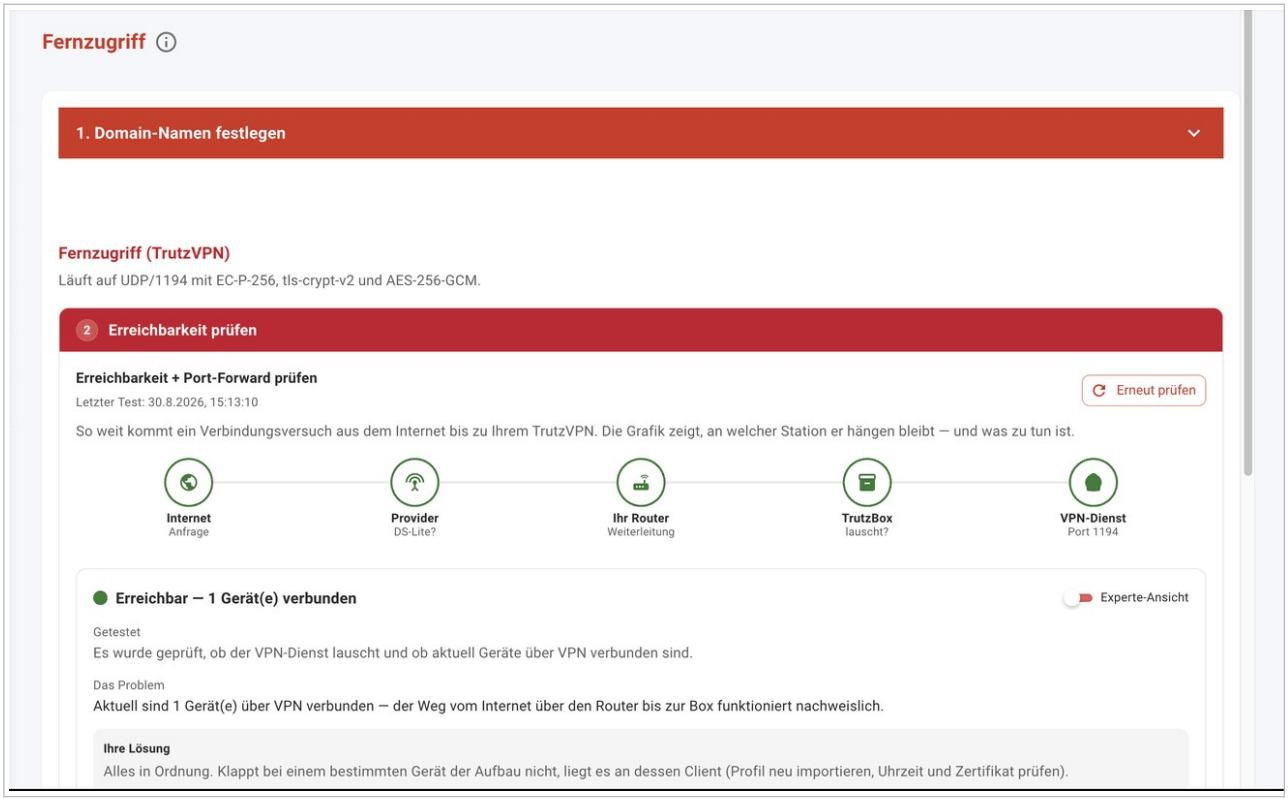


Abbildung 12-3: Die Erreichbarkeitsprüfung: Die Kette zeigt, wie weit ein Verbindungsversuch aus dem Internet kommt, darunter steht das Ergebnis im Klartext. (© 2026 Comidio GmbH)

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

Unter der Kette steht in ganzen Sätzen, was geprüft wurde, woran es hakt und was zu tun ist. 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 12.5 weitermachen.

Anschluss ohne eigene IPv4-Adresse (DS-Lite)?

Kommt beim Test trotz richtiger Portfreigabe nichts an, vergibt Ihr Anbieter vermutlich keine eigene öffentliche IPv4-Adresse an Ihren Anschluss. Provider nennen das DS-Lite; verbreitet ist es bei Kabel- und Glasfaser-Anschlüssen. Eingehende IPv4-Verbindungen sind dann nicht möglich, egal wie der Router eingestellt ist.

Zwei Wege führen trotzdem zum Ziel. Erstens: TrutzVPN auch über **IPv6** anbieten, wie in Abschnitt 12.11 beschrieben. Das klappt dann aus allen Netzen, die selbst IPv6 haben, etwa aus den meisten Mobilfunknetzen. Zweitens: eine echte öffentliche IPv4-Adresse beim Anbieter anfragen. Viele Anbieter stellen den Anschluss auf Wunsch um, oft unter der Bezeichnung „Dual-Stack", und häufig genügt dafür ein Anruf.

Test meldet Fehler, obwohl alles stimmt?

Manche Router beherrschen das „Hairpin"-Verfahren des Selbsttests nicht. Dann meldet der Test einen Fehler, obwohl der Zugang von außen funktioniert. Machen Sie im Zweifel nach Abschluss der Einrichtung einen echten Verbindungsversuch: mit dem Smartphone über Mobilfunk, WLAN dabei ausschalten.

12.5 Schritt 4: VPN-Server einrichten und einschalten

Jetzt kommt der eigentliche VPN-Server an die Reihe. Klicken Sie in Karte **3. VPN-Server einrichten** auf **VPN einrichten**. Die Box erzeugt dabei einmalig ihr eigenes Zertifikatszentrum und die nötigen Schlüssel. Das dauert nur etwa 15 Sekunden, den Fortschritt sehen Sie live.

Menüpfad: Netzwerk → Fernzugriff

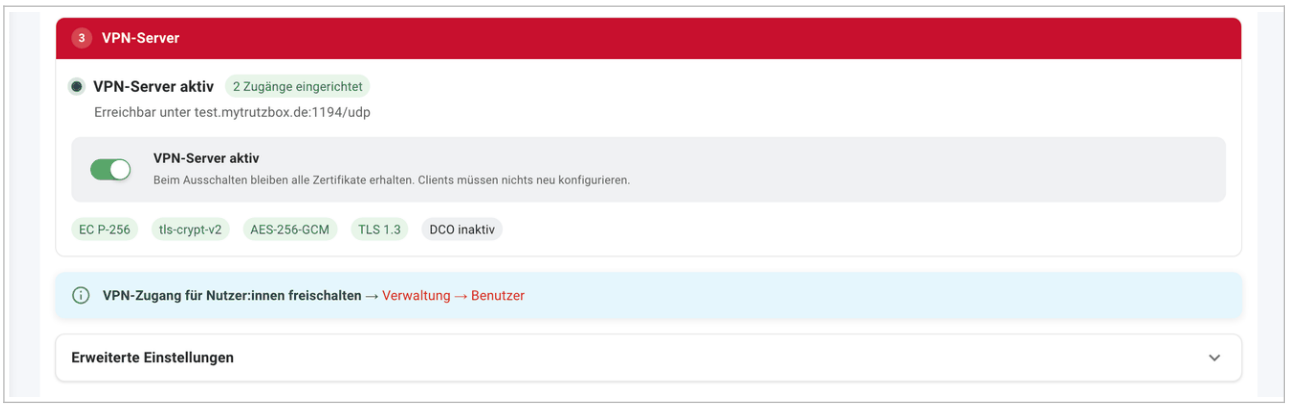


Abbildung 12-4: Der laufende VPN-Server: Adresse, Zahl der Zugänge und die verwendeten Verfahren, darunter der Verweis auf die Freischaltung je Benutzer. (© 2026 Comidio GmbH)

Danach zeigt die Karte den laufenden Server: den grünen Schalter **VPN-Server aktiv**, die Adresse, unter der er erreichbar ist, und die Zahl der eingerichteten Zugänge. Über den Schalter können Sie den Server jederzeit anhalten. Alle Zertifikate bleiben dabei erhalten, und Ihre Geräte müssen nichts neu einrichten.

Server aus = Tür zu

Wenn Sie längere Zeit keinen Fernzugriff brauchen, schalten Sie den Server einfach ab. Dann ist Port 1194 aus dem Internet nicht mehr erreichbar, und automatische Scanner können erst gar keinen Anlauf nehmen. Zur nächsten Reise schalten Sie ihn mit einem Klick wieder ein.

12.6 Schritt 5: Benutzer freischalten und Profil herunterladen

Wer die VPN-Verbindung nutzen darf, legen Sie pro Benutzer fest, und zwar in der Benutzerverwaltung unter **Verwaltung → Benutzer**. Am schnellsten kommen Sie dorthin über den Verweis *„VPN-Zugang für Nutzer:innen freischalten"* unten auf der Fernzugriff-Seite; er führt direkt zur richtigen Stelle. Für jeden freigeschalteten Benutzer erzeugt die Box eine persönliche Konfigurationsdatei, das **VPN-Profil** mit der Endung `.ovpn`. Diese eine Datei enthält alles, was ein Endgerät braucht.

Menüpfad: Netzwerk → Fernzugriff

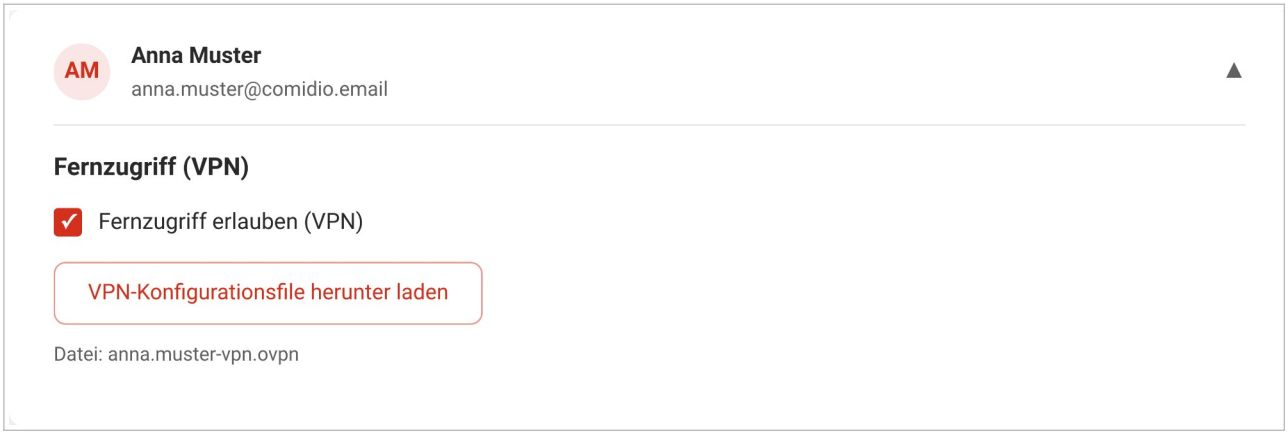


Abbildung 12-5: Beim Benutzer wird der Fernzugriff erlaubt und das VPN-Profil heruntergeladen. (© 2026 Comidio GmbH)

1. Öffnen Sie **Verwaltung → Benutzer** und klappen Sie den gewünschten Benutzer auf.
2. Setzen Sie im Abschnitt **Fernzugriff (VPN)** das Häkchen *„Fernzugriff erlauben (VPN)"*.
3. Klicken Sie auf **VPN-Konfigurationsfile herunter laden**. Sie erhalten eine Datei wie `anna.muster-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 Profil erlaubt **eine** Verbindung gleichzeitig. Sollen Laptop und Smartphone derselben Person zeitgleich verbunden sein, legen Sie dafür einfach einen zweiten Benutzer an (Kapitel 7).

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 12.11).

12.7 Ihre Geräte einrichten

Auf dem Endgerät brauchen Sie ein VPN-Programm, das OpenVPN-Profile versteht. Das Vorgehen ist überall gleich und besteht aus drei Handgriffen:

1. VPN-Programm installieren (Empfehlung je System siehe unten).
2. Die `.ovpn`-Datei im Programm importieren.
3. Verbindung einschalten. Fertig.

Die Programme ändern sich mit jeder Version ein wenig; Bildschirmfotos wären hier schnell veraltet. Maßgeblich sind deshalb die Anleitungen der Hersteller. 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

Auf dem Mac hat sich das freie Programm **Tunnelblick** bewährt (tunnelblick.net). Dort ziehen Sie die Profildatei einfach auf das Programmsymbol. Alternativ funktioniert auch hier OpenVPN Connect.

iPhone und iPad

Installieren Sie **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 iOS einmalig, ob die App VPN-Konfigurationen hinzufügen darf. Das bestätigen Sie.

Android

Installieren Sie **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.

> **Läuft die Box auf WireGuard?**
> Ihre TrutzBox kann statt OpenVPN auch den neueren Tunnel WireGuard anbieten. Dann brauchen Ihre Geräte ein anderes Programm und eine andere Zugangsdatei. Welches der beiden läuft, steht auf der Fernzugriff-Seite im Umschalter. Die Einrichtung je System steht in Abschnitt 12.12.

> **Andere VPN-Programme?**
> Jedes Programm, das den OpenVPN-Standard beherrscht, funktioniert. Unter Linux zum Beispiel importiert der NetworkManager die Profildatei direkt. 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.

12.8 Unterwegs verbinden

Unterwegs genügt künftig ein Fingertipp im VPN-Programm. Sobald die Verbindung steht, erkennbar am Schlüssel- oder VPN-Symbol in der Statusleiste, läuft Ihr gesamter Datenverkehr durch den Tunnel zu Ihrer TrutzBox: Werbe- und Trackerfilter greifen, gefährliche Seiten bleiben blockiert, und im Monitor der Box taucht Ihr Gerät wie gewohnt auf, als „TrutzVPN-Einwahl" 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 Box wählt das VPN-Programm selbst. Im eigenen Heimnetz verbindet es sich immer über IPv4 mit dem Netzwerknamen der Box. Haben Sie **VPN auch über IPv6 anbieten** eingeschaltet (Abschnitt 12.11), 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.

12.9 Wenn es nicht klappt

Der häufigste Fall: Das VPN-Programm meldet keinen Verbindungsaufbau oder bleibt bei „Verbinde…" hängen. Ihre TrutzBox hilft bei der Ursachensuche mit einer Diagnose-Grafik auf der Fernzugriff-Seite. Sie ist überschrieben mit *„So weit kommt ein Verbindungsversuch aus dem Internet bis zu Ihrem TrutzVPN"* und zeigt Station für Station, wie weit eine Anfrage von außen kommt und woran sie scheitert.

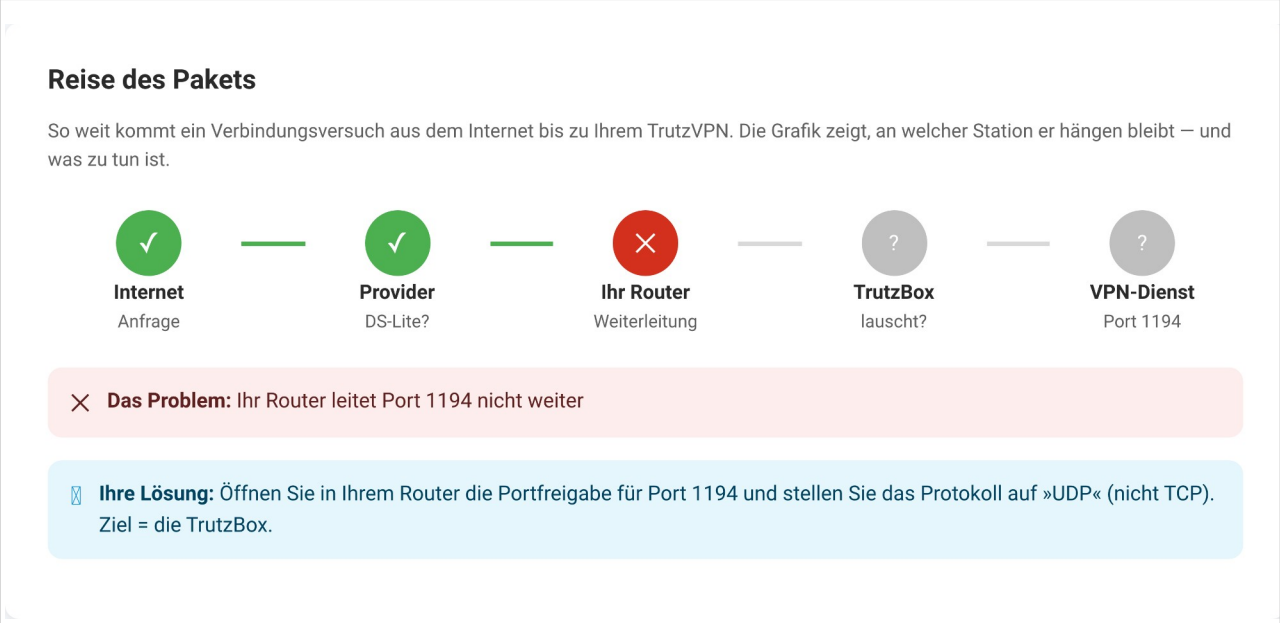


Abbildung 12-6: Die Diagnose zeigt: Bis zum Provider kommt das Paket, der Router leitet aber nicht weiter, samt Lösungsvorschlag. (© 2026 Comidio GmbH)

Symptom	Wahrscheinliche Ursache	Das hilft
Diagnose stoppt bei „Ihr Router"	Portfreigabe fehlt oder steht auf TCP; seltener ein Anschluss ohne eigene IPv4-Adresse (DS-Lite)	Freigabe prüfen: UDP, Port 1194, Ziel TrutzBox (Abschnitt 12.3); bei DS-Lite siehe Abschnitte 12.4 und 12.11
Diagnose stoppt beim „Provider"	Die Box kann ihre öffentliche Internet-Adresse nicht ermitteln	Internetverbindung der Box prüfen und den Test wiederholen
Diagnose stoppt bei „TrutzBox"	VPN-Dienst läuft nicht	Schalter „VPN-Server aktiv" einschalten (Abschnitt 12.5)

Symptom	Wahrscheinliche Ursache	Das hilft
„Von außen erreichbar", Verbindung klappt trotzdem nicht	Problem liegt am Endgerät	Profil neu importieren; Datum und Uhrzeit des Geräts prüfen; notfalls Häkchen beim Benutzer aus- und wieder einschalten und das neue Profil verwenden
Verbindung klappt zuhause im WLAN nicht	Test findet innerhalb des eigenen Netzes statt	Zum Testen Mobilfunk verwenden, WLAN am Smartphone ausschalten
IPv6 eingeschaltet, aber unterwegs keine Verbindung	Meist steckt in der App noch das alte Profil; seltener fehlt die IPv6-Freigabe oder das Netz unterwegs hat kein IPv6	Profil neu herunterladen und in der App ersetzen, Freigabe prüfen, Mobilfunk verwenden (Abschnitt 12.11)
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 12.11)
Zweite TrutzBox am selben Router: keine Verbindung, keine klare Meldung	Das Profil landet über IPv4 bei der anderen Box, die es abweist	Für diese Box IPv6 mit eigener IPv6-Freigabe einrichten und das Profil neu laden (Abschnitt 12.11)

Führt das alles nicht weiter, hält die Fernzugriff-Seite unter *„Technische Details (für Support)"* einen Diagnosetext bereit, den Sie kopieren und dem Comidio-Support schicken können. Mehr dazu in Kapitel 18.

12.10 Was der Fernzugriff sonst noch ermöglicht

Der VPN-Tunnel bringt Sie nicht nur geschützt ins Internet, er bringt Sie auch nach Hause. 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 10 und 11);
- 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.

12.11 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 zusätzlich den Weg über IPv6. Das lohnt sich in zwei Fällen:

- **Anschluss ohne eigene IPv4-Adresse (DS-Lite, Abschnitt 12.4).** Von außen ist Ihre Box dann nur über IPv6 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 Box braucht den Weg über IPv6 mit einer eigenen Freigabe am Router. Landet ein Profil über IPv4 bei der falschen Box, weist diese es ab, und die App zeigt keinen verständlichen Fehler.

Der Tunnel selbst bleibt dabei unverändert, IPv6 ist nur der Weg zur Box. Den Schalter können Sie erst umlegen, wenn der VPN-Server läuft (Abschnitt 12.5) und die TrutzBox eine globale, also im ganzen Internet gültige IPv6-Adresse hat. Fehlt diese, steht an seiner Stelle *„Nicht verfügbar: Die Box 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 Box. Sie wird aus der Hardware-Adresse der Box 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 12.3 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 Box und fragt dafür die Interface-ID ab.
3. Klappen Sie auf derselben Seite den Bereich **Erweiterte Einstellungen** auf und schalten Sie in der ersten Zeile **VPN auch über IPv6 anbieten** ein.
4. Laden Sie für jeden Benutzer das VPN-Profil neu herunter (Abschnitt 12.6). Löschen Sie in der VPN-App das alte Profil und importieren Sie das neue.
5. Testen Sie unterwegs, etwa mit dem Smartphone über Mobilfunk bei ausgeschaltetem WLAN.

Beispiel Fritzbox

Unter „Internet" → „Freigaben" die TrutzBox als Gerät auswählen, im Feld „IPv6 Interface-ID" den Wert aus Schritt 1 eintragen und eine Freigabe mit Protokoll UDP, Port 1194 und „Internetzugriff über IPv6" anlegen. Ein grüner Punkt neben der Freigabe heißt nur, dass die Regel aktiv ist, nicht, dass die Box von außen erreichbar ist. Die aktuelle Anleitung finden Sie unter avm.de/service.

Nur mit Freigabe einschalten, danach Profile ersetzen

Ist der Schalter 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 Profile auf der Box 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 Profil steht

Das Profil enthält mehrere Adressen, die die VPN-App der Reihe nach probiert. Ist der Schalter aus, sind es zwei: der Netzwerkname der TrutzBox im Heimnetz 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 zuhause immer IPv4 und IPv6 nur unterwegs. Der VPN-Server auf der Box nimmt Verbindungen über beide Wege an; welchen Weg ein Gerät versucht, bestimmt allein das Profil.

12.12 Geräte einrichten, wenn die Box WireGuard nutzt

WireGuard ist der zweite Tunnel Ihrer TrutzBox. Er verbindet nach einem Netzwechsel in Sekunden neu und schont den Akku; verschlüsselt wird bei beiden Wegen gleich stark. Läuft die Box auf WireGuard, gilt statt der `.ovpn`-Datei eine `.conf`-Datei, und statt OpenVPN Connect brauchen Ihre Geräte die offizielle WireGuard-App. Beide Tunnel benutzen denselben Anschluss UDP 1194, an der Freigabe im Router ändert sich also nichts.

Es läuft immer nur einer der beiden Tunnel, denn beide benutzen denselben Anschluss. Welcher es ist, stellen Sie auf der Fernzugriff-Seite im Umschalter über der Karte ein. Beim Wechsel richtet die Box WireGuard beim ersten Mal selbst ein, hält OpenVPN an und übergibt den Anschluss. 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.

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 Heimnetz erreichen Sie die TrutzBox danach wie gewohnt, von unterwegs erst wieder über den neuen Tunnel.

Menüpfad: Netzwerk → Fernzugriff

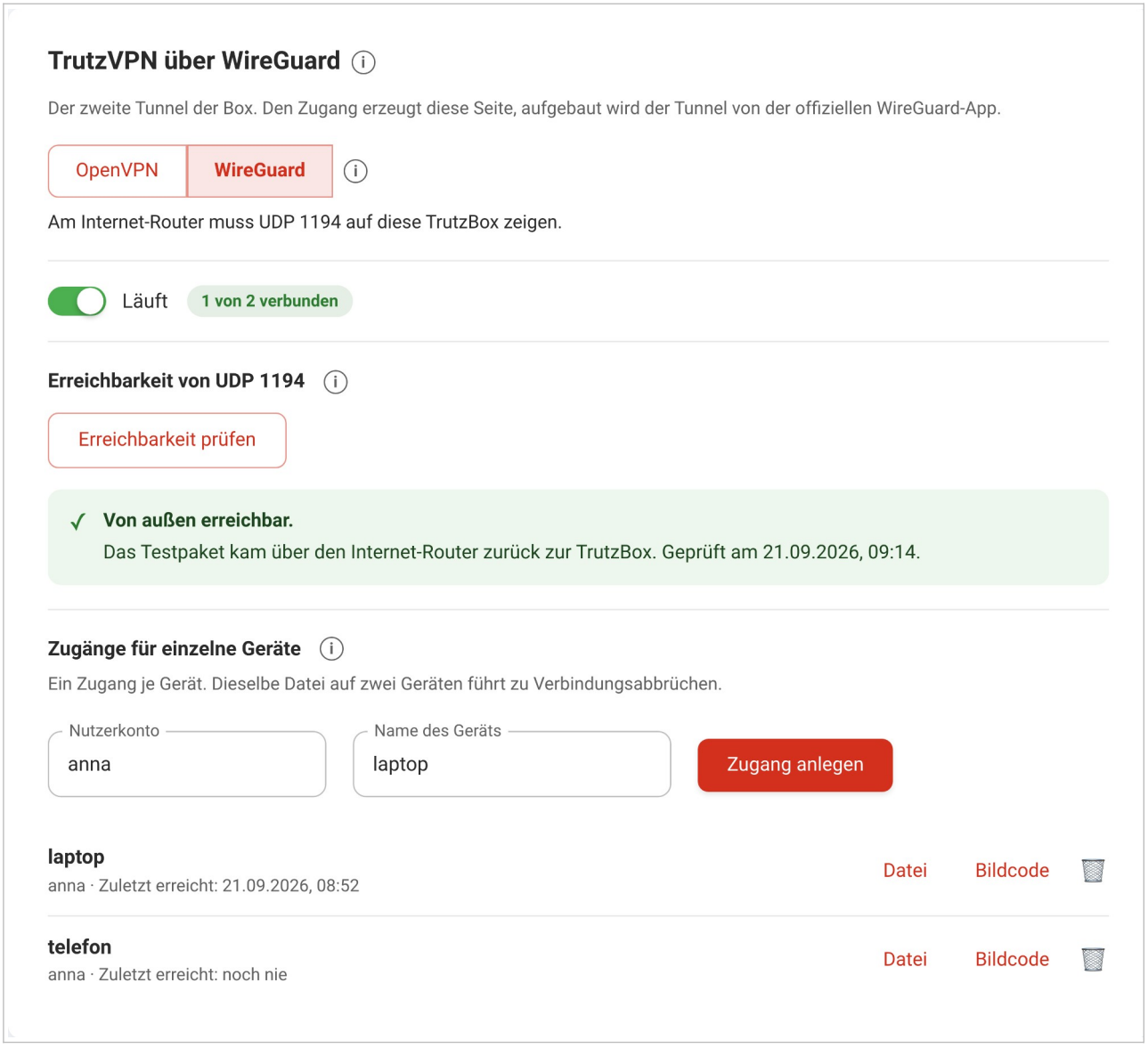


Abbildung 12-7: Die WireGuard-Karte: oben der Umschalter zwischen den beiden Tunneln, darunter der Zustand, die Erreichbarkeitsprüfung und die Zugänge der einzelnen Geräte. (© 2026 Comidio GmbH)

Den Zugang für ein Gerät erzeugen Sie auf der Fernzugriff-Seite unter *„Zugänge für einzelne Geräte"*: Nutzerkonto wählen, Gerätenamen eintragen, **Zugang anlegen**. Danach steht der Zugang in der Liste und lässt sich jederzeit erneut öffnen, als Bildcode zum Abfotografieren oder als Datei.

1. WireGuard-App installieren (Bezugsquelle je System siehe unten).
2. Zugang hineinbringen: am Telefon den Bildcode einlesen, am Rechner die `.conf`-Datei importieren.
3. Verbindung einschalten. Fertig.

Menüpfad: Netzwerk → Fernzugriff

Abbildung 12-8: Der Zugang eines Geräts: links der Bildcode für das Telefon, rechts derselbe Inhalt als Text, dazu der Knopf für die Datei. (© 2026 Comidio GmbH)

Windows

Die App **WireGuard für Windows** von wireguard.com, kostenlos unter wireguard.com/install. Nach der Installation *„Tunnel aus Datei importieren"* wählen und die `.conf`-Datei öffnen. Die Verbindung starten Sie mit *„Aktivieren"* neben dem Tunnelnamen.

macOS

WireGuard aus dem Mac App Store. In der App *„Tunnel aus Datei importieren"* wählen. Beim ersten Einschalten fragt macOS einmalig, ob die App VPN-Verbindungen einrichten darf; das bestätigen Sie mit Ihrem Anmeldekennwort.

iPhone und iPad

WireGuard aus dem App Store. In der App auf *„Hinzufügen"* tippen, dann *„Aus QR-Code erstellen"* wählen und den Bildcode von der Fernzugriff-Seite abfotografieren. Beim ersten Verbinden fragt iOS einmalig, ob die App VPN-Konfigurationen hinzufügen darf. Das bestätigen Sie.

Android

WireGuard aus dem Play Store. In der App auf das Pluszeichen tippen, *„Aus QR-Code scannen"* wählen und den Bildcode einlesen. Wer lieber die Datei nimmt, kopiert sie auf das Gerät und wählt *„Aus Datei oder Archiv importieren"*. Auch Android fragt beim ersten Start einmalig um Erlaubnis.

Linux

WireGuard steckt im Linux-Kern; es fehlen nur die Werkzeuge, unter Debian und Ubuntu das Paket `wireguard`. Die `.conf`-Datei nach `/etc/wireguard/trutzbox.conf` legen und mit `wg-quick up trutzbox` einschalten, mit `wg-quick down trutzbox` wieder aus. Der NetworkManager kann die Datei ebenfalls importieren.

> **Ein Zugang gehört zu einem Gerät**
> Jeder Zugang trägt seinen eigenen Schlüssel. Dieselbe Datei auf zwei Geräten führt zu ständigen Verbindungsabbrüchen, weil beide dieselbe Anschrift im Tunnel beanspruchen. Legen Sie deshalb je Gerät einen eigenen Zugang an. Die Datei ist ein Schlüssel: nicht per unverschlüsselter E-Mail verschicken, und verlorene Zugänge auf der Fernzugriff-Seite entfernen.

Ob der Weg von außen offen ist, beantwortet die Box selbst: der Knopf **Erreichbarkeit prüfen** in der WireGuard-Karte schickt ein Testpaket über Ihren Router zurück zur Box und zeigt das Ergebnis in derselben Grafik wie bei OpenVPN (Abschnitt 12.9). Anders als dort muss der Tunnel dafür nicht angehalten werden.

Häufige Fragen zu TrutzVPN

Können mehrere Geräte gleichzeitig verbunden sein?

Ja, jedes braucht aber sein eigenes Profil und damit seinen eigenen Benutzer. Ein einzelnes Profil lässt bewusst nur eine Verbindung gleichzeitig zu.

Was passiert, wenn ich zwischen OpenVPN und WireGuard umschalte?

Die Box 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 OpenVPN Connect für OpenVPN und die WireGuard-App für WireGuard. Wer unterwegs umstellt, sollte daran denken, dass die eigene Verbindung dabei abbricht.

Was kostet TrutzDynDNS?

Nichts. Der Dienst gehört zu Ihrer TrutzBox; Comidio speichert dabei nur die jeweils aktuelle IP-Adresse Ihres Anschlusses, ohne Verlauf.

Funktioniert TrutzVPN auch an einem Anschluss mit DS-Lite?

Ja, über IPv6: am Router die IPv6-Freigabe einrichten, den Schalter **VPN auch über IPv6 anbieten** einschalten und die Profile neu laden (Abschnitt 12.11). Verbinden können Sie sich dann aus allen Netzen mit IPv6, also meist im Mobilfunk, in manchen Hotel-WLANs aber nicht.

Warum ist IPv6 nicht ab Werk eingeschaltet?

TrutzDynDNS veröffentlicht die IPv6-Adresse Ihrer Box immer, prüft aber nicht, ob sie von außen erreichbar ist. Fehlt die Freigabe am Router, hängen die Apps an einer toten Adresse, und OpenVPN Connect auf iPhone und iPad bricht dabei teils ganz ab. Ob die Freigabe eingerichtet ist, weiß nur, wer den Router verwaltet. Deshalb entscheiden Sie selbst.

Ist meine Box 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 gültiges Zertifikat 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 14.4). Wer das Restrisiko weiter senken will, schaltet den VPN-Server einfach ab, wenn er längere Zeit nicht gebraucht wird.

13 TrutzBrowse: zusätzlicher Schutz für Browser und Apps

Der Webfilter aus Kapitel 8 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 Tracker aus Browser und Apps keinen wiedererkennbaren „Fingerabdruck" Ihres Geräts bilden können. TrutzBrowse ist für erfahrene Anwender gedacht und wird je Gerät einzeln eingeschaltet.

13.1 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 neun Stufen von „wenig Eingriff, alles funktioniert" bis „maximale Anonymität". 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 feiner geht es kaum: Sogar einzelne Pfade einer Domain lassen sich unterschiedlich behandeln, das Tracking-Skript 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 Tracker 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 14.4).

> **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.

13.2 Woraus ein Fingerabdruck entsteht

Um zu verstehen, woran TrutzBrowse ansetzt, hilft ein Blick auf das, was ein Tracking-Skript 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.

13.3 Webfilter und TrutzBrowse: zwei Stufen, ein Ziel

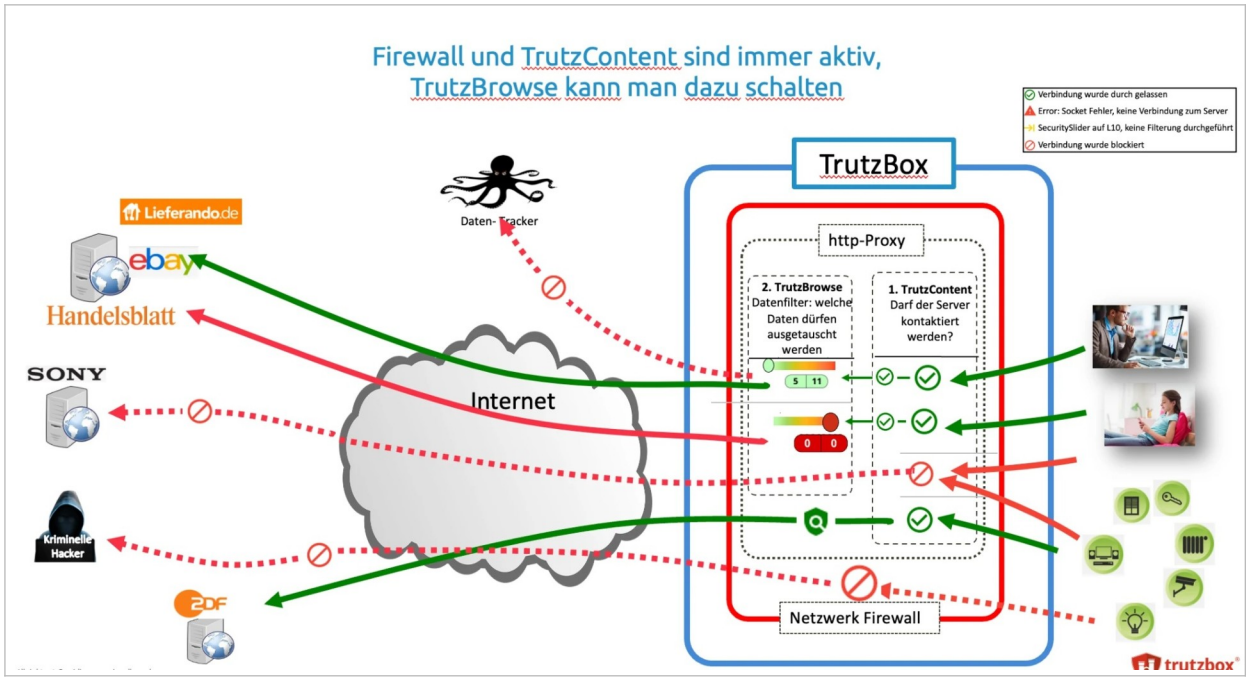


Abbildung 13-1: Firewall und TrutzContent sind immer aktiv; TrutzBrowse lässt sich als zweite Stufe dazuschalten. (© 2026 Comidio GmbH)

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 ein Tracker, ein Werbenetz oder eine Schadcode-Quelle ist. TrutzBrowse setzt danach an: Es entschärft die Verbindungen, die den Webfilter passiert haben, inhaltlich.

	Webfilter (TrutzContent)	**TrutzBrowse**
Zustand	immer aktiv, sobald Verkehr über die Box 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	Tracker-Server, Werbe-Domains, Schadcode-Quellen	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 19). Ist TrutzBrowse für ein Gerät ausgeschaltet, reicht die Box das Zertifikat des besuchten Servers unverändert bis zum Gerät durch, und der Webfilter arbeitet trotzdem weiter.

13.4 Was der Security-Slider praktisch bewirkt

Der Security-Slider kennt neun Positionen, von L1 bis L9, dazu die Sonderstellung L10. 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 Datentracker selbst und zuletzt die Cookies fremder Seiten. Zwei Voreinstellungen sind besonders praxisnah: Datentracker bleiben bis einschließlich L6 blockiert, und Cookies von fremden Seiten bleiben bis einschließlich L7 zurückgehalten. Eine Seite, die ohne Tracker gar nicht funktioniert, lässt sich damit auf L7 benutzen, ohne dass die Tracker 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, sondern nur durch eine ausdrückliche Einstellung. 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

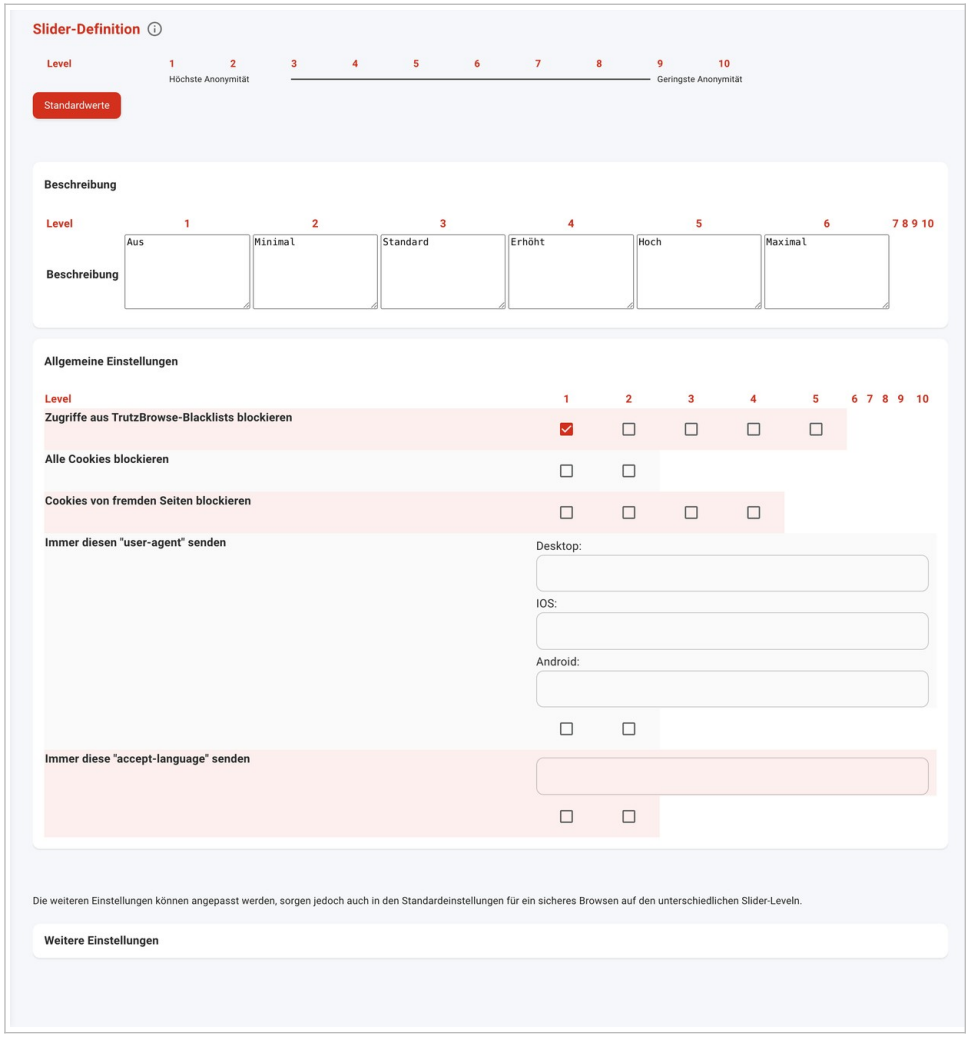


Abbildung 13-2: Die Slider-Definition: zehn Stufen in den Spalten, die einzelnen Filter in den Zeilen. (© 2026 Comidio GmbH)

Wer wissen möchte, was genau auf welcher Stufe passiert, findet das im Admin-Panel: **Slider-Definition** zeigt eine Tabelle mit den zehn Stufen 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**
>
> Stellen Sie den Regler nach Möglichkeit nur für die eine Seite herunter, die zickt, nicht gleich für das ganze Gerät. Die Einstellung bleibt für diesen Server gespeichert, alle anderen Seiten behalten den vollen Schutz.

13.5 Das TrutzBurg-Menü im Browser

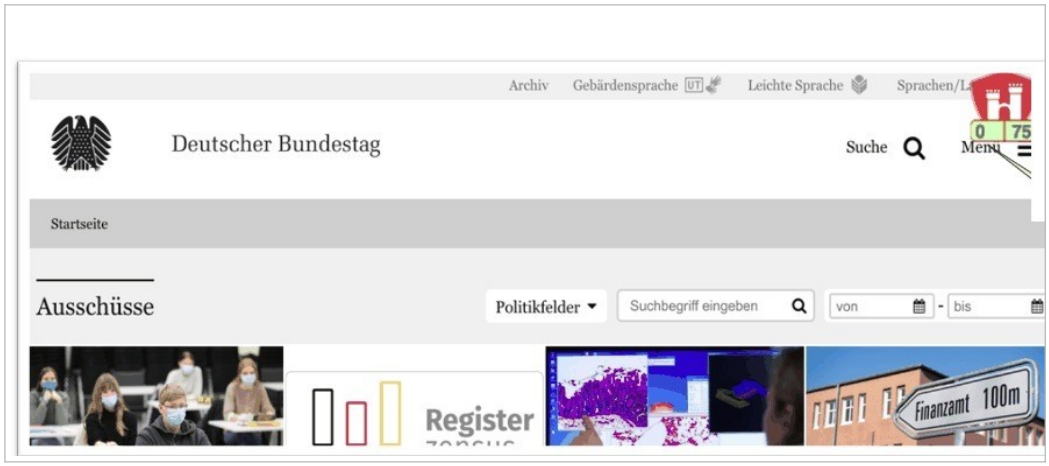


Abbildung 13-3: Die TrutzBurg oben rechts in einer aufgerufenen Seite. Grün heißt geschützt; die Zahlen nennen blockierte und erlaubte Hintergrund-Zugriffe. (© 2026 Comidio GmbH)

Damit Sie den Regler nicht jedes Mal im Admin-Panel suchen müssen, blendet TrutzBrowse ein kleines Bedienelement in die aufgerufene Seite ein: die **TrutzBurg**. 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.

Die TrutzBurg lässt sich je Gerät abschalten, unter **Verwaltung → Geräte** über den Schalter für das TrutzBurg-Symbol; auch die Bildschirmecke, in der sie erscheint, ist dort wählbar. Sinnvoll ist das Abschalten, wenn das Symbol 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 die TrutzBurg nicht einbauen.

Menüpfad: Browseranonymität

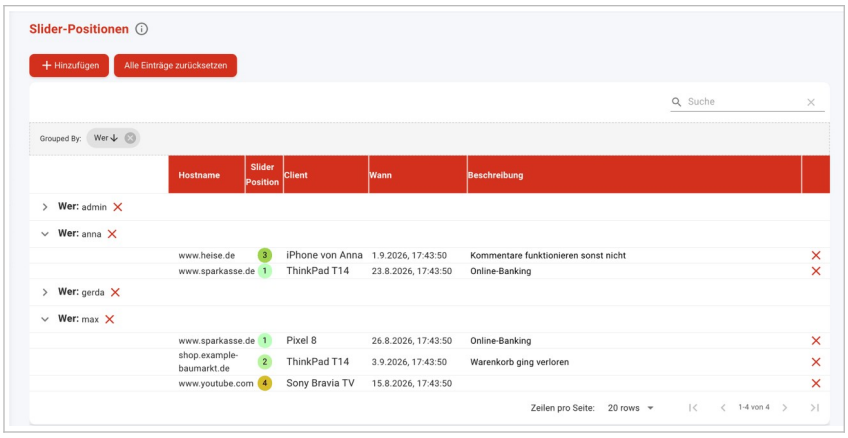


Abbildung 13-4: Slider-Positionen: für welche Server der Regler jemals verstellt wurde, gruppierbar nach Verursacher. (© 2026 Comidio GmbH)

13.6 TrutzBrowse je Gerät einschalten

Abbildung 13-5: TrutzBrowse je Gerät: Schalter und Security-Slider bestimmen den Anonymisierungsgrad. (© 2026 Comidio GmbH)

1. Installieren Sie auf dem Gerät das TrutzBox-Root-Zertifikat (Kapitel 19). 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** und schalten Sie beim gewünschten Gerät **TrutzBrowse** ein.
3. Lassen Sie die Standardposition des Security-Sliders zunächst auf der Werkseinstellung L1. Dort ist der Schutz am höchsten, und bei den allermeisten Seiten bleibt der Regler auch dauerhaft dort. Erhöhen Sie ihn nur, 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.

13.7 Wenn eine Seite nicht richtig funktioniert

Je höher der Slider, 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. Slider für diese Seite eine Stufe herunterstellen und die Seite neu laden, am schnellsten über das TrutzBurg-Menü.
2. Hilft das nicht, weiter herunterstellen. Auf L7 sind Datentracker erlaubt, deren Cookies aber weiterhin blockiert; sehr viele hartnäckige Fälle lösen sich genau hier.
3. Bleibt es dabei, für genau diesen Server eine Ausnahme setzen, also TrutzBrowse für ihn abschalten. Alle übrigen Seiten behalten dabei ihren Schutz.
4. Im Monitor prüfen, ob stattdessen der Webfilter blockiert (Kapitel 9.5); dann ist die Freigabe dort einen Klick entfernt.
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 Box grundsätzlich nicht.

13.8 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 9.3) gibt es zu jedem Server-Kontakt zwei Spalten. Die Spalte **TrutzContent** zeigt als Symbol, wie der Webfilter den Kontakt behandelt hat: durchgelassen, blockiert, ungefiltert oder mit Verbindungsfehler. Die Spalte **TrutzBrowse** erscheint für Geräte mit eingeschaltetem TrutzBrowse und zeigt zweierlei: als Farbe die tatsächlich wirksame Slider-Stufe und als Zahlenpaar, wie viele der unsichtbaren Folgeaufrufe blockiert wurden, etwa „3 | 17" für drei blockierte von siebzehn angeforderten.

Beides ist nicht nur Anzeige, sondern Bedienung. Ein Klick auf das Symbol in der Spalte **TrutzBrowse** 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 Box zurückgehalten hat.

Häufige Fragen zu TrutzBrowse

Wird das Surfen mit TrutzBrowse langsamer?

Ja, merklich. Die Box 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.

14 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 Box 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.

14.1 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". 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 Box getrennt vom internen Netzwerk führt; von dort leitet die Box 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 Box 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 Box 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 4.2.

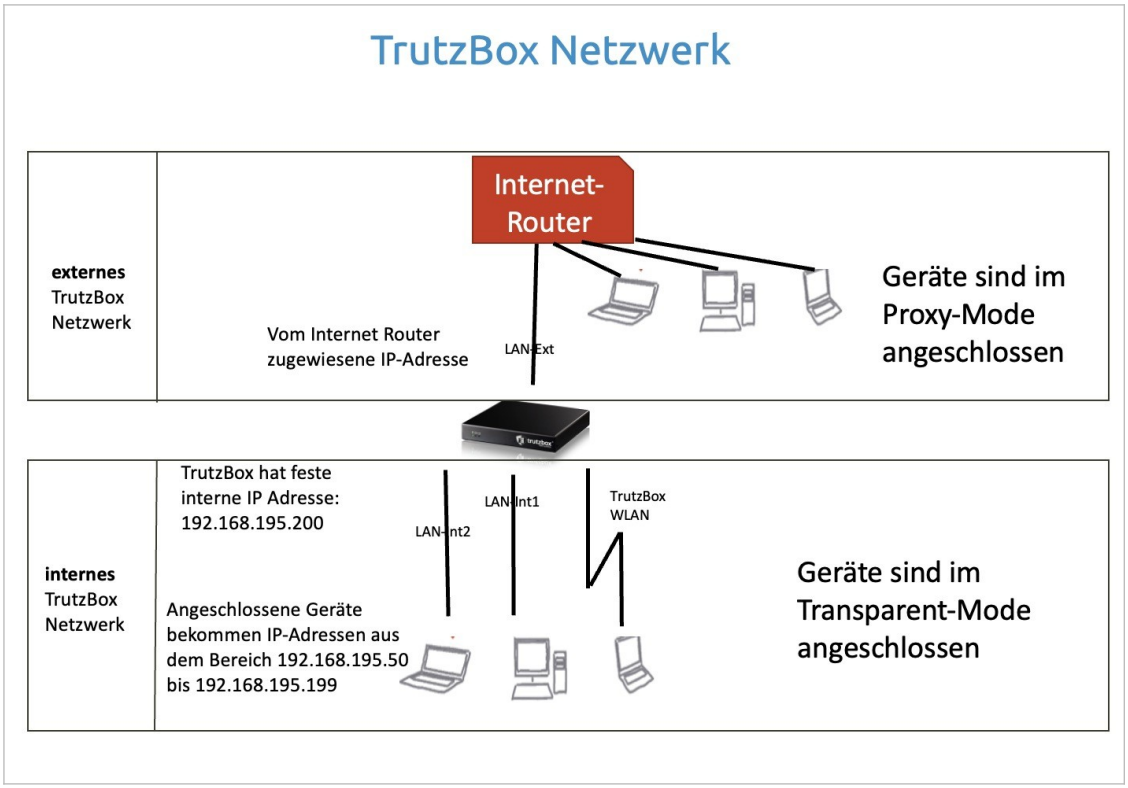


Abbildung 14-1: Außen das Netz des Internet-Routers, innen das geschützte TrutzBox-Netz mit den Adressen ab 192.168.195.50. (© 2026 Comidio GmbH)

Im inneren Netz vergibt die Box 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 Box aber in dieses Netz weitergeleitet, weshalb Sie von unterwegs genau dieselben Dienste erreichen wie zuhause und in der Firma.

Die Status-Seite

Die Seite **Netzwerk → Status** ist in zwei Bereiche gegliedert. Oben steht **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. 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.

14.2 Das WLAN der TrutzBox

Menüpfad: Netzwerk → WLAN

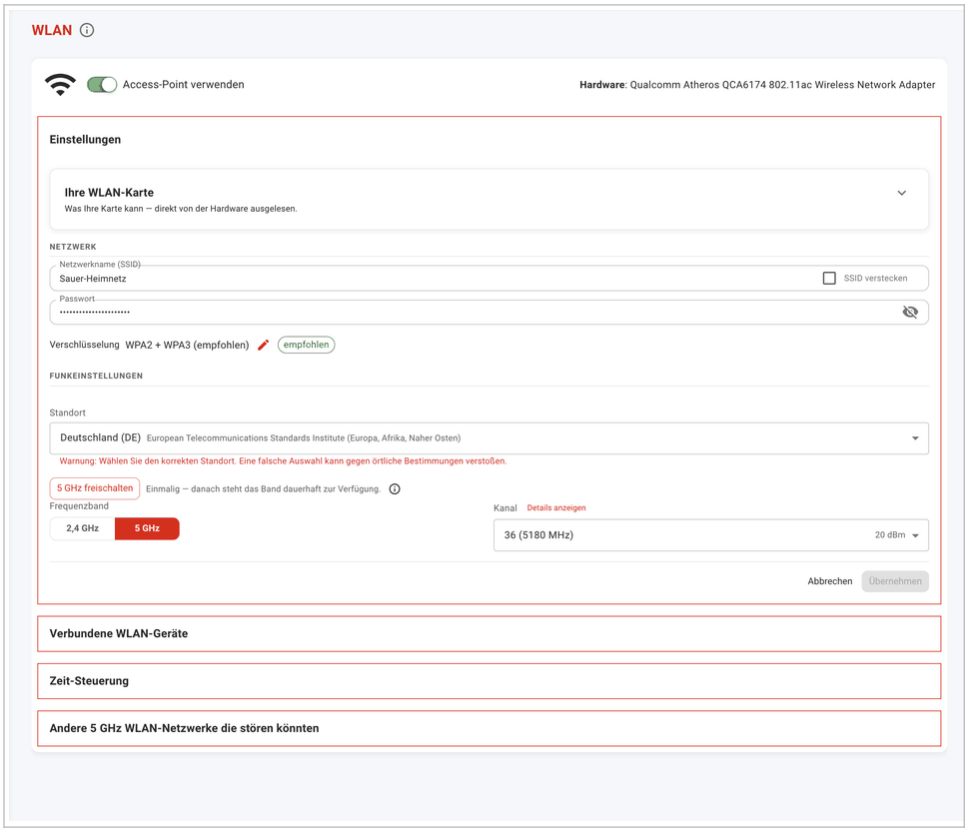


Abbildung 14-2: Das eigene WLAN der Box: Geräte darin sind automatisch geschützt. (© 2026 Comidio GmbH)

Steckt in Ihrer Box 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 **Access-Point verwenden**; Name (SSID) und Passwort legen Sie darunter 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. In vier Schritten steht Ihr eigenes Funknetz:

1. Öffnen Sie **Netzwerk → WLAN** und schalten Sie **Access-Point verwenden** ein.
2. Vergeben Sie unter **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 acht Zeichen. Nehmen Sie ein anderes als das des Router-WLANs und notieren Sie es; jedes Gerät braucht es beim ersten Verbinden einmal.

4. Speichern Sie. Das Funknetz ist nach wenigen Sekunden verfügbar. Verbinden Sie danach Ihre Geräte damit; sie sind dann automatisch komplett geschützt (Kapitel 4.2).

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. Die Box wechselt bei Bedarf selbständig den zugrunde liegenden Funkdienst, ein Eingriff ist dafür nicht nötig.
- **Frequenzband und Kanal:** 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. Beim Ändern startet die Box 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 im Haushalt reduziert, ohne dass jemand abends einen Knopf drücken muss.

Andere WLANs in der Umgebung

Am unteren Rand der Seite zeigt die Box 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 Box selbst sendet; angezeigt werden die Netze des gerade aktiven Frequenzbands. 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 Box überhaupt auf 5 GHz funkt, hängt von der jeweils eingebauten WLAN-Karte ab. Manche Karten geben das Band für den Betrieb als Zugangspunkt frei, andere nicht. Was Ihr Modul kann, steht in der Karte **Ihre WLAN-Karte**; bietet die Seite nur das 2,4-GHz-Band an, gibt die Karte 5 GHz für diesen Betrieb nicht frei.

14.3 DNS-Schutz und verschlüsselte Namensauflösung

Menüpfad: Netzwerk → Netzwerkdienste

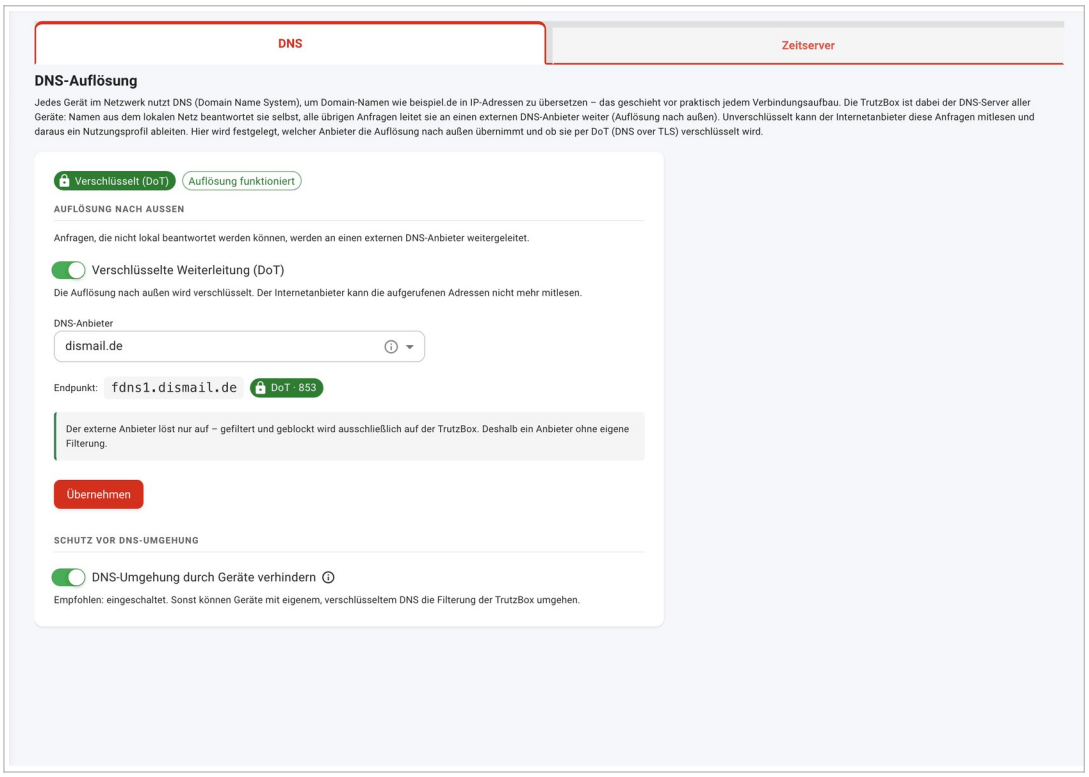


Abbildung 14-3: Verschlüsseltes DNS: Status, Anbieterwahl und der Schutz vor DNS-Umgehung. (© 2026 Comidio GmbH)

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 Box schaltet die Verschlüsselung selbsttätig ein und prüft sie selbst. Lässt der Anschluss sie gerade nicht zu, bleibt es vorübergehend unverschlüsselt, und die Box versucht es alle vier Stunden erneut, etwa bis sie in ein anderes Netz umzieht. 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 Box, 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 Box 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 Box 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

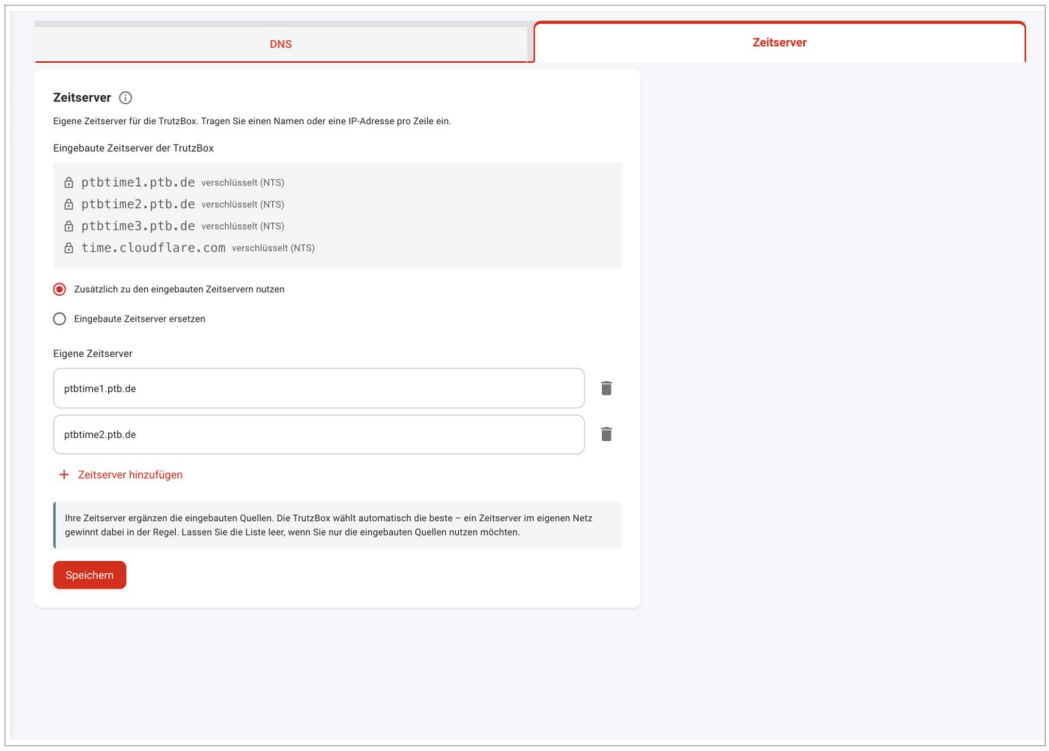


Abbildung 14-4: Der Reiter Zeitserver: eigene Zeitquellen ergänzen die eingebauten, ersetzen sie aber nicht. (© 2026 Comidio GmbH)

Der zweite Reiter derselben Seite verwaltet die Zeitquellen. Korrekte Zeit ist die Grundlage jeder Zertifikatsprüfung, deshalb holt die Box 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 Box wählt automatisch die beste Quelle, wobei ein Server im eigenen Netz in der Regel gewinnt. Bleibt die Liste leer, nutzt die Box nur die eingebauten Quellen.

14.4 Angriffsschutz: Firewall und Wächter

Menüpfad: Netzwerk → Angriffsschutz

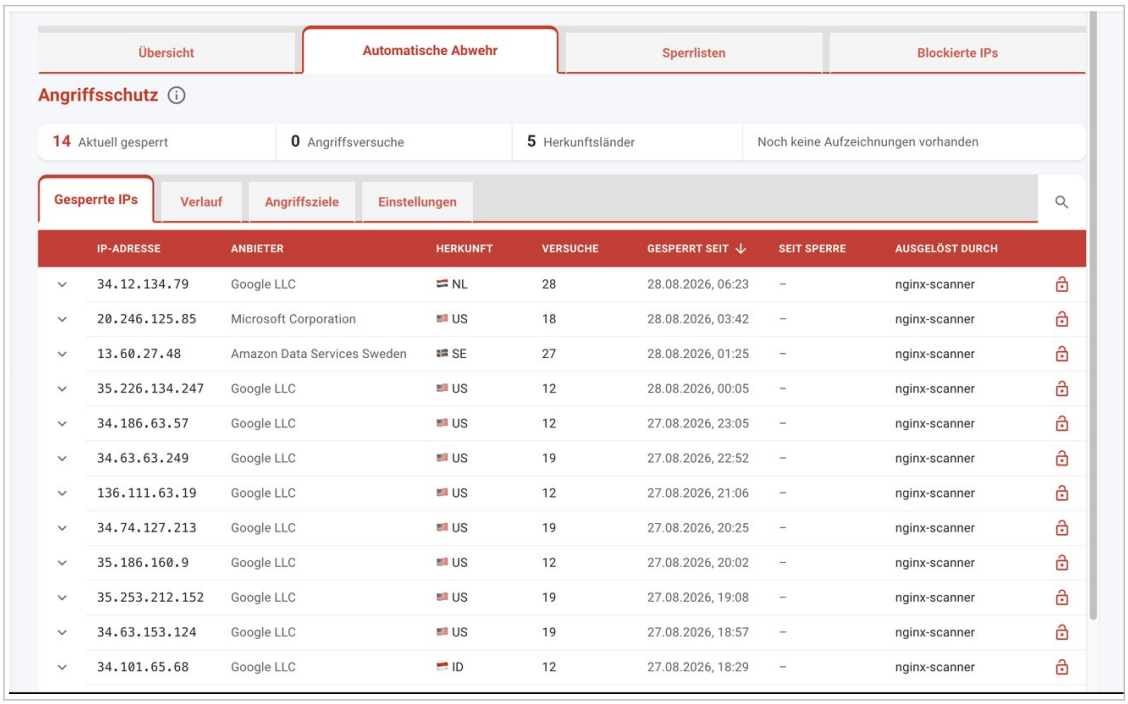


Abbildung 14-5: Die Angriffsschutz-Seite: Kennzahlen, gesperrte Adressen und die Angriffsziele in Alltagssprache. (© 2026 Comidio GmbH)

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 Box. 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 Box 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 Box 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.

In der Spalte, die den Auslöser nennt, erkennen Sie zwei verschiedene Wächter, und beide sind ab Werk unterschiedlich eingestellt. Der Wächter für Scan-Versuche ist der einzige, der zum Internet hin aktiv ist; er greift nach vier Versuchen innerhalb eines Tages und sperrt die Adresse dann dauerhaft. Der Wächter für fehlgeschlagene Anmeldungen am Chat greift nach zehn Versuchen innerhalb von zehn Minuten und sperrt nur für sechs Stunden, denn dahinter steckt meist ein eigenes Gerät mit einem alten Passwort, das sich sonst dauerhaft selbst aussperren würde.

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. 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 Box 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: Früher entfernte ein Freigeben den sperrenden Eintrag, und die nächtliche Aktualisierung trug ihn stillschweigend wieder ein. 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 Box ab. Sonst genügte eine einzige zu weit gefasste Ausnahme, um den Angriffsschutz wirkungslos zu machen.

Reiter Blockierte IPs

Menüpfad: Netzwerk → Angriffsschutz → Blockierte IPs

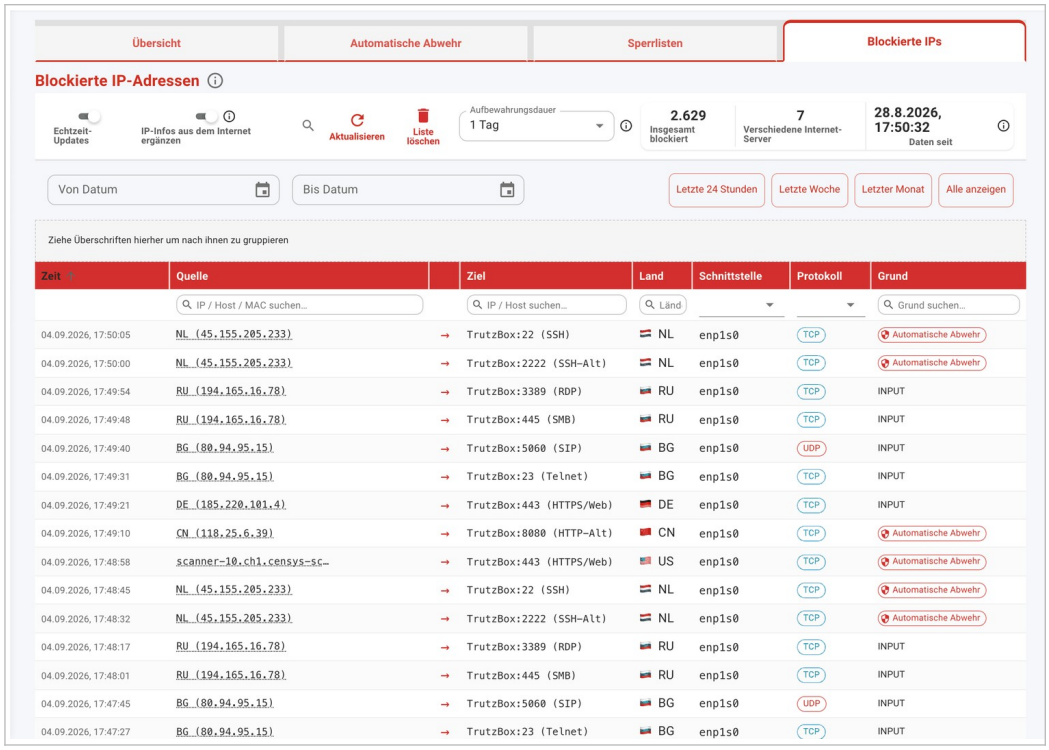


Abbildung 14-6: Der Reiter Blockierte IPs: jeder abgewehrte Verbindungsversuch mit Quelle, Ziel und Land. (© 2026 Comidio GmbH)

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, Sprachassistenten und Spielkonsolen fragen oft einen fest eingebauten Namensdienst im Internet statt den der Box. Der Schutz vor DNS-Umgehung fängt das ab (Abschnitt 14.3).
- Browser und Apps verschlüsseln ihre Namensanfragen zunehmend selbst. Die Box sperrt deshalb die bekannten Anbieter solcher Dienste und erzwingt den eigenen Weg (Abschnitt 14.3).

- 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 Box: 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 9.5).

14.5 Netzwerk-Einstellungen ändern

Änderungen an der Außenseite (feste Adresse statt automatischer, andere DNS-Vorgaben) nehmen Sie unter **Netzwerk → Status** vor. Die Box 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 Box vollautomatisch.

Diese Zurückhaltung hat einen praktischen Grund. Ein falsch gesetzter Wert an dieser Stelle kann die Box 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.

14.6 Webmin: der Experten-Zugang

Hinter **Systemeinstellungen → Webmin** verbirgt sich eine zweite, technische Verwaltungsoberfläche mit direktem Zugriff auf das Betriebssystem der Box, 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.

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 Box 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. Updates kommen ohnehin automatisch (Kapitel 15); ein manueller Eingriff sollte immer mit dem Support abgesprochen sein.

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 Box versucht es alle vier Stunden von selbst erneut.

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.

15 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 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 Box sich versorgt, kann auch einschätzen, warum das sicher ist.

15.1 Die drei Arten von Updates

Menüpfad: Systemeinstellungen → Vertrag und Pakete

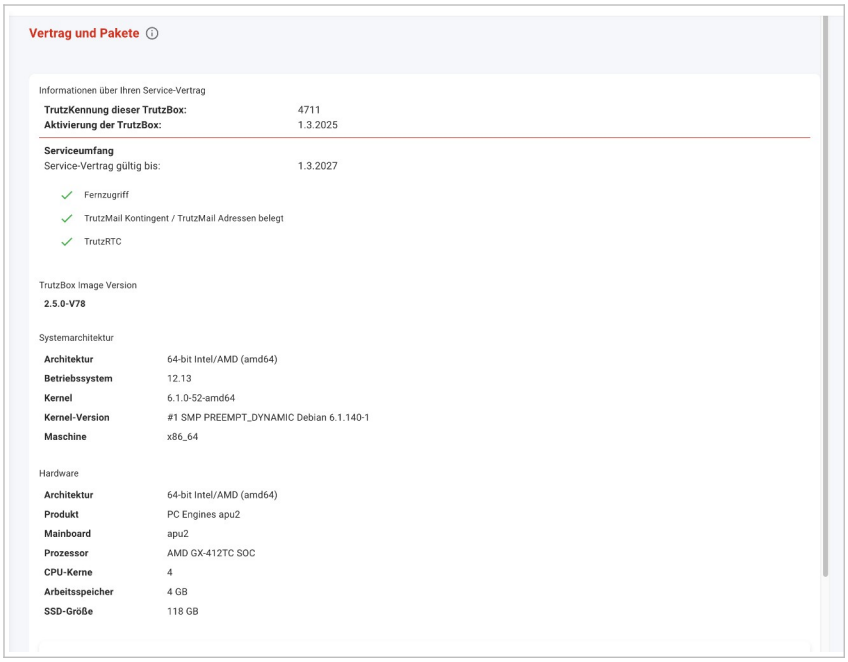


Abbildung 15-1: Die Seite Vertrag und Pakete: Vertragsstand, Abbild-Version, Systemangaben und die Paketliste mit installierter und verfügbarer Fassung. (© 2026 Comidio GmbH)

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 Box werden gegen neuere Fassungen 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 Box Tracker, Werbung, Schadcode-Quellen und bösartige Internet-Adressen erkennt, werden täglich erneuert.
- **Komplette Image-Updates:** Das gesamte Betriebssystem der Box wird neu aufgespielt. Das ist die Ausnahme und kein Teil des täglichen Ablaufs (Abschnitt 15.7).

15.2 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 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 Boxen der Kunden. Das kostet ein paar Tage, verhindert aber, dass eine fremde Änderung Ihre Box aus dem Tritt bringt.

Updates schon während der Einrichtung

Bereits beim Setup prüft die Box zweimal auf Neues: zu Beginn, ob es das Setup-Programm selbst in einer neueren Fassung gibt, und am Ende, ob für die übrigen Pakete neuere Fassungen vorliegen (Kapitel 3.9). Eine frisch eingerichtete Box ist damit auf demselben Stand wie eine, die seit Jahren läuft.

Der nächtliche Ablauf im Betrieb

Im laufenden Betrieb prüft die Box jede Nacht zu fester Uhrzeit selbstständig, ob neue Pakete bereitstehen, und installiert sie gegebenenfalls. Ein manuelles Einspielen gibt es bewusst nicht, und es fehlt Ihnen auch nichts: Es gibt schlicht nichts zu tun.

15.3 Filter- und Sperrlisten-Updates

Die Schutzwirkung der Box lebt von aktuellen Listen, denn Tracker- und Werbeserver wechseln ihre Adressen ständig. Vier Dinge werden hier gepflegt:

- **Filterlisten für Webfilter und TrutzBrowse:** Comidio pflegt weit über hundert Listen zur Erkennung von Tracker- und Werbeservern, Schadcode-Quellen und thematischen Sperrkategorien. Sie werden täglich aktualisiert und an alle Boxen verteilt (Kapitel 8.3).
- **Sperrliste kompromittierter TrutzMail-Adressen:** Wird eine TrutzMail-Adresse kompromittiert, etwa weil eine Box gestohlen wurde, führt Comidio sie zentral auf einer Sperrliste. Jede Box 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.
- **IP-Sperrlisten:** Diese werden nicht zentral verteilt, sondern liegen bei Ihnen (Kapitel 14.4). Ergänzt werden sie automatisch durch den Angriffsschutz, der auffällige Internet-Adressen selbst einträgt.

15.4 Warum diese Updates sicher sind

Ein Update-Weg ist ein empfindlicher Punkt: Wer ihn übernimmt, könnte eigene Software auf die Box 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 Box prüft den Server, auch der Server prüft Ihre Box. Ein fremder Server kann sich damit nicht als Comidio ausgeben.

Dazu kommt eine schlichte, aber wirksame Vorsichtsmaßnahme: Die Box 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 Updates sind ab Werk eingeschaltet, die Prüfung läuft jede Nacht zu fester Uhrzeit, 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.

15.5 Voraussetzung: ein gültiger TrutzServices-Vertrag

Die hier beschriebenen Update-Arten sind Leistungen des TrutzServices-Vertrags. Solange er läuft, erhält Ihre Box 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 Box hört deswegen nicht auf zu arbeiten: Sie filtert mit dem Stand weiter, den sie hat. Nur nutzt sich dieser Stand ab, weil neue Tracker- und Angriffsserver 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 Servicevertrag. Wenden Sie sich dafür an den Support. Comidio empfiehlt, den Vertrag durchgehend zu verlängern.

15.6 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:** die Karte **Filterlisten** 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 orange und nennt die verfügbare Fassung und den Zeitpunkt, seit dem die Box 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 Box auf, einschließlich der zugrunde liegenden Debian-Pakete. Das macht die Zusammensetzung der Box nachprüfbar, auch für eine externe Prüfung.
- **Verwaltung, Filterlisten:** an jeder einzelnen Liste steht dort das Datum der letzten Aktualisierung.

15.7 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 Box 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 16.4. Der zweite ist der USB-Stick, den der folgende Abschnitt komplett beschreibt. Für beide gilt: Legen Sie vorher eine Sicherung an, sofern die Box das noch hergibt, sonst sind Postfächer und Schlüssel verloren (Kapitel 16).

Das System per USB-Stick neu aufspielen

Dieser Weg funktioniert auch dann noch, wenn die Box gar nicht mehr startet oder das Speichermedium getauscht wurde, denn er braucht weder die Oberfläche noch ein lauffähiges System auf der Box. Sie erstellen an einem PC einen Start-Stick mit dem kompletten TrutzBox-System und lassen die Box davon booten; der Stick schreibt das System dann selbsttätig auf das interne Speichermedium. Comidio nennt diesen Stick auch „Tank-Stick", weil die Box 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.

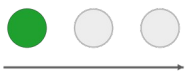
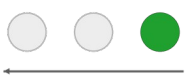
Nehmen Sie dafür am besten einen gewöhnlichen USB-Speicherstick, gern auch einen älteren mit USB 2.0. Geräte, die als **USB-SSD** verkauft werden, funktionieren erst mit den Image-Dateien ab V79. Ältere Fassungen erkennen sie nicht: Die Box startet zwar vom Stick, bleibt dann aber beim Suchen des Datenträgers stehen, sichtbar an LED 1 dauerhaft an und LED 2 blinkend. Ein größerer Stick schadet nicht, bringt aber auch keinen Vorteil, weil nur die ersten 16 GB genutzt werden.

1. Laden Sie die aktuelle Image-Datei auf Ihren PC herunter: update.trutzbox.org/download/x86_64/tank-stick/tank-stick-trutzbox-2.5.0-V79.amd.img.gz. Die Datei ist rund 1,6 GB groß. Der Dateiname trägt Betriebssystem- und Abbild-Version,

hier 2.5.0 und V79; erscheint eine neuere Fassung, nennt Ihnen der Support den aktuellen Namen.

2. Entpacken müssen Sie nichts: Das Schreibprogramm im nächsten Schritt liest die gepackte Datei unmittelbar. Wer sichergehen will, dass der Download unversehrt ist, lädt die gleichnamige Datei mit der Endung `.sha256` dazu und vergleicht die Prüfsumme.
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 Box 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 Box piept dreimal; etwa 30 Sekunden später schaltet sie sich selbst ab.
8. Trennen Sie die Box vom Strom, ziehen Sie den Stick ab und schließen Sie den Strom wieder an. Die Box startet nun mit dem frischen System und meldet sich mit dem Setup (Kapitel 3).
9. Durchlaufen Sie das Setup mit Ihrer TrutzLegitimation und spielen Sie im Schritt „Aktualisierung des Setups" Ihre Sicherung ein (Kapitel 16.3).

Was die LEDs während des Vorgangs bedeuten:

Die drei Leuchtdioden	Was gerade passiert
	Die Box 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 Boxen deutlich länger.
	Lauflicht von rechts nach links: Das Geschriebene wird geprüft, noch einmal etwa 5 bis 10 Minuten.
	Fertig, dazu drei Pieptöne. Die Box schaltet sich in etwa 30 Sekunden selbst ab.

Die drei Leuchtdioden	Was gerade passiert
	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 hat eine eingebaute Sicherung:** Er schreibt ausschließlich auf TrutzBox-Hardware und prüft das Geschriebene anschließend anhand einer Prüfsumme. An einem gewöhnlichen PC richtet er nichts an.
- **Denken Sie an das Root-Zertifikat:** Nach dem Neuaufspielen erzeugt die Box 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 19.6).
- **Wenn die Box nicht vom Stick startet:** Das kommt praktisch nicht vor, denn der Stick hat beim Starten Vorrang vor dem internen Speichermedium. Startet die Box 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.

15.8 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 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 Boxen aus. Bei besonders kritischen Fällen geschieht das auch außerhalb des Tagesrhythmus.

Häufige Fragen zu Updates

Startet die Box nach einem Update neu?

Im Regelfall nicht. Die Updates werden im laufenden Betrieb eingespielt; einzelne Dienste starten dabei kurz neu, was Sie im Alltag nicht bemerken.

Kann ich ein Update selbst anstoßen oder verschieben?

Nein, und das ist Absicht. Ein einheitlicher, automatischer Ablauf lässt keine Box mit veralteter Software zurück. Sollte im Einzelfall etwas nachzuhelfen sein, leitet der Support Sie an.

Nach einem Update verhält sich etwas anders als vorher. Was tun?

Erst im Forum nachsehen, ob die Änderung dort beschrieben ist, dann den Betriebszustand prüfen. Bleibt es unklar, hilft der Support weiter (Kapitel 17.13 und Kapitel 18).

16 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 Box 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.

16.1 Was in der Sicherung steckt

Menüpfad: Systemeinstellungen → Sichern und Wiederherstellen

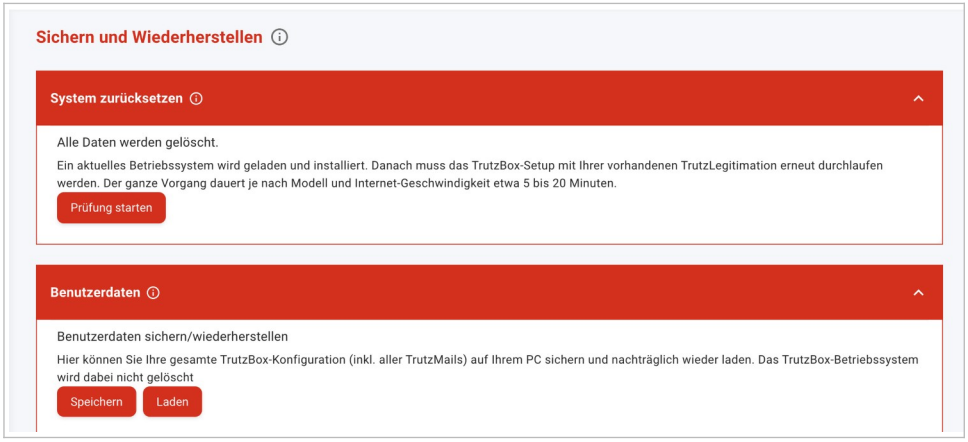


Abbildung 16-1: Sichern, Wiederherstellen und Zurücksetzen an einer Stelle. (© 2026 Comidio GmbH)

Die Sicherung fasst den kompletten Zustand Ihrer Box 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 Box,
- die Filtergruppen und Sicherheitsstufen,
- die Sperrlisten,
- sämtliche TrutzMail-Konten samt ihrer persönlichen Schlüssel und der zugehörigen versteckten Adressen im Tor-Netzwerk,
- die TrutzChat-Daten mit Gesprächsverläufen und Gruppen.

Nicht enthalten ist das Betriebssystem der Box. 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 Box selbst nicht mehr sauber läuft.

> **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.

16.2 Eine Sicherung anlegen

1. Öffnen Sie **Systemeinstellungen → Sichern und Wiederherstellen**.
2. Klicken Sie auf **Speichern**, vergeben Sie eine Passphrase und laden Sie die Datei auf Ihren PC herunter.
3. Bewahren Sie die Datei außerhalb der Box 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 Box 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.

16.3 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 Box läuft und Sie nur auf einen früheren Stand zurück möchten.
- **Während des Setups:** im Schritt „Aktualisierung des Setups" über die Schaltfläche **Backup laden** (Kapitel 3.5). Genau dieser Weg ist gedacht, wenn Sie eine Box ersetzen oder nach einem Zurücksetzen wieder aufbauen: Die Box übernimmt den gesicherten Zustand, und **Weiter** führt anschließend direkt ins Admin-Panel. Das Setup ist damit beendet, die übrigen Schritte entfallen, weil die Sicherung sie bereits mitbringt.

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 Box 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.

Denken Sie danach an die Geräte: Nach einem Neuaufbau kann sich das Root-Zertifikat der Box geändert haben. Ist das der Fall, löschen Sie auf allen Geräten das alte Zertifikat und importieren das neue (Kapitel 19), sonst zeigen die Browser Warnungen an.

16.4 System zurücksetzen (Werksreset)

Das Zurücksetzen löscht alle Daten auf der Box 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 3); der Vorgang dauert je nach Modell und Internet-Geschwindigkeit etwa 5 bis 25 Minuten.

Der Ablauf Schritt für Schritt

1. Legen Sie zuerst eine vollständige Sicherung an und laden Sie sie auf Ihren PC (Abschnitt 16.2). 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 Box prüft nun sieben Voraussetzungen der Reihe nach: die Internetverbindung, das Betriebssystem-Abbild 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 Abbild überhaupt auf den Systembereich Ihrer Box 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-Abbild. Sie nennt, was der Update-Server für genau Ihre Box bereithält: Version und Bau-Nummer, die entpackte Größe und die enthaltenen Betriebssystem-Kerne, etwa *Gefunden: TrutzBox 2.5.0 Build V78.amd, 6,0 GiB*. So sehen Sie vor dem Auslösen, auf welchen Stand die Box 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 Box alle fünf Sekunden unter ihrem Namen und unter ihren bisherigen Adressen und springt von selbst in den Einrichtungsassistenten, sobald sie wieder antwortet. Meldet sie sich binnen 45 Minuten nicht, nennt die Seite stattdessen die Adresse zum Eintippen und bietet eine erneute Suche an. Trennen Sie die Box in dieser Zeit keinesfalls vom Strom.
6. Am Ende meldet sich die Box von selbst wieder zurück, und zwar unter ihrem Auslieferungsnamen `trutzbox`. Hatten Sie ihr einen anderen Netzwerknamen gegeben, ist der damit weg. Der Einrichtungsassistent liegt unter `http://trutzbox/setup/`, an einer Fritzbox auch unter `http://trutzbox.fritz.box/setup/`. Durchlaufen Sie dann das Setup mit Ihrer TrutzLegitimation und spielen Sie im Schritt „Aktualisierung des Setups" Ihre Sicherung ein.

Ein Sonderfall betrifft nur den Sprung am Ende: Haben Sie die Verwaltung über eine `https`-Adresse geöffnet, wechselt die Seite nicht von selbst in den Einrichtungsassistenten. Ein Browser darf aus einer verschlüsselten Seite heraus keine unverschlüsselte Adresse abfragen. Rufen Sie den Assistenten 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 Box lässt sich auch dann zurücksetzen, wenn Sie sich nicht mehr anmelden können.

- **Doppelklick auf die Taste am Gehäuse:** Zwei Klicks innerhalb von zwei Sekunden lösen den Vorgang aus; ein einzelner Druck bewirkt nichts. Gemeint ist die Taste an der Gerätefront; sie schaltet die Box nicht hart ab. Die Box führt dieselbe Prüfung durch wie in der Oberfläche. Fällt sie durch, etwa weil kein Netzwerk anliegt, geschieht nichts, und die drei LEDs blitzen fünfmal gemeinsam auf.
- **Startmenü der Box:** Beim Einschalten zeigt die Box 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 währenddessen anzeigen

Sobald die Box 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. 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 Box wartet auf Netzwerk und Namensauflösung und holt die Beschreibungsdatei vom Update-Server. Das dauert nur wenige Sekunden.
	Das Abbild wird geladen, auf die Systempartition geschrieben und die Prüfsumme kontrolliert. Das dauert etwa vier Minuten.
	Nacharbeit: Der Startbereich wird erneuert und das Datenverzeichnis auf den Werkszustand gebracht. Das dauert knapp eine Minute.
	Alles ist geschrieben. Die Anzeige bleibt zehn Sekunden stehen, dann startet die Box 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	Abbild ließ sich nicht laden

Die drei Leuchtdioden	Takt	Fehler	Mögliche Ursache
● ○ ●	mittel	Prüfsumme	Abbild 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: Box kurz vom Strom trennen und den Vorgang wiederholen. Bleibt es beim selben Muster, gehört es in die Meldung an den Support (Kapitel 18).

Ältere Boxen zeigen im Wartungssystem noch keine Anzeige. Dort bleiben die LEDs während des Vorgangs einfach so, wie sie beim Neustart waren; die Box arbeitet trotzdem.

Nach dem Neustart in das frische System gilt wieder die gewohnte Anzeige: Die drei LEDs gehen aus, kurz darauf leuchtet die linke dauerhaft, dann werden alle drei für einen Moment dunkel, weil nun das Betriebssystem die Leuchtdioden übernimmt, danach leuchtet die linke wieder, bis das System steht. Es folgt langsames Blinken und schließlich das schnelle Herzschlag-Blinken, sobald die Bedienoberfläche antwortet. Das kurze Dunkel dazwischen ist kein Fehler.

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 Box wird vollständig mit dem frischen Abbild 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 Box heißt wieder `trutzbox`, und das Admin-Passwort vergeben Sie im Einrichtungsassistenten neu. 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 18.8) oder löschen es mit dem eingebauten Löschbefehl des Laufwerks und spielen danach ein frisches Abbild auf (Kapitel 15.7).

Ihre TrutzMail-Adressen bleiben Ihnen erhalten

Beim Zurücksetzen werden auch alle Benutzer und deren TrutzMail-Adressen auf der Box gelöscht. Freigegeben werden die Adressen dadurch aber nicht: Die zentrale Verwaltung bei Comidio lässt eine erneute Einrichtung nur zu, wenn sie von einer Box 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 7).

16.5 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 Box nicht wieder in Betrieb nehmen.
- 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 Box lädt das Betriebssystem aus dem Internet nach.

Nachher

- Setup mit der TrutzLegitimation durchlaufen und die Sicherung im Schritt „Aktualisierung des Setups" eingespielt.
- Nur wenn Sie ohne anschließende Wiederherstellung neu aufgesetzt haben: auf allen Geräten das alte Root-Zertifikat der Box gelöscht und das neue importiert (Kapitel 19). 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 7).
- Eine Testmail an die eigene Adresse geschickt und den Chat kurz geöffnet.
- Sofort eine frische Sicherung des neuen Zustands angelegt.

16.6 Die TrutzBox weitergeben

Wird die Box 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 16.2). Sie enthält Ihre TrutzMail-Konten mit ihren Schlüsseln. Ohne sie sind diese Schlüssel nach dem Zurücksetzen weg, auch Comidio hat keine Kopie.
- Dann die Box auf den Werkszustand zurücksetzen (Abschnitt 16.4). 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 Box 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 Box 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 Einrichtungsassistenten nicht durch.
- Auf Ihren eigenen Geräten das Root-Zertifikat dieser Box entfernen, in Firefox und Thunderbird zusätzlich in deren eigenem Zertifikatsspeicher (Kapitel 19). Ebenso die VPN-Profile und die Mail-Konten löschen, die auf diese Box zeigen.
- Am Internet-Router die Freigaben zurücknehmen, die Sie für diese Box 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 Box 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 Box wieder anlegen (Kapitel 7). 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 Box, 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 Box 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 16.3). Auf einer Box 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 16.1. Deshalb kann die Datei je nach Postfachgröße auch mehrere hundert Megabyte groß werden.

17 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 wer 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 Box selbst. Ist sie gelb oder rot, nennt die betroffene Karte Ursache und Empfehlung im Klartext.

Die Ampel kennt vier Zustände: grün für „in Ordnung", gelb für „Beachtung ratsam", rot für einen konkreten Fehler und neutral für Funktionen, die Sie selbst abgeschaltet haben. Eine bewusst abgeschaltete Funktion zieht die Ampel also nie auf Gelb oder Rot.

17.1 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 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 Box reagiert überhaupt nicht mehr	17.12
Nach einem Update funktioniert etwas nicht mehr	17.13
Der Speicherplatz wird knapp	17.14
Die Box soll neu gestartet oder zurückgesetzt werden	17.15
Das Passwort für das Admin-Panel ist nicht mehr bekannt	17.16
Sie ziehen um oder bekommen einen neuen Internet-Router	17.17

17.2 … 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 Box, 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 5.3).
5. Betrifft es nur ein Gerät, schauen Sie im Monitor nach, ob dessen Verbindungen blockiert werden (Kapitel 9). 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 4.2), hat es die Box gar nicht erreicht, und Sie sind bei Abschnitt 17.7 richtig.
7. Hilft nichts: die Box neu starten, am besten über den entsprechenden Menüpunkt in der Verwaltungsoberfläche. Nur wenn diese nicht mehr erreichbar ist, trennen Sie die Box vom Strom, warten zehn Sekunden und schließen sie wieder an.

17.3 … eine Seite blockiert wird

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, die Werbung von denselben Servern beziehen wie die Tracker.

Zeigt der Browser die Sperrseite der TrutzBox, nennt sie Ihnen bereits den Grund, also Filterliste oder Regel. Freigeben geht am schnellsten über den Monitor: Eintrag suchen, Details öffnen, Domain erlauben. Die Adresse landet in der Standard-TrutzContent-WL und ist sofort wieder erreichbar (Kapitel 8.3).

Erscheint keine Sperrseite, sondern nur ein allgemeiner Verbindungsfehler, ist das bei verschlüsselten Seiten ohne TrutzBrowse der Normalfall: Dort kann die Box keine eigene Seite einblenden (Kapitel 8.6). Prüfen Sie im Monitor, ob der Webfilter oder TrutzBrowse blockiert hat, und stellen Sie bei TrutzBrowse den Slider für diese Seite niedriger (Kapitel 13.7).

1. Öffnen Sie den Monitor und suchen Sie den betroffenen Server im gewünschten Zeitraum.

2. Schauen Sie in die Spalte **TrutzContent**: Ein Symbol zeigt, ob der Webfilter durchgelassen oder blockiert hat. Ein Klick darauf gibt die Verbindung für die Zukunft frei; ein Dialog erlaubt, die Freigabe auf einen Teil der Domain einzugrenzen.
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 8.2).

17.4 … 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, geht es um die Leitung, nicht um die Box.
2. Öffnen Sie den Monitor in der Darstellung **Datendurchsatz**. Sie sehen dort je Gerät die übertragene Datenmenge und die aktuelle Bandbreite. Meist findet sich hier der Vielfraß, etwa ein laufendes Backup oder ein Videodienst in hoher Qualität.
3. 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.
4. 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.
5. Prüfen Sie auf der Betriebszustand-Seite die Karte **Arbeitsspeicher**. Ist die Box dauerhaft sehr voll, 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 13.7 beschreibt das Vorgehen.

17.5 … der Browser eine Zertifikatswarnung zeigt

Damit die Box 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 Box nicht erneuert, meldet der Browser eine Warnung. Dieselbe Warnung erscheint, wenn ein Mail-Programm verschlüsselt auf den Mail-Server der Box zugreift, ohne das Zertifikat zu kennen.

1. Prüfen Sie unter **Verwaltung → Geräte**, ob für dieses Gerät **TrutzBrowse** eingeschaltet ist. Ist es aus und die Warnung erscheint trotzdem, hat sie mit der Box nichts zu tun; dann stimmt am Server selbst etwas nicht, und Sie sollten die Seite nicht öffnen.
2. Installieren Sie das Root-Zertifikat auf dem Gerät (Kapitel 19). Die Datei laden Sie unter **Verwaltung → Allgemeine Einstellungen** über **Root Zertifikat herunterladen** herunter.

3. Wurde die Box 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.

17.6 … eine E-Mail nicht ankommt

TrutzMails gehen nicht über einen Mail-Server im Internet, sondern direkt von Box zu Box. Das macht sie sicher, hat aber eine Folge: Ist die Box des Empfängers gerade aus, kann niemand die Mail zwischenlagern. Ihre Box 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 10.7, insbesondere ob die Empfänger-Box eingeschaltet ist; die eigene Box 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 Box 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 Boxen ihre Schlüssel abgeglichen haben (Kapitel 10.6).
5. Bei sehr großen Mails hilft ein Neustart der Box. Anhänge werden für den Versand in Textzeichen umgewandelt und dabei deutlich größer; ist der Arbeitsspeicher knapp, scheitert der Versand. Der Neustart räumt den Speicher.

17.7 … ein Gerät nicht auftaucht

Die Geräteliste zeigt, was über die Box läuft. Fehlt ein Gerät dort, läuft sein Verkehr an der Box 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 4.2). Eine andere Adresse bedeutet: Das Gerät hat sie nicht von der Box 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 Box (Kapitel 4.2).
4. Bleibt es dabei, schalten Sie das WLAN des Internet-Routers ab. Dann gibt es keinen Weg mehr an der Box 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 Box selbsttätig die Einträge, zu denen weder eine MAC-Adresse noch ein Hostname vorliegt. Alles andere bleibt erhalten.

17.8 … 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.

17.9 … Gäste in der Videokonferenz eine Zertifikatswarnung sehen

Ihre Gäste kommen über einen öffentlichen Namen auf Ihre Box. Damit deren Browser diesen Namen ohne Warnung akzeptiert, braucht die Box 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**, Karteikarte **Videokonferenz**, und prüfen Sie Schritt 1: TrutzDynDNS muss eingeschaltet und das kostenlose LetsEncrypt-Zertifikat aktiviert sein (Kapitel 11.2).
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 Box. Für die interne Adresse gibt es kein öffentlich anerkanntes Zertifikat, und die Warnung wäre die logische Folge.

17.10 … ein Chat-Kontakt dauerhaft als nicht erreichbar erscheint

Der farbige Punkt neben einem Kontakt zeigt dessen Anwesenheit. Er erscheint erst, wenn die Gegenseite die Kontaktaufnahme bestätigt hat. Und weil Nachrichten zwischen TrutzBoxen direkt von Box zu Box laufen, bedeutet ein grauer Punkt schlicht: Auf der anderen Seite ist gerade niemand angemeldet, oder deren Box läuft nicht.

1. Prüfen Sie, ob die Gegenseite die Kontaktaufnahme bestätigt hat. Ohne Bestätigung sehen beide Seiten die Anwesenheit des anderen nicht.
2. Prüfen Sie die Schreibweise der TrutzMail-Adresse des Kontakts. Ein Tippfehler erzeugt einen Kontakt, den es nicht gibt.
3. Lassen Sie auf der Karteikarte **TrutzChat** den **Chat-Selbsttest** laufen. Er prüft in etwa zehn Sekunden den Nachrichtenweg auf Ihrer eigenen Box 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 Box 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 Box eingeschaltet ist. Nachrichten gehen trotzdem nicht verloren, sie werden zugestellt, sobald die Gegenseite wieder da ist.
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 11.5). Von unterwegs verbinden Sie sich zuerst über den VPN-Zugang.

17.11 … 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 der Box. Im internen Netz der Box ist das immer `https://192.168.195.200`; von einem PC im Heimnetz am Router aus die Adresse, die der Router der Box gegeben hat (Geräteübersicht des Routers, Kapitel 3.2).
2. Prüfen Sie, ob Ihr PC überhaupt mit der Box verbunden ist: entweder im internen Netz der Box mit einer Adresse von ihr (192.168.195.50 bis 199) oder im Heimnetz am selben Router wie die Box.
3. Warten Sie nach einem Neustart zwei bis drei Minuten; die Dienste brauchen etwas Anlauf. Nach einem Update oder beim allerersten Start kann es auch länger dauern.
4. 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.

5. Als Notzugang für Fortgeschrittene läuft Webmin eigenständig unter `http://trutzbox:10000` weiter (Kapitel 14.6), am besten nur nach Anleitung des Supports.

17.12 … die Box überhaupt nicht mehr reagiert

Die linke LED an der Gerätefront sagt Ihnen zuerst, woran Sie sind. Dauerleuchten heißt: Die Box startet gerade. Langsames, gleichmäßiges Blinken heißt: Das Betriebssystem läuft, die Oberfläche startet noch. Schnelles Blinken im Herzschlag-Rhythmus heißt: Alles ist bereit. Dunkel wird die LED im Betrieb nie. Ist sie dunkel, fehlt Strom.

1. Prüfen Sie Netzteil und Steckdose, wenn keine LED an ist.
2. Steht die LED auf Dauerleuchten oder langsamem Blinken, geben Sie der Box fünf Minuten. Nach 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.
4. Starten Sie die Box neu. Der übliche Weg dafür ist der entsprechende Menüpunkt in der Verwaltungsoberfläche. Antwortet diese nicht mehr, trennen Sie die Box 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 18). Kommen Sie noch in Webmin hinein, können Sie den Systemstatus für die Analyse dort selbst herunterladen; der Support sagt Ihnen, wie.

> **Warum die Box lieber etwas abschaltet als stehenzubleiben**
>
> Die Box 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 Box 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.

17.13 … nach einem Update etwas nicht mehr funktioniert

Updates werden vor der Auslieferung getestet, auch die Pakete des Betriebssystems (Kapitel 15.2). Trotzdem kann eine Neuerung eine Einstellung anders auslegen als zuvor. Meist geht es dann nicht um einen Fehler, sondern um eine bewusste Änderung, die im Forum beschrieben ist.

1. Öffnen Sie den Betriebszustand. Eine gelbe oder rote Karte nennt Ursache und Empfehlung im Klartext, oft mit einem konkreten Handlungsvorschlag.
2. Sehen Sie im TrutzBox-Forum unter forum.trutzbox.de im Bereich „TrutzBox-Updates" nach, was das Update geändert hat.

3. Starten Sie die Box einmal neu. Manche Dienste übernehmen eine Änderung erst beim Start vollständig.
4. Betrifft es Chat oder Videokonferenz, schalten Sie TrutzRTC einmal aus und wieder ein.
5. Prüfen Sie unter **Systemeinstellungen → Vertrag und Pakete**, ob installierte und verfügbare Version übereinstimmen. Weichen sie ab, ist das Update vielleicht gar nicht vollständig angekommen.
6. Bleibt es unklar, senden Sie den Support-Bericht an Comidio und beschreiben Sie, was seit dem Update anders ist (Kapitel 18).

17.14 … der Speicherplatz knapp wird

Die Box 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 Box 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 der Karteikarte **TrutzChat** den Platzbedarf der Gesprächsverläufe. Dort lässt sich die Aufbewahrungsdauer verkürzen, und **Alle Verläufe löschen** räumt gesammelt ab. Anhänge entfernt die Box ohnehin nach 30 Tagen von selbst.
4. Verwechseln Sie Speicherplatz nicht mit Arbeitsspeicher. Die Karte **Arbeitsspeicher** betrifft den flüchtigen Speicher; 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 16) und melden Sie sich beim Support.

17.15 … 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 Box 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.

Beides 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 Box 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 5.3).

Das vollständige Zurücksetzen auf den Werkszustand beschreibt Kapitel 16.4. Denken Sie unbedingt vorher an eine Sicherung: Ohne sie sind Postfächer und Schlüssel verloren. Denken Sie

außerdem an das Root-Zertifikat: Bauen Sie die Box ohne Wiederherstellung neu auf, erzeugt sie ein neues, das auf allen Geräten das alte ersetzen muss (Kapitel 19). 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.

17.16 … 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 Box 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 Box die Anmeldung absichtlich aus und nennt Ihnen die Wartezeit; danach geht es wieder.
3. Führt das nicht zum Ziel, bleibt nur das Zurücksetzen auf den Werkszustand nach Kapitel 16.4. Dabei gehen alle Daten auf der Box verloren. Ein Doppelklick auf die Taste am Gehäuse löst den Vorgang auch ohne Anmeldung aus; wo diese Taste sitzt und was die LEDs dabei anzeigen, steht in Kapitel 16.4.
4. Richten Sie die Box danach mit Ihrer TrutzLegitimation neu ein und vergeben Sie ein neues Admin-Passwort (Kapitel 3).

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 Box, so wie Sie es mit der Passphrase Ihrer Sicherung ohnehin tun sollten.

17.17 … 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 Box 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 16.2). 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 12.3), eine etwaige IPv6-Freigabe (Kapitel 12.11) und, falls genutzt, die für die Videokonferenz (Kapitel 11.2).
3. Bauen Sie am neuen Ort wie gehabt auf: Router-Kabel in **LAN-Ext**, Geräte an **LAN-Int1** und **LAN-Int2** (Kapitel 2.2). 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 Box liegt, und gehen beim Routerwechsel deshalb verloren.
5. Prüfen Sie anschließend unter **Netzwerk → Fernzugriff** die Erreichbarkeit. Der Name Ihrer Box unter mytrutzbox.de bleibt unverändert; die Box meldet die neue Adresse von selbst dorthin. Kommt trotz richtiger Freigabe von außen nichts an, hat der neue Anschluss vermutlich keine eigene IPv4-Adresse (DS-Lite, Kapitel 12.4). TrutzVPN funktioniert dann nur noch über IPv6 (Kapitel 12.11).
6. Starten Sie zum Schluss die angeschlossenen Geräte einmal neu und schalten Sie, falls gewünscht, auch im neuen Router das WLAN ab (Kapitel 2.5).

Ein Wechsel des Internet-Anbieters ändert daran nichts Grundsätzliches. Neu sein können allerdings zwei Dinge: ein Anschluss ohne eigene öffentliche IPv4-Adresse, an dem TrutzVPN nur noch über IPv6 funktioniert (Kapitel 12.11), 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.

18 Support kontaktieren

Kommen Sie mit Kapitel 17 nicht weiter, hilft Comidio gerne. Je genauer Ihre Angaben, desto schneller die Lösung. Dieses Kapitel zeigt, welche Unterlagen die Box 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.

18.1 Zuerst: die Selbstdiagnose der Box

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 zurücksetzen:** quittiert Hinweise, die Sie zur Kenntnis genommen haben.
- **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.

18.2 Was in den Support-Bericht gehört

Menüpfad: Systemeinstellungen → Betriebszustand → Bericht an den Support senden

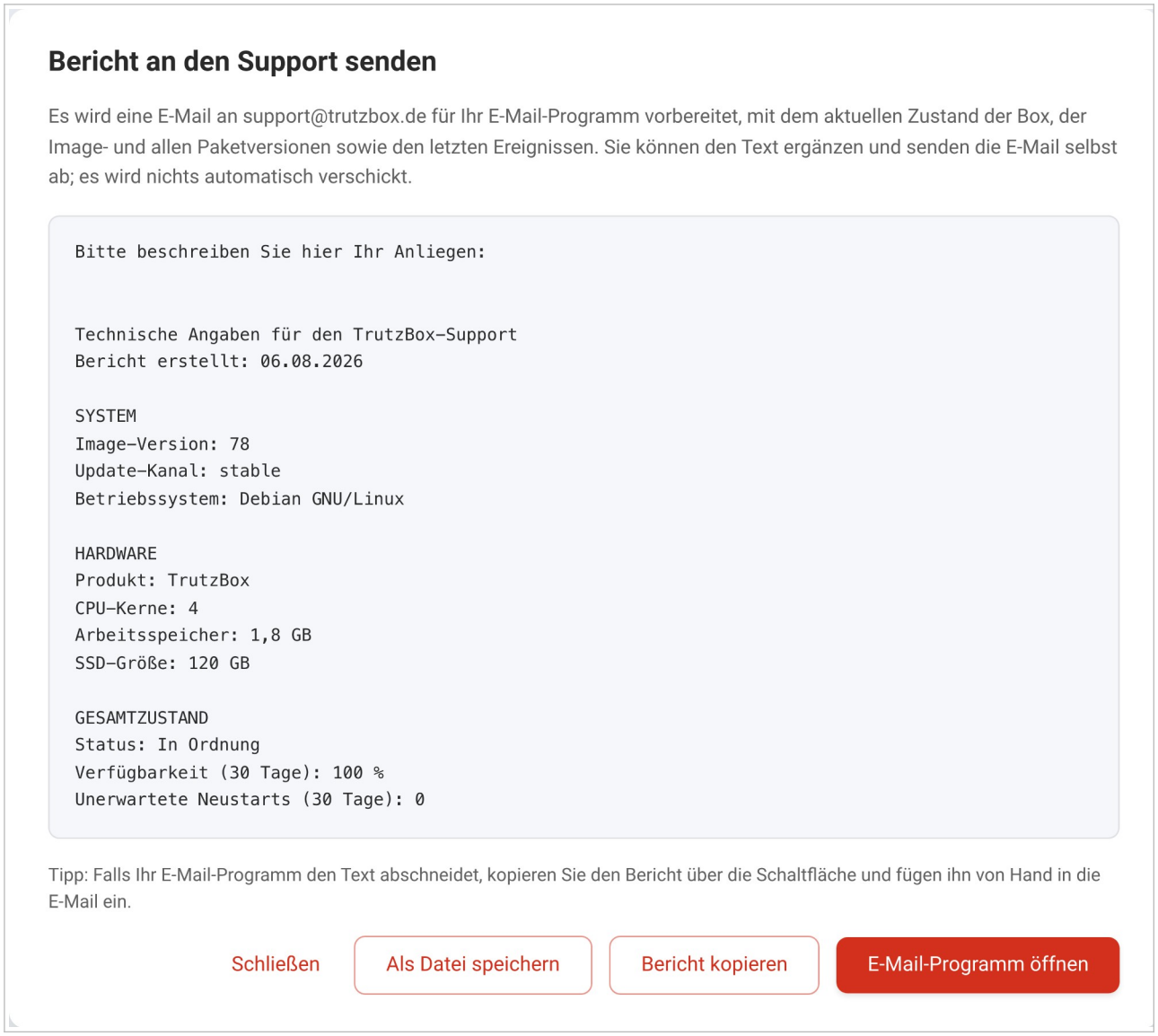


Abbildung 18-1: Der Support-Bericht: Sie sehen den vollständigen Text, bevor irgendetwas Ihre Box verlässt. (© 2026 Comidio GmbH)

Den technischen Teil erledigt die Box für Sie. In vier Schritten ist die Anfrage fertig:

1. Öffnen Sie **Systemeinstellungen → Betriebszustand** und klicken Sie auf **Bericht an Support**. Es öffnet sich ein Dialog, 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: **Bericht kopieren** legt den Text in die Zwischenablage, **Als Datei speichern** sichert ihn auf Ihrem PC, und **E-Mail-Programm öffnen** übergibt ihn an Ihr Mail-Programm.

4. Beim letzten Weg öffnet sich Ihr Mail-Programm mit vorbereitetem Text und bereits eingetragener Empfängeradresse. Ergänzen Sie Ihre Beschreibung und schicken Sie die Nachricht ab. Von selbst verschickt die Box nichts.

Der Bericht enthält den Zustand der Box, wie ihn die Betriebszustand-Seite ermittelt: die Zustände der einzelnen Karten, Angaben zu Speicher, Datenträger und Laufzeit sowie die Versionsstände. Genau das sind die Angaben, nach denen der Support sonst zuerst fragen müsste.

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 geht 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 17 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.

18.3 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 Box über bestimmte Vorgänge verschickt. Diese Mails hält die Box 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 Box 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 (Kapitel 14.6) lässt sich auf Anleitung des Supports ein Systemstatus der Box 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.

18.4 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 Box setzt sie selbst ein.
- **Forum:** forum.trutzbox.de mit Bereichen zu Updates und häufigen 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 über den normalen nächtlichen Update-Weg an alle Boxen aus; bei besonders kritischen Fällen auch außerhalb des Tagesrhythmus (Kapitel 15.8).

18.5 Das Forum sinnvoll nutzen

Das TrutzBox-Forum ist mehr als eine Fragestunde. Im Bereich „TrutzBox-Updates" beschreibt Comidio, was jedes 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 Box, die dort nicht hingehören. Solche Unterlagen schicken Sie besser per E-Mail an den Support.

18.6 Was Comidio nicht kann und nicht tut

Einen dauerhaften Fernwartungszugang von außen gibt es bewusst nicht. Niemand bei Comidio kann sich auf Ihre Box 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.

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 Box verlässt. Der Support arbeitet dafür mit gezielten Anleitungen, die Sie an Ihrer Box 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 16.1). Verlorene Passwörter und Passphrasen sind verloren. Was in diesem Fall noch bleibt, beschreibt Kapitel 17.16.

18.7 Hardware-Defekt und Tausch des Boot-Mediums

Geht die Hardware kaputt, ist das weniger dramatisch, als es klingt. Alle Authentisierungsschlüssel Ihrer Box 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. Weil die Echtheit eines Mail-Nutzers an Ihre TrutzLegitimation gebunden ist und nicht an ein bestimmtes Bauteil, stellen Sie danach Ihre bisherige Authentizität gegenüber Ihren Mail-Partnern wieder her, ohne Ihre Anonymität gegenüber Comidio aufgeben zu müssen. Ihre TrutzMail-Adressen bleiben Ihnen also erhalten.

Nach einem Tausch des Speichermediums ist die Box 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; der Weg führt über den USB-Stick. Den können Sie komplett selbst gehen, die Schritt-für-Schritt-Anleitung samt Bedeutung der LEDs steht in Kapitel 15.7.

1. Melden Sie den Defekt beim Support und beschreiben Sie, was die LEDs an der Gerätefront anzeigen (Kapitel 17.12).
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 3).
4. Spielen Sie im Setup-Schritt „Aktualisierung des Setups" Ihre Sicherung ein (Kapitel 16.3). 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 19). Mit Sicherung kehrt das bisherige Zertifikat zurück, und auf den Geräten ist nichts zu tun.

> **Ohne Sicherung geht Ihre Identität verloren**
>
> Die geheimen Schlüssel Ihrer TrutzMail-Konten gibt es nur einmal, und zwar auf Ihrer Box. Ein Hardware-Defekt ohne vorhandene Sicherung bedeutet, dass Ihre Partner Sie nicht mehr als dieselbe Person erkennen können. Legen Sie eine Sicherung an, solange die Box noch läuft, und bewahren Sie sie außerhalb der Box auf (Kapitel 16.2).

18.8 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 Boxen 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 Box vorher über das Energie-Menü der Oberfläche herunter (Kapitel 17.15) und ziehen Sie danach alle Kabel ab, auch das Netzteil. Am geöffneten Gerät wird nicht gearbeitet, solange Strom anliegt.

1. Die Box 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 Box ist nach dem Tausch leer und braucht ein frisches System. Das spielen Sie mit dem Tank-Stick auf (Kapitel 15.7), danach durchlaufen Sie das Setup mit Ihrer TrutzLegitimation und spielen im Schritt „Aktualisierung des Setups" Ihre Sicherung ein (Kapitel 16.3). Ihre TrutzMail-Adressen kehren damit zurück, denn sie hängen an Ihrer TrutzLegitimation und nicht an der getauschten Karte.

Wenn Sie das nicht selbst machen möchten

Der Tausch ist keine Pflichtübung. Melden Sie sich beim Support (Abschnitt 18.4), beschreiben Sie den Fehler und was die LEDs anzeigen; Comidio nennt Ihnen dann die passende Karte oder übernimmt den Tausch. Solange die Box noch läuft, legen Sie vorher unbedingt eine Sicherung an.

19 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.

19.1 Wann Sie das Root-Zertifikat brauchen

Es gibt genau zwei Anlässe:

- **TrutzBrowse (Kapitel 13):** Diese Zusatzfunktion entfernt identifizierende Merkmale aus dem Datenverkehr. Dafür muss die Box 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 Box (Kapitel 10), ein Chat-Programm meldet sich am Chat-Server an (Kapitel 11), 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 Box 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 Box nie, und beglaubigt wird damit ausschließlich, was Ihre eigene Box prüft. Das Root-Zertifikat zu installieren heißt also: Ihrem eigenen Gerät zu sagen, dass es Ihrer eigenen Box vertrauen darf.

19.2 Das Root-Zertifikat herunterladen

Menüpfad: Verwaltung → Allgemeine Einstellungen

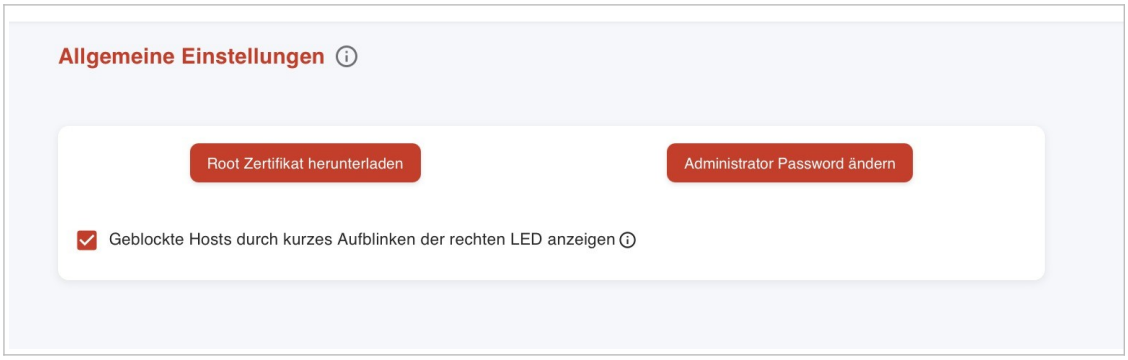


Abbildung 19-1: Der Download liegt unter Verwaltung, Allgemeine Einstellungen. (© 2026 Comidio GmbH)

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.

19.3 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.

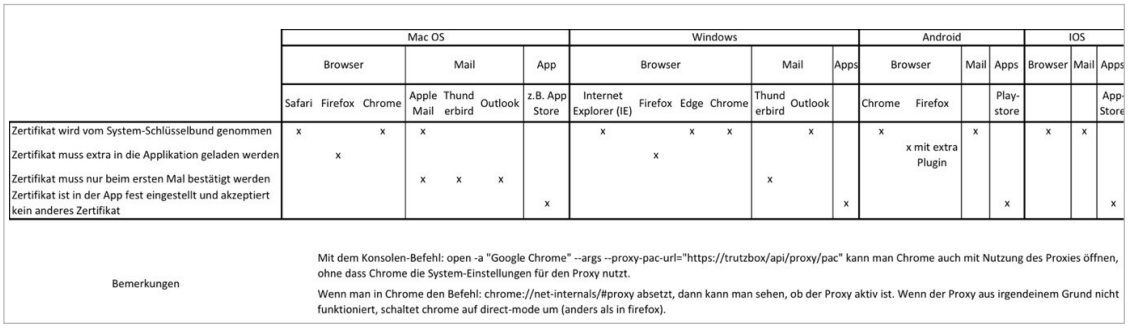
System	Der Weg im Groben	Aktuelle Anleitung
Windows	Zertifikat öffnen und unter „Vertrauenswürdige Stammzertifizierungsstellen" importieren. Das Werkzeug dafür heißt „Benutzerzertifikate verwalten" und ist über die Suche im Startmenü zu finden.	support.microsoft.com
Android	Auf die heruntergeladene Datei 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 Vertrauen für das Zertifikat einzuschalten.	support.apple.com

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.

19.4 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 19-2: 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.

19.5 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 13.6). 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, empfiehlt es sich, TrutzBrowse gleich für alle neuen Geräte abzuschalten. Die entsprechende Voreinstellung finden Sie auf der Geräte-Seite (Kapitel 6.1).

19.6 Nach einem Zurücksetzen der Box

Wird die TrutzBox auf den Werkszustand zurückgesetzt (Kapitel 16.4), 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 19.1 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 Box liegt schlicht das alte Zertifikat auf dem Gerät.

20 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.

20.1 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 Box 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 2.4).
- **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 Box 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 Box im Normalfall über die Verwaltungsoberfläche herunter, statt einfach den Stecker zu ziehen. Die Box 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 Box ist darauf ausgelegt.

20.2 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 Box liegen Ihre Postfächer, Ihre Schlüssel und Ihre Einstellungen. Setzen Sie die Box deshalb vor jedem Besitzerwechsel und vor der Entsorgung auf den Werkszustand zurück (Kapitel 16.4). Legen Sie vorher eine Sicherung an, falls Sie die Daten auf einer anderen Box weiterverwenden möchten. Was sonst noch dazugehört, vor allem der Umgang mit Ihrer TrutzLegitimation, steht in Abschnitt 16.6.

20.3 Gewährleistung und Ersatzteile

Für die TrutzBox gelten die gesetzlichen Gewährleistungsfristen. Weil ein Sicherheitsgerät ohne Aktualisierungen wertlos wäre, liefert Comidio Updates über die gesamte vereinbarte Dauer aus; die gesetzliche Grundlage dafür steht in Kapitel 15.5.

Geht die Hardware kaputt, bedeutet das nicht den Verlust Ihrer Identität: Ihre TrutzMail-Adressen hängen an Ihrer TrutzLegitimation, nicht am Gehäuse. Das Vorgehen beim Hardware-Defekt beschreibt Kapitel 18.7. Ersatznetzteile, Netzwerkkabel und das WLAN-Modul erhalten Sie über den Support.

20.4 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 Box. Comidio hat darauf keinen Zugriff und keinen Fernwartungszugang (Kapitel 18.6).

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 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 18.2).

20.5 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 Box	Systemeinstellungen → Vertrag und Pakete nennt Image-Version, Hardware 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 Kapitelangaben 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 14.4).

Betriebszustand Die Gesundheitsseite der Box mit einer Ampel für den Gesamtzustand und Karten für die einzelnen Bereiche (Kapitel 5.2).

Blacklist Eine Sperrliste: Was darin steht, wird blockiert. Das Gegenstück zur Whitelist (Kapitel 8.3).

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 14.3).

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 14.3).

DS-Lite Anschlussart mancher Anbieter ohne eigene öffentliche IPv4-Adresse. Von außen ist die TrutzBox dort nur über IPv6 erreichbar; TrutzVPN funktioniert dann mit dem Schalter „VPN auch über IPv6 anbieten" (Kapitel 12.4 und 12.11).

Fernzugriff Der Zugang zur eigenen TrutzBox von außerhalb des Hauses, über TrutzVPN (Kapitel 12).

Filtergruppe Ein Filterprofil, das mehrere Filterlisten bündelt und einem Gerät oder Benutzer zugewiesen wird (Kapitel 8.2).

Filterliste Ein Verzeichnis von Internet-Adressen zu einem Thema, etwa „Tracker" oder „Werbung", das gesperrt oder erlaubt wird (Kapitel 8.3).

Firewall Die Schutzschicht, die unerwünschte Verbindungen auf Netzwerkebene abwehrt, unabhängig davon, welches Programm sie aufbaut.

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 10.3).

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 12.11).

Internes TrutzBox-Netzwerk Weg 1, ein Gerät mit der Box zu verbinden: Das Gerät hängt per Kabel oder über das TrutzBox-WLAN hinter der Box, sein gesamter Verkehr läuft automatisch durch sie. Der empfohlene Weg (Kapitel 4.2).

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 12.11).

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.

LetsEncrypt 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 11.2).

MAC-Adresse Die vom Hersteller vergebene Hardware-Kennung einer Netzwerk-Schnittstelle. Daran erkennt die Box ein Gerät wieder. Neuere Smartphones und Notebooks können aus Datenschutzgründen zufällige Adressen verwenden; dann ist die Wiedererkennung nicht mehr eindeutig (Kapitel 6.1).

Metadaten Die Begleitdaten einer Nachricht: wer schreibt wem, wann, wie oft. Bei TrutzMail zwischen TrutzBoxen bleiben auch sie verborgen.

Monitor Die Live-Ansicht aller Verbindungen im Netz, mit Liste, Verbindungsbild, Blasendiagramm und Datendurchsatz (Kapitel 9).

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 6.7).

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 16.2).

PGP Ein offener Standard zur Verschlüsselung von E-Mail. Die TrutzBox nutzt ihn für Partner ohne eigene TrutzBox (Kapitel 10.5).

Portweiterleitung Eine Regel im Internet-Router, die Anfragen aus dem Internet an ein bestimmtes Gerät im Netz weiterreicht. Für den VPN-Zugang nötig (Kapitel 12.3).

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 Box zu verbinden: Das Gerät bleibt im Netz des Routers und bekommt die TrutzBox nur als Proxy eingetragen. Proxy-Port 8081 oder automatische Konfiguration (Kapitel 4.3).

QUIC Ein modernes Übertragungsprotokoll, das an klassischen Filtern vorbeiläuft. Die TrutzBox kann es deshalb gezielt sperren.

Root-Zertifikat Die Datei, mit der ein Gerät der TrutzBox vertraut. Nötig für TrutzBrowse und für Programme, die sich mit der Box verbinden, nicht für den normalen Webfilter (Kapitel 19).

Security-Slider Der Regler mit neun Stufen, mit dem der Anonymisierungsgrad von TrutzBrowse eingestellt wird (Kapitel 13).

Speicher-Wächter Die Überwachung des Arbeitsspeichers. Wird er knapp, hält sie gezielt Dienste an, zuerst TrutzRTC und danach TrutzMail, damit die Box nicht einfriert, und startet sie wieder, sobald genug frei ist (Kapitel 5.3).

Sperrseite Die Seite, die die TrutzBox anstelle einer blockierten Webseite anzeigt, mit Angabe des Grundes (Kapitel 8.6).

SSID Der Name eines Funknetzes, also das, was auf dem Smartphone in der WLAN-Liste erscheint (Kapitel 14.2).

Switch Ein Verteiler mit mehreren Netzwerkbuchsen. Er erweitert die internen Anschlüsse der TrutzBox; alles daran bleibt geschützt (Kapitel 2.5).

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 6.7).

Transparent Die Verbindungsart von Geräten im internen TrutzBox-Netzwerk: Ihr Verkehr läuft durch die Box, ohne dass am Gerät etwas eingestellt werden müsste (Kapitel 4.2).

TrutzBase Der Sicherheitsteil der Box: Firewall, Angriffserkennung und VPN-Server.

TrutzBrowse Die Anonymisierungsfunktion, die identifizierende Merkmale aus dem Datenverkehr entfernt (Kapitel 13).

TrutzBurg Das kleine Bedienelement, das TrutzBrowse in aufgerufene Seiten einblendet. Darüber lässt sich der Security-Slider für die gerade besuchte Seite verstellen (Kapitel 13.5).

TrutzChat Der Nachrichtendienst der TrutzBox auf Basis des offenen XMPP-Standards (Kapitel 11).

TrutzContent Der Webfilter der TrutzBox, der anhand von Filtergruppen über jeden Zugriff entscheidet (Kapitel 8).

TrutzDynDNS Der kostenlose Dienst von Comidio, der Ihrer Box einen festen Namen unter mytrutzbox.de gibt, auch wenn die IP-Adresse wechselt (Kapitel 12.2).

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 Box Ihnen gehört.

TrutzMail Die E-Mail-Funktion der TrutzBox mit automatischer Verschlüsselung; Adressen enden auf @comidio.email (Kapitel 10).

TrutzMeeting Der Videokonferenz-Dienst auf der eigenen Box; Gäste brauchen nur einen Browser und einen Link (Kapitel 11.2).

TrutzRTC Der gemeinsame Unterbau von TrutzChat und TrutzMeeting auf Ihrer Box. Er gehört zur Business-Ausstattung und erscheint als eigene Karte auf der Betriebszustand-Seite (Kapitel 11).

TrutzSchlüssel Der 16-stellige Schlüssel im Format XXXX-XXXX-XXXX-XXXX vom Beileger, für die Registrierung der Box.

VPN Ein verschlüsselter Tunnel durch das Internet. Er verbindet Geräte unterwegs mit der TrutzBox zuhause (Kapitel 12).

Webmin Die technische Zweit-Oberfläche der Box für erfahrene Administratoren und den Notfall (Kapitel 14.6).

Whitelist Eine Ausnahmeliste: Was darin steht, ist erlaubt, auch wenn andere Filter es sperren würden.

WPA2 und WPA3 Die beiden gebräuchlichen Verschlüsselungsverfahren für WLAN. WPA3 ist das neuere und sicherere, WPA2 versteht auch ältere Geräte (Kapitel 14.2).

XMPP Der offene Standard hinter TrutzChat, den viele Chat-Programme auf allen Systemen unterstützen.

Stichwortverzeichnis