TETRACONTROL 5.4 · ANLEITUNG

TETRAcontrol im Internet erreichbar machen

mit einem Cloudflare Tunnel

Stand: 18.09.2026 · Betrifft: TETRAcontrol 5.4 mit WebUI 2.0

Diese Anleitung führt Schritt für Schritt dorthin, dass Sie die Weboberfläche von TETRAcontrol von unterwegs aufrufen können — vom Dienst-Laptop, vom Tablet oder vom Mobiltelefon —, ohne dafür Ihren Router zu öffnen.

Sie brauchen dafür keine Vorkenntnisse in Netzwerktechnik. Wo eine Entscheidung ansteht, steht die Empfehlung dabei.

Inhalt

1. Was dabei herauskommt
2. Bevor Sie anfangen
3. Schritt 1 — Konto bei Cloudflare anlegen
4. Schritt 2 — Domain einrichten
5. Schritt 3 — Tunnel anlegen
6. Schritt 4 — cloudflared auf dem Rechner installieren
7. Schritt 5 — Die Weboberfläche veröffentlichen
8. Schritt 6 — Zugriff absichern
9. Schritt 7 — Die Domain absichern
10. Abschlusstest
11. Laufender Betrieb
12. Wenn etwas nicht geht
13. Was Sie sich damit einhandeln
14. Spickzettel

1. Was dabei herauskommt

Heute läuft TETRAcontrol auf einem Rechner in Ihrem Netz und liefert die Weboberfläche an alle aus, die im selben Netz sind. Von außen kommt niemand daran — und das ist auch gut so, denn der übliche Weg nach außen wäre eine Portfreigabe im Router. Damit stünde der Webserver für jeden im Internet offen, und Angriffe darauf beginnen erfahrungsgemäß innerhalb von Minuten.

Ein Cloudflare Tunnel dreht die Richtung um.

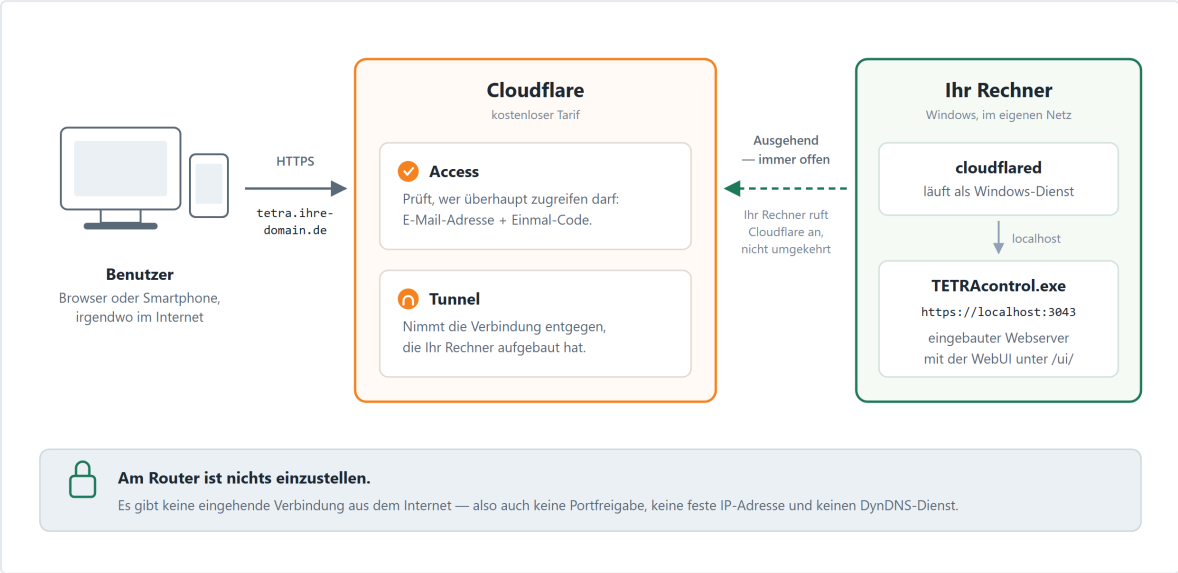


Bild 1 — Der Weg der Daten. Entscheidend ist der grüne Pfeil: Er zeigt nach links.

Auf dem Rechner mit TETRAcontrol läuft künftig ein kleines Zusatzprogramm namens **cloudflared**. Es baut von sich aus eine Verbindung zu Cloudflare auf und hält sie offen. Ruft jemand später `https://tetra.ihre-domain.de` auf, landet er bei Cloudflare, und Cloudflare schickt die Anfrage durch diese bereits bestehende Verbindung zu Ihnen.

Daraus folgt das Angenehme daran:

- **Keine Portfreigabe.** Von außen gibt es keine Verbindung zu Ihrem Netz, die ein Angreifer ansprechen könnte. Es gibt nur die eine, die Ihr Rechner selbst aufgebaut hat.
- **Keine feste IP-Adresse, kein DynDNS.** Wechselt Ihre Internetadresse, baut cloudflared die Verbindung neu auf. Das merkt niemand.
- **Ein gültiges Zertifikat.** Die Adresse ist echtes HTTPS, ohne die Zertifikatswarnung, die Sie im eigenen Netz gewohnt sind.
- **Eine Tür mit Schloss davor.** Wer die Adresse kennt, kommt trotzdem nicht hinein — davor steht eine Anmeldung, die Sie selbst bestücken.

Die zwei Anmeldungen

Danach gibt es zwei Anmeldungen hintereinander. Das klingt umständlich, ist aber der Kern der Sache, deshalb hier gleich zu Anfang:

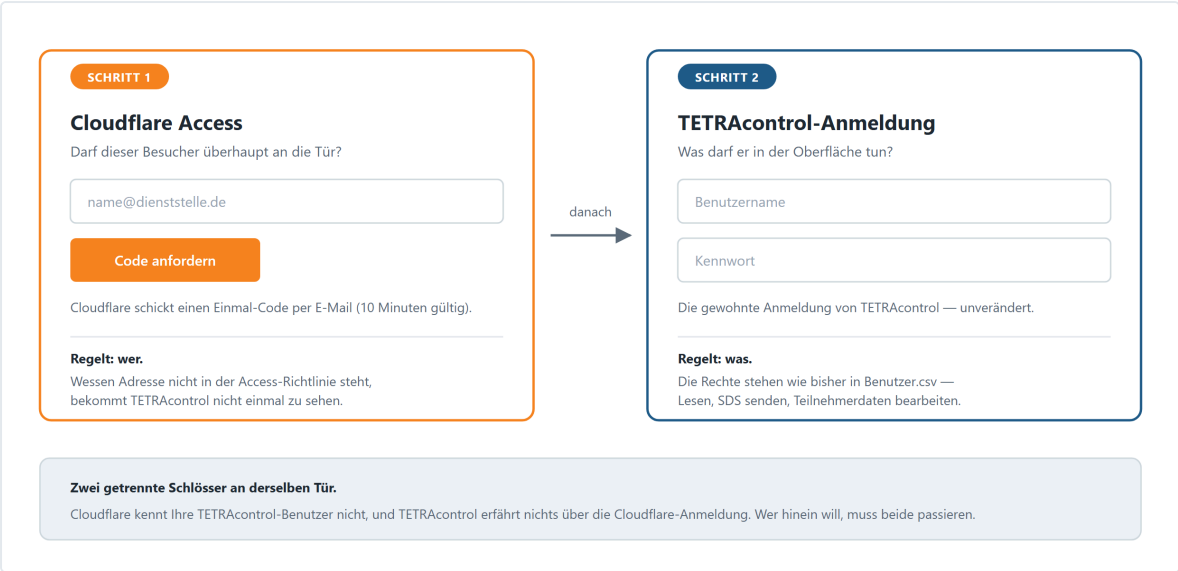


Bild 2 — Zwei Schlösser an derselben Tür. Sie sind voneinander unabhängig.

Cloudflare Access entscheidet, **wer** überhaupt bis zu TETRAcontrol vordringt. Die TETRAcontrol-Anmeldung entscheidet wie bisher, **was** derjenige dann tun darf. Ihre Benutzer aus `Benutzer.csv` bleiben unverändert; es kommt nur eine Prüfung davor.

Was es kostet und wie lange es dauert

Cloudflare ist für diesen Zweck kostenlos: Der Tunnel kostet nichts, und die Zugriffsprüfung (Access) ist bis 50 Personen kostenlos. Geld kostet nur der Domainname, üblicherweise 10 bis 15 Euro im Jahr — und den brauchen Sie nur, falls Sie noch keinen haben.



Bild 3 — Gut eine Stunde reine Arbeitszeit. Bei Schritt 2 kommt Wartezeit dazu, auf die Sie keinen Einfluss haben.

2. Bevor Sie anfangen

2.1 Das brauchen Sie

TETRAcontrol	Version 5.4 mit der neuen Weboberfläche (WebUI 2.0), Serverstand ab 08/2026
TLS eingeschaltet	In den Servereinstellungen muss `SSLServerPort` gesetzt sein. Diese Portnummer notieren — in dieser Anleitung ist es beispielhaft **3043**.
Der Rechner läuft durch	Ist TETRAcontrol aus, ist auch die Weboberfläche von außen nicht erreichbar.
Windows-Administratorrechte	Einmalig, für die Installation von cloudflared.
Eine E-Mail-Adresse	Für das Cloudflare-Konto.
Ein Domainname	Vorhanden oder neu gekauft — siehe Schritt 2.

> **Prüfen Sie zuerst, ob die Weboberfläche im eigenen Netz läuft.** Rufen Sie am TETRAcontrol-Rechner `https://localhost:3043/ui/` auf und melden Sie sich an. Die Zertifikatswarnung des Browsers ist an dieser Stelle normal und darf bestätigt werden. Erst wenn das funktioniert, lohnt sich der Rest dieser Anleitung.

2.2 Ein Wort zur Sicherheit, bevor es losgeht

Sobald etwas aus dem Internet erreichbar ist, wird es gefunden — nicht nach Wochen, sondern meist innerhalb von Minuten. Das hat nichts mit Ihnen zu tun: Automaten fahren den gesamten Adressraum des Internets rund um die Uhr ab und probieren an allem, was antwortet, eine Liste bekannter Schwachstellen durch. Niemand muss Ihre Adresse kennen, und es hilft auch nicht, sie geheim zu halten.

Eine Anmeldemaske allein ist gegen so etwas ein dünner Schutz. Sie muss dann nämlich dauerhaft standhalten: gegen das automatische Durchprobieren von Kennwörtern, gegen Zugangsdaten, die anderswo abgeflossen sind und hier erneut versucht werden, und gegen Fehler in der Anmeldung selbst. Eine Weboberfläche bietet dafür viel Fläche — jede Adresse, jedes Eingabefeld, jeder Parameter ist ein möglicher Ansatzpunkt, und es genügt eine einzige Stelle, die nicht hält.

Dazu kommt, dass Software für den Betrieb im geschlossenen Netz anders gebaut wird als Software fürs offene Internet. Im Hausnetz darf man annehmen, dass ohnehin nur Befugte davorsitzen; diese Annahme trägt draußen nicht mehr. Und die Daten, um die es hier geht, sind keine beliebigen: Standorte von Einsatzkräften, Alarmierungen, Gesprächsverkehr.

Deshalb ist **Schritt 6 nicht optional**. Cloudflare Access hält jeden Unbefugten schon an der Außenkante ab, also lange bevor eine Anfrage den TETRAcontrol-Webserver überhaupt erreicht. Genau dadurch wird die Veröffentlichung vertretbar.

Lassen Sie Schritt 6 nicht weg, auch nicht „vorerst". Ein Tunnel ohne Access ist eine Portfreigabe mit besserem Zertifikat.

Lesen Sie außerdem Abschnitt 13, bevor Sie personenbezogene Einsatzdaten dauerhaft über einen Dienstleister leiten.

2.3 Zu den Beschriftungen in dieser Anleitung

Cloudflare übersetzt seine Oberfläche nur teilweise. Auf ein und demselben Bildschirm stehen deutsche und englische Beschriftungen nebeneinander — der Schalter heißt *TLS-Zertifikats-Überprüfung deaktivieren*, die Installationsschritte direkt darüber stehen auf Englisch. Mit der nächsten Aktualisierung kann sich das verschieben.

Diese Anleitung nennt die deutsche Bezeichnung und setzt die englische dahinter, wo beide vorkommen — etwa **Gesund** (*Healthy*). Finden Sie eine Schaltfläche nicht unter dem genannten Namen, suchen Sie nach der jeweils anderen Fassung.

3. Schritt 1 — Konto bei Cloudflare anlegen

1. Rufen Sie **dash.cloudflare.com/sign-up** auf.
2. E-Mail-Adresse und ein Kennwort eintragen, Konto anlegen.
3. Cloudflare schickt eine Bestätigungsmail. Den Link darin anklicken.

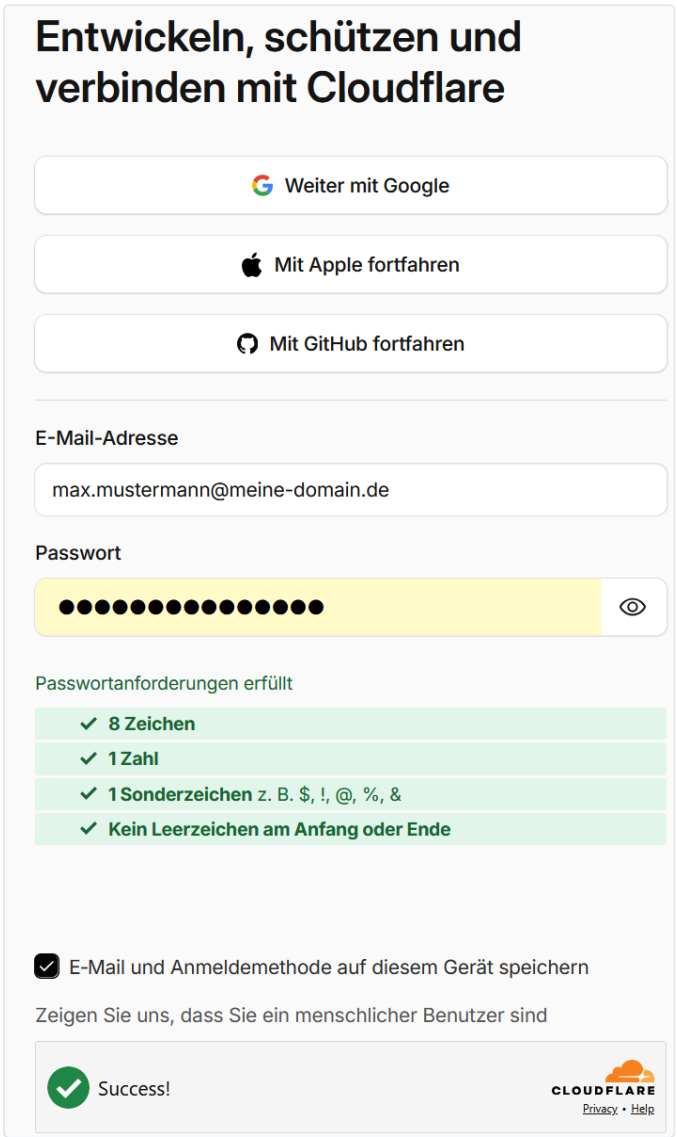


Bild 4 — Die Registrierungsseite.

> **Nehmen Sie eine Adresse, auf die mehr als eine Person Zugriff hat** — etwa ein Funktionspostfach der Dienststelle. An diesem Konto hängt später der Zugang zu Ihren Einsatzdaten. Geht die Adresse einer einzelnen Person verloren, wird es unangenehm.

Zwei-Faktor-Anmeldung einschalten — bitte sofort

Wer in dieses Konto kommt, kann die Zugriffsregeln ändern und sich damit selbst Zutritt zu TETRAcontrol verschaffen. Ein Kennwort allein ist dafür zu wenig.

Oben rechts auf Ihr Profil klicken → **My Profile** → **Authentication** → **Two-Factor Authentication** einschalten und mit einer Authenticator-App einrichten. Die angezeigten Wiederherstellungscodes ausdrucken und verwahren.

Das dauert drei Minuten. Holen Sie es nicht „später" nach.

4. Schritt 2 — Domain einrichten

Sie brauchen einen eigenen Domainnamen, zum Beispiel `ffw-musterstadt.de`. Die Weboberfläche bekommt dann eine Unteradresse davon, etwa `tetra.ffw-musterstadt.de`.

Wichtig ist nur eines: **Die Domain muss bei Cloudflare verwaltet werden.** Dafür gibt es zwei Wege.

Weg A — Neue Domain direkt bei Cloudflare kaufen *(einfacher)*

Haben Sie noch keine Domain, kaufen Sie sie gleich bei Cloudflare. Dann ist alles Weitere bereits richtig eingestellt und es gibt keine Wartezeit.

1. Im Dashboard links auf **Domain Registration** → **Register Domains**.
2. Wunschnamen suchen, auswählen, Kontaktdaten eintragen und bezahlen.
3. Fertig. Weiter bei Schritt 3.

> Cloudflare verkauft Domains zum Einkaufspreis, ohne Aufschlag. Dafür können Sie die Namensverwaltung später nicht zu einem anderen Anbieter umziehen, solange die Domain dort registriert ist.
>
> **ICANN verlangt, dass Sie die hinterlegte E-Mail-Adresse bestätigen.** Kommt eine entsprechende Mail, klicken Sie den Link darin an. Sonst wird die Domain nach einiger Zeit stillgelegt — und damit auch Ihr Zugang.

Weg B — Vorhandene Domain zu Cloudflare umziehen

Haben Sie bereits eine Domain bei einem anderen Anbieter (Strato, IONOS, united-domains …), bleibt sie dort registriert. Nur die Namensverwaltung wandert zu Cloudflare.

1. Im Dashboard **Add a domain** wählen, den Domainnamen eintragen.
2. Als Tarif **Free** auswählen.
3. Cloudflare liest die bestehenden DNS-Einträge ein und zeigt sie an.

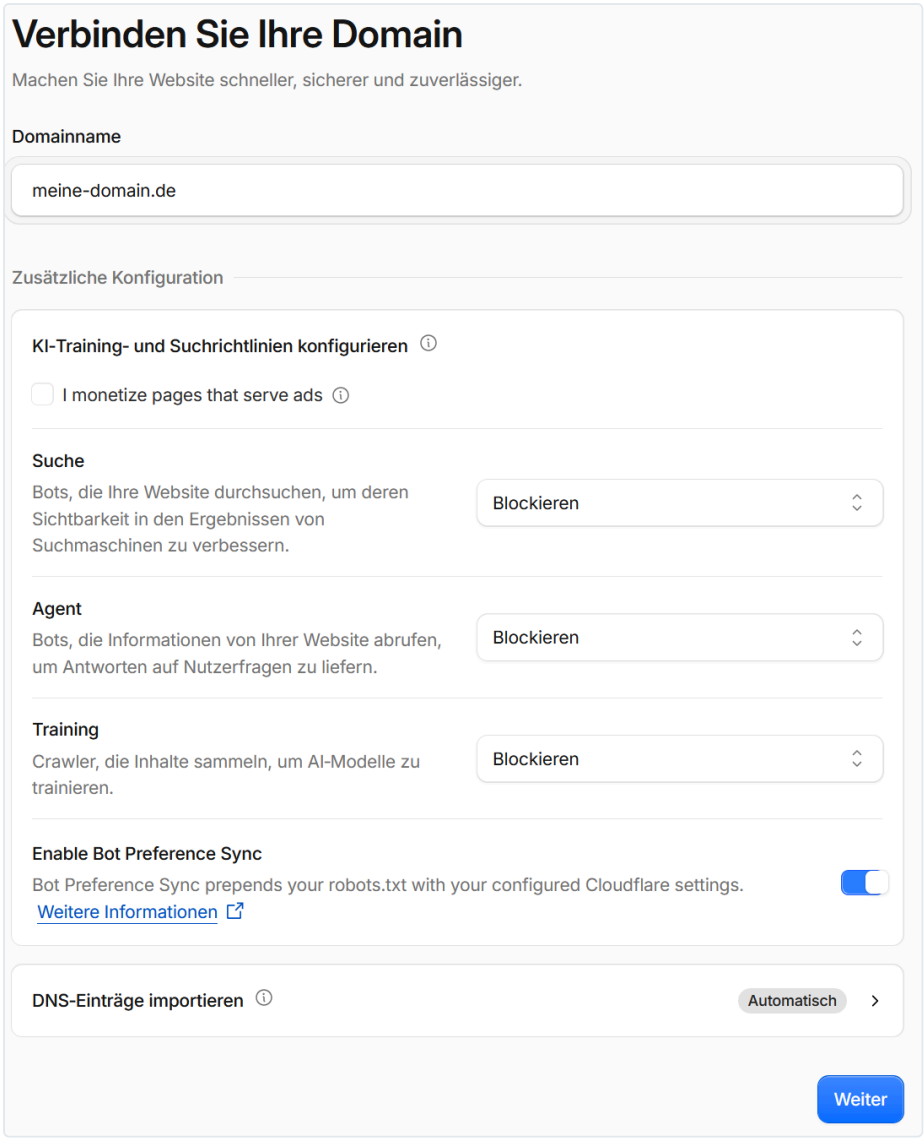


Bild 5 — Domain hinzufügen und Tarif wählen.

> **Hier bitte genau hinsehen.** Vergleichen Sie die eingelesene Liste mit dem, was bei Ihrem bisherigen Anbieter steht — besonders die `MX`-Einträge für E-Mail und alle `TXT`-Einträge. Was Cloudflare nicht übernimmt, funktioniert nach der Umstellung nicht mehr. Fehlt ein Eintrag, tragen Sie ihn von Hand nach, **bevor** Sie weitermachen.
>
> Wird über dieselbe Domain auch dienstliche E-Mail abgewickelt, machen Sie diesen Schritt nicht allein und nicht an einem Freitagnachmittag.

4. Cloudflare zeigt Ihnen zwei Nameserver, etwa `dana.ns.cloudflare.com` und `rob.ns.cloudflare.com`. Diese beiden tragen Sie bei Ihrem bisherigen Anbieter anstelle der dortigen Nameserver ein. Wo das geht, heißt bei den meisten Anbietern „Nameserver ändern" oder „DNS-Einstellungen".

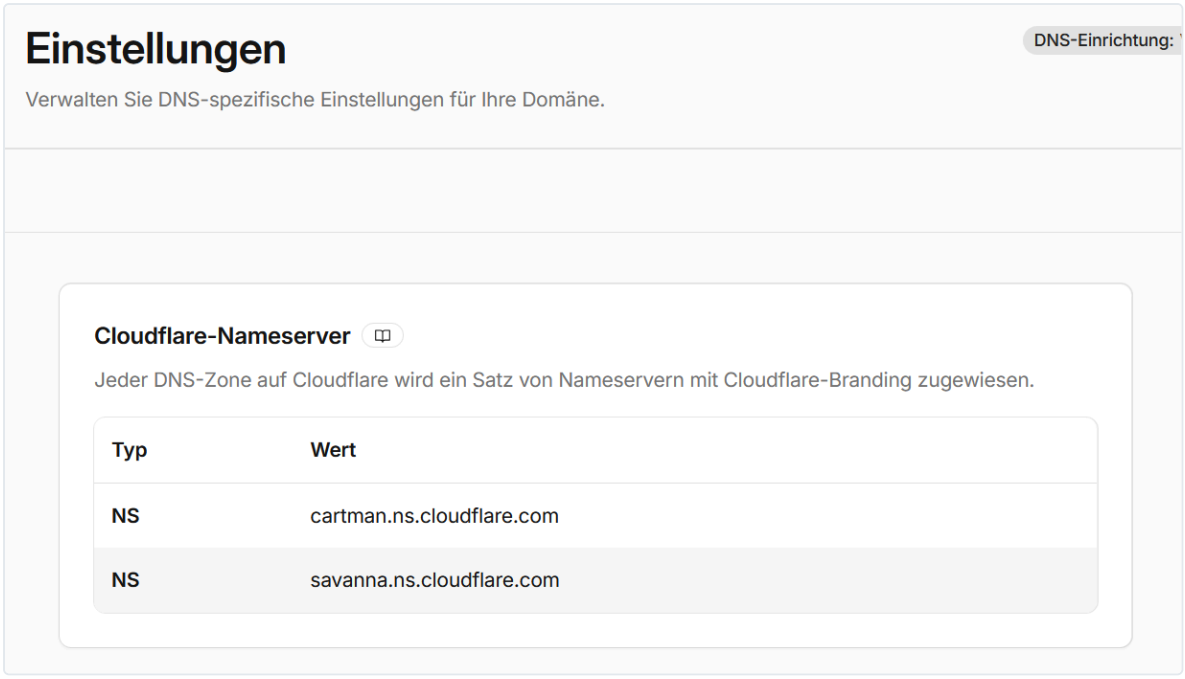


Bild 6 — Die beiden Cloudflare-Nameserver.

5. Jetzt heißt es warten. Meist ist es nach wenigen Minuten erledigt, es kann aber bis zu 24 Stunden dauern. Cloudflare schickt eine E-Mail, sobald die Domain übernommen ist; im Dashboard steht die Domain dann auf **Active**.

Warten Sie diese Bestätigung ab. Solange die Domain nicht aktiv ist, schlägt Schritt 5 fehl, und die Fehlermeldung sagt Ihnen nicht, dass es daran liegt.

Welche Unteradresse?

Die Weboberfläche bekommt eine eigene Unteradresse. `tetra.ihre-domain.de` oder `leitstelle.ihre-domain.de` sind gute Namen. Sie müssen dafür **keinen DNS-Eintrag von Hand anlegen** — das erledigt Cloudflare in Schritt 5 automatisch.

5. Schritt 3 — Tunnel anlegen

Der Tunnel ist die Verbindung zwischen Cloudflare und Ihrem Rechner. Angelegt wird er im Browser; auf dem Rechner selbst passiert erst in Schritt 4 etwas.

1. Im Cloudflare-Dashboard links **Networking** → **Tunnel** öffnen. *(Je nach Stand der Oberfläche liegt derselbe Punkt unter Zero Trust → Networks → Tunnels.)*
2. **Tunnel erstellen** anklicken. Wird dabei nach dem Connector-Typ gefragt, **Cloudflared** wählen.
3. Unter **Tunnelname** einen Namen vergeben, der etwas aussagt — zum Beispiel `TC-FW-01` oder `tetracontrol-leitstelle`. Der Name ist nur für Sie; er taucht nirgends öffentlich auf.
4. Mit **Tunnel erstellen** bestätigen.

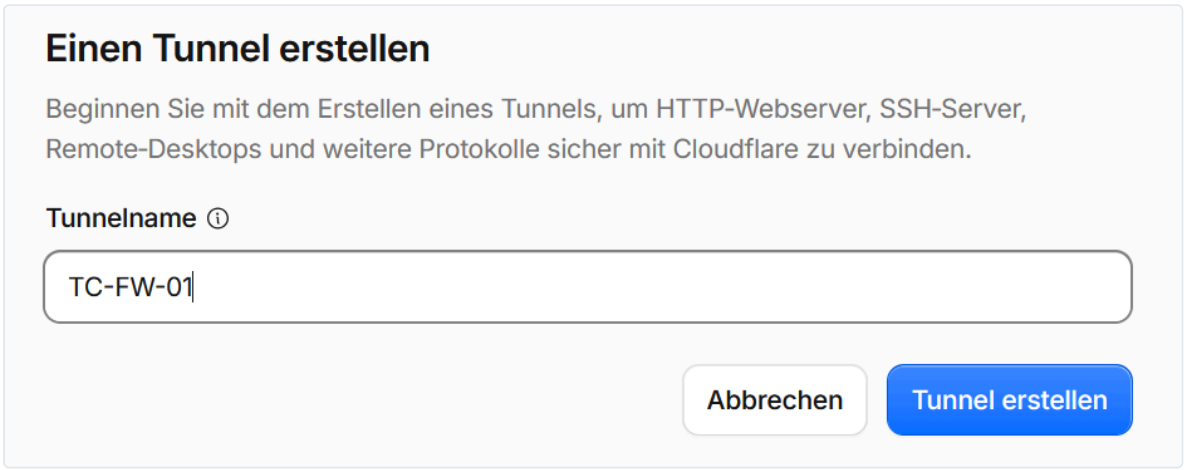


Bild 7 — Mehr als einen Namen braucht es hier nicht.

Cloudflare zeigt Ihnen jetzt den Installationsbefehl. Lassen Sie diese Seite offen und machen Sie am TETRAcontrol-Rechner weiter.

6. Schritt 4 — cloudflared auf dem Rechner installieren

Dies ist der einzige Schritt, der **am Rechner mit TETRAcontrol** stattfindet.

1. Auf der noch offenen Cloudflare-Seite unter **Umgebung einrichten** das **Betriebssystem** *Windows* und die **Architektur** *64-bit* auswählen.
2. Unter **Installieren und Ausführen** zeigt Cloudflare nun einen Befehl, der so aussieht:

```
cloudflared.exe service install eyJhIjoiNzk4M...sehr langer Text...In0=
```

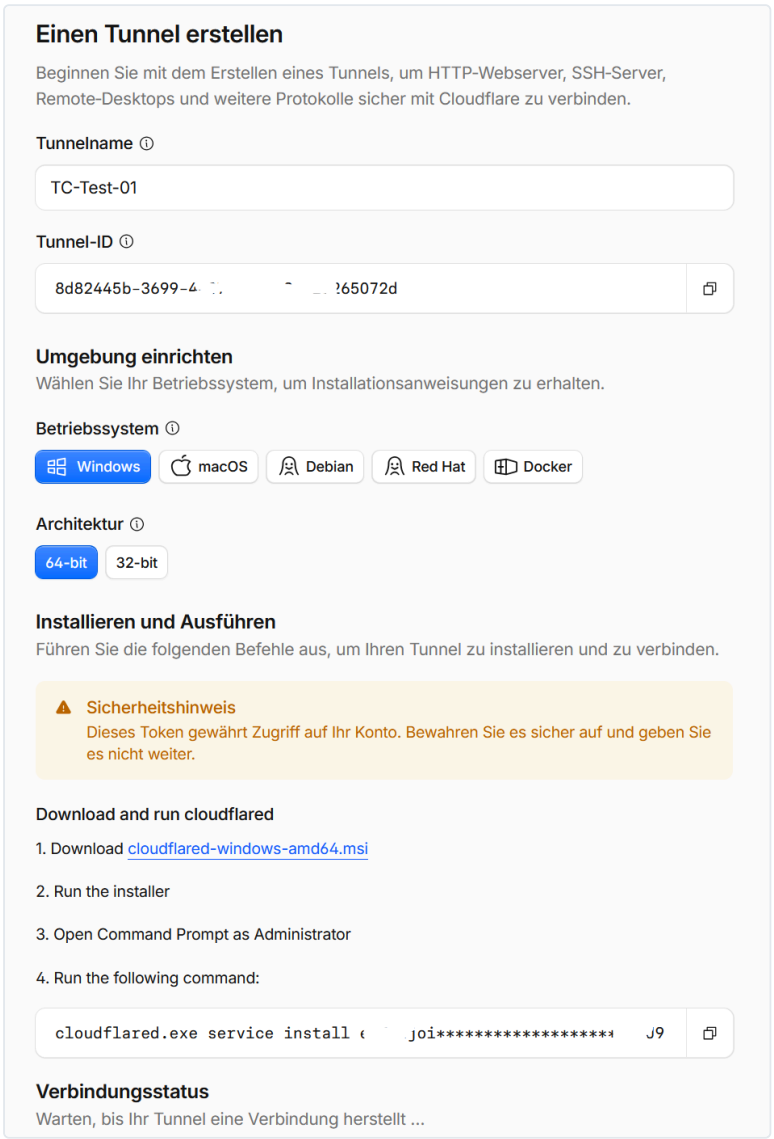


Bild 8 — Der Installationsbefehl mit dem Token.

> **Der lange Text hinter `install` ist ein Schlüssel zu Ihrem Netz.** Cloudflare weist an derselben Stelle als *Sicherheitshinweis* darauf hin — zu Recht. Wer ihn hat, kann sich als Ihr Tunnel ausgeben. Verschicken Sie ihn nicht per E-Mail oder Messenger, und schwärzen Sie ihn auf Bildschirmfotos. Ist er einmal abhandengekommen, löschen Sie den Tunnel in Cloudflare und legen ihn neu an — einen anderen Weg gibt es nicht.

3. **cloudflared herunterladen.** Cloudflare verlinkt die Datei `cloudflared-windows-amd64.msi` direkt auf derselben Seite; herunterladen und installieren. Alternativ geht es über die Eingabeaufforderung:

```
bash winget install --id Cloudflare.cloudflared
```

4. **Eingabeaufforderung als Administrator öffnen:** Startmenü → `cmd` eintippen → Rechtsklick auf *Eingabeaufforderung → Als Administrator ausführen*.
5. Den kopierten Befehl aus Schritt 2 einfügen (Rechtsklick fügt ein) und mit Enter bestätigen.

Das war es. cloudflared ist damit als Windows-Dienst eingerichtet, startet künftig automatisch mit dem Rechner und meldet sich von selbst wieder an, wenn die Internetverbindung einmal weg war.

Hat es geklappt?

Zwei Kontrollen:

Auf dem Rechner: Startmenü → `services.msc` → in der Liste steht **Cloudflare Tunnel** mit dem Status *Wird ausgeführt*.

Im Browser: Solange Cloudflare noch wartet, steht unten auf der Seite **Verbindungsstatus — Warten, bis Ihr Tunnel eine Verbindung herstellt …**. Nach etwa einer halben Minute steht Ihr Tunnel in der Liste unter **Networking** → **Tunnel** auf **Gesund** (*Healthy*, grün).

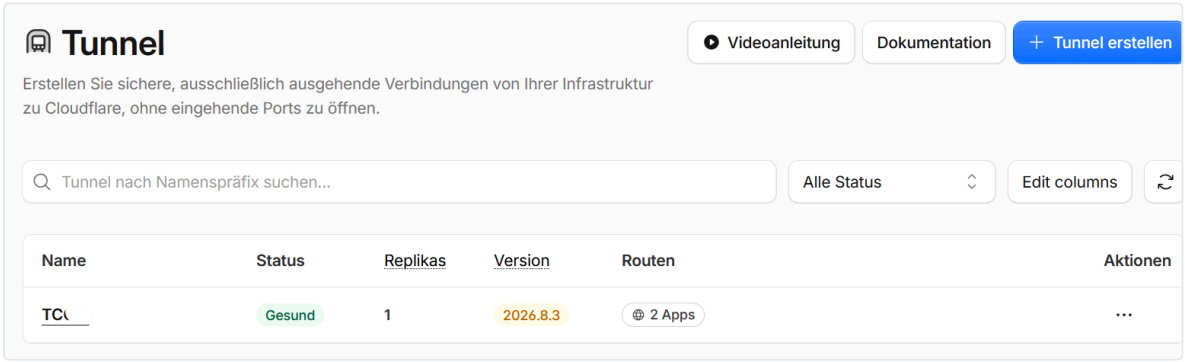


Bild 9 — Der Tunnel ist verbunden.

Bleibt der Status rot bzw. auf *Down* oder *Inactive*, siehe Abschnitt 12.

> **Zum Merken:** cloudflared aktualisiert sich unter Windows **nicht** von selbst. Tragen Sie sich eine Erinnerung ein, etwa halbjährlich nachzusehen (Abschnitt 11).

7. Schritt 5 — Die Weboberfläche veröffentlichen

Jetzt bekommt der Tunnel gesagt, wohin er die Anfragen weiterreichen soll.

1. Im Dashboard **Networking** → **Tunnel**, Ihren Tunnel anklicken.
2. Auf den Reiter **Routen**, dann **Route hinzufügen** → **Veröffentlichte Anwendung**. Es öffnet sich der Dialog *Veröffentlichte Anwendung hinzufügen*.
3. Adresse und Ziel eintragen:

Feld	Eintrag	
Subdomain	`tetra`	Oder ein anderer Name Ihrer Wahl
Domain	`ihre-domain.de`	Aus der Liste auswählen
Pfad (optional)	*leer lassen*	**Wichtig — siehe Kasten unten**
Dienst-URL	`https://localhost:3043`	Mit `https://` davor

Unter **Vollständiger Hostname** zeigt der Dialog zur Kontrolle die fertige Adresse — `tetra.ihre-domain.de`. Ein DNS-Eintrag ist nicht nötig, den legt Cloudflare selbst an.

Die Portnummer ist Ihr `SSLServerPort` aus den TETRAcontrol-Einstellungen. Läuft cloudflared ausnahmsweise auf einem *anderen* Rechner als TETRAcontrol, tragen Sie statt `localhost` die IP-Adresse des TETRAcontrol-Rechners ein.

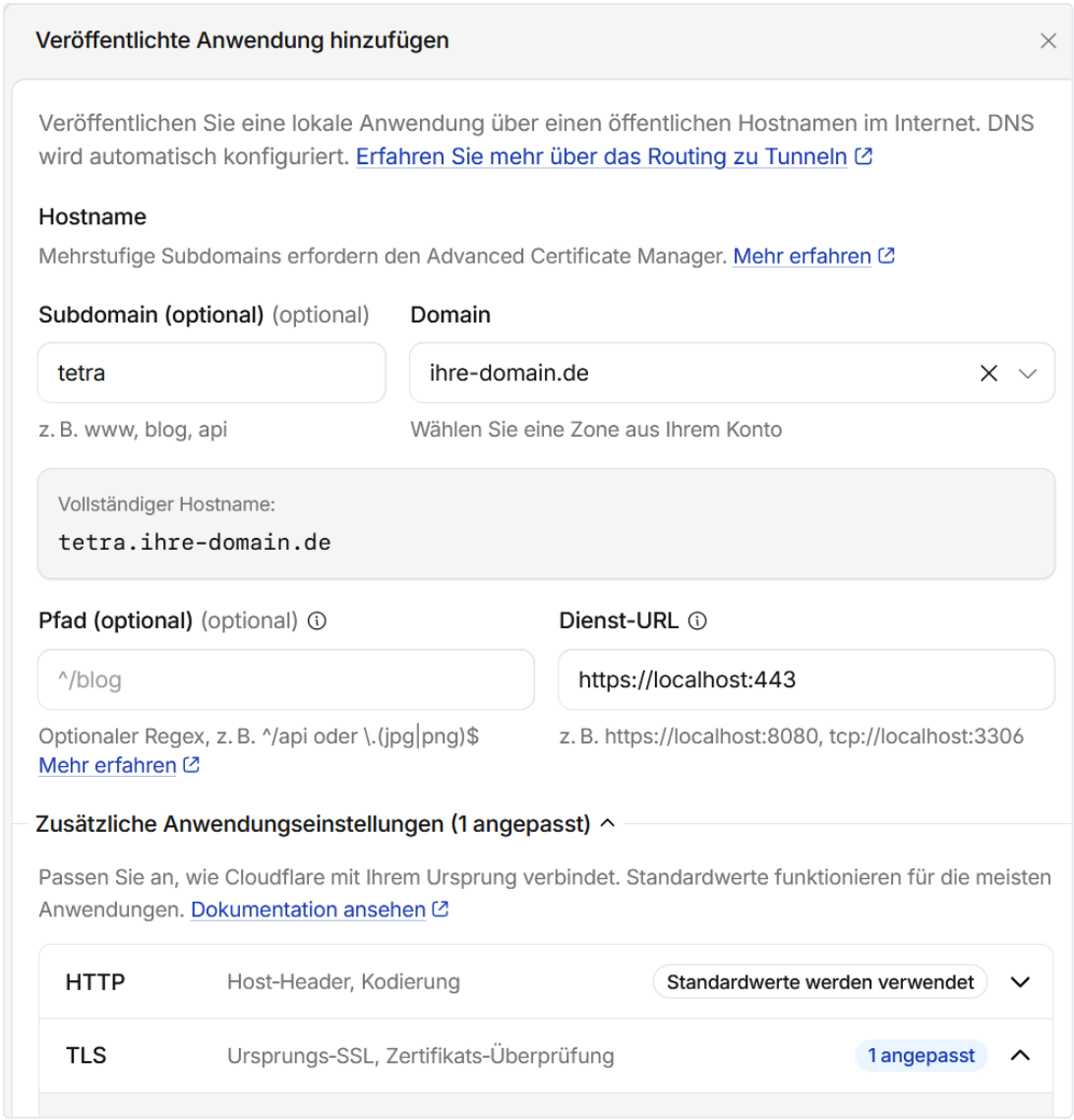


Bild 10 — Adresse und Ziel der Anwendung. Im Bild steht beispielhaft Port 443 — tragen Sie Ihren eigenen Port ein.

> **Das Feld `Pfad` bleibt leer.**
>
> Es liegt nahe, hier `/ui` einzutragen, weil die Oberfläche ja unter `/ui/` liegt. Tun Sie das nicht. Die Oberfläche holt sich ihre Live-Daten über eine WebSocket-Verbindung zu `/live.json` **im Wurzelverzeichnis**, und auch die Anmeldung läuft über `/login.now`. Beides läge außerhalb eines auf `/ui` eingeschränkten Pfades. Das Ergebnis wäre eine Oberfläche, die lädt, sich aber nicht anmelden lässt und keine Daten zeigt.

7.1 Die Zertifikatsprüfung abschalten — und warum das hier in Ordnung ist

TETRAcontrol benutzt für seinen HTTPS-Server ein selbst ausgestelltes Zertifikat. cloudflared kennt dessen Aussteller nicht und verweigert die Verbindung, solange Sie ihm das nicht abgewöhnen.

4. **Zusätzliche Anwendungseinstellungen** aufklappen → Abschnitt **TLS** (*Ursprungs-SSL, Zertifikats-Überprüfung*).
5. **TLS-Zertifikats-Überprüfung deaktivieren** einschalten.

Die übrigen Felder dieses Abschnitts — *Ursprungs-Server-Name*, *CA-Pool*, *TLS-Timeout* — bleiben leer, und die Schalter darunter bleiben aus.

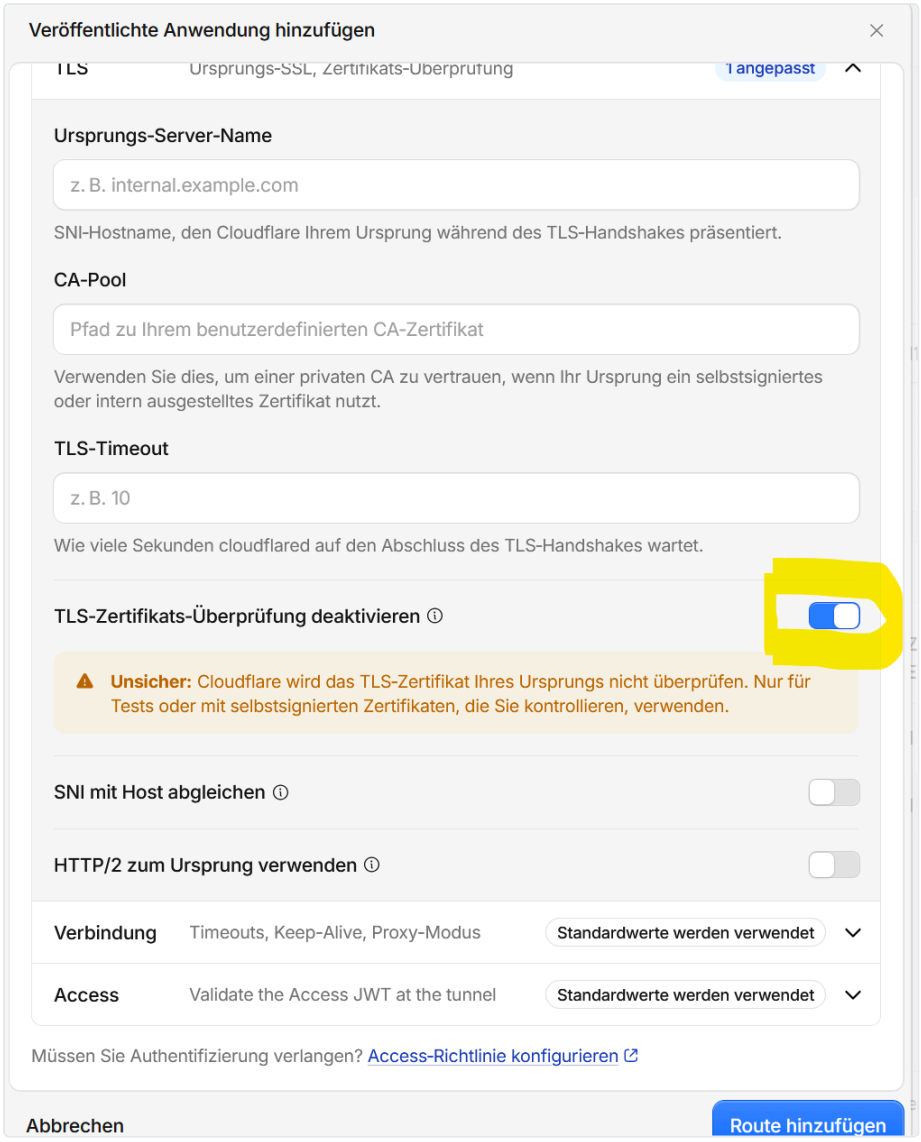


Bild 11 — Der Schalter, um den es geht.

Cloudflare warnt an dieser Stelle in Rot. Die Warnung ist berechtigt, trifft Ihren Fall aber nicht: Sie gilt Verbindungen, die durch ein unsicheres Netz laufen. Hier läuft die Verbindung von cloudflared zu TETRAcontrol über `localhost`, verlässt den Rechner also nie. Zwischen den beiden Programmen gibt es niemanden, der mithören könnte.

> **Läuft cloudflared auf einem anderen Rechner als TETRAcontrol**, gilt das nicht mehr — dann läuft die Verbindung durch Ihr Netz. Das ist in einem Dienststellennetz meist noch vertretbar, aber es ist eine bewusste Entscheidung. Die einfachere Lösung ist, cloudflared auf demselben Rechner zu betreiben.

6. Unten **Route hinzufügen** anklicken.

7.2 Erster Aufruf

Rufen Sie jetzt `https://tetra.ihre-domain.de/ui/` auf. Die Anmeldeseite von TETRAcontrol sollte erscheinen — diesmal ohne Zertifikatswarnung.

Wenn das klappt, ist die Oberfläche in diesem Moment für das gesamte Internet offen. Deshalb geht es direkt weiter mit Schritt 6. Legen Sie jetzt keine Pause ein.

> Um die Live-Daten müssen Sie sich nicht kümmern: Cloudflare reicht WebSocket-Verbindungen ohne weitere Einstellung durch. Die Oberfläche schickt alle 45 Sekunden ein Lebenszeichen, womit sie auch unterhalb der Zeitgrenzen bleibt, ab denen ruhende Verbindungen sonst getrennt würden.

8. Schritt 6 — Zugriff absichern

Jetzt kommt das Schloss vor die Tür: **Cloudflare Access**. Ab hier muss sich jeder, der die Adresse aufruft, erst bei Cloudflare ausweisen — sonst sieht er von TETRAcontrol nichts, nicht einmal die Anmeldeseite.

Wir richten die einfachste brauchbare Variante ein: **Anmeldung per Einmal-Code an eine E-Mail-Adresse**. Niemand muss ein weiteres Kennwort verwalten, und Sie pflegen nur eine Liste von Adressen.

8.1 Einmal-Code freischalten

1. Im Dashboard links auf **Zero Trust**. Beim ersten Aufruf fragt Cloudflare nach einem Teamnamen — wählen Sie etwas Kurzes wie `ffw-musterstadt`; er wird Teil der internen Anmeldeadresse. Als Tarif **Free** auswählen. *(Fragt Cloudflare dabei nach einer Zahlungsart, ist das für den kostenlosen Tarif unbedenklich — abgebucht wird nichts, solange Sie unter 50 Personen bleiben.)*
2. **Integrations** → **Identity providers** → **Add new**.
3. **One-time PIN** auswählen und speichern.

Mehr ist hier nicht einzustellen. In der Liste **Your identity providers** steht danach ein Eintrag *One-time PIN*; das genügt.

8.2 Die Anwendung anlegen

1. **Access controls** → **Applications** → **Add an application** *(je nach Stand der Oberfläche heißt die Schaltfläche Create new application)*.
2. Als Typ **Self-hosted** wählen — in neueren Fassungen heißt der Eintrag **Self-hosted and private**.
3. Einen Namen vergeben, etwa `TETRAcontrol Leitstelle`.
4. Unter **Public hostname** (bzw. **Add public hostname**) Ihre Adresse eintragen: Subdomain `tetra`, Domain `ihre-domain.de`, Pfad leer.
5. **Session Duration**: `24 hours` ist ein vernünftiger Anfang. Danach ist eine erneute Anmeldung fällig. Wer sein Gerät oft wechselt, wählt kürzer.

Die Adresse muss **genau** mit der aus Schritt 5 übereinstimmen. Ein Tippfehler führt nicht zu einer Fehlermeldung — er führt dazu, dass Access für Ihre Adresse gar nicht greift und die Oberfläche offen bleibt. Prüfen Sie diese Zeile zweimal.

8.3 Festlegen, wer hinein darf

Jetzt die eigentliche Regel:

1. Bei **Access policies** eine neue Richtlinie anlegen.
2. Name: zum Beispiel `Berechtigte Personen`.
3. **Action**: `Allow`.

4. Unter **Include** den Selektor **Emails** wählen und die E-Mail-Adressen eintragen, die Zugang bekommen sollen — eine pro Zeile.

> **Einzelne Adressen sind einer ganzen Domain vorzuziehen.** Cloudflare bietet auch *Emails ending in* `@ihre-domain.de` an. Das ist bequem, lässt aber jeden hinein, der irgendwann einmal eine Adresse Ihrer Dienststelle bekommt — auch wenn er mit dem Funk nichts zu tun hat. Bei einer überschaubaren Zahl von Personen pflegen Sie die Liste besser einzeln.

5. Speichern, dann die Anwendung speichern.

Access ist grundsätzlich verschlossen: Wer auf keine `Allow`-Regel passt, kommt nicht hinein. Sie müssen also niemanden ausdrücklich aussperren — Sie lassen nur ausdrücklich jemanden herein.

Der häufigste Fehler an dieser Stelle

> **Einmal-Code kommt nicht an?**
>
> Prüfen Sie, ob die berechtigte Adresse wirklich unter **Einschließen** → **E-Mails** (*Include* → *Emails*) eingetragen ist.
>
> Verwenden Sie **nicht allein Authentifizierungsmethode** → **One-time PIN** als Einschließen-Regel. Diese Auswahl legt keine berechtigte E-Mail-Adresse fest. Passt die eingegebene Adresse zu keiner `Allow`-Regel, versendet Cloudflare **keinen** Code — zeigt aus Sicherheitsgründen aber trotzdem an, es sei eine E-Mail gesendet worden.
>
> Man sucht dann im Spam-Ordner, während der Fehler in der Richtlinie sitzt.

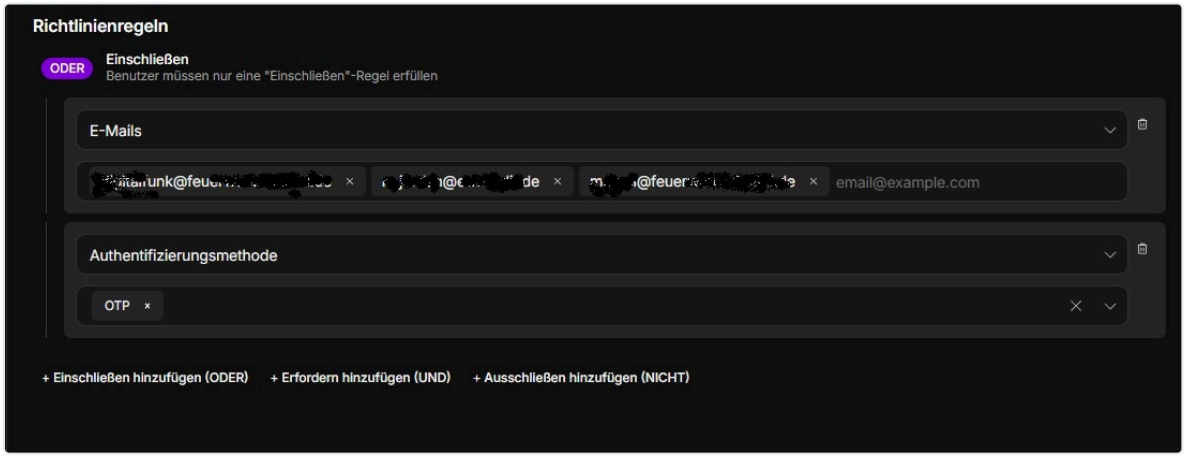


Bild 14 — Oben richtig, unten überflüssig: Die Liste unter E-Mails muss da sein. Die Zeile Authentifizierungsmethode darunter gehört nicht hierher — warum, steht im nächsten Kasten.

> ***Und wenn beides unter „Einschließen" steht, ist die E-Mail-Liste wirkungslos.***
>
> *Cloudflare verknüpft mehrere Einschließen-Regeln mit **ODER** — die Oberfläche schreibt es selbst dazu: „Benutzer müssen nur eine ‚Einschließen'-Regel erfüllen." Steht neben der E-Mail-Liste noch **Authentifizierungsmethode = OTP**, genügt folglich schon die Anmeldung per Einmal-Code, und die sorgfältig gepflegte Adressliste zählt nicht mehr.*
>
> *Cloudflare führt genau diesen Eintrag in seiner Dokumentation unter den häufigen Fehlkonfigurationen auf, mit der Folge: **jeder kommt hinein.***
>
> *Löschen Sie die Zeile **Authentifizierungsmethode** über das Papierkorbsymbol rechts. Wollen Sie den Einmal-Code ausdrücklich verlangen, gehört er unter **+ Erfordern hinzufügen (UND)** — dort wird er zur zusätzlichen Bedingung statt zur Alternative. Ist der Einmal-Code ohnehin Ihr einziges Anmeldeverfahren, brauchen Sie ihn auch dort nicht.*

***Verlassen Sie sich nicht darauf, sondern prüfen Sie es:** Test 2 im Abschlusstest (Abschnitt 10) ist genau dafür da — eine nicht freigegebene Adresse darf **nicht** hineinkommen.*

8.4 So erleben es Ihre Benutzer

Vor der gewohnten TETRAcontrol-Anmeldung liegt ab jetzt eine schlichte Seite mit dem Cloudflare-Zeichen, einem Feld für die E-Mail-Adresse und einer Schaltfläche darunter. Sie lässt sich nicht überspringen.

1. *Benutzer ruft `https://tetra.ihre-domain.de/ui/` auf.*
2. *Cloudflare fragt nach der E-Mail-Adresse.*
3. *Steht die Adresse in Ihrer Regel, kommt ein Einmal-Code per Mail (10 Minuten gültig, einmal verwendbar). Steht sie nicht darin, kommt **keine** Mail und der Zugang bleibt verschlossen — die Seite behauptet dann trotzdem, eine E-Mail sei unterwegs. Das ist Absicht: Sonst könnte man an dieser Stelle ausprobieren, welche Adressen berechtigt sind.*
4. *Code eingeben → jetzt erst erscheint die Anmeldeseite von TETRAcontrol.*
5. *Dort wie gewohnt mit Benutzername und Kennwort anmelden.*

Für die nächsten 24 Stunden entfällt Schritt 2 bis 4 auf diesem Gerät.

9. Schritt 7 — Die Domain absichern

Access entscheidet, wer hineindarf. Anklopfen darf aber weiterhin die ganze Welt, und der größte Teil dessen, was anklopft, sind die Automaten aus Abschnitt 2.2.

Dagegen gibt es drei Einstellungen, alle kostenlos:

- *eine **Länderregel**, die alles außer Deutschland gar nicht erst durchlässt,*
- *eine **Durchsatzbegrenzung**, die das schnelle Durchprobieren von Kennwörtern an der TETRAcontrol-Anmeldung ausbremst,*
- *die **Bot-Einstellungen**, die bekannte Automaten und KI-Crawler abweisen.*

*Alle drei gehören **zur Domain**, nicht zum Tunnel und nicht zu Zero Trust. Sie gelten damit für alles, was unter dieser Domain erreichbar ist.*

9.1 Alle Länder außer Deutschland sperren

***Die Empfehlung lautet: von Anfang an alle Länder außer Deutschland sperren.** Das kostet fünf Minuten und nimmt einem großen Teil der möglichen Angreifer die Gelegenheit.*

1. *Im Cloudflare-Dashboard **Ihre Domain** anklicken — nicht Zero Trust, sondern die Domainübersicht.*
2. *Links **Sicherheit** → **Sicherheitsregeln**.*
3. *Rechts oben **Regel erstellen** → **Benutzerdefinierte Regeln**.*
4. *Einen Namen vergeben, etwa `DE`, und als Beschreibung `Land ungleich DE`.*
5. *Die Bedingung zusammenklicken:*

Feld	*Land*
Operator	*ungleich*
Wert	*Deutschland*

6. *Unter Dann Aktion ausführen als Aktion **Blockieren** wählen.*
7. *Speichern und bereitstellen.*

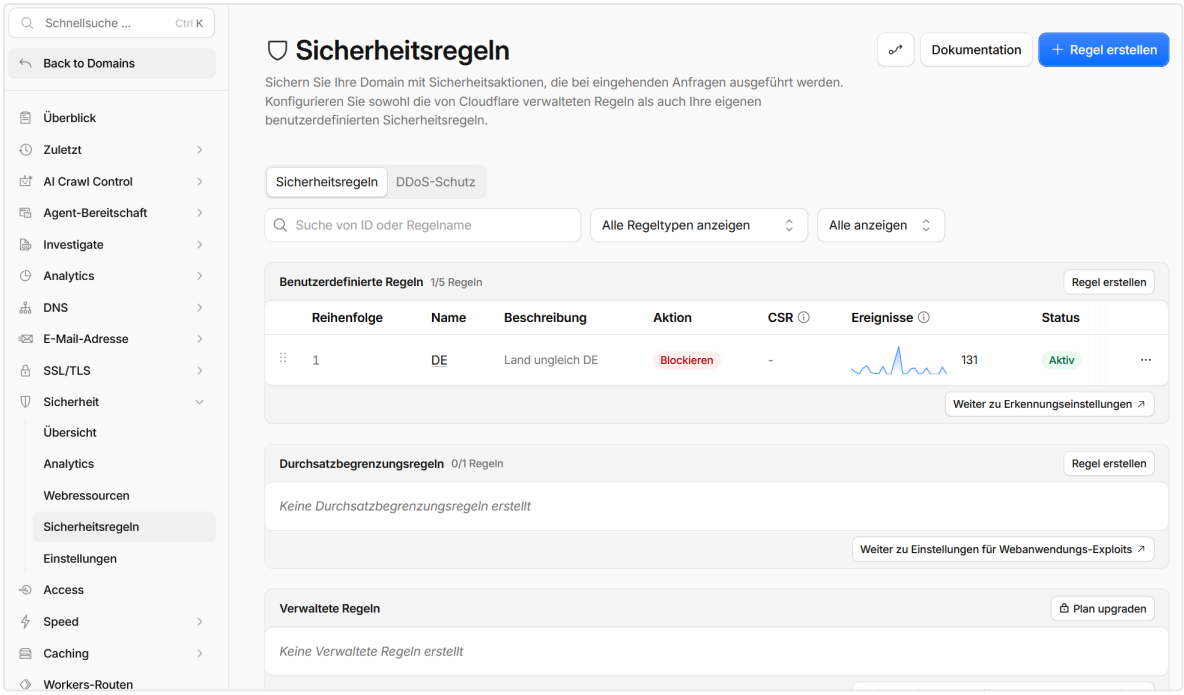


Bild 12 — Die fertige Länderregel. Die Zackenlinie unter „Ereignisse" zeigt, wie viel dadurch gar nicht erst durchkommt. Darunter liegt der Block für die Durchsatzbegrenzung aus Abschnitt 9.4.

Wer lieber tippt, schaltet im Regeleditor auf den Ausdruckseditor um:

```
(ip.src.country ne "DE")
```

Sollen Österreich und die Schweiz mit hinein:

```
(not ip.src.country in {"DE" "AT" "CH"})
```

9.2 Zwei Dinge, die Sie vorher wissen sollten

> ***Sie sperren damit auch die eigenen Leute aus, sobald sie im Ausland sind.*** *Urlaub, Lehrgang, eine Mobilfunkzelle jenseits der Grenze, ein dienstliches VPN, das im Ausland herauskommt — in allen diesen Fällen kommt statt der Anmeldeseite eine Sperrseite von Cloudflare.*
>
> *Planbare Fälle lösen Sie, indem Sie das Land in der Regel ergänzen. Für den Einzelfall lässt sich die Regel unter* ***Status*** *kurz auf inaktiv stellen — aber bitte daran denken, sie wieder einzuschalten.*
>
> ***Die Regel gilt für die gesamte Domain.*** *Liegt darauf noch etwas anderes, etwa die Internetseite der Dienststelle, ist auch die aus dem Ausland nicht mehr erreichbar. Wollen Sie nur TETRAcontrol einschränken, hängen Sie den Hostnamen an die Bedingung:*
>
> ```
> (ip.src.country ne "DE" and http.host eq "tetra.ihre-domain.de")
> ```

9.3 Was die Länderregel leistet — und was nicht

Die Sperre nimmt Ihnen den Großteil des automatisierten Verkehrs ab, und zwar ohne dass davon irgendetwas Ihren Rechner erreicht: Eine blockierte Anfrage wird bei Cloudflare abgewiesen, sie läuft weder durch den Tunnel noch an TETRAcontrol.

*Sie ist aber **kein Ersatz für Access**. Wer es gezielt auf Sie abgesehen hat, mietet sich für ein paar Euro einen Server in Deutschland oder nimmt ein VPN mit deutschem Ausgang, und schon steht er wieder vor der Tür. Auch die Zuordnung von Adressen zu Ländern ist nicht fehlerfrei. Die Länderregel siebt das Grundrauschen aus; die Tür bleibt Access.*

9.4 Anmeldeversuche begrenzen

*Auf derselben Seite gibt es unter **Durchsatzbegrenzungsregeln** eine zweite Art von Regel. Sie zählt Anfragen je Absender-IP und schreitet ein, wenn zu viele in zu kurzer Zeit kommen. Der klassische Fall dafür ist genau unserer: die Anmeldung.*

Das Anmeldeformular von TETRAcontrol schickt seine Daten an `/Login.now`. Das ist der Pfad, den die Regel beobachtet.

> ***Was im kostenlosen Tarif nicht geht — damit Sie nicht vergeblich suchen.***
>
> *Dort sind **Zeitraum und Sperrdauer fest auf 10 Sekunden** eingestellt; wählbar ist nur die Anzahl der Anfragen. „Fünf Versuche pro Minute, danach eine Stunde Sperre" verlangt also den kostenpflichtigen **Pro-Tarif**.*
>
> *Und: Eine **Challenge lässt sich unterhalb von Enterprise nicht mit einer Sperrdauer verbinden** — Challenge-Aktionen drosseln immer nur. Wer für eine Stunde sperren will, muss als Aktion **Blockieren** wählen.*

	Kostenlos (Free)	***Pro***
Zeitraum	*fest 10 Sekunden*	*bis 1 Minute*
Sperrdauer	*fest 10 Sekunden*	*bis 1 Stunde*
Felder in der Bedingung	*nur Pfad*	*Host, URI, Pfad, Query*
Anzahl Regeln	*1*	*2*

***So legen Sie die Regel an** (die Werte in Klammern gelten für den kostenlosen Tarif):*

1. *Domain → **Sicherheit** → **Sicherheitsregeln**.*
2. ***Regel erstellen** → **Durchsatzbegrenzungsregeln**.*
3. *Name: etwa `Anmeldeversuche`.*
4. *Bedingung: Feld **Pfad**, Operator **ist gleich**, Wert `/Login.now`.*
5. *Mit denselben Merkmalen: **IP** — im kostenlosen Tarif die einzige Wahl.*
6. *Wenn die Rate überschreitet: **5** Anfragen pro **1 Minute** (kostenlos: pro 10 Sekunden).*
7. *Dann Aktion ausführen: **Blockieren**.*
8. *Für die Dauer: **1 Stunde** (kostenlos: fest 10 Sekunden).*
9. *Bereitstellen.*

Im Ausdrucksеditor lautet die Bedingung:

```
(http.request.uri.path eq "/login.now")
```

Weil die Regel nur auf diesen einen Pfad passt, bleiben die Live-Daten unberührt: Der WebSocket auf `/live.json` *und alle übrigen Seiten werden nicht mitgezählt.*

> ***Access steht davor.*** *Wer keine gültige Access-Sitzung hat, kommt überhaupt nicht bis zur TETRAcontrol-Anmeldung. Diese Regel wirkt also vor allem gegen jemanden, der Access bereits passiert hat — etwa weil ein E-Mail-Postfach übernommen wurde. Sie ist die dritte Lage, nicht die erste. Wegzulassen ist sie deswegen trotzdem nicht: Sie greift auch dann noch, wenn an Access einmal etwas verstellt wurde.*
>
> ***Gezählt wird pro IP-Adresse — und zwar jeder Aufruf.*** *Zwei Folgen daraus:*
>
> *Sitzt die ganze Dienststelle hinter einem Anschluss, teilen sich alle denselben Zähler. Melden sich nach einem Neustart mehrere gleichzeitig an, ist eine Grenze von fünf schnell erreicht. Setzen Sie im Zweifel großzügiger an — zehn pro Minute halten das maschinelle Durchprobieren immer noch auf, sperren aber niemanden versehentlich für eine Stunde aus.*
>
> *Cloudflare sieht außerdem nicht, ob eine Anmeldung geglückt ist; gezählt werden geglückte und misslungene gleichermaßen. Nur die Fehlversuche zu zählen — über den Antwortcode — gibt es erst ab dem Business-Tarif.*

Und im kostenlosen Tarif? *Aus „fünf Versuche, dann eine Stunde Ruhe" wird „fünf Versuche je zehn Sekunden". Das nimmt dem Durchprobieren die Geschwindigkeit — statt tausender Versuche je Minute bleiben rund dreißig —, sperrt aber niemanden aus. Als alleiniger Schutz wäre das zu wenig. Hinter Access und der Länderregel ist es eine sinnvolle dritte Lage, und sie kostet nichts.*

9.5 Bot Fight Mode und die KI-Bot-Richtlinien

Diese beiden Schalter liegen nicht bei den Regeln, sondern eine Ebene daneben, unter ***Sicherheit*** *→* ***Einstellungen*** *(Security → Settings). Beide sind im kostenlosen Tarif enthalten.*

Bot Fight Mode

Auf der Einstellungsseite nach ***Bot-Verkehr*** *filtern und* ***Bot fight mode*** *einschalten. Cloudflare erkennt dann Anfragen, die den Mustern bekannter Automaten folgen, und stellt ihnen eine rechenaufwendige Aufgabe. Für einen Massenscanner, der Millionen Adressen abklappert, wird das unwirtschaftlich; ein normaler Browser merkt nichts davon.*

> ***Ein Vorbehalt, den Sie vorher kennen sollten.*** *Bot Fight Mode lässt sich* ***nicht einschränken*** *— keine benutzerdefinierte Regel und keine Ausnahmeliste greift daran vorbei. Cloudflare schreibt selbst, dass dabei auch API- oder App-Zugriffe getroffen werden können.*
>
> *Für die Weboberfläche im Browser ist das unkritisch. Rufen Sie über dieselbe Adresse aber das* ***HTTP-API von TETRAcontrol*** *ab — aus einem Skript, einer Alarmweitergabe oder einer Überwachung —, kann Bot Fight Mode diese Zugriffe abweisen, und der Fehler ist von außen schwer zu deuten. Dann bleibt nur, den Schalter wieder auszuschalten; Ausnahmen gibt es erst mit Super Bot Fight Mode ab dem Pro-Tarif.*
>
> *Ob tatsächlich etwas hängenbleibt, sehen Sie unter* ***Sicherheit*** *→* ***Analytics*** *im Reiter Events: Betroffene Anfragen tragen im Feld Service den Eintrag „Bot Fight Mode".*

Mit Bot Fight Mode schaltet Cloudflare zwangsweise die JavaScript Detections mit ein und fügt dafür eine kleine Prüfroutine in die ausgelieferten Seiten ein. Das kollidiert gelegentlich mit einer Content-Security-Policy — die WebUI von TETRAcontrol setzt keine, hier ist also nichts zu beachten.

KI-Bot-Richtlinien

Auf derselben Seite ***Configure AI bot policies*** *öffnen. Cloudflare unterscheidet drei Arten von KI-Zugriffen:*

Kategorie	***Was dahintersteckt***
Search	*Bots, die Inhalte für Suchergebnisse erfassen*
Agent	*Bots, die im Auftrag eines Menschen in Echtzeit Inhalte abrufen*
Training	*Crawler, die Inhalte zum Trainieren von KI-Modellen sammeln*

Für eine Leitstelle gibt es in keiner der drei Kategorien etwas zu holen: alle drei auf ***Block*** *stellen und* ***Save****.*

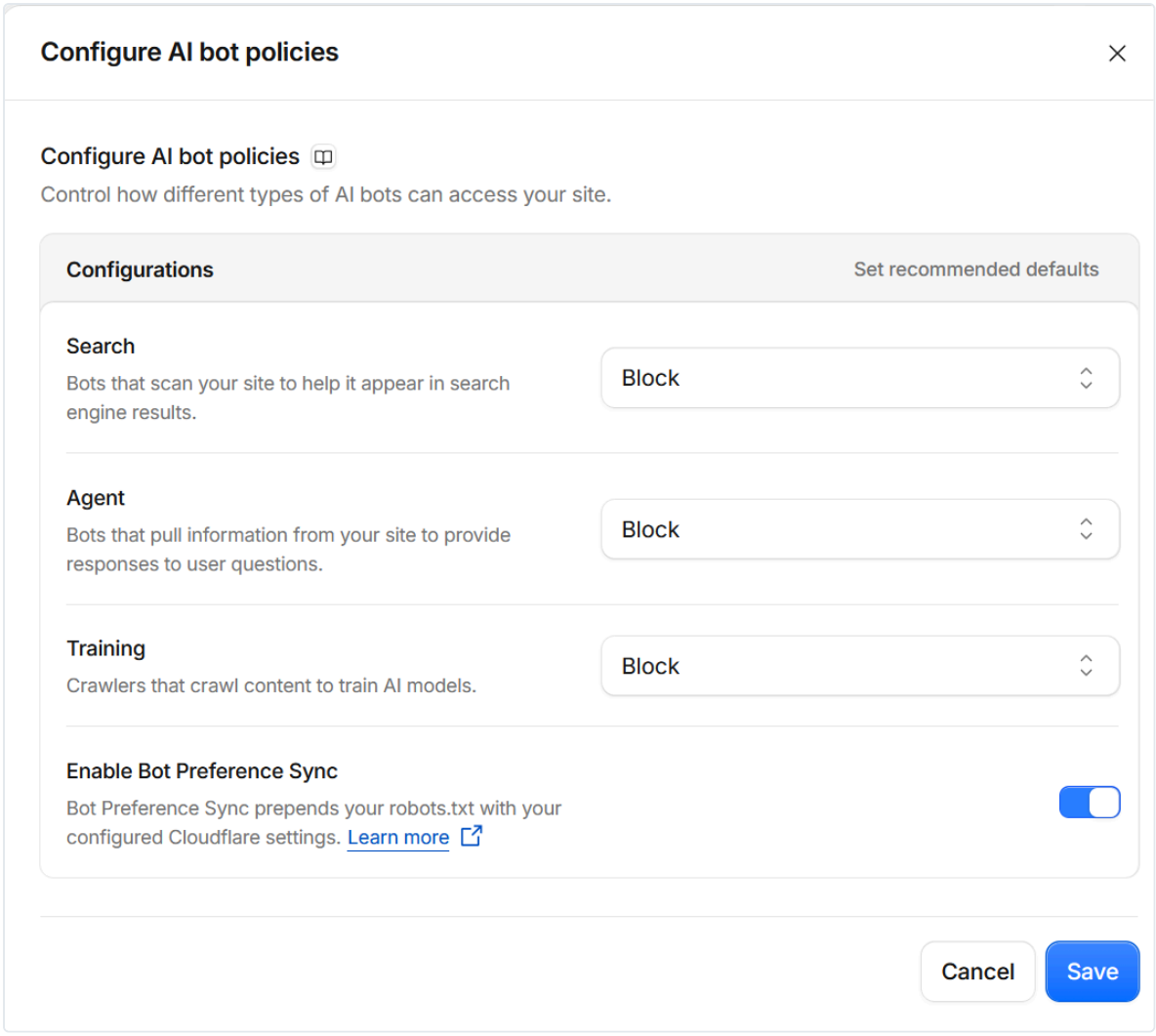


Bild 13 — Alle drei Kategorien auf „Block".

Die Schaltfläche Set recommended defaults setzt Cloudflares eigene Empfehlung ein. Die lässt Suchmaschinen zu und ist für eine öffentliche Website gedacht — nicht für diese. Stellen Sie die drei Werte von Hand.

*Der Schalter **Enable Bot Preference Sync** stellt Ihre Entscheidung zusätzlich der `robots.txt` der Domain voran. Das ist eine Bitte an gutwillige Crawler, kein Zwang; schaden kann es nicht.*

> ***Beides ist hier ehrlicherweise Beiwerk.** Hinter Access kommt ohnehin kein Crawler an Inhalte — er bekommt die Anmeldeseite von Cloudflare zu sehen und sonst nichts. Der Gewinn liegt darin, dass die Einstellung für die **ganze Domain** gilt, also auch für das, was dort sonst noch ohne Access erreichbar ist. Zwei Minuten Aufwand, die man mitnehmen kann — aber keine Lage, auf die Sie sich verlassen sollten.*

9.6 Was der kostenlose Tarif hergibt

Benutzerdefinierte Regeln	*5 Stück — für die Länderregel reicht eine*
Durchsatzbegrenzungsregeln	*1 Stück — die Anmelderegel aus 9.4, mit fest 10 Sekunden*

Bot Fight Mode	*Enthalten, aber ohne jede Ausnahmemöglichkeit*
KI-Bot-Richtlinien	*Enthalten*
Verwaltete Regeln	*Nur in kostenpflichtigen Tarifen; hier nicht nötig*

*Unter **Sicherheit** → **Analytics** sehen Sie später, was die Regel abgefangen hat. Ein Blick dorthin nach der ersten Woche ist aufschlussreich.*

10. Abschlusstest

*Bitte einmal vollständig durchgehen — am besten von einem Mobiltelefon **über Mobilfunk**, nicht über das WLAN der Dienststelle. Nur so testen Sie wirklich den Weg von außen.*

#	Test	Erwartet
1	`https://tetra.ihre-domain.de/ui/` *in einem **privaten Fenster** aufrufen*	*Anmeldeseite von **Cloudflare**, nicht von TETRAcontrol*
2	*Eine **nicht** freigegebene Adresse eingeben*	*Es kommt keine Mail und **kein Zugang** — auch wenn die Seite das Gegenteil andeutet. Kommt man hinein, ist die Richtlinie falsch: siehe 8.3*
3	*Eine freigegebene Adresse eingeben, Code eintragen*	*Jetzt die Anmeldeseite von TETRAcontrol*
4	*Mit einem TETRAcontrol-Benutzer anmelden*	*Die Ereignisliste erscheint*
5	*Verbindungsanzeige oben prüfen*	***Grün** — der WebSocket steht*
6	*Ein Funkgerät sendet einen Status*	*Der Eintrag erscheint innerhalb von Sekunden, ohne Neuladen*
7	*Kartenansicht öffnen*	*Positionen und Symbole werden angezeigt*
8	*Statuspanel öffnen*	*Kacheln erscheinen vollständig*
9	*Am Router nachsehen*	***Keine** Portfreigabe für TETRAcontrol vorhanden*
10	*Sicherheit → Sicherheitsregeln aufrufen*	*Die Länderregel steht auf **Aktiv***

Test 5 und 6 sind die wichtigsten. Sie zeigen, dass nicht nur Seiten geladen werden, sondern die Live-Verbindung wirklich durch den Tunnel läuft.

11. Laufender Betrieb

Jemanden hinzufügen oder entfernen

Zero Trust → ***Access controls*** → ***Applications*** → *Ihre Anwendung → Richtlinie bearbeiten → Adresse ergänzen oder streichen → speichern. Das wirkt sofort.*

Scheidet jemand aus, ***streichen Sie ihn hier zuerst*** *und erst danach in* `Benutzer.csv`*. Ein bereits angemeldetes Gerät bleibt sonst bis zum Ablauf der Sitzungsdauer drin.*

cloudflared aktuell halten

cloudflared aktualisiert sich unter Windows nicht selbst. Halbjährlich nachsehen, oder wenn etwas nicht mehr funktioniert:

```
bash cloudflared.exe --version
```

Zum Aktualisieren die neue Fassung installieren (`winget upgrade --id Cloudflare.cloudflared`*) und den Dienst neu starten:*

```
bash sc stop cloudflared
```

```
bash sc start cloudflared
```

Der Tunnel bleibt dabei bestehen; es ändert sich nur das Programm. Ein kurzer Ausfall während des Neustarts ist normal.

Wenn der Rechner umzieht

Kommt TETRAcontrol auf einen anderen Rechner, installieren Sie cloudflared dort mit demselben Befehl aus Schritt 4 — der Token bleibt gültig. Auf dem alten Rechner den Dienst entfernen:

```
bash cloudflared.exe service uninstall
```

Was Sie sich aufschreiben sollten

Cloudflare-Konto (E-Mail), Domainname, Tunnelname, verwendeter Port, und wo die Wiederherstellungscodes der Zwei-Faktor-Anmeldung liegen. Abschnitt 14 hat dafür eine Vorlage.

12. Wenn etwas nicht geht

Sie sehen	Ursache	Abhilfe
Error 1033 oder „Tunnel not found"	cloudflared läuft nicht oder erreicht Cloudflare nicht	`services.msc` : Dienst Cloudflare Tunnel starten. Kommt der Rechner überhaupt ins Internet?
Error 502 Bad Gateway	Der Tunnel steht, aber TETRAcontrol antwortet nicht	Läuft TETRAcontrol? Stimmt die Portnummer? Ist `SSLServerPort` gesetzt?
502, obwohl alles läuft	Die Zertifikatsprüfung ist noch an	Abschnitt 7.1 — TLS-Zertifikats-Überprüfung deaktivieren einschalten
Seite lädt, aber **keine Daten**, Anzeige bleibt gelb	Im Feld `Pfad` steht etwas	Abschnitt 7, `Pfad` leeren und speichern
Anmeldung bei TETRAcontrol schlägt immer fehl	ebenfalls ein eingetragener `Pfad`	wie oben
Kein Einmal-Code kommt an, obwohl die Seite den Versand bestätigt	Die Adresse steht nicht unter Einschließen → E-Mails	Abschnitt 8.3 — der häufigste Einrichtungsfehler. Erst danach den Spam-Ordner prüfen
Anmeldeseite von TETRAcontrol **ohne** Cloudflare-Abfrage davor	Access greift für diese Adresse nicht	Abschnitt 8.2: Stimmt der eingetragene Hostname genau?
Tunnel bleibt **Down** nach der Installation	Der Token wurde unvollständig eingefügt	Befehl erneut aus dem Dashboard kopieren, `cloudflared.exe service uninstall` , dann neu installieren
Domain lässt sich in Schritt 5 nicht auswählen	Die Domain ist noch nicht **Active**	Abschnitt 4 — auf die Bestätigungsmail warten
Alles war in Ordnung, seit heute **Error 1033**	Rechner neu gestartet und Dienst nicht hochgekommen, oder Internetausfall	`services.msc` prüfen; Starttyp muss Automatisch sein
Sperrseite von Cloudflare statt der Anmeldung, nur bei einzelnen Personen	Diese Person ist gerade im Ausland — die Länderregel greift	Abschnitt 9.2; Land ergänzen oder Regel kurz deaktivieren
Nach mehreren Anmeldeversuchen kommt gar keine Antwort mehr	Die Durchsatzbegrenzung hat die Adresse gesperrt	Ablauf der Sperrdauer abwarten; ist die Grenze zu eng, in Abschnitt 9.4 heraufsetzen

Sie sehen	*Ursache*	*Abhilfe*
Der Browser geht, aber ein Skript oder eine Überwachung am HTTP-API wird abgewiesen	*Bot Fight Mode hält den Zugriff für einen Automaten*	*Sicherheit → Analytics, Reiter Events prüfen; trifft es zu, Bot Fight Mode abschalten (Abschnitt 9.5)*

Wo Sie nachsehen können: *Im Cloudflare-Dashboard zeigt der Tunnel unter dem Reiter* ***Connectors*** *die letzten Verbindungsereignisse. Auf dem Rechner protokolliert TETRAcontrol jeden Zugriff in* `Logs\HTTP_<Datum>.Log` *— dort sehen Sie, ob eine Anfrage überhaupt angekommen ist. Das trennt die beiden Hälften des Weges sauber voneinander.*

13. Was Sie sich damit einhandeln

Zur Vollständigkeit gehört, was diese Lösung nicht kann und was Sie bedenken sollten.

Cloudflare sieht die Daten. *Die HTTPS-Verbindung des Benutzers endet bei Cloudflare, dort werden die Daten entschlüsselt und für den Tunnel neu verschlüsselt. Technisch ist Cloudflare also in der Lage, Statusmeldungen, Gesprächsdaten und GPS-Positionen im Klartext zu sehen. Das ist bei jedem solchen Dienst so und lässt sich im Rahmen dieser Lösung nicht ändern.*

Datenschutz. *Sie leiten damit personenbezogene Daten — Positionen von Einsatzkräften, Alarmierungen — über einen Dienstleister. Dafür ist ein Auftragsverarbeitungsvertrag nötig; Cloudflare stellt einen bereit. Ob die Verarbeitung außerhalb der EU für Ihre Einsatzdaten zulässig ist, entscheidet nicht diese Anleitung — sprechen Sie mit Ihrem Datenschutzbeauftragten, bevor Sie in den Dauerbetrieb gehen. Wenn eine Verarbeitung ausschließlich in der EU verlangt wird, bietet Cloudflare das an, allerdings nur in kostenpflichtigen Tarifen.*

Access schützt den Eingang, nicht den Server. *Wer die Prüfung passiert hat, trifft auf denselben Webserver wie im eigenen Netz — mit allem, was er kann und was er nicht kann. Access verschiebt die Verteidigung nach außen, es härtet nichts dahinter. Das ist vertretbar, solange der Kreis der Berechtigten klein und namentlich bekannt ist. Je größer dieser Kreis wird, desto weniger trägt diese Rechnung.*

Bis 50 Personen kostenlos. *Darüber hinaus wird Access kostenpflichtig.*

Kein zugesicherter Betrieb. *Der kostenlose Tarif kommt ohne Verfügbarkeitszusage. Für den gelegentlichen Blick von unterwegs ist das angemessen.* ***Als alleinigen Weg zu einsatzkritischen Informationen sollten Sie ihn nicht einplanen*** *— die Windows-Oberfläche in der Dienststelle bleibt der verlässliche Zugang.*

Ein Tab, eine Verbindung. *Jeder geöffnete Tab hält eine eigene WebSocket-Verbindung und belastet den Server. Für Wandmonitore ein Tab je Anzeige, nicht mehr. Das gilt über den Tunnel genauso wie im eigenen Netz.*

14. Spickzettel

*Zum Ausfüllen und Verwahren — aber **nicht** offen neben dem Rechner.*

Cloudflare-Konto (E-Mail)	.....
Wiederherstellungscodes 2FA liegen	.....
Domainname	.....
Öffentliche Adresse	`https://` ..... `/ui/`
Tunnelname in Cloudflare	.....
Rechner mit cloudflared	.....
`SSLServerPort` *von TETRAcontrol*	.....
Eingerichtet am / von	.....
cloudflared zuletzt aktualisiert	.....

Wichtigste Handgriffe

Aufgabe	***Weg***
Jemanden freischalten	*Zero Trust → Access controls → Applications → Richtlinie → **Einschließen** → **E-Mails***
Jemanden aussperren	*ebenda, Adresse streichen — wirkt sofort*
Tunnelzustand ansehen	*Networking → Tunnel*
Ziel oder Port ändern	*Networking → Tunnel → Tunnel → **Routen***
Dienst neu starten	`sc stop cloudflared` / `sc start cloudflared`
Land freigeben oder sperren	*Domain → Sicherheit → **Sicherheitsregeln** → Regel* `DE`
Anmeldesperre ändern	*ebenda, unter **Durchsatzbegrenzungsregeln***
Bot-Einstellungen	*Domain → Sicherheit → **Einstellungen***
Alles abschalten	*Dienst Cloudflare Tunnel beenden — die Adresse ist sofort tot*

Weiterführend

- `Dokumentation\WebUI_Betrieb.md` — *Betrieb der Weboberfläche, Berechtigungen, Konfiguration und Störungssuche innerhalb von TETRAcontrol*
- `Dokumentation\Anleitung_TETRAcontrol_HTTP-API.pdf` — *der eingebaute Webserver im Detail*
- *developers.cloudflare.com/cloudflare-one — Cloudflare-Dokumentation (englisch)*