Cloudflare Reverse Tunnel

A simple explanation of reverse tunnels, how Cloudflare Tunnel works, how to deploy it, and why it is secure.

1. What is a reverse Tunnel?

A reverse tunnel is a secure, outbound-only connection created from your server to a trusted relay (such as Cloudflare).
It reverses the traditional idea of “clients connect to the server” by letting the server initiate the connection.

Normal connection (inbound)

User → Internet → Server Public IP → Server Port

Reverse tunnel (outbound)

Server → Cloudflare (outbound tunnel)

Then:
User → Cloudflare → Tunnel → Server (localhost)

Simple analogy:

Imagine your server is a house with the door locked from the outside.

No matter how hard visitors knock, they cannot come in because the house refuses to open the door to people without VPN or UWnets.

This is like a server behind:

- a firewall
- no public IP
- no open ports

Visitors cannot reach the server directly.

Normal connection (inbound)

In a normal situation:

> Visitors walk to your house, knock on the door, and you open it for them.

This requires:

- your house door (port) to be unlocked and reachable
- a clear address (public IP)
- no walls blocking the way

⭐ Reverse tunnel analogy

Imagine our server is a house whose door cannot be opened from the outside.

Visitors cannot come in no matter how hard they knock.

So the house does something clever:

> It throws a long rope out to a public meeting point (Cloudflare).

This rope is the only safe, approved way back into the house.

But visitors cannot directly grab the rope.

Instead:

1. **Visitors must go to the meeting point first.**
2. **At the meeting point, a guard checks who they are**
    - Are they allowed in?
    - Are they on the list?
    - Do they have proper identification? (Zero Trust / Access policy)
3. **Only approved visitors are guided onto the rope.**
4. **They follow the rope back to the house safely.**

Even though the house never opened its door to the public.

> ***We already have the account identification in openwebui, so we don't need the zero trust one for now.***

Mapping the analogy to reality

- **The rope = Cloudflare Tunnel**
- **The meeting point = Cloudflare Edge Network**
- **The guard checkinglist = Cloudflare Access / Zero Trust authentication**
- **Visitors = Users trying to access our application**
- **The house = Our server (VM) which stays fully closed to the public**

Key idea:

Instead of exposing a public IP for the world to reach,
your server dials out, and Cloudflare becomes the public entry point.

This eliminates the need for:

- opening ports
- public IP address exposure
- firewall adjustments
- DDNS
- manual TLS certificates

In our case, the uwnet firewall does not need to open any inbound ports to the public.

2. Compare to normal HTTPS

> Normal HTTPS exposes the server to the world;
> Cloudflare Tunnel exposes Cloudflare to the world, and Cloudflare privately connects to the server.

⭐ Side-by-side comparison table

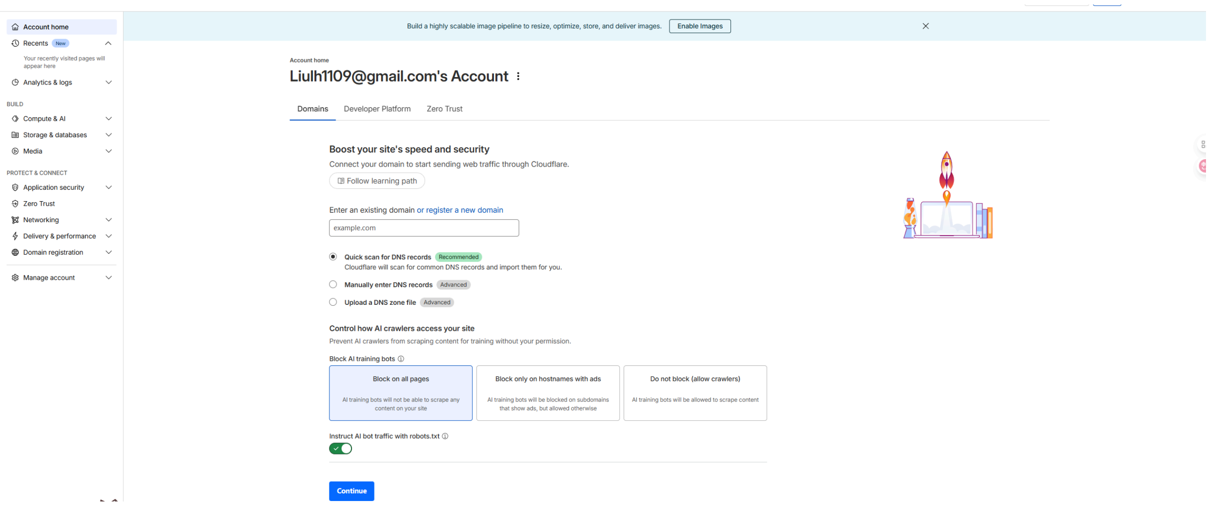
Feature	Normal HTTPS	Cloudflare Tunnel
Public IP required	Yes	No
Open ports	Required (443/80)	None
SSL certificates	Manual / Certbot	Automatic
Firewall	Must allow inbound	No inbound rules

Feature	Normal HTTPS	Cloudflare Tunnel
Exposure	Server visible to internet	Hidden behind Cloudflare
DDoS handling	Server must absorb	Cloudflare absorbs
DDNS needed	Yes, if IP changes	No
Maintenance	Medium to high	Very low

3. How to Implement Cloudflare Tunnel (Step-by-Step)

Register a team

Here is the page after you login into the cloudfare



Build a highly scalable image pipeline to resize, optimize, store, and deliver images.

Account home

Liulh1109@gmail.com's Account

Boost your site's speed and security

Connect your domain to start sending web traffic through Cloudflare.

Enter an existing domain or register a new domain

example.com

● Quick scan for DNS records Recommended
Cloudflare will scan for common DNS records and import them for you.

○ Manually enter DNS records Advanced

○ Upload a DNS zone file Advanced

Control how AI crawlers access your site

Prevent AI crawlers from scraping content for training without your permission.

Block AI training bots

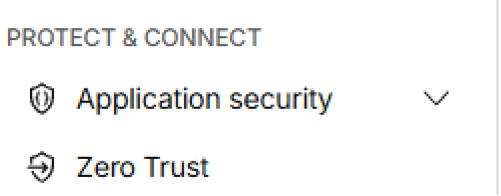
Block on all pages
AI training bots will not be able to scrape any content on your site

Block only on hostnames with ads
AI training bots will be blocked on subdomains that show ads, but allowed otherwise

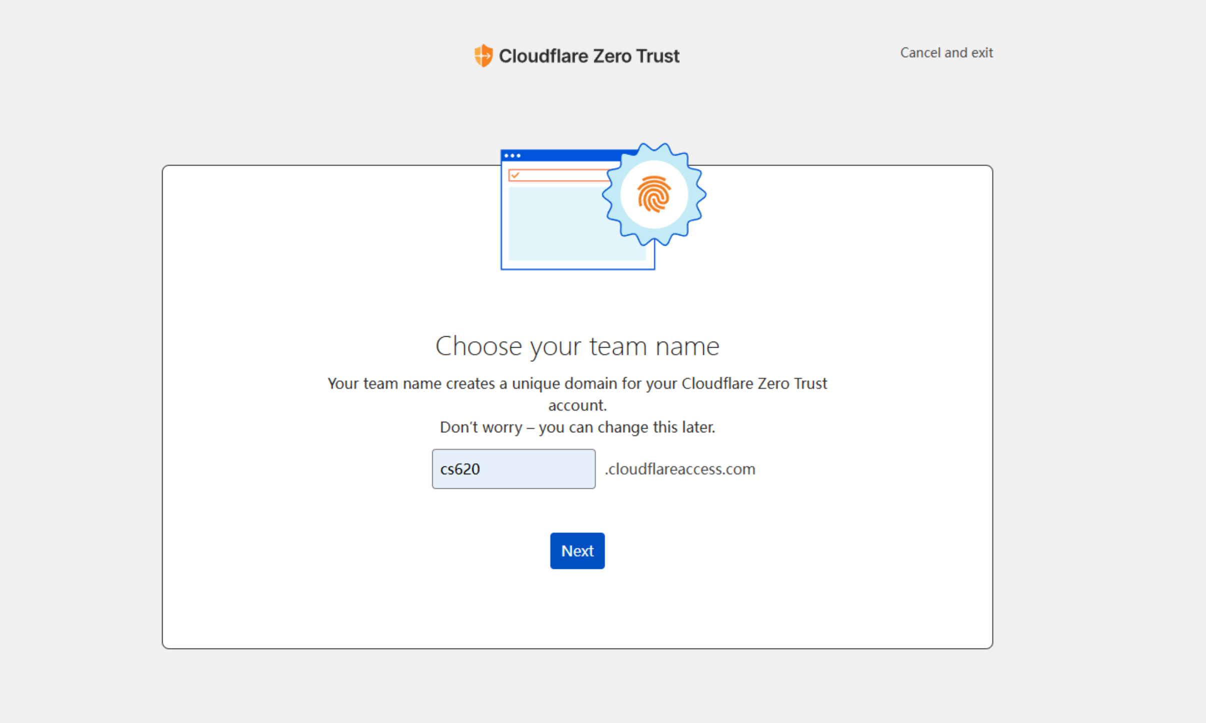
Do not block (allow crawlers)
AI training bots will be allowed to scrape content

Instruct AI bot traffic with robots.txt ✓

> 💡 Click the “zero trust” in the sidebar



Create a name



Cloudflare Zero Trust

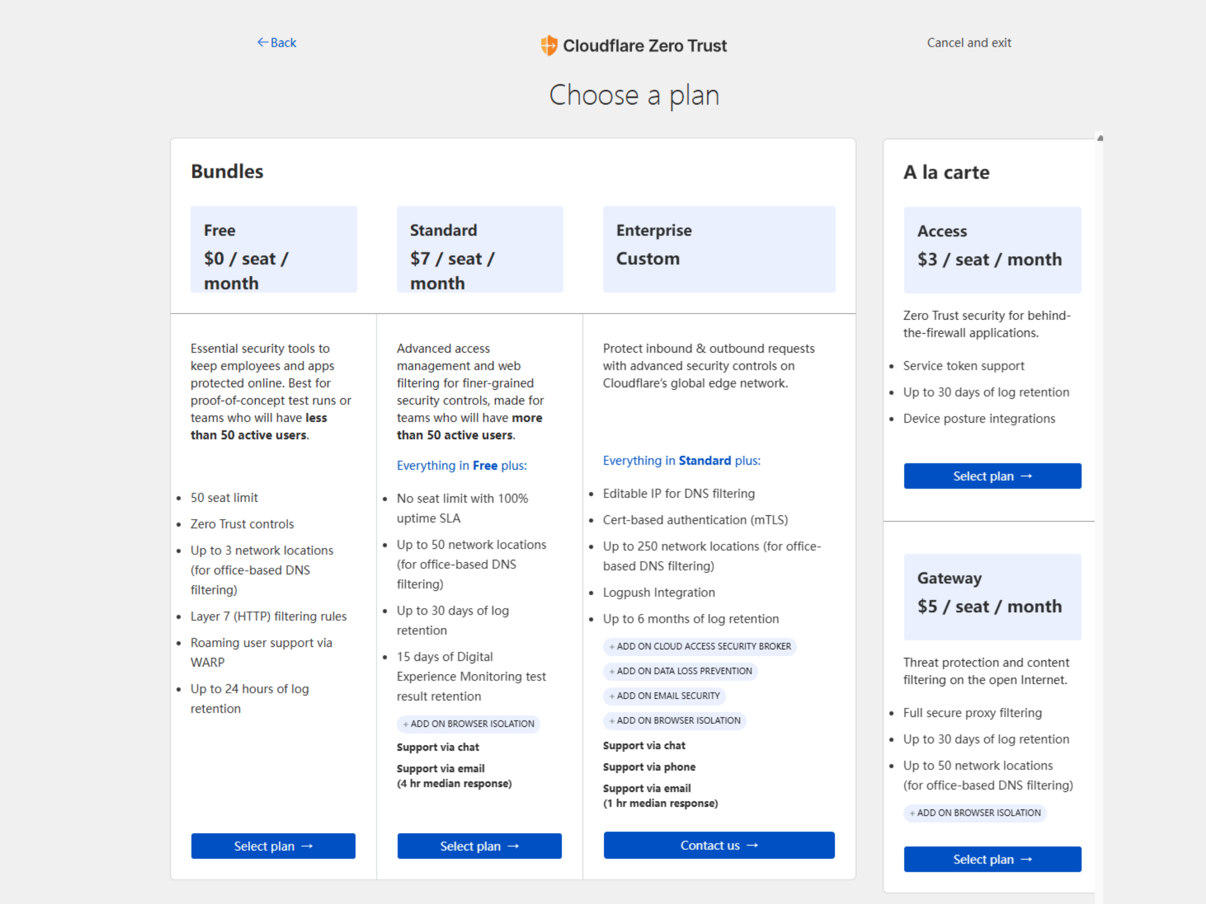
Cancel and exit

Choose your team name

Your team name creates a unique domain for your Cloudflare Zero Trust account.
Don't worry – you can change this later.

cs620 .cloudflareaccess.com

Choose the free plan, don't worry about the users limit.



← Back

Cloudflare Zero Trust

Cancel and exit

Choose a plan

Bundles

Free
$0 / seat / month

Essential security tools to keep employees and apps protected online. Best for proof-of-concept test runs or teams who will have **less than 50 active users**.

- 50 seat limit
- Zero Trust controls
- Up to 3 network locations (for office-based DNS filtering)
- Layer 7 (HTTP) filtering rules
- Roaming user support via WARP
- Up to 24 hours of log retention

Standard
$7 / seat / month

Advanced access management and web filtering for finer-grained security controls, made for teams who will have **more than 50 active users**.

Everything in **Free** plus:

- No seat limit with 100% uptime SLA
- Up to 50 network locations (for office-based DNS filtering)
- Up to 30 days of log retention
- 15 days of Digital Experience Monitoring test result retention

+ ADD ON BROWSER ISOLATION

Support via chat

Support via email
(4 hr median response)

Enterprise
Custom

Protect inbound & outbound requests with advanced security controls on Cloudflare's global edge network.

Everything in **Standard** plus:

- Editable IP for DNS filtering
- Cert-based authentication (mTLS)
- Up to 250 network locations (for office-based DNS filtering)
- Logpush Integration
- Up to 6 months of log retention

+ ADD ON CLOUD ACCESS SECURITY BROKER

+ ADD ON DATA LOSS PREVENTION

+ ADD ON EMAIL SECURITY

+ ADD ON BROWSER ISOLATION

Support via chat

Support via phone

Support via email
(1 hr median response)

A la carte

Access
$3 / seat / month

Zero Trust security for behind-the-firewall applications.

- Service token support
- Up to 30 days of log retention
- Device posture integrations

Gateway
$5 / seat / month

Threat protection and content filtering on the open Internet.

- Full secure proxy filtering
- Up to 30 days of log retention
- Up to 50 network locations (for office-based DNS filtering)

+ ADD ON BROWSER ISOLATION

Zero Trust seats are only used when Cloudflare has to **verify the identity of a real user**.

Seats are counted **only** when a person must log in through one of Cloudflare's authentication methods, such as:

✔️ Google Login required

When a user must log in using their Google account.

✔️ GitHub login required

When a user authenticates using a GitHub identity.

✔️ Email OTP required

When the application requires the user to receive a one-time passcode via email.

✔️ Corporate SSO required

When login happens through enterprise identity providers (Okta, Azure AD, etc.).

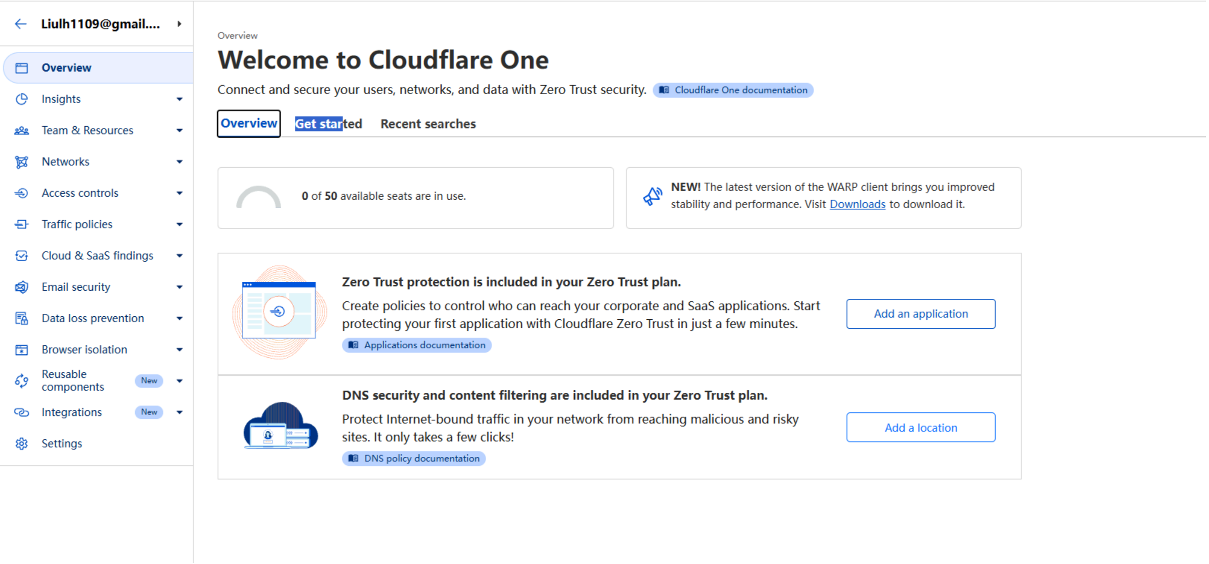
✔️ Zero Trust Access rules

When traffic is restricted and users must pass an identity check (e.g., "Only allow users from @company.com").

All of these actions involve **Cloudflare verifying a real human user**, so each unique user consumes **one seat**.

> 💡 Since we are only using Cloudflare Tunnel (no identity verification), we use 0 seats.
> Therefore, the free plan is fully sufficient for our deployment.

Create a tunnel



Overview

Welcome to Cloudflare One

Connect and secure your users, networks, and data with Zero Trust security.

0 of 50 available seats are in use.

NEW! The latest version of the WARP client brings you improved stability and performance. Visit Downloads to download it.

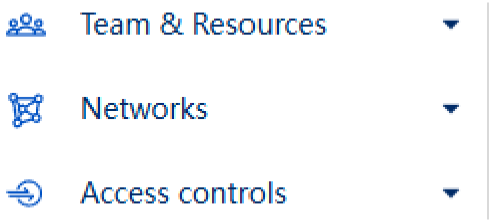
Zero Trust protection is included in your Zero Trust plan.

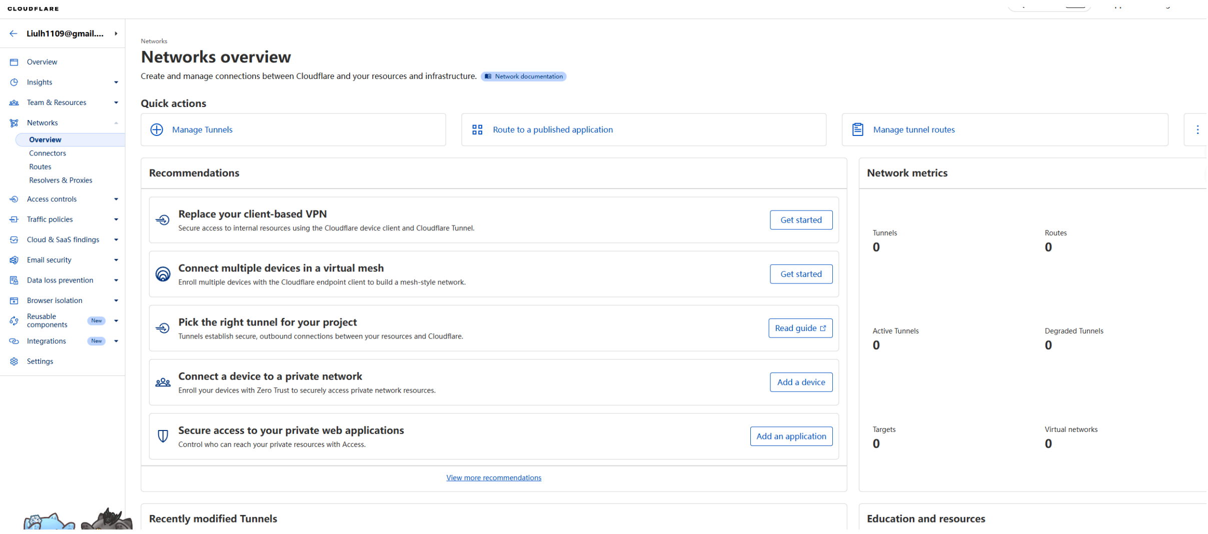
Create policies to control who can reach your corporate and SaaS applications. Start protecting your first application with Cloudflare Zero Trust in just a few minutes.

DNS security and content filtering are included in your Zero Trust plan.

Protect Internet-bound traffic in your network from reaching malicious and risky sites. It only takes a few clicks!

1. go to the “network” in the sidebar





Networks

Networks overview

Create and manage connections between Cloudflare and your resources and infrastructure.

Quick actions

Recommendations

Replace your client-based VPN
Secure access to internal resources using the Cloudflare device client and Cloudflare Tunnel.

Connect multiple devices in a virtual mesh
Enroll multiple devices with the Cloudflare endpoint client to build a mesh-style network.

Pick the right tunnel for your project
Tunnels establish secure, outbound connections between your resources and Cloudflare.

Connect a device to a private network
Enroll your devices with Zero Trust to securely access private network resources.

Secure access to your private web applications
Control who can reach your private resources with Access.

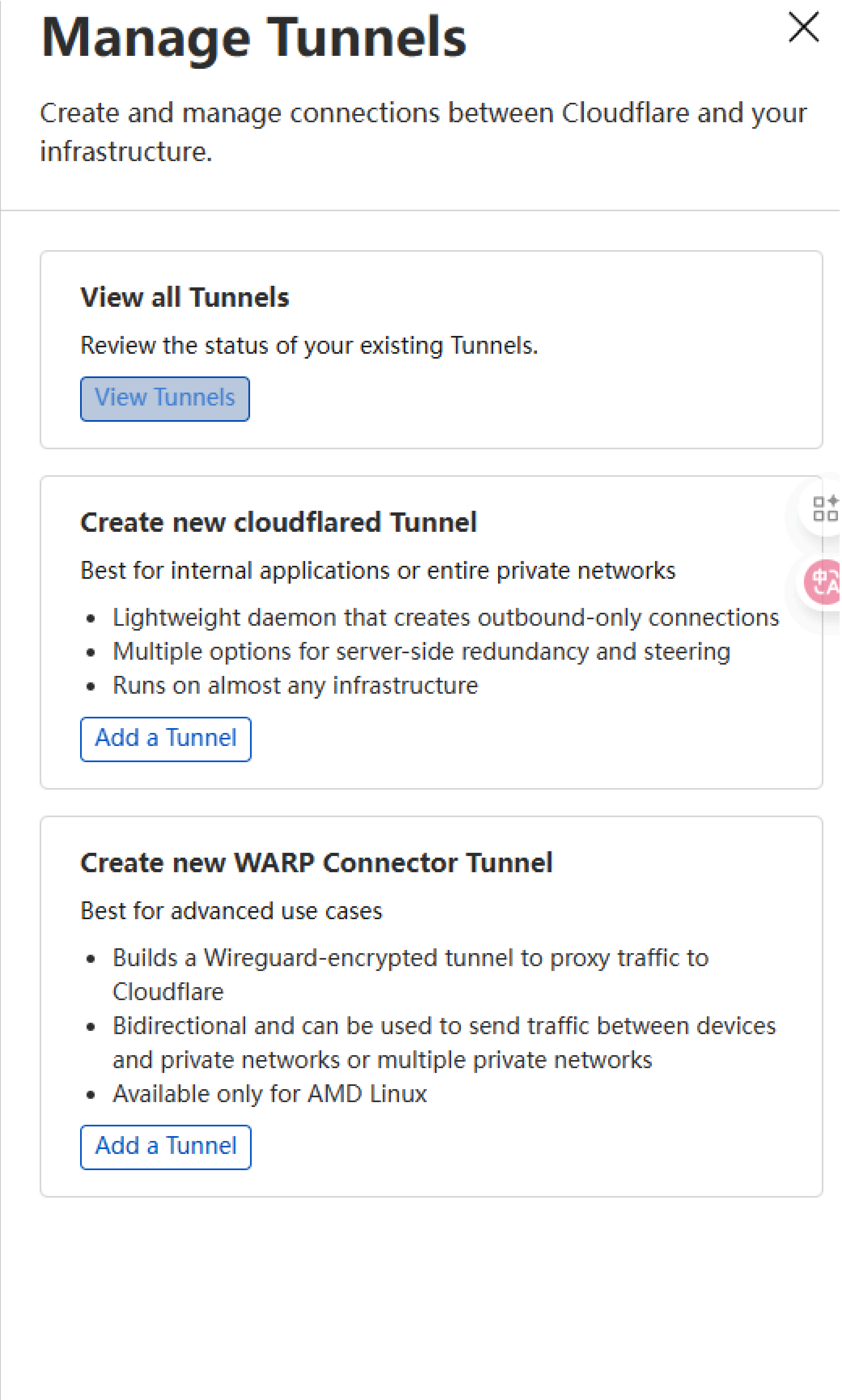
Network metrics

Tunnels 0	Routes 0
Active Tunnels 0	Degraded Tunnels 0
Targets 0	Virtual networks 0

Recently modified Tunnels

Education and resources

2. Click “manage tunnel” and “add a tunnel”



Manage Tunnels

Create and manage connections between Cloudflare and your infrastructure.

View all Tunnels

Review the status of your existing Tunnels.

Create new cloudflared Tunnel

Best for internal applications or entire private networks

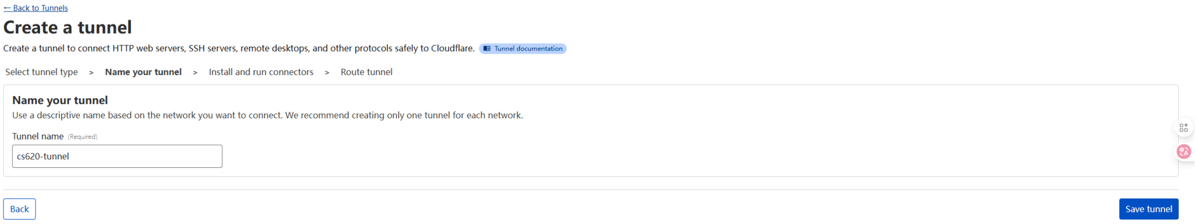
- Lightweight daemon that creates outbound-only connections
- Multiple options for server-side redundancy and steering
- Runs on almost any infrastructure

Create new WARP Connector Tunnel

Best for advanced use cases

- Builds a Wireguard-encrypted tunnel to proxy traffic to Cloudflare
- Bidirectional and can be used to send traffic between devices and private networks or multiple private networks
- Available only for AMD Linux

3. Follow the instructions



← Back to Tunnels

Create a tunnel

Create a tunnel to connect HTTP web servers, SSH servers, remote desktops, and other protocols safely to Cloudflare.

Select tunnel type > **Name your tunnel** > Install and run connectors > Route tunnel

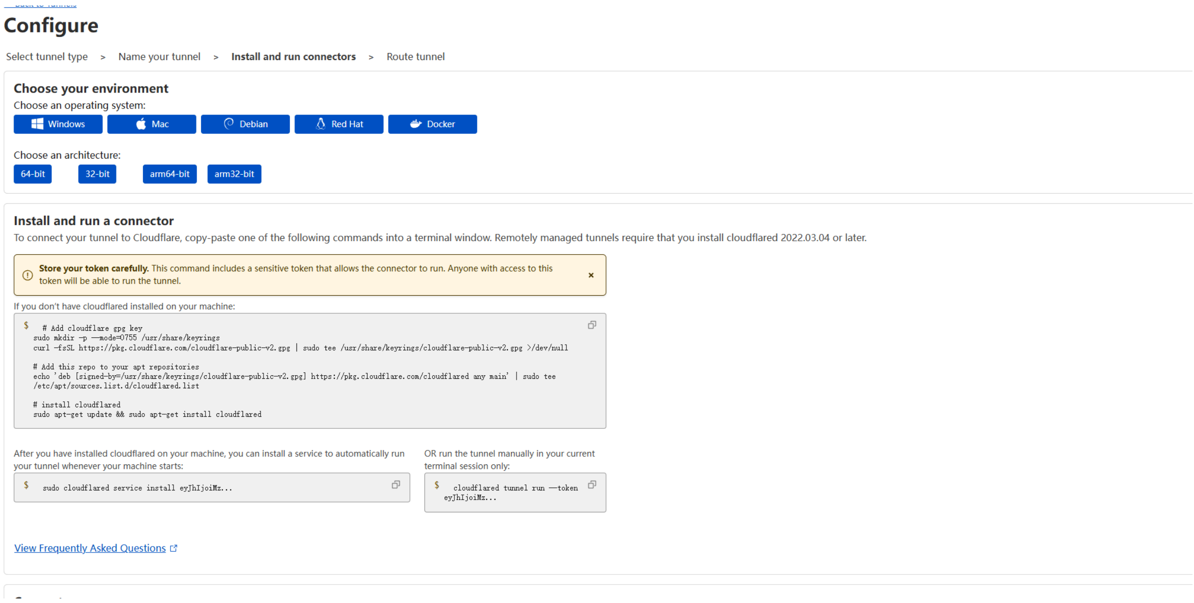
Name your tunnel

Use a descriptive name based on the network you want to connect. We recommend creating only one tunnel for each network.

Tunnel name (Required)

cs620-tunnel

4. Choose “Debian” “64bit” and it will show you some commands.



Configure

Select tunnel type > Name your tunnel > **Install and run connectors** > Route tunnel

Choose your environment

Choose an operating system:

Choose an architecture:

Install and run a connector

To connect your tunnel to Cloudflare, copy-paste one of the following commands into a terminal window. Remotely managed tunnels require that you install cloudflared 2022.03.04 or later.

Store your token carefully. This command includes a sensitive token that allows the connector to run. Anyone with access to this token will be able to run the tunnel.

If you don't have cloudflared installed on your machine:

```
$   # Add cloudflare gpg key
  sudo mkdir -p --mode=0755 /usr/share/keyrings
  curl -fsSL https://pkg.cloudflare.com/cloudflare-public-v2.gpg | sudo tee /usr/share/keyrings/cloudflare-public-v2.gpg >/dev/null

  # Add this repo to your apt repositories
  echo 'deb [signed-by=/usr/share/keyrings/cloudflare-public-v2.gpg] https://pkg.cloudflare.com/cloudflared any main' | sudo tee
  /etc/apt/sources.list.d/cloudflared.list

  # install cloudflared
  sudo apt-get update && sudo apt-get install cloudflared
```

After you have installed cloudflared on your machine, you can install a service to automatically run your tunnel whenever your machine starts:

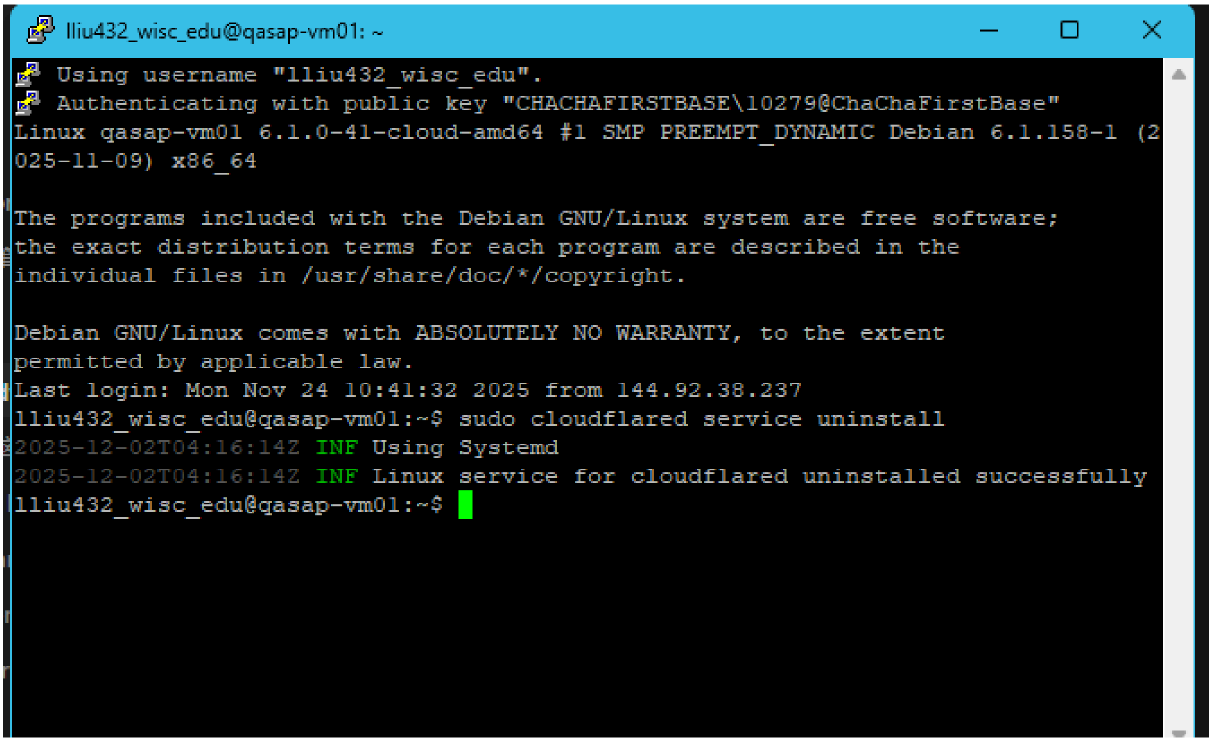
```
$   sudo cloudflared service install eyJhIjoiMz...
```

OR run the tunnel manually in your current terminal session only:

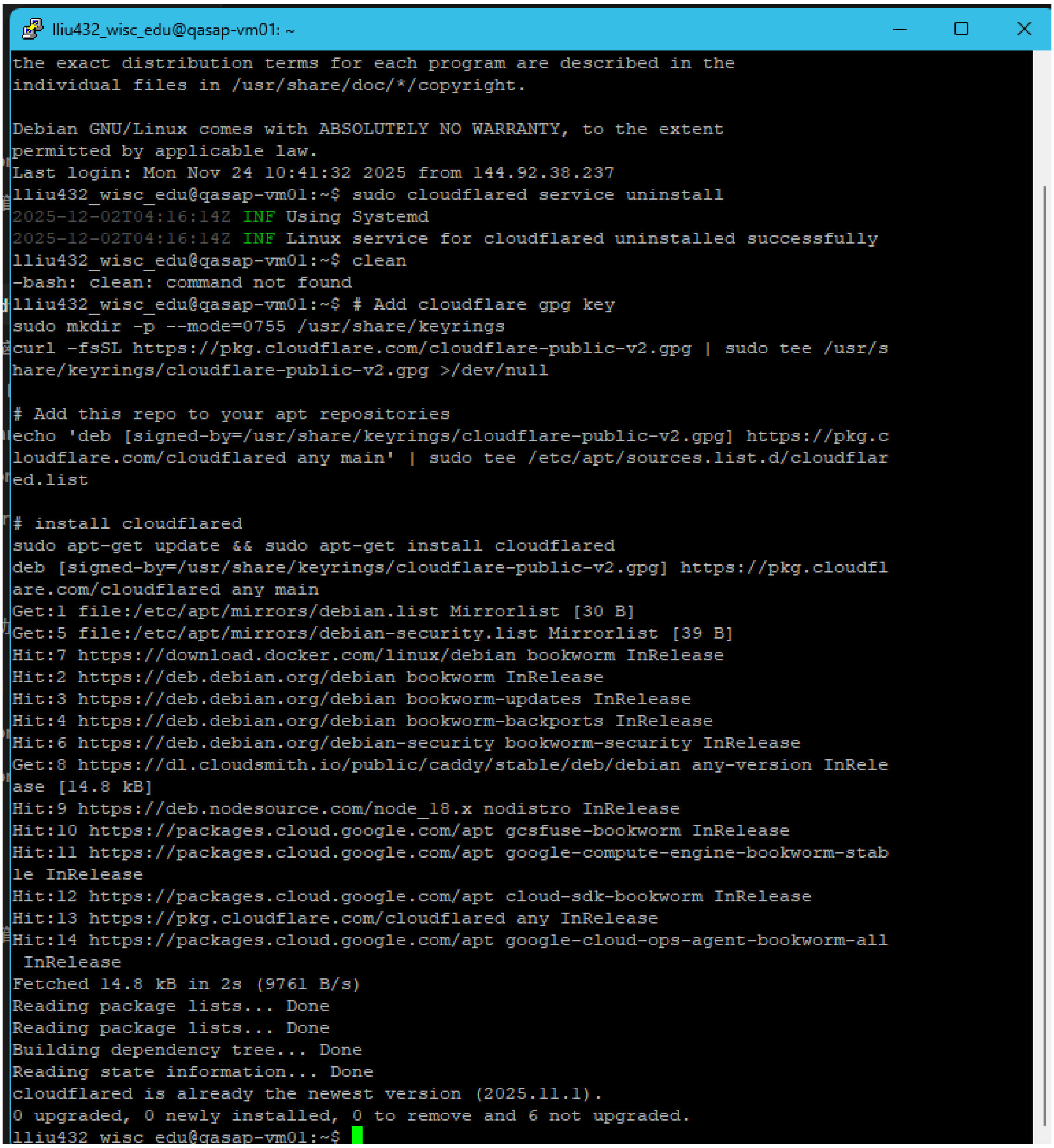
```
$   cloudflared tunnel run --token
  eyJhIjoiMz...
```

View Frequently Asked Questions

5. Use the Google cloud sdk shell to ssh to our vm. Copy and run the command, it will automatically install the tunnel service



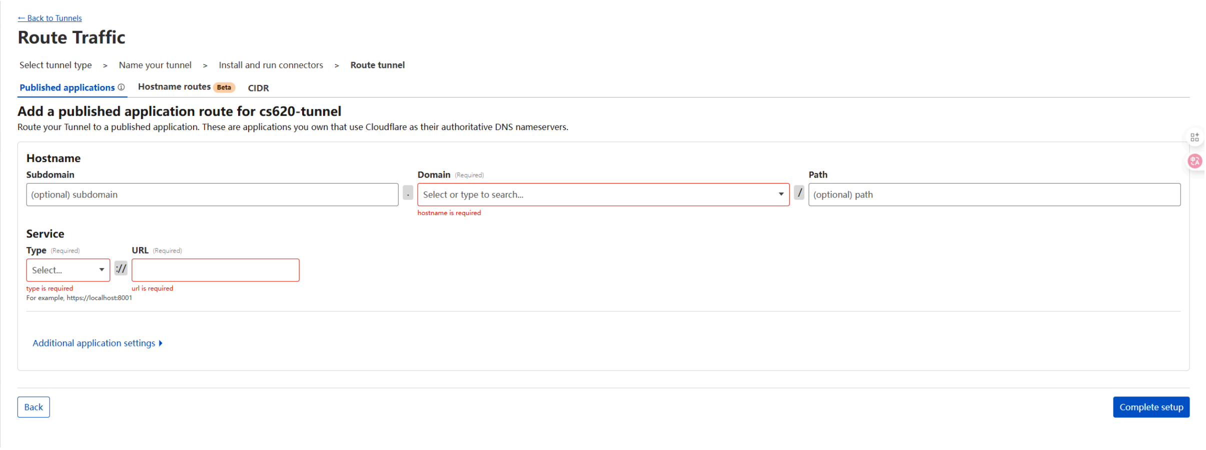
```
 Using username "lliu432_wisc_edu".
 Authenticating with public key "CHACHAFIRSTBASE\10279@ChaChaFirstBase"
Linux qasap-vm01 6.1.0-41-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.158-1 (2
025-11-09) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov 24 10:41:32 2025 from 144.92.38.237
lliu432_wisc_edu@qasap-vm01:~$ sudo cloudflared service uninstall
2025-12-02T04:16:14Z INF Using Systemd
2025-12-02T04:16:14Z INF Linux service for cloudflared uninstalled successfully
lliu432_wisc_edu@qasap-vm01:~$
```



```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov 24 10:41:32 2025 from 144.92.38.237
lliu432_wisc_edu@qasap-vm01:~$ sudo cloudflared service uninstall
2025-12-02T04:16:14Z INF Using Systemd
2025-12-02T04:16:14Z INF Linux service for cloudflared uninstalled successfully
lliu432_wisc_edu@qasap-vm01:~$ clean
-bash: clean: command not found
lliu432_wisc_edu@qasap-vm01:~$ # Add cloudflare gpg key
sudo mkdir -p --mode=0755 /usr/share/keyrings
curl -fsSL https://pkg.cloudflare.com/cloudflare-public-v2.gpg | sudo tee /usr/s
hare/keyrings/cloudflare-public-v2.gpg >/dev/null

# Add this repo to your apt repositories
echo 'deb [signed-by=/usr/share/keyrings/cloudflare-public-v2.gpg] https://pkg.c
loudflare.com/cloudflared any main' | sudo tee /etc/apt/sources.list.d/cloudflar
ed.list

# install cloudflared
sudo apt-get update && sudo apt-get install cloudflared
deb [signed-by=/usr/share/keyrings/cloudflare-public-v2.gpg] https://pkg.cloudfl
are.com/cloudflared any main
Get:1 file:/etc/apt/mirrors/debian.list Mirrorlist [30 B]
Get:5 file:/etc/apt/mirrors/debian-security.list Mirrorlist [39 B]
Hit:7 https://download.docker.com/linux/debian bookworm InRelease
Hit:2 https://deb.debian.org/debian bookworm InRelease
Hit:3 https://deb.debian.org/debian bookworm-updates InRelease
Hit:4 https://deb.debian.org/debian bookworm-backports InRelease
Hit:6 https://deb.debian.org/debian-security bookworm-security InRelease
Get:8 https://dl.cloudsmith.io/public/caddy/stable/deb/debian any-version InRele
ase [14.8 kB]
Hit:9 https://deb.nodesource.com/node_18.x nodistro InRelease
Hit:10 https://packages.cloud.google.com/apt gcsfuse-bookworm InRelease
Hit:11 https://packages.cloud.google.com/apt google-compute-engine-bookworm-stab
le InRelease
Hit:12 https://packages.cloud.google.com/apt cloud-sdk-bookworm InRelease
Hit:13 https://pkg.cloudflare.com/cloudflared any InRelease
Hit:14 https://packages.cloud.google.com/apt google-cloud-ops-agent-bookworm-all
 InRelease
Fetched 14.8 kB in 2s (9761 B/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
cloudflared is already the newest version (2025.11.1).
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
lliu432_wisc_edu@qasap-vm01:~$
```

> After you have installed cloudflared on your machine, you can install a service to automatically run your tunnel whenever your machine starts:
>
> ```
> $  sudo cloudflared service install eyJhIjoiMz...
> ```

6. In the next page, you can set up the domain, if you bought the domain on cloudflare, it should appear in the domain selection list.


← Back to Tunnels
Select tunnel type > Name your tunnel > Install and run connectors > Route tunnel
Published applications
Hostname routes
Beta
CIDR
Additional application settings
Back
Complete setup

Route Traffic

Add a published application route for cs620-tunnel

Route your Tunnel to a published application. These are applications you own that use Cloudflare as their authoritative DNS nameservers.

Hostname

Subdomain: (optional) subdomain

Domain (Required): Select or type to search...

hostname is required

Path: (optional) path

Service

Type (Required): Select...

URL (Required):

type is required

url is required

For example, https://localhost:8001

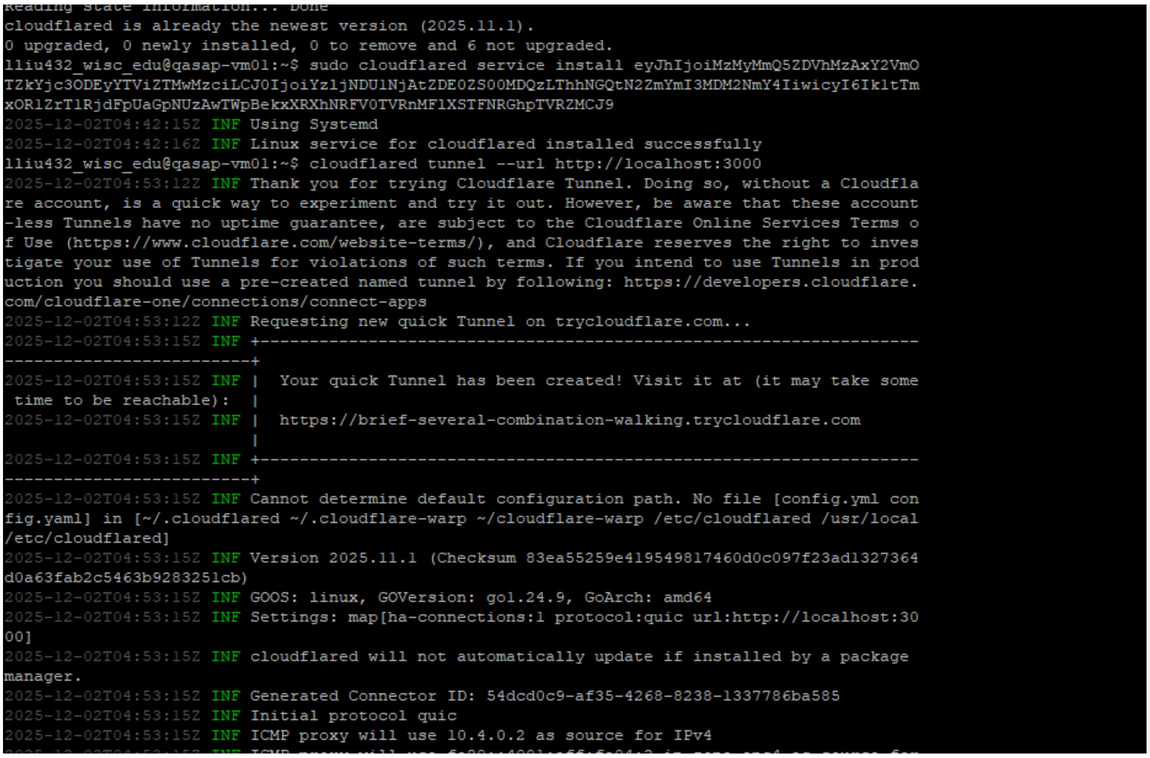
Service

- Type: **HTTP**
- URL: `localhost:3000`

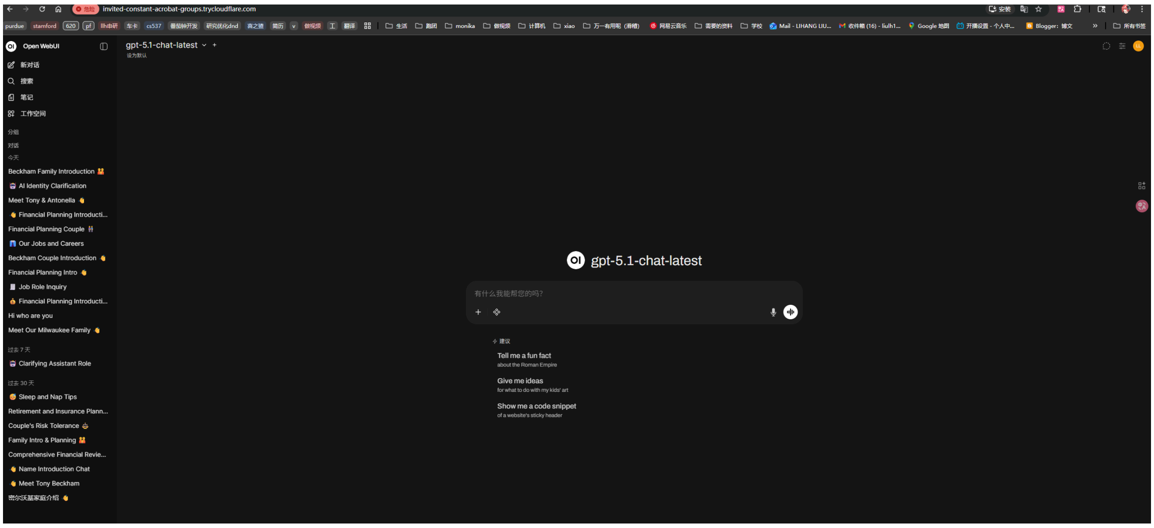
> Even though the public URL uses HTTPS, the local service behind Cloudflare Tunnel should use HTTP unless you manually configured your localhost service to run HTTPS.
>
> For OpenWebUI on port 3000, the correct configuration is:
>
> **Type: HTTP, URL: localhost:3000.**

After setting up, the cloudflare should give you a https domain so that you can access the openwebui without using uw net.

7. Since I don’t have access to the domain, I will just show the temporary tunnel
    a. cloudflared tunnel --url http://localhost:3000
    b. it will give you a temporary link points to the openwebui



```
Reading state information... Done
cloudflared is already the newest version (2025.11.1).
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
lliu432_wisc_edu@qasap-vm01:~$ sudo cloudflared service install eyJhIjoiMzMyMmQ5ZDVhMzAxY2VmO
TZkYjc3ODEyYTViZTMwMzciLCJ0IjoiYzljNDU1NjAtZDE0ZS00MDQzLThhNGQtN2ZmYmI3MDM2NmY4IiwicyI6IkltTm
xOR1ZrT1RjdFpUaGpNUzAwTWpBekxXRXhNRFV0TVRnMFlXSTFNRGhpTVRZMCJ9
2025-12-02T04:42:15Z INF Using Systemd
2025-12-02T04:42:16Z INF Linux service for cloudflared installed successfully
lliu432_wisc_edu@qasap-vm01:~$ cloudflared tunnel --url http://localhost:3000
2025-12-02T04:53:12Z INF Thank you for trying Cloudflare Tunnel. Doing so, without a Cloudfla
re account, is a quick way to experiment and try it out. However, be aware that these account
-less Tunnels have no uptime guarantee, are subject to the Cloudflare Online Services Terms o
f Use (https://www.cloudflare.com/website-terms/), and Cloudflare reserves the right to inves
tigate your use of Tunnels for violations of such terms. If you intend to use Tunnels in prod
uction you should use a pre-created named tunnel by following: https://developers.cloudflare.
com/cloudflare-one/connections/connect-apps
2025-12-02T04:53:12Z INF Requesting new quick Tunnel on trycloudflare.com...
2025-12-02T04:53:15Z INF +--------------------------------------------------------------------
------------------------+
2025-12-02T04:53:15Z INF |  Your quick Tunnel has been created! Visit it at (it may take some
 time to be reachable):  |
2025-12-02T04:53:15Z INF |  https://brief-several-combination-walking.trycloudflare.com
                         |
2025-12-02T04:53:15Z INF +--------------------------------------------------------------------
------------------------+
2025-12-02T04:53:15Z INF Cannot determine default configuration path. No file [config.yml con
fig.yaml] in [~/.cloudflared ~/.cloudflare-warp ~/cloudflare-warp /etc/cloudflared /usr/local
/etc/cloudflared]
2025-12-02T04:53:15Z INF Version 2025.11.1 (Checksum 83ea55259e419549817460d0c097f23ad1327364
d0a63fab2c5463b9283251cb)
2025-12-02T04:53:15Z INF GOOS: linux, GOVersion: go1.24.9, GoArch: amd64
2025-12-02T04:53:15Z INF Settings: map[ha-connections:1 protocol:quic url:http://localhost:30
00]
2025-12-02T04:53:15Z INF cloudflared will not automatically update if installed by a package
manager.
2025-12-02T04:53:15Z INF Generated Connector ID: 54dcd0c9-af35-4268-8238-1337786ba585
2025-12-02T04:53:15Z INF Initial protocol quic
2025-12-02T04:53:15Z INF ICMP proxy will use 10.4.0.2 as source for IPv4
2025-12-02T04:53:15Z INF ICMP proxy will use fe80::4001:aff:fe04:2 in zone ens4 as source for
```



Beckham Family Introduction 👪
🤖 AI Identity Clarification
Meet Tony & Antonella 👋
👋 Financial Planning Introducti...
Financial Planning Couple 👫
👖 Our Jobs and Careers
Beckham Couple Introduction 👋
Financial Planning Intro 👋
📃 Job Role Inquiry
💰 Financial Planning Introducti...
Hi who are you
Meet Our Milwaukee Family 👋

🤖 Clarifying Assistant Role

😴 Sleep and Nap Tips
Retirement and Insurance Plann...
Couple's Risk Tolerance ⚖
Family Intro & Planning 👪
Comprehensive Financial Revie...
👋 Name Introduction Chat
👋 Meet Tony Beckham
密尔沃基家庭介绍 👋

gpt-5.1-chat-latest
设为默认

gpt-5.1-chat-latest

有什么我能帮您的吗?

Tell me a fun fact
about the Roman Empire

Give me ideas
for what to do with my kids' art

Show me a code snippet
of a website's sticky header