Epic Games - Cloud Developer Platform

Accessing Substrate Over VPN

Downloaded from Epic Games Confluence
Date: 2025-07-12 04:06:43
Original URL: https://confluence-epicgames.atlassian.net/wiki/spaces/CDE/pages/81068342

Document Level Classification

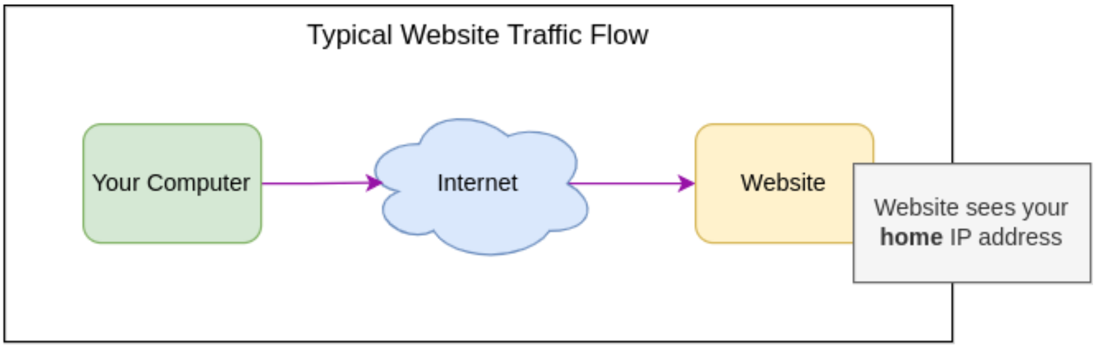
100

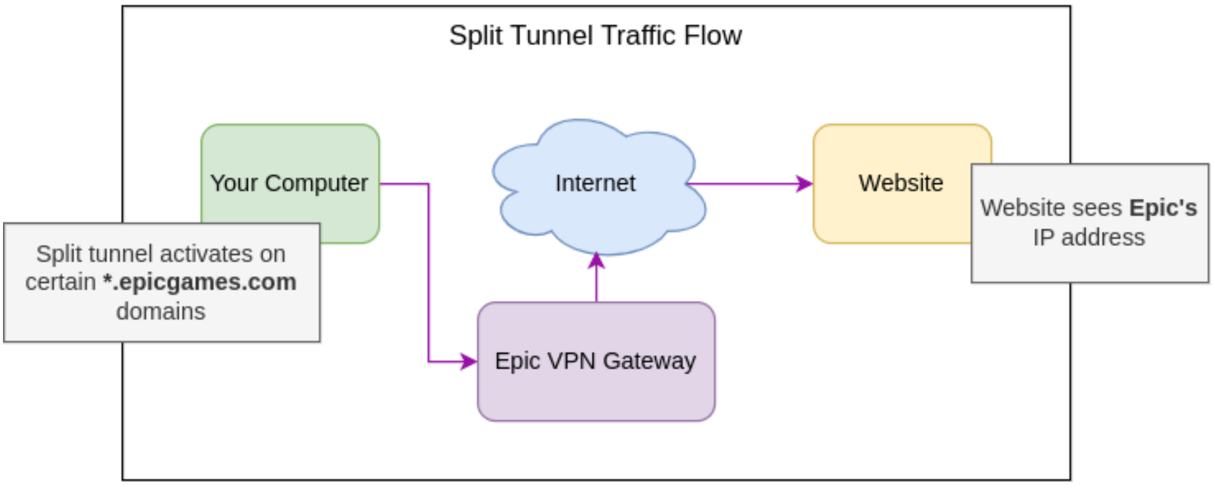
Introduction

Epic primarily uses the Global Protect VPN. We may also have older clients using AnyConnect, and many developers use OpenConnect or other VPN clients, especially on Linux. Because of variation in VPN settings and clients, you may have trouble connecting to Substrate services.

Understanding Access Problems

Access to services in Substrate frequently relies on a VPN feature called **split tunnel**. Split tunnel directs certain traffic to use Epic's VPN, when that traffic would normally flow over the public internet. The result of using split tunnel is that your traffic can be identified as originating from Epic Games network, instead of your home ISP or local coffee shop.

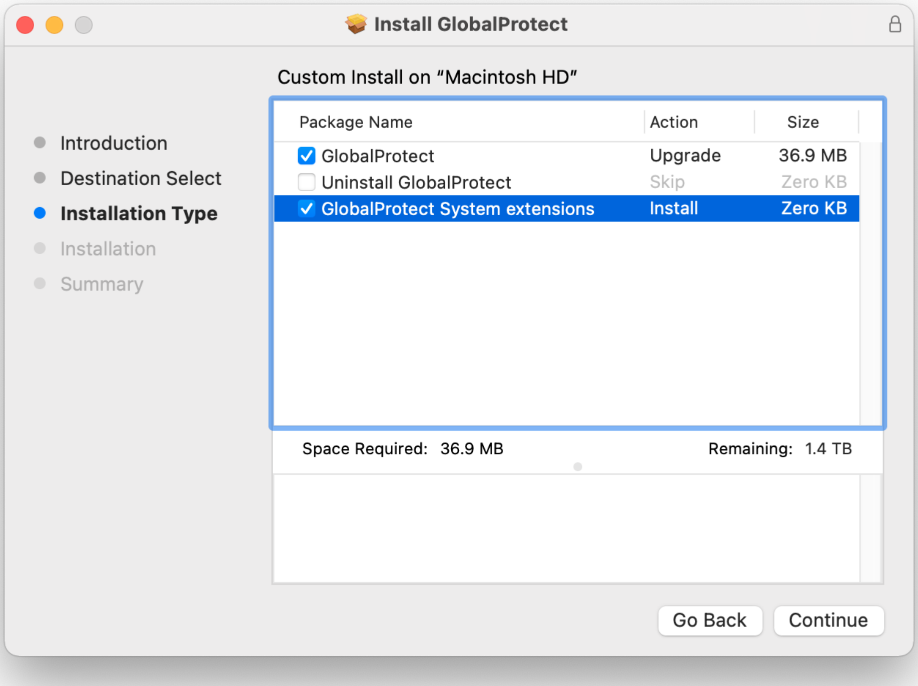

Typical Website Traffic Flow
Your Computer
Internet
Website
Website sees your **home** IP address


Split Tunnel Traffic Flow
Your Computer
Internet
Website
Website sees **Epic's** IP address
Epic VPN Gateway
Split tunnel activates on certain ***.epicgames.com** domains

Setup on MacOS

When you install the GlobalProtect client on MacOS you **must install GlobalProtect System extensions**. See the screenshot for reference. This feature allows GlobalProtect to inspect your DNS lookups and automatically add routes for certain domains. If you don't install the system extension you will still be able to connect Epic's private network but you will be unable to reach Substrate services in AWS because those routes will be missing.

If you have already installed GlobalProtect you can simply re-run the installer, check the **GlobalProtect System extensions** box, complete the re-installation process, and then restart your computer. After rebooting, you will need to open the **Security and Privacy** section of MacOS System Preferences and **Allow** the system extension to run.



Custom Install on “Macintosh HD”

Package Name	Action	Size
☑ GlobalProtect	Upgrade	36.9 MB
□ Uninstall GlobalProtect	Skip	Zero KB
☑ GlobalProtect System extensions	Install	Zero KB

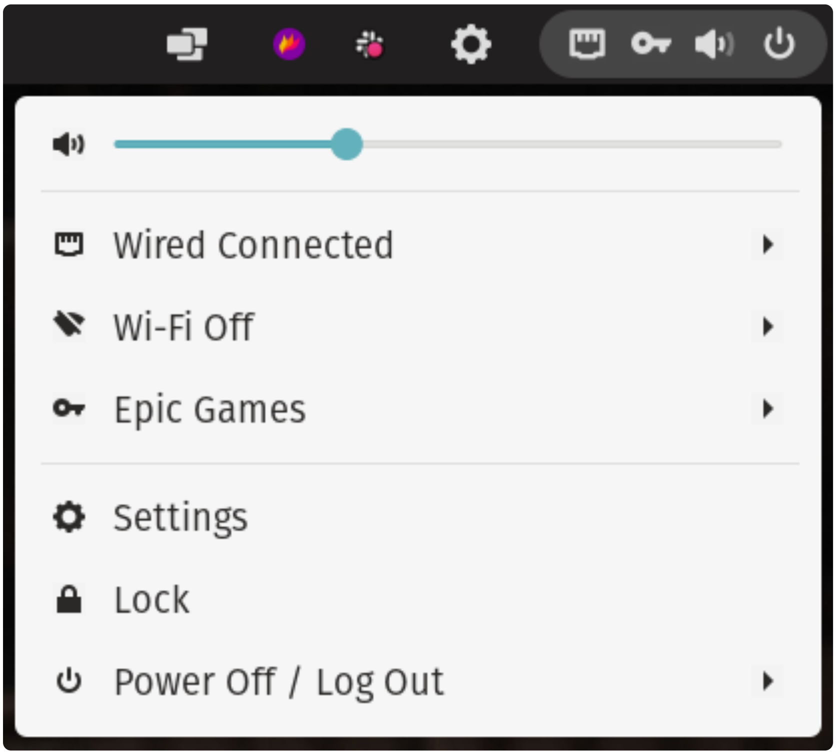
Space Required: 36.9 MB   Remaining: 1.4 TB

Global Protect Client Versions

If you are using MacOS Catalina (10.15) you must use Global Protect **5.1.3**. MacOS Big Sur (11.0) works with newer versions of Global Protect. Apple changed the way system extensions work in Big Sur so newer versions of GP VPN are not backwards compatible with previous MacOS versions. If you need a different version of the GP VPN client, please reach out to IT via `#it-globalprotect-discuss-ext` in Slack, or create a ticket.

Setup on Linux

The recommended approach on Linux is to use OpenConnect, which supports the GlobalProtect VPN protocol and integrates very well into GNOME-based distros.



In addition to configuring the VPN connection, you will also need to install `estd` (details below) to handle split tunnel DNS.

If you need to help someone who cannot access the VPN in the first place, you can **Export to PDF** using the ... menu and send it to them on Slack.

You can also use Palo Alto network's official GlobalProtect for Linux. If you're interested in this option reach out to IT.

VPN Endpoint

Epic's VPN can be accessed via **vpn-portal.epicgames.com**.

RADIUS Requirement

In order to use either option on Linux you will first need to reach out to IT and ask them to change your VPN connection to use RADIUS instead of SAML. OpenConnect and GlobalProtect clients on Linux do not properly handle the 2fa login flow using SAML authentication.

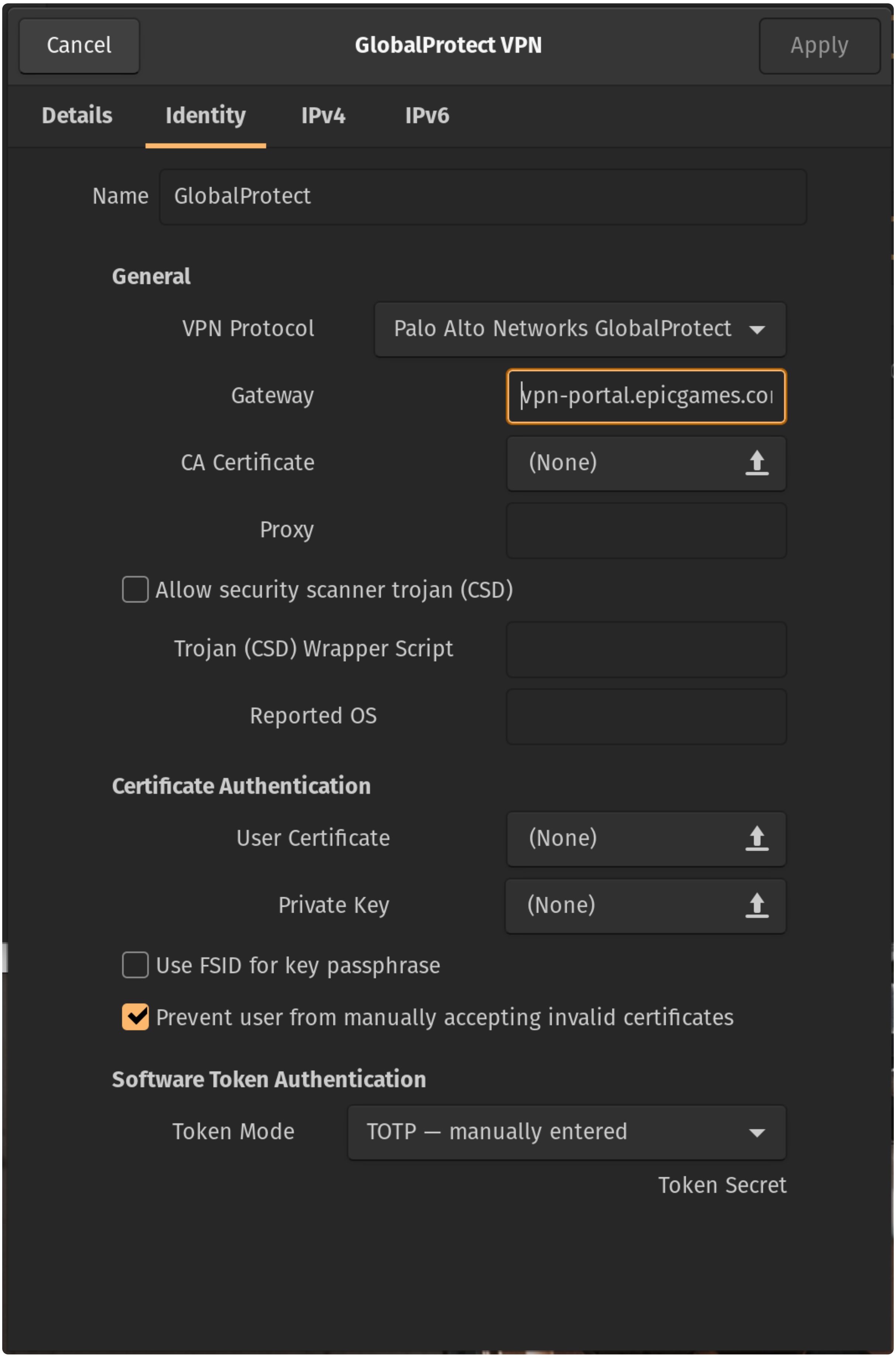
If you are stuck with SAML auth you may still be able to get it to work, thanks to a workaround from Ryan Finnie .

OpenConnect

OpenConnect is an open source VPN client. Recent versions support authentication to GlobalProtect VPN endpoints and support 2fa out of the box. On Pop!_OS 21.10 and other newer distros, it *Just Works*™, with the exception of split tunnel (see `estd` below). For example:

```
sudo apt install --no-install-recommends \
  openconnect \
  network-manager-openconnect \
  network-manager-openconnect-gnome
```

Here is an example configured via the Network → VPN panel in Gnome:



Name: GlobalProtect

General

VPN Protocol: Palo Alto Networks GlobalProtect

Gateway: vpn-portal.epicgames.co

CA Certificate: (None)

Proxy:

☐ Allow security scanner trojan (CSD)

Trojan (CSD) Wrapper Script:

Reported OS:

Certificate Authentication

User Certificate: (None)

Private Key: (None)

☐ Use FSID for key passphrase

☑ Prevent user from manually accepting invalid certificates

Software Token Authentication

Token Mode: TOTP — manually entered

Token Secret

Global Protect

If your distro has an older version of OpenConnect, the UI may not support supplying the 2fa credentials during login or it may not support the GlobalProtect protocol at all. In this case, you can try using the official Global Protect client package.

You can download PanGPLinux from Google Drive. The package includes debian, rpm, and other packages for various architectures, and includes installers for GUI and CLI clients.

`estd` - Epic Split Tunnel Daemon

As mentioned earlier, Substrate and some other services use public names and IPs, but only whitelist known Epic source IPs. In GlobalProtect parlance, this is referred to as "DNS Split Tunnel". In short, GlobalProtect watches your DNS queries and dynamically adds routes to your workstation's network configuration when you connect to certain domains.

On linux, the GlobalProtect client does not have this feature, and if you use OpenConnect it likewise does not have this feature. However, Adam Harrison wrote a tool to fix this, called estd. It runs locally as a systemd unit, monitors your DNS calls, and dynamically adds routes for the VPN endpoint when it detects an Epic domain.

You can install estd from github: https://github.ol.epicgames.net/cloud-eng/estd/

estd does not block outbound TCP connections so it may race to add routes when a connection is started to a new domain. In that case, retrying the connection once should resolve the issue.

In practice, this will look like the first call to a URL fails, while refreshing the page or retrying the command will work. There is a branch here that may mitigate this issue. Please test it and let us know!

Note: if you can't see the `estd` repo in GitHub please reach out for help in #cloud-ops-support-ext.

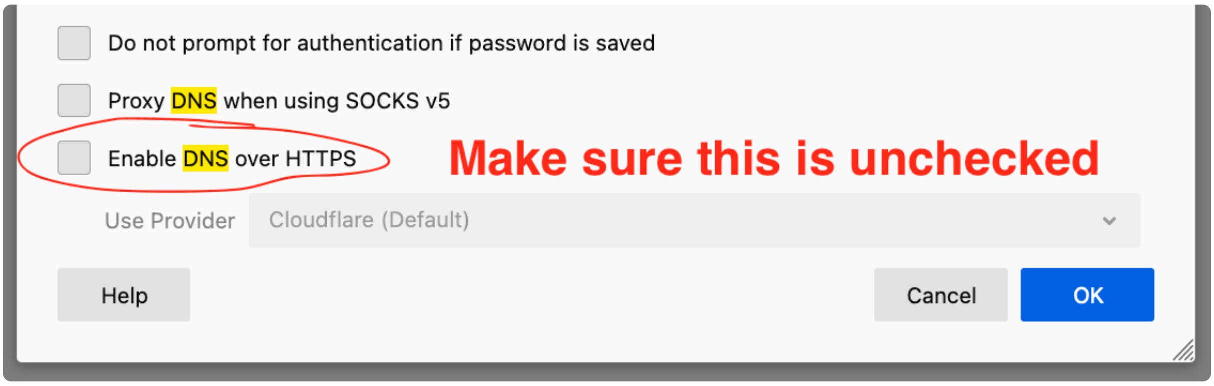
DNS Over HTTPS

GlobalProtect VPN adds routes dynamically when you connect to certain domains. It does this by inspecting outbound DNS requests from your computer and identifying subdomains of `on.epicgames.com`. After resolving the name, it routes traffic to the target IP address over the VPN.

Recently, browsers including Firefox and Chrome added a feature called DNS over HTTPS, which encrypts DNS lookups to hide them from your ISP. Unfortunately, this also hides the DNS lookup from GlobalProtect and that means the dynamic routes do not get added. You will need to disable DNS over HTTPS in your browser, or add routes manually.

Firefox

In Firefox you can find this in your preferences by searching for "dns" or by going to General → Network Settings → Enable DNS over HTTPS. Make sure this box is **unchecked**.



□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

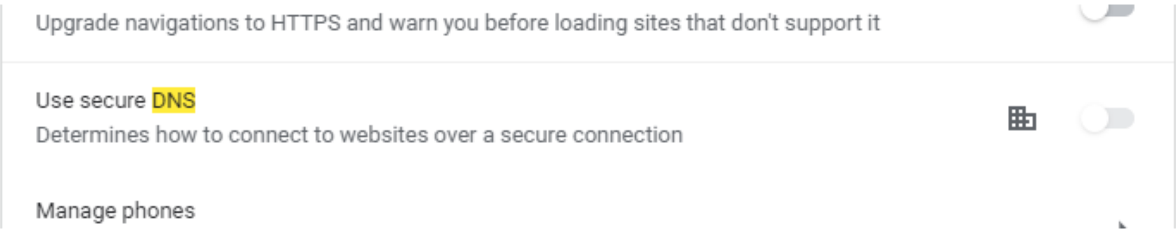
□ Enable DNS over HTTPS

Make sure this is unchecked

Use Provider Cloudflare (Default)

Chrome

In Chrome this setting is called "Use secure DNS". You'll need to **Disable** this setting and then **restart your browser**.



Upgrade navigations to HTTPS and warn you before loading sites that don't support it

Use secure DNS
Determines how to connect to websites over a secure connection

Manage phones

Troubleshooting Guide

In versions of MacOS prior to Big Sur (11.0) you may need to use Network Utility instead of the command-line versions of the tools mentioned below. In Big Sur and later, Network Utility has been removed.

Identifying Substrate Services

Substrate services such as Substrate Vault, UAM, and CodeFresh have public internet addresses (IPs). You can determine whether a particular service is hosted on substrate by using `dig`. Services that are hosted internally will have IPs that start with `10.`, while public IPs start with a different octet.

```
$ dig +short vault.substrate.on.epicgames.com    <- Substrate service
3.95.84.131     <- Public IP
18.210.182.101  <- Public IP
$ dig +short github.ol.epicgames.net   <- Non-Substrate service
internal-github-enterprise-prod-green-1840762635.us-east-1.elb.amazonaw
10.40.93.47     <- Internal IP
10.40.91.231    <- Internal IP
```

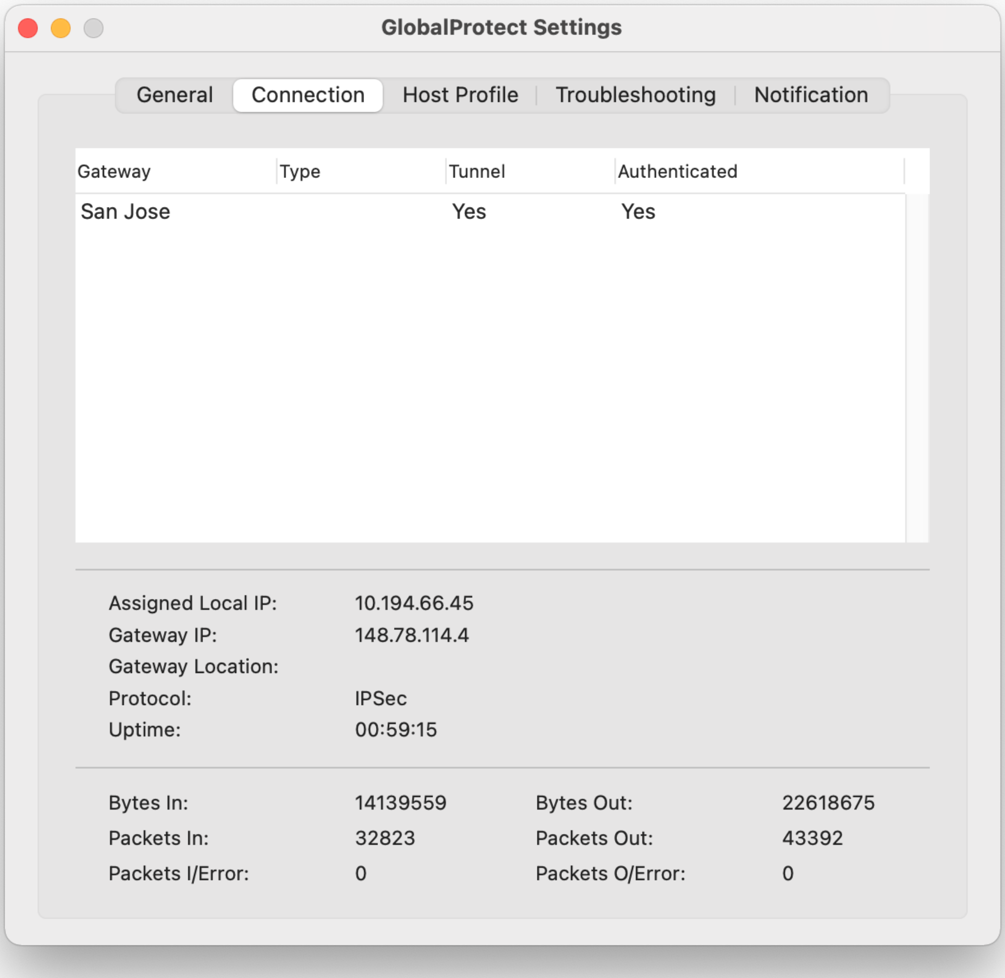
If you can't reach *any* services, this is likely a broader networking problem. However, if you can reach internal services like GitHub Enterprise and Confluence, but not Substrate Vault or CodeFresh, these steps may help.

Adding Custom Routes

An easy way to troubleshoot connection issues with Substrate services is to manually add routes to your VPN connection. If you can access the service after adding the route manually we know this is a Global Protect DNS problem. If you cannot access the service after adding the route, we are dealing with a broader problem either with the VPN or the network in general.

You can ask IT for help via `#tmp-infra-globalp-vpn-testing` in Slack, or create a ticket. Let's continue with the steps below first, though, to learn more.

This screenshot shows an example of GlobalProtect's connection tab. You will add routes to your **Assigned Local IP** – `10.194.66.45` in our example. After doing so, your traffic will appear to originate from `148.78.144.4` instead of your home or mobile IP address. Depending on where you live, you may connect to a different VPN endpoint and the IPs will probably be different.



Gateway	Type	Tunnel	Authenticated
San Jose		Yes	Yes

Assigned Local IP: 10.194.66.45
Gateway IP: 148.78.114.4
Gateway Location:
Protocol: IPSec
Uptime: 00:59:15

Bytes In:	14139559	Bytes Out:	22618675
Packets In:	32823	Packets Out:	43392
Packets I/Error:	0	Packets O/Error:	0

A few things to note:

- Substrate services are accessed by DNS name, but routes are added by IP address.
- If you need to access multiple services, you will need to add multiple routes.
- **Gateway** has different meanings on your computer vs. the **Gateway IP** you see in the VPN client, which can be confusing.

MacOS

On MacOS you can add a route like this:

```
$ dig +short vault.substrate.on.epicgames.com | xargs -I "@" sudo route
```

Note that we use **Assigned Local IP** here, *not* **Gateway IP**.

After adding the route, try again and see if your access issue is resolved. If so, we know this is a problem with DNS.

Linux

On Linux you can add a route like this:

```
$ dig +short vault.substrate.on.epicgames.com | xargs -I "@" sudo route
- OR -
$ dig +short vault.substrate.on.epicgames.com | xargs -I "@" sudo ip ro
```

You can find [additional tips in `#linux-general`](#) on Slack.

Your VPN client may call **Assigned Local IP** something else. Remember that you want to use your assigned internal (`10.*`) IP address, not one starting with `148.*`.

After adding the route, try again and see if your access issue is resolved. If so, we know this is a problem with DNS.

How to Find Help

If the troubleshooting steps here did not help you solve the problem, reach out to IT for help in `#tmp-infra-globalp-vpn-testing` in Slack, or [create a ticket](#).

Page Information:
Page ID: 81068342
Space: Cloud Developer Platform
Downloaded: 2025-07-12 04:06:43