

Cấu hình Cloudflare Tunnel cho Proxmox

Bài này sẽ thực hiện triển khai Cloudflare Tunnel trên hệ thống Proxmox. Đồng thời loại bỏ cách cũ

- [Tìm hiểu về Cloudflare Tunnel](#)
- [Triển khai Cloudflare Tunnel trên Proxmox](#)

Tìm hiểu về Cloudflare Tunnel

Cloudflare Tunnel là gì?

Cloudflare Tunnel là một phương thức kết nối server với mạng lưới Cloudflare và publish server với Internet mà không cần mở bất kì cổng nào trên router

Cloudflare Tunnel hoạt động thế nào?

Theo cách truyền thống, router cần mở cổng 80 và 443. Theo đó khi có truy cập thì người dùng khác sẽ đi thẳng tới server của bạn.

Với Cloudflare Tunnel, khi có truy cập thì người dùng này sẽ đi qua máy chủ Cloudflare và tới server của bạn thông qua một đường hầm được đào bởi `cloudflared-agent`.

Cloudflare Tunnel có tác dụng gì?

Ẩn giấu: Router của bạn sẽ không cần mở bất kỳ cổng nào. Không thể bị scan IP public

Vượt rào: Giúp bạn có thể kết nối server của mình với internet ngay cả khi không thể mở port.

Định tuyến thông minh: Cloudflare Tunnel sẽ đóng vai trò như một reverse proxy. Khi có truy cập tới `your.domain.com` nó sẽ đẩy dữ liệu thông qua đường hầm do `cloudflared-agent` đã đào để đi tới server của bạn. Từ đó loại bỏ nhu cầu sử dụng reverse proxy trung gian như NPM

Triển khai Cloudflare Tunnel trên Proxmox

Trong phần này chúng ta sẽ thực hiện cài đặt cloudflared agent trên một CT trên Proxmox và sau đó là cấu hình hình Cloudflared Tunnel trên Cloudflare

Phần thực hiện này sẽ loại bỏ Nginx Reverse Proxy đang sử dụng. Nên hãy đảm bảo bạn có quyền truy cập khác ngoài sử dụng domain name.

Ok. Let's go!

Chuẩn bị

Tắt NPM và đóng cổng

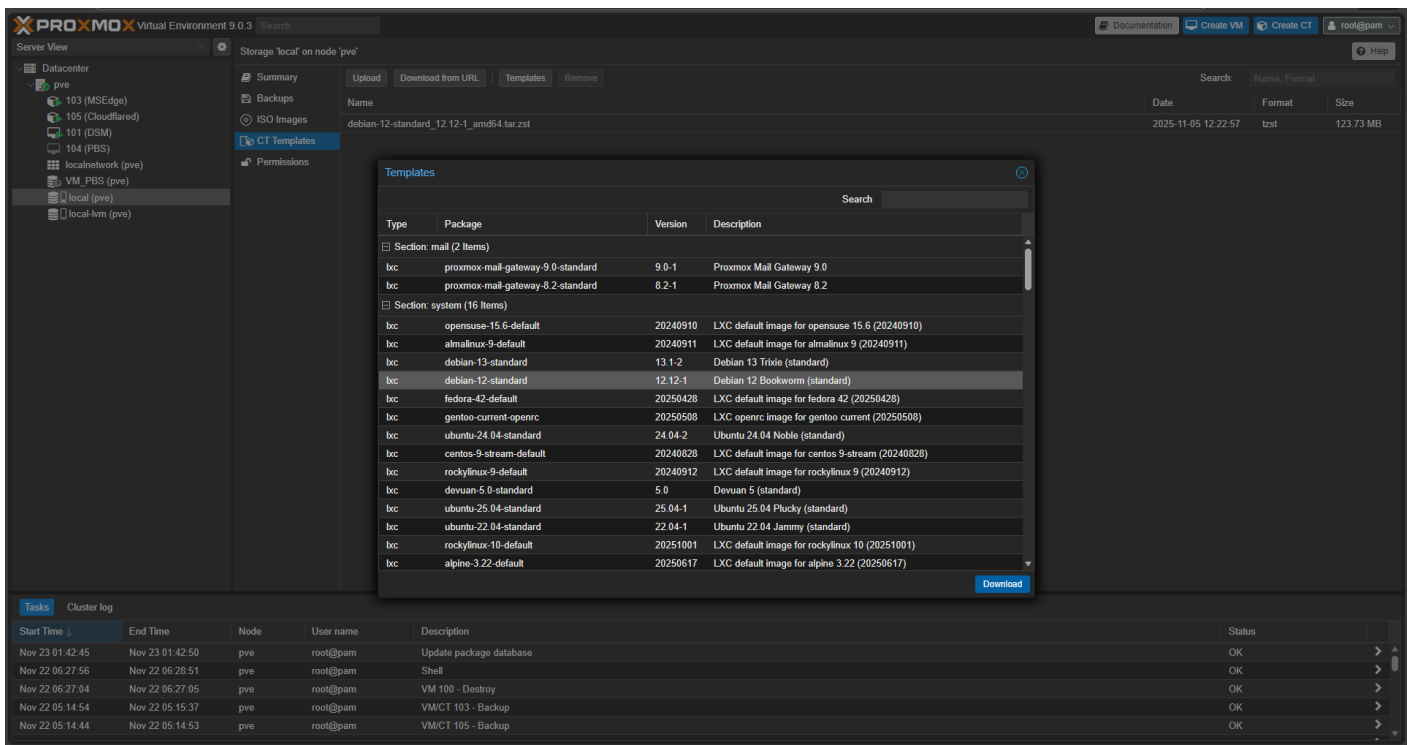
Để đảm bảo chắc chắn các setup tiếp theo hoạt động đúng và tránh trường hợp setup sai nhưng vẫn truy cập được thông qua NPM mình khuyến cáo nên thực hiện 2 việc sau:

- Đóng các port 80, 443 đã mở trên router
- Tắt CT NPM hoặc disable các domain trên NPM

Trong lúc thực hiện nên disable các domain trên NPM trước để có thể cứu được nếu gặp lỗi. Sau khi setup tất cả thành công thì đóng cổng và xóa NPM sau.

Tìm CT Templates

Truy cập PVE web > Storage > CT Templates > Templates > Tải debian-12-standard (version 12.12-1) > **Download**



Tạo CT

Trong phần tạo CT này chỉ nhắc đến những mục quan trọng cần lưu ý. Những mục khác có thể để default.

- General
 - Unprivileged container: Nên tích chọn (nếu chưa tick)
 - Nhớ điền password mới next được,
- Template
 - Chọn template vừa tải
- Disks
 - 2 - 4GiB
- CPU
 - 1 core
- Memory
 - Memory (MiB): 512
 - Swap (MiB): 512
- Network
 - IPv4 **Static**
 - IPv4/CIDR: 192.168.1.xxx/24
 - Gateway (IPv4): 192.168.1.1
- DNS
 - 8.8.8.8
- Confirm > **Finish**

Cấu hình CT

Chọn CT đã tạo và Start nó.

Tại màn hình console hãy đăng nhập với account `root` và password đã tạo ở bước trên.

Cập nhật hệ thống và cài `curl` (cần để tải cloudflared)

- `apt update && apt upgrade -y`
- `apt install curl -y`

CT này cần chạy thì mới có thể tạo ra tunnel. Vậy nên chắc chắn bạn sẽ muốn nó được khởi động cùng với proxmox. Hãy truy cập Options > Start at boot > **Enable**

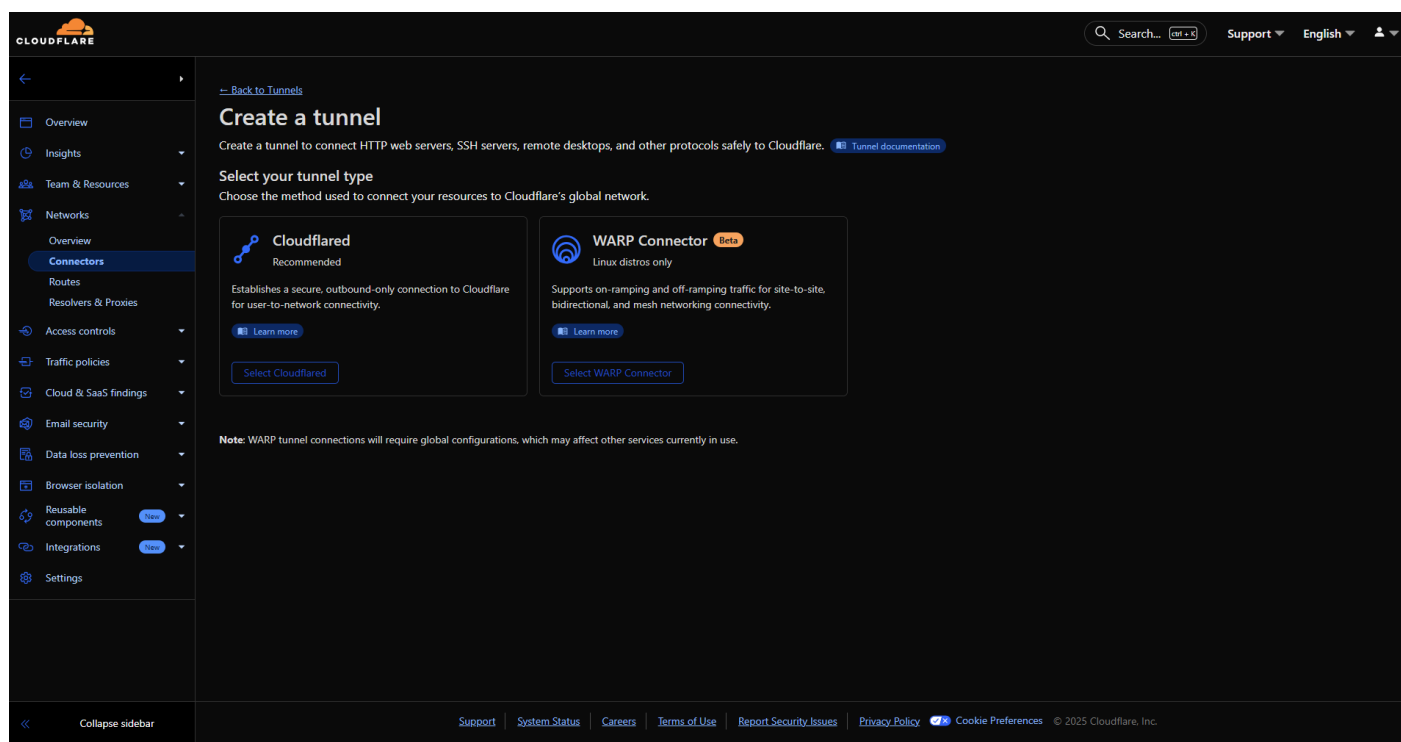
Tạo và kết nối Tunnel

Trên Cloudflare

Để cài đặt Tunnel chúng ta sẽ cần làm việc với Zero Trust. Nên hãy truy cập

<https://one.dash.cloudflare.com/>

Zero Trust > Networks > Connectors > Create a tunnel > **Select Cloudflared**



Điền tên của tunnel > **Next**

Tiếp theo, chọn hệ điều hành mà chúng ta đang cài tunnel. Ở đây đang cài trên template Debian nên chọn Debian (64-bit). Trên cửa sổ này Cloudflare sẽ cho chúng ta lệnh cài đặt trên Debian.

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

Choose your environment

Choose an operating system:

Windows Mac Debian Red Hat Docker

Choose an architecture:

64-bit 32-bit arm64-bit arm32-bit

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.

① **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 eyJhIjo1Nz...
```

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

```
$ cloudflared tunnel run --token eyJhIjo1Nz...
```

[View Frequently Asked Questions](#)

Trên Proxmox

Trở về máy chủ PVE, tại console của CT đã cài đặt và chạy lần lượt từng lệnh trên. (Nếu đã đăng nhập với account root thì bỏ sudo trong lệnh)

Sau khi chạy xong sẽ thấy trong cửa sổ Cloudflare xuất hiện Connectors như hình là OK.

Connectors

Connector ID	Status	Version
47f5988d-avb2b-41b0-b629-372b31021cd2	Connected	2025.11.1

Test	cloudflared	1b0cfddb-3696-4730-905d-6fc84f91f39a	252313a8-3972-4353-b632-ca90bd6b9ba4	--	HEALTHY	3 minutes
------	-------------	--------------------------------------	--------------------------------------	----	---------	-----------

Cấu hình Routing

Phần này chúng ta sẽ cấu hình để domain name trở về đúng địa chỉ IP local của từng dịch vụ.

Quay lại với Cloudflare, chọn Tunnel mà chúng ta đã tạo ở phần trên và chọn Edit nó.

Đi tới Published application routes và thực hiện thêm mới.

Published application routes

Add a published application route for Test

Hostname

Subdomain

demo

Domain (Required)

thanhdv.com

Path

(optional) path

 DNS Record for demo.thanhdv.com will be created

Service

Type (Required)

HTTP

URL (Required)

://

192.168.1.88:9902

For example, https://localhost:8001

[Additional application settings](#) ▶

Save

Thông tin cơ bản có thể điền như trên. Có vài trường hợp chúng ta cần lưu ý như sau:

Kết nối HTTP

Với đa phần các dịch vụ chúng ta sẽ sử dụng kết nối HTTP này. Phần mã hoá đã được tunnel lo.

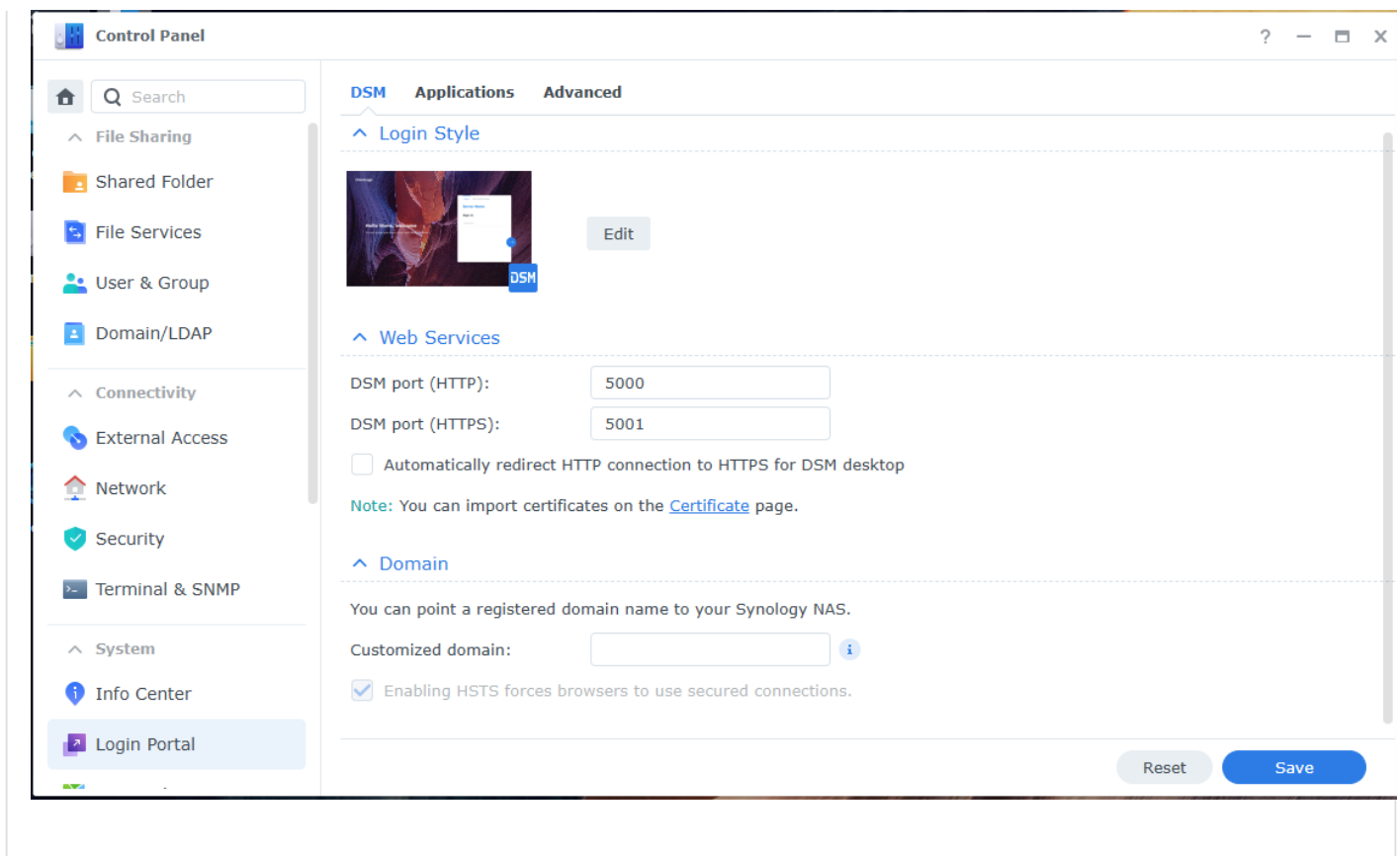
Thông tin, chỉ cần điền như trên và Save lại là xong.

Chú ý, phần Service Type chọn là HTTP.

Lưu ý với Synology/XPEnology

Khi truy cập tới dsm có thể sẽ gặp lỗi *"Too many redirects"*.

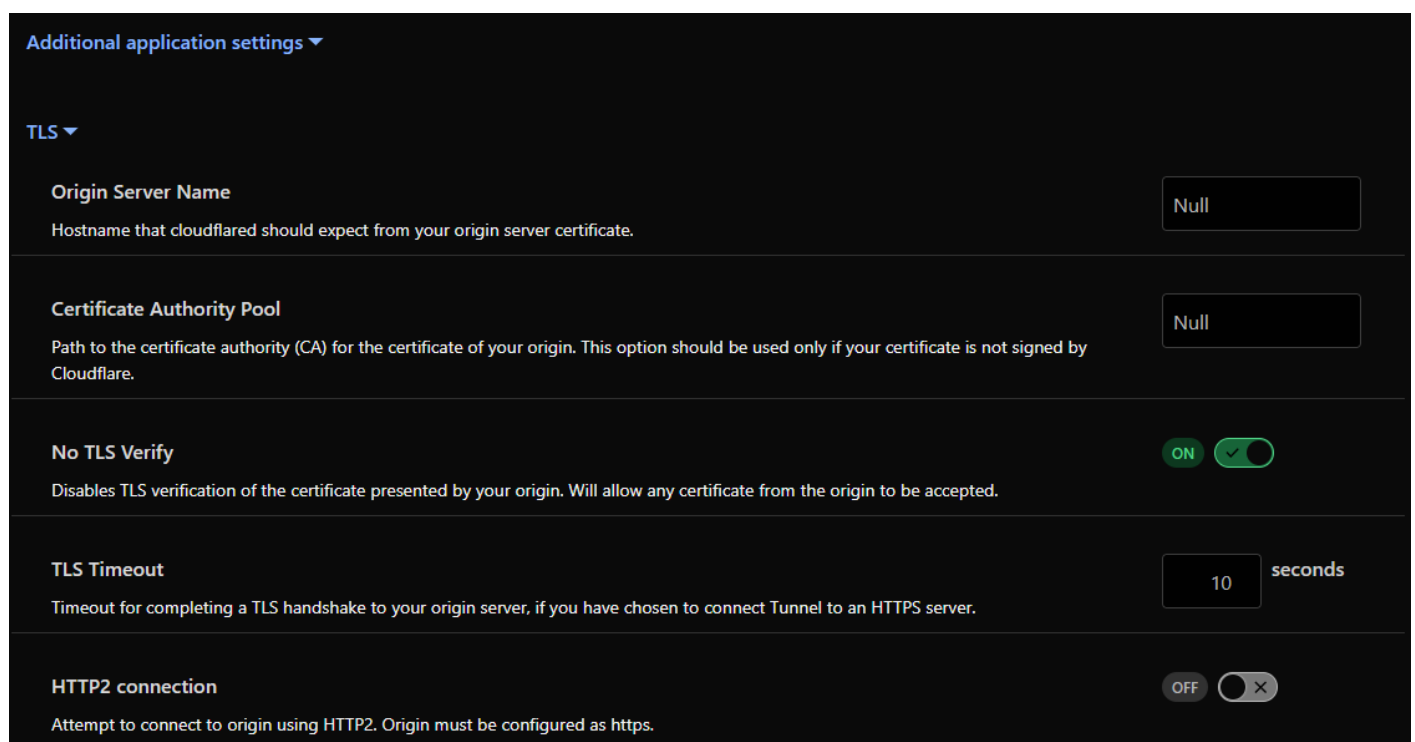
Nếu gặp lỗi này hãy, tới DSM > Control Panel > Login Portal > DSM > **Tắt** *"Automatically redirect HTTP connections to HTTPS for DSM desktop"*



K?t n?i HTTPS

Một số trang như Proxmox VE sẽ yêu cầu bắt buộc sử dụng HTTPS với *Self-signed certificate*. Với kết nối loại này sẽ mặc định bị Cloudflare từ chối. Vậy nên chúng ta cần config để bỏ qua bước này.

Lần này với **Service Type** hãy chọn là **HTTPS**, trong Additional application settings > TLS > **Bật No TLS Verify** > **Save**.



Ok, như vậy là xong rồi. Hãy đảm bảo là đã đóng cổng trên router và disable thư domain trong NPM trước khi test thử với địa chỉ vừa config. Nếu truy cập thành công là có thể xoá NPM rồi đấy :D