



Wirescale

Andy Clemenko
Geek



@clemenko



clemenko

clemenko@gmail.com



<https://andyc.info/wire>

Requirements

- **Terraform - Bash**
- An **Nginx** service that is only reachable by users connected using **WireGuard**.
- A public deployment of **Keycloak** to authenticate users by username/password and holds
- WireGuard secrets needed to connect to the server hosting **Nginx**.
- A script that accepts username/password and authenticates with **Keycloak**, retrieves the secrets, and locally configures **WireGuard**.
- Use Vault or AWS secrets store to store and distribute secrets.
- The tool can work on either Linux or Mac, whatever is more convenient.
Provide easy to use **README** and getting started guides.



Interpretation

- **Bash** - Build env and preform login
- Private **Nginx**.
- **Keycloak** - Public
- WireGuard secrets needed to connect to the server hosting **Nginx**.
- A script that accepts username/password and authenticates with **Keycloak**, retrieves the secrets, and locally configures **WireGuard**.
- Vault - key store
- Same script for both functions - build, login

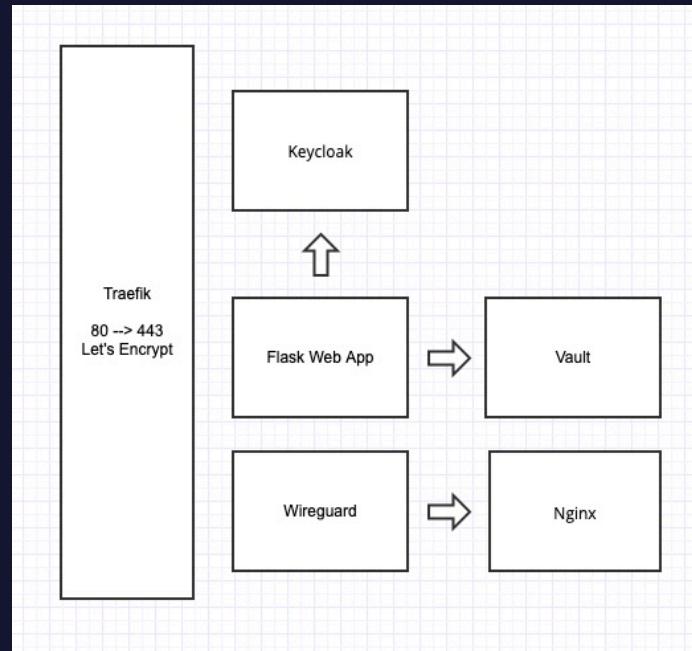


Implementation

- **Bash** - Build env and preform login
- **Docker-Compose** - Contain all the things
- **Nginx** - Private
- **Keycloak** - Public
- **Flask** - Web app
- **Traefik** - TLS all the things
- **Vault** - Store things



Implementation - Diagram



DEMO



Demo Stack

- **DigitalOcean** - Ubuntu 20.04 VMS
- **Docker** - Contain all the things
- **Traefik** - Ingress Controller
- **Keycloak** - Authentication
- **Wireguard** - Private Nework
- **Nginx** - Private web server
- **Flask** - Web app
- **Vault** - Store things



My 2 cents...

- **Overly complicated**
- **Key Rotation**
- **Scaling issues - mtls**
- **Contain Client**
- **Narrow Focus**

