Away Team VPN Solution for Linux

The basic idea

Plenty of office spaces are conusmed for people to work in, however they are just delivering their job through a network, they are connected through a computer to. Obviously in many cases the employees would be able to do their jobs from anywhere (preferably home). Technically, the user can be anywhere in the globe, the only requirements are a working Internet connection and VPN-capable device or devices such as cell phone, tablet PC or computer.

About VPN generally

VPN (Virtual Private Network) is not a new invention, and many companies already use them to provide access to their network resources for their employees remotely. The more these companies store sensitive data on their servers within their networks, the more security and insurance are required to be placed. In the meanwhile it is also quite important for the users to install and use these the simpliest way.

The VPN connectivity provides a secure encrypted connection to a remote network which makes secure access to shared drives, databases, even printers and any other network resources.

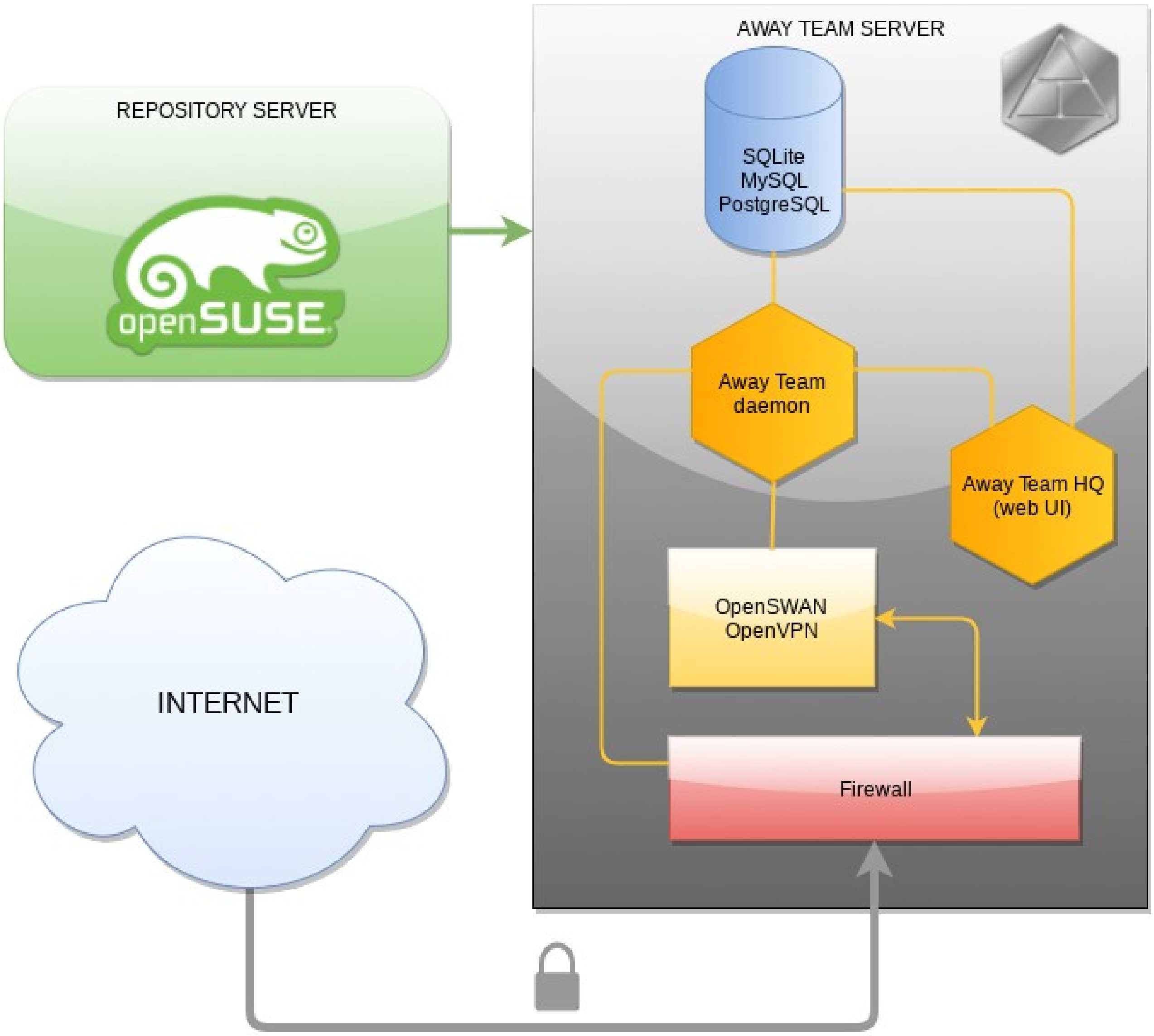
What does AT do?

Away Team runs a deamon in the background which handles the OpenVPN or OpenSWAN itself, loads or unloads the configuration, create users, monitoring the incoming connections. It is connected to a SQL-based database running in the background, reading the parameters and or configuration and applies them immediately.

There is a WebUI as well, which is able to connect to the database to create new entries or alter the existing ones. Meanwhile it is also connected to the AT daemon too through a socket and has a capability to force that to start/stop OpenVPN or OpenSWAN. Technically the user is controlling the VPN services through the browser.

As the VPN is an entry point to a disclosed network of a company, the security is an important question. Not just the VPN should be secured with the communication, but the server providing the VPN service as well. For security measurements FirewallD is responsible. As the VPN is using a TUN or TAP interface additional rules are required for the firewall to secure those interfaces to. For this reason AT daemon is also communicating with FirewallD to implement the necessary rules accordingly.

FirewallD also provides the opportunity for the customer to have more than one isolated VPN sessions controlled by one VPN server, for example if the company has more departments and they intend to separate them from each other in the matter of networking.



About the daemon in details

The daemon is written in Python3, using its capabilities to:

- opening sockets
- listen to them
- easly connecting to databases

Through these it can handle calles for OpenVPN or OpenSWAN, read the necessary information directly from the provided database, and even manage FirewallD to implement or remove rules.

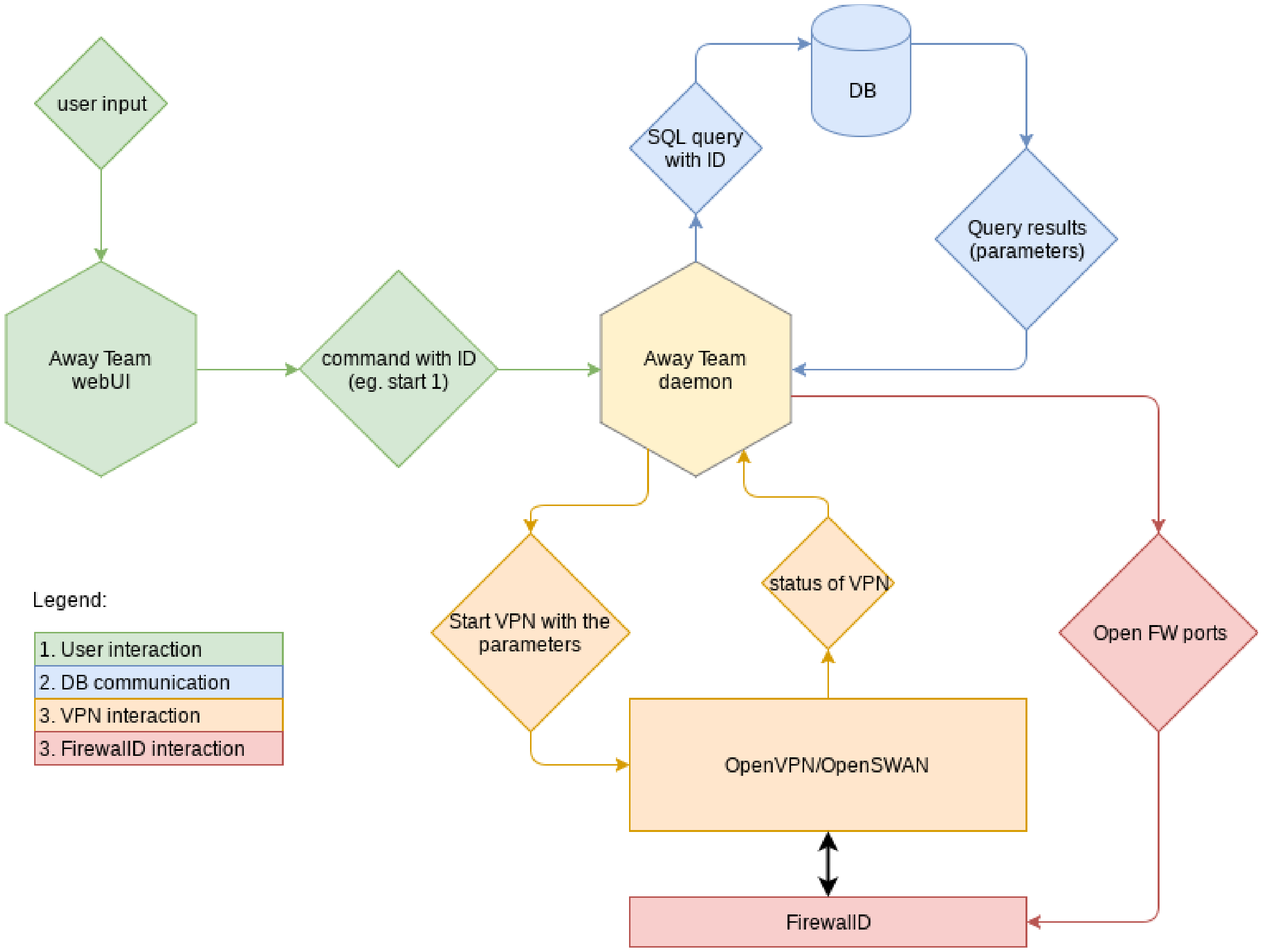
As being a daemon it runs continously in the background, and monitoring the status of running OpenVPN and OpenSWAN processes and in case of failure act according the preferrences, eg restarting or shutting down. As the events can be predefined, the chance for combining it with an action is being left in the customers‘ hands.

The pre-defined actions

- Start OpenVPN/OpenSWAN with the specified parameters
- Stop OpenVPN/OpenSWAN with the specified parameters
- Interact with FirewallD (add/remove rules)
- Interact with Watchdog to be notified any faulty actions of OpenVPN/OpenSWAN

User issued commands

The deamon listens to a socket waiting for inputs from the start. As it receives a command with configuration from the web UI, including the configuration ID, it connects to the database, runs a query for the parameters related to that ID, collecting the necessary parameters within that query and then execute the OpenVPN/OpenSWAN with these parameters. From that point it marks that OpenVPN/OpenSWAN is in running status. The figure below displays the workflow of a user issued command of VPN service.



Fail-safe mechanisms

As the daemon marks the actual status of the VPN service, and watches it carefully, in case of unexpected changes of operation mode it can act accordingly. This action is also based on rules of user defined values. The procedure is explained on the worklow below: