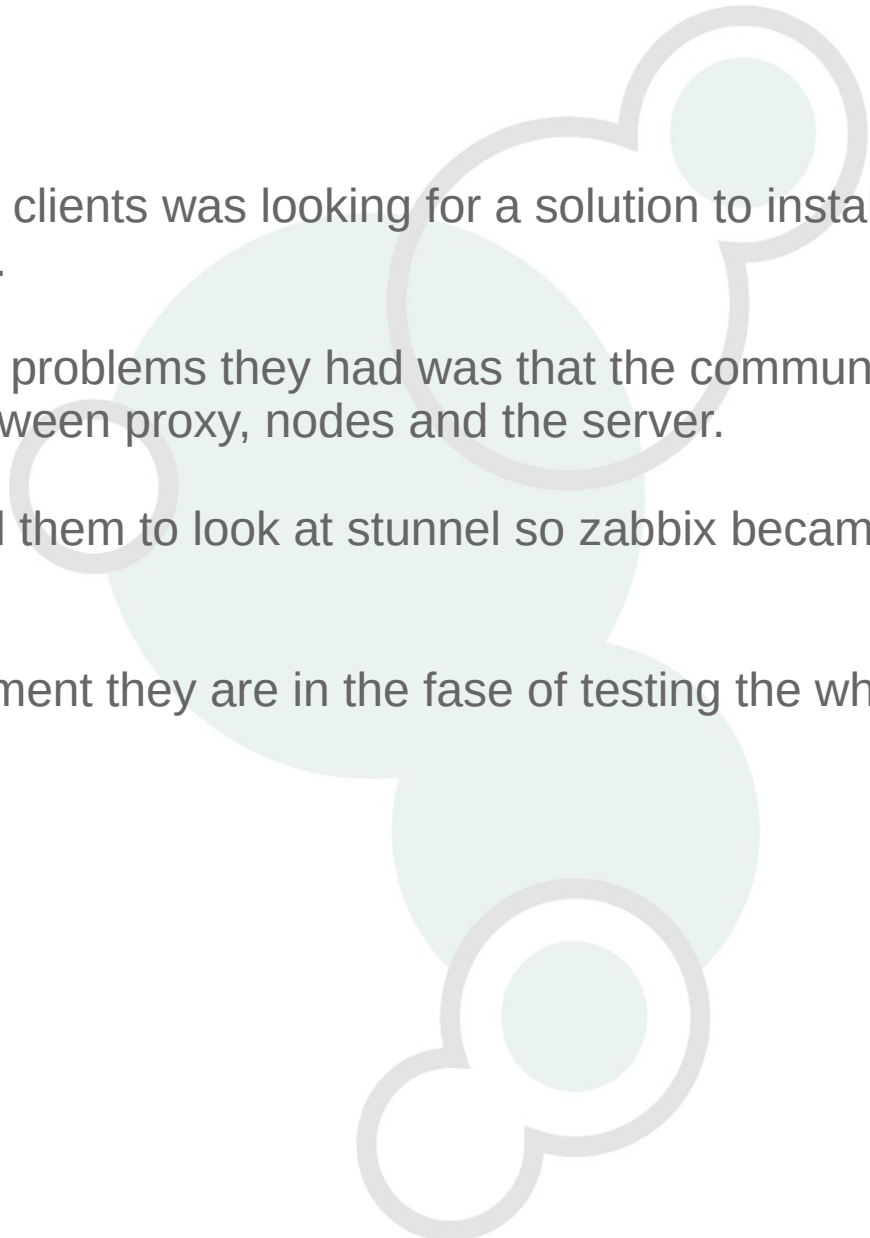


My name is Patrik and I had 16 years of experience in IT and monitoring of mainframes before I joined Open-Future, B.V.B.A in end of 2012.

As the company was a long-time partner of Zabbix already before I joined them the logical step was to get certified in zabbix. So in the beginning of 2013 I decided to progress to the next level and attend training in Riga to become a Zabbix Certified Trainer.

I was involved in the delivery of several successful Zabbix projects and migrations to customers in Belgium.

The rest of the time I work for Open-future BVBA as an open-source consultant.



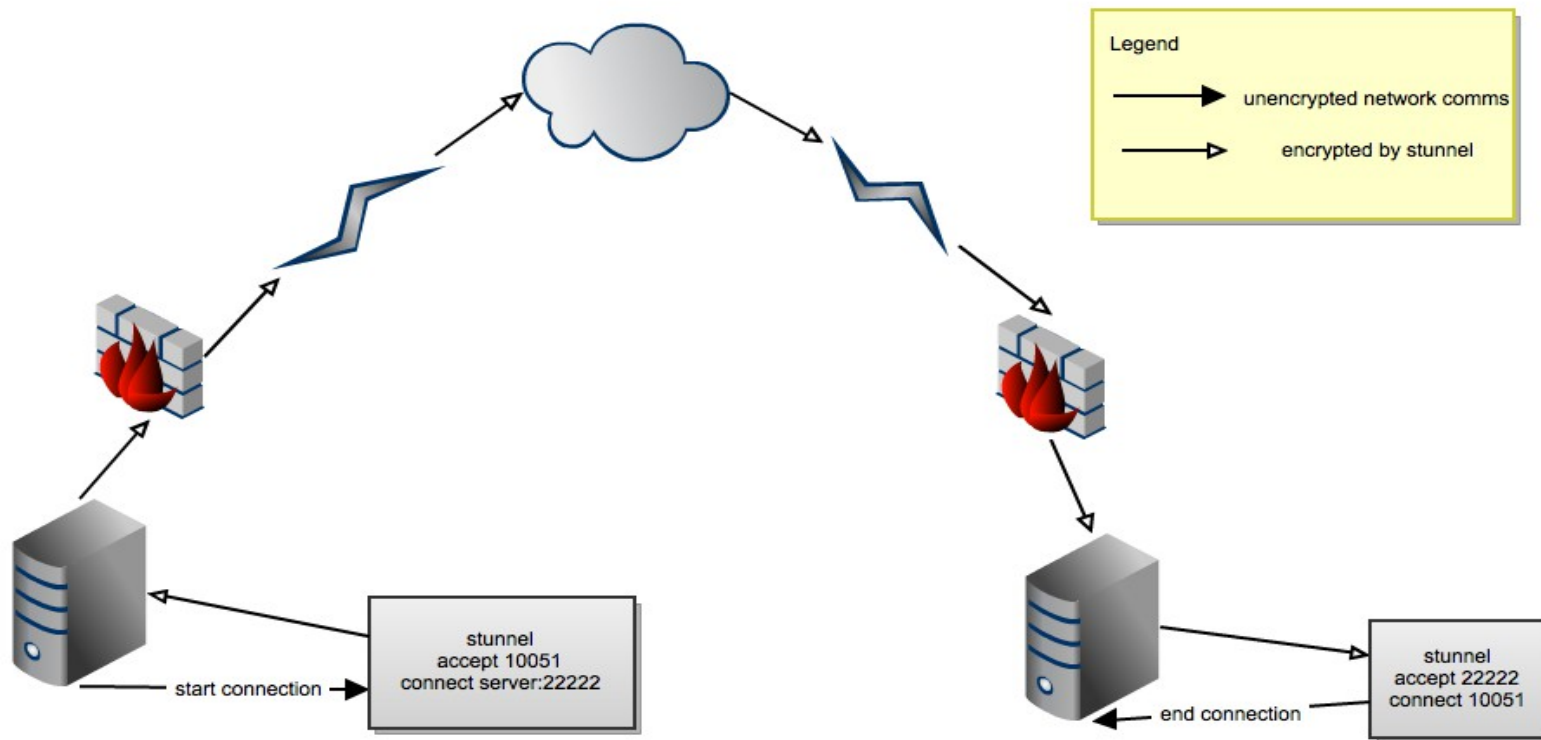
One of our clients was looking for a solution to install zabbix at their customers.

One of the problems they had was that the communication was not secure between proxy, nodes and the server.

We offered them to look at stunnel so zabbix became a valuable option for them.

At this moment they are in the fase of testing the whole concept.

# Securing with Stunnel



- Zabbix proxy sends it's data unencrypted stunnel will capture it and send it encrypted over port 11612 to the server.
- Data from port 11612 will be send unencrypted to port 10050 or 10051.
- Stunnel can run multiple ip's and certs in one instance (v4.15+)
- Stunnel server can accept multiple clients
- Reference : <http://www.mrvoip.com.au/blog/secure-zabbix-proxy-communications-stunnel>

## A Few Good Practices to install Zabbix at your clients

- Explain to your customer that Zabbix lives. Infrastructure changes so zabbix needs to evolve.
- With this in mind try to sell a Zabbix course to your customer or tell him that u can provide that service. (1 Day crash course ? )
- Zabbix + Nodes + Stunnel => provide Zabbix as a service to your customers
- When installation is finished go back after a few weeks to do some tweaking
- Take contact with your customers on regular basis ex: Every year to see if Zabbix needs to be adapted