Setup of a ssl certificate with let’s encrypt

Clément Levallois

2017-04-09

Table of Contents

last modified: 2018-02-04

System

- I use Debian, version 8.7 (why?)
- Vi is used as a text editor in the following

Why SSH?

- SSH allows 2 computers to connect to each other , even with a firewall on each computer (how?).
- The data transitting between the 2 servers is not encrypted, but it is tunnelled in a way that protects it from preying eyes (how?)
- For this reason, SSH tunneling is a nice way to have a couple or even more computers to discuss with each other: to go from a single server to a cluster!
- My use case: a prod server that does the heavy lifting, a small server which receives the API requests from the public and polls the prod server for answers.

Difficulty: SSH is pretty hard to setup for beginners.

Setup

Prod server: A.A.A API server: B.B.B

I want the db in A.A.A to be tunneled to B.B.B. The API server on B.B.B. can query the db as if it was in localhost.

From B.B.B. : - creating a pair of keys: source: https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys—2

```
ssh-keygen -t rsa
```

This generates a private key id_rsa and a public key id_rsa.pub, both of them in the folder /home/user/.ssh/

On A.A.A.: - copying the id_rsa.pub made on B.B.B and pasting it as a new line in authorized_keys in A.A.A. - restart sshd with: service sshd restart

From B.B.B.: ssh -Nf -L 9200:localhost:9200 myuser@A.A.A -p 22

(9200 is because I want to tunnel Elasticsearch) (actually replace 22 by the port you configured in sshd_config in A.A.A)

(the Nf option puts the SSH connection in the background. Indeed, we don't care about it - we don't want an interactive session in a console. Just the port 9200 to be tunneled.)

(see http://stackoverflow.com/questions/25048045/elasticsearch-remote-access-through-ssh) Closing an SSH tunnel: http://stackoverflow.com/questions/9447226/how-to-close-this-ssh-tunnel

SCP

here: make sure you have access to the file you want to move, both in origin and dest folders!

scp -P 1234 /var/redis/6379/dump.rdb username@destinationhost:/home/username

To copy a full directory:

scp -r -P 1234 /var/folder username@destinationhost:/home/username/folder

the end

Author of this tutorial: Clement Levallois

All resources on linux security: https://seinecle.github.io/linux-security-tutorials/