Accessing a Remote Service
Intelie Challenge – Support Analyst

The challenge

Explain a possible solution to remotely access a running service that is on a locked port. We have the ClientA that needs to access a service on ServerB, on port 8000, using the HTTP protocol, but there is no route available between them. It is known that the only connection between ClientA and ServerA and between ServerA and ServerB is via SSH. We have another service running on port 8000 of Server A and this can not be impacted. It should be noted that all servers run on CentOS7 without X.

Applied Solution - Port Forwarding by SSH Tunneling

SSH tunneling is mainly used for testing, however, it is not suitable for the production environment because of security breaches. It should be applied only as a palliative for urgent problems. The correct way to apply it would be to configure SGs (Security Groups) and VPC (Virtual Private Cloud) settings, if the services are virtualized (AWS). Otherwise, the configuration must be changed on the Network to give the port permission via VPN or endpoint of this restricted access.

Possible failures: Restrictions due to Firewall configuration or network configuration account.

Accessing a Remote Service
Intelie Challenge – Support Analyst

Application

ClientA: We must access via SSH terminal the ClientA server, logging in with root user privileges. After this action, you must edit the sshd_config configuration file, setting the AllowTcpForwarding parameter to 'yes' and removing all comments from the (#) line. Once this is done, the service must be restarted. Here are the commands:

1. Login as root (or other user and sudo privileges)

2. Editing the configuration file: *# vi /etc/ssh/sshd_config*

   #AllowTcpForwarding no → AllowTcpForwarding yes

3. Save the change: esc → *:wq!*

4. Restarting the service: *# systemctl restart sshd*

5. Checking the status of the service: *# systemctl status sshd*

5. Running the tunneling: *# ssh -g -L777: serverA:777 user@serverA*

Explanation: Here, we will forward the <ClientA>:777 to <ServerA>:777, using a user capable of logging into ServerA

Accessing a Remote Service
Intelie Challenge – Support Analyst

ServerA: On this server, you must make the same change in the sshd configuration file (sshd_config), performed in the ClientA, except the tunneling command, which should read as follows:

```
# ssh -g -L777:serverB:8000 user@serverB
```

Explanation: Here, we forward the <ClientA>:777 to <ServerB>:8000, using a user able to log in to ServerB.

ServerB: On ServerB, the same change must be made to the sshd configuration file (sshd_config), which is performed in the ClientA, except for the tunneling command, which does not require execution on this server.

Accessing a Remote Service
Intelie Challenge – Support Analyst

IMPORTANT

It is worth emphasizing the importance of the "-g" option in the tunneling performed between the servers, since this allows the clientA to remotely access the serverB, because without this option, access is only possible when performed locally on serverA.

After these actions, ClientA can access the content of the service that is contained in ServerB. You can call the service in the following ways:

```
# curl serverA:777
```

or

```
# curl -I http://serverA:777
```

Thank you for the opportunity.

Sincerely, Leandro Marques