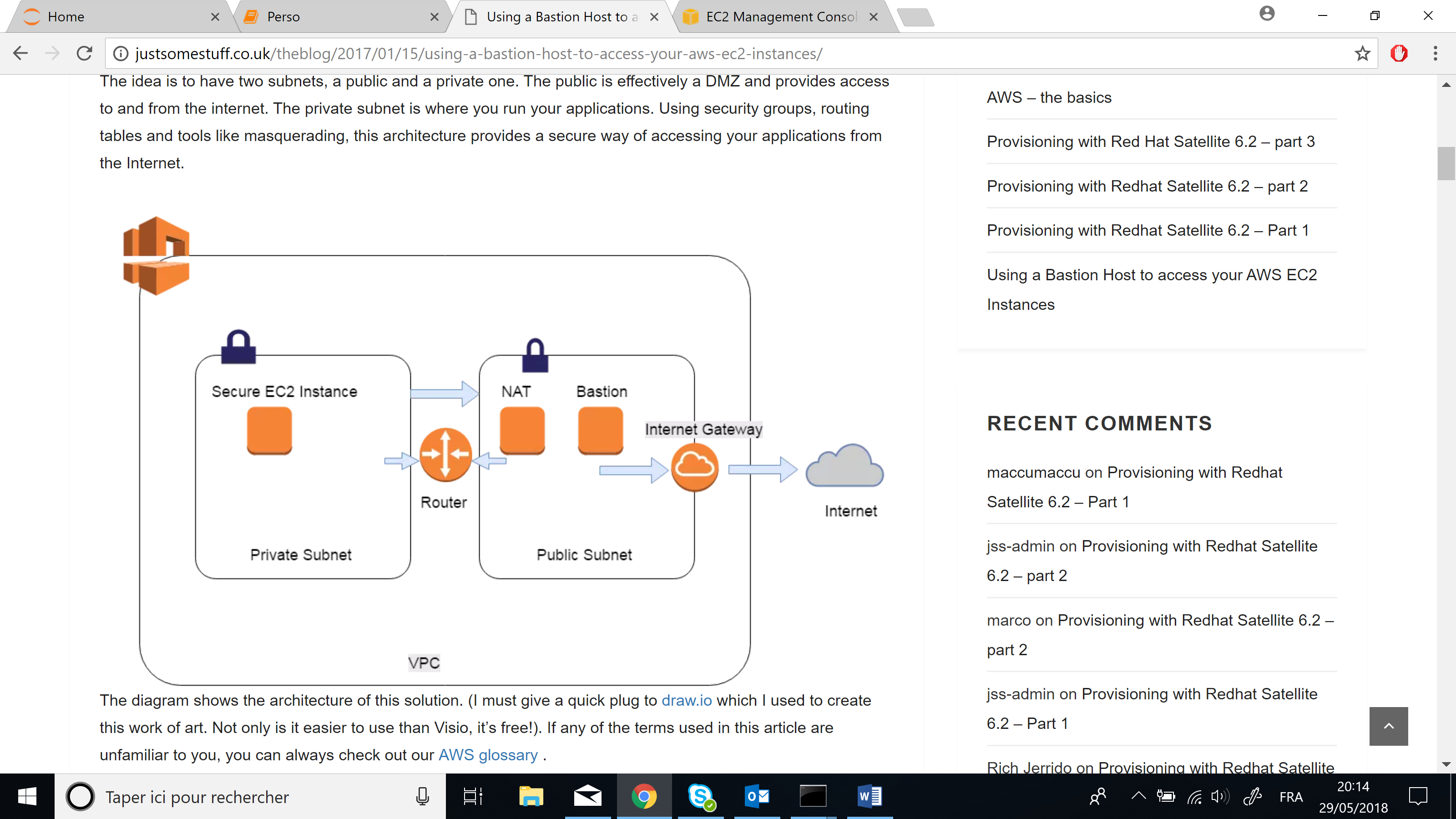
AWS Bastion Host

L’objectif est de construire un VPC avec un sous-réseau public relié à un sous-réseau privé qui contient une instance EC2 qui ne peut pas être connectée depuis Internet mais uniquement depuis un bastion hôte placé dans le sous-réseau public. Ainsi, la sécurité de l’instance privée est augmentée.

Ci-dessous est représentée l’architecture globale du système.



Architecture globale de la solution

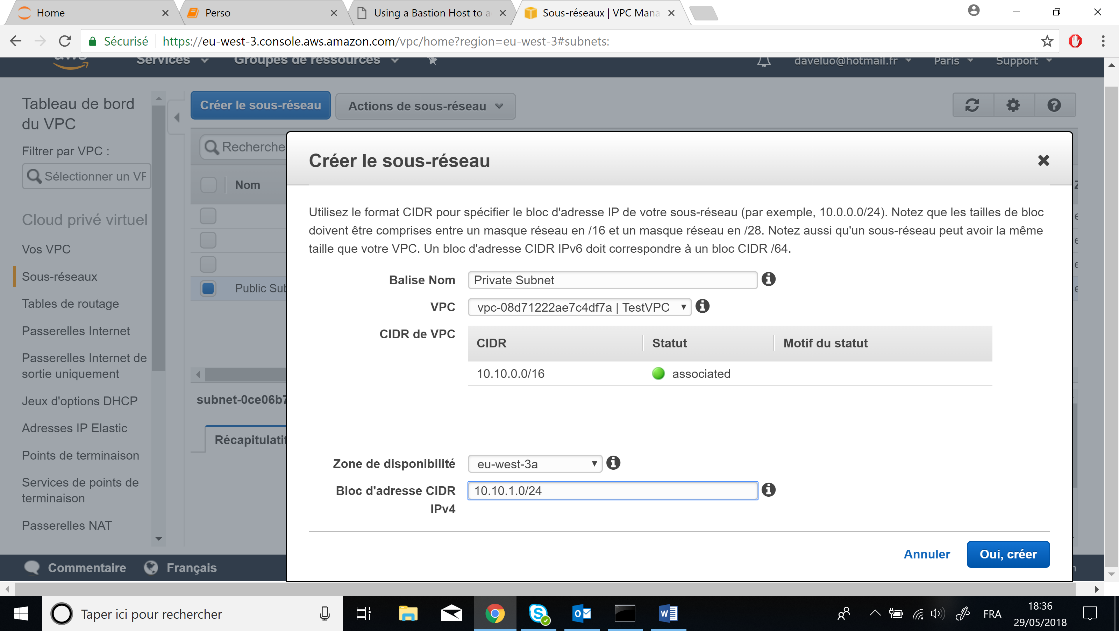
Implémentation de la solution

On crée d’abord le VPC : On choisit comme nom TestVPC, comme CIDR Block 10.10.0.0/16, et les autres paramètres par défaut.

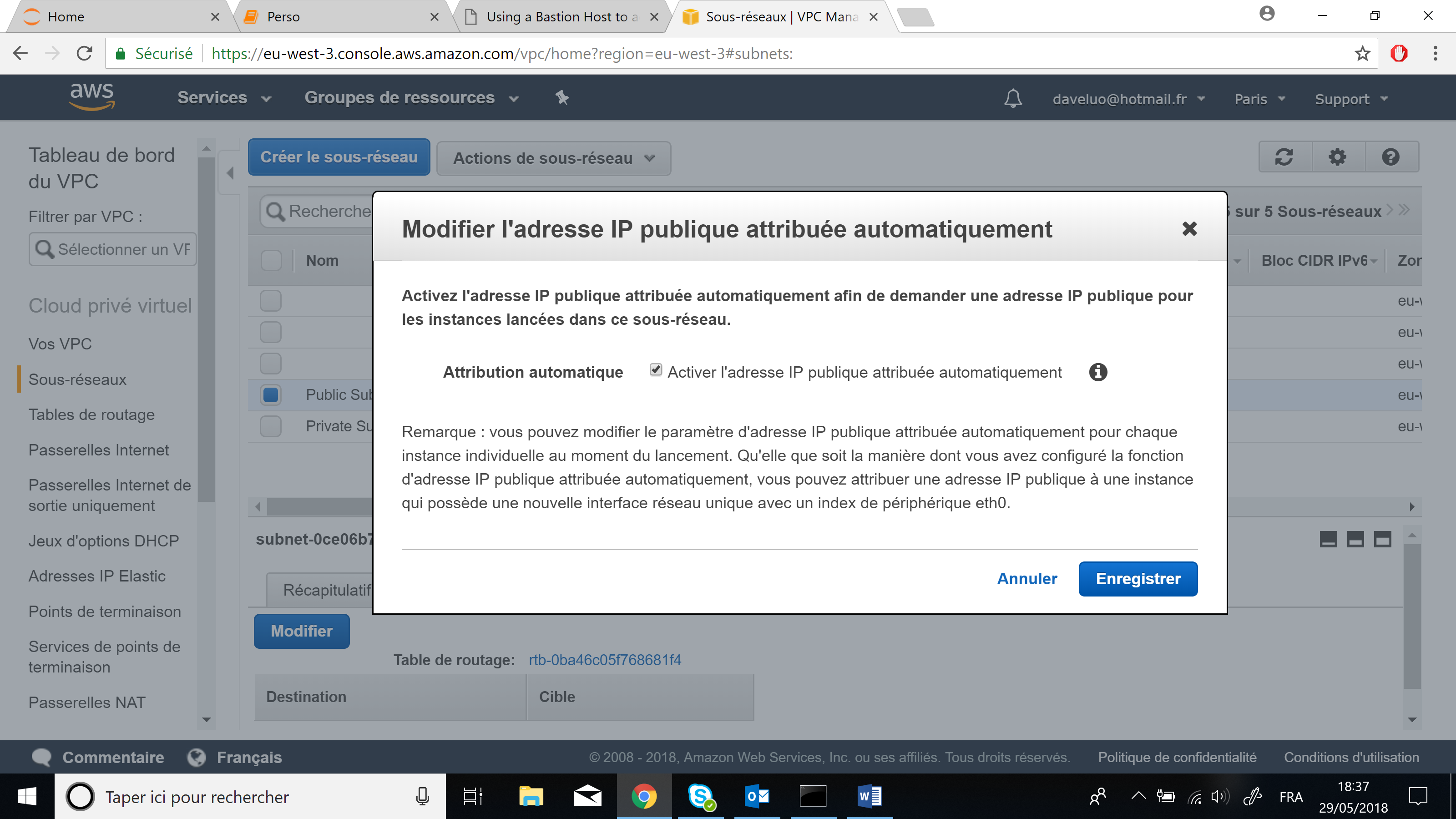
On crée ensuite les réseaux privés et publics :

Privé: Nom : Public Subnet, VPC : TestVPC, Availability Zone : whatever, CIDR Block : 10.10.0.0/24,

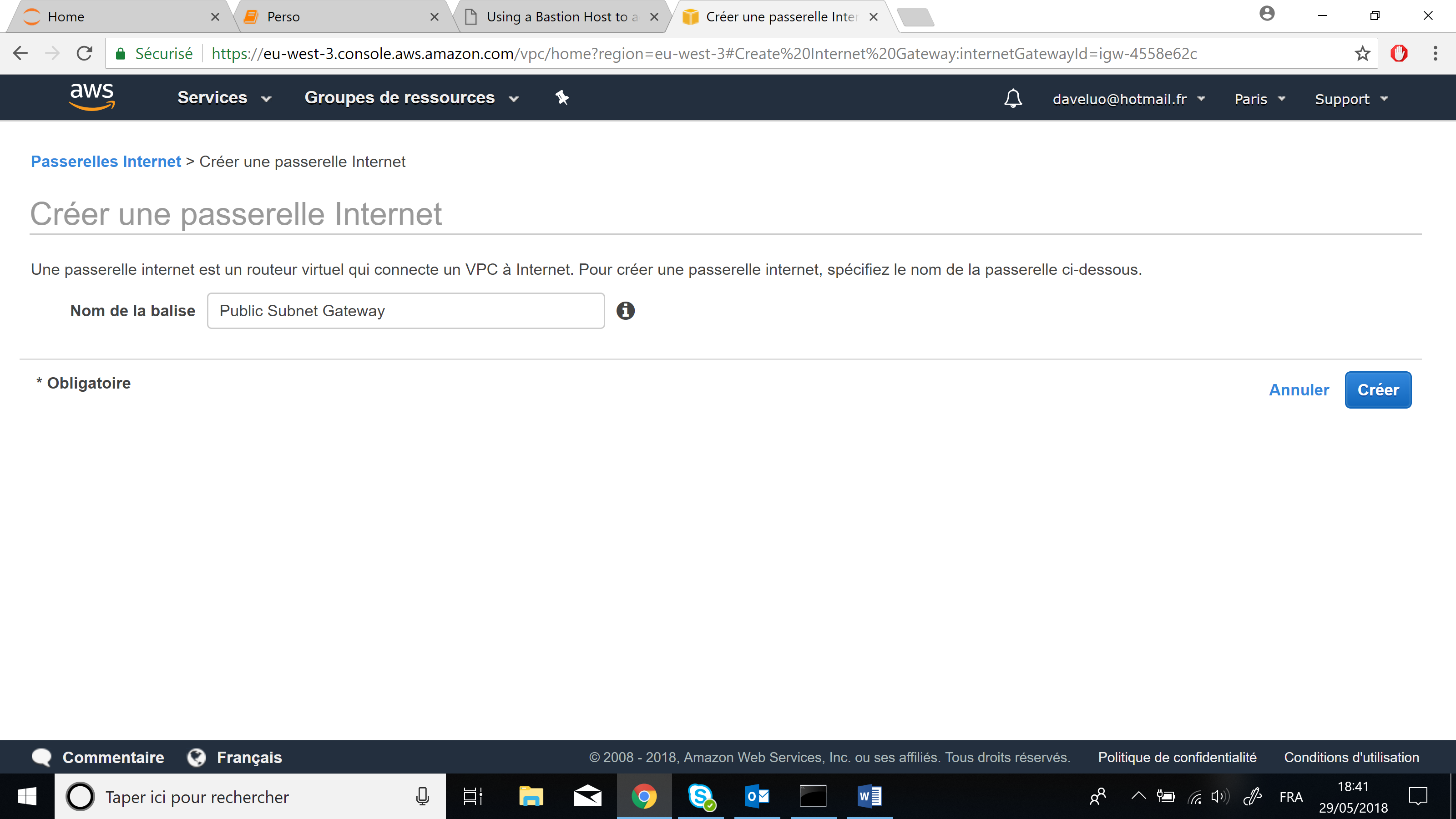
Public: Nom : Private Subnet, VPC : Même qu’avant, Availability Zone : same, CIDR Block: 10.10.1.0/24



On choisit l’option « Modify Auto-Assign Public IP » pour le réseau public.



On crée ensuite la passerelle Internet. Dans le dashboard VPC, on choisit Internet Gateways. Dans la boite de dialogue, on entre Public Subnet Gateway et on valide. Puis on attache la passerelle au VPC.



Maintenant, on crée une table de routage :

Name tag : Public Route Table

VPC: TestVPC

Dans l’onglet Routes tab, on ajoute la destination : 0.0.0.0/0, avec la cible Public Subnet Gateway.

Dans l’onglet Subnet Associations, on associe le sous-réseau public.

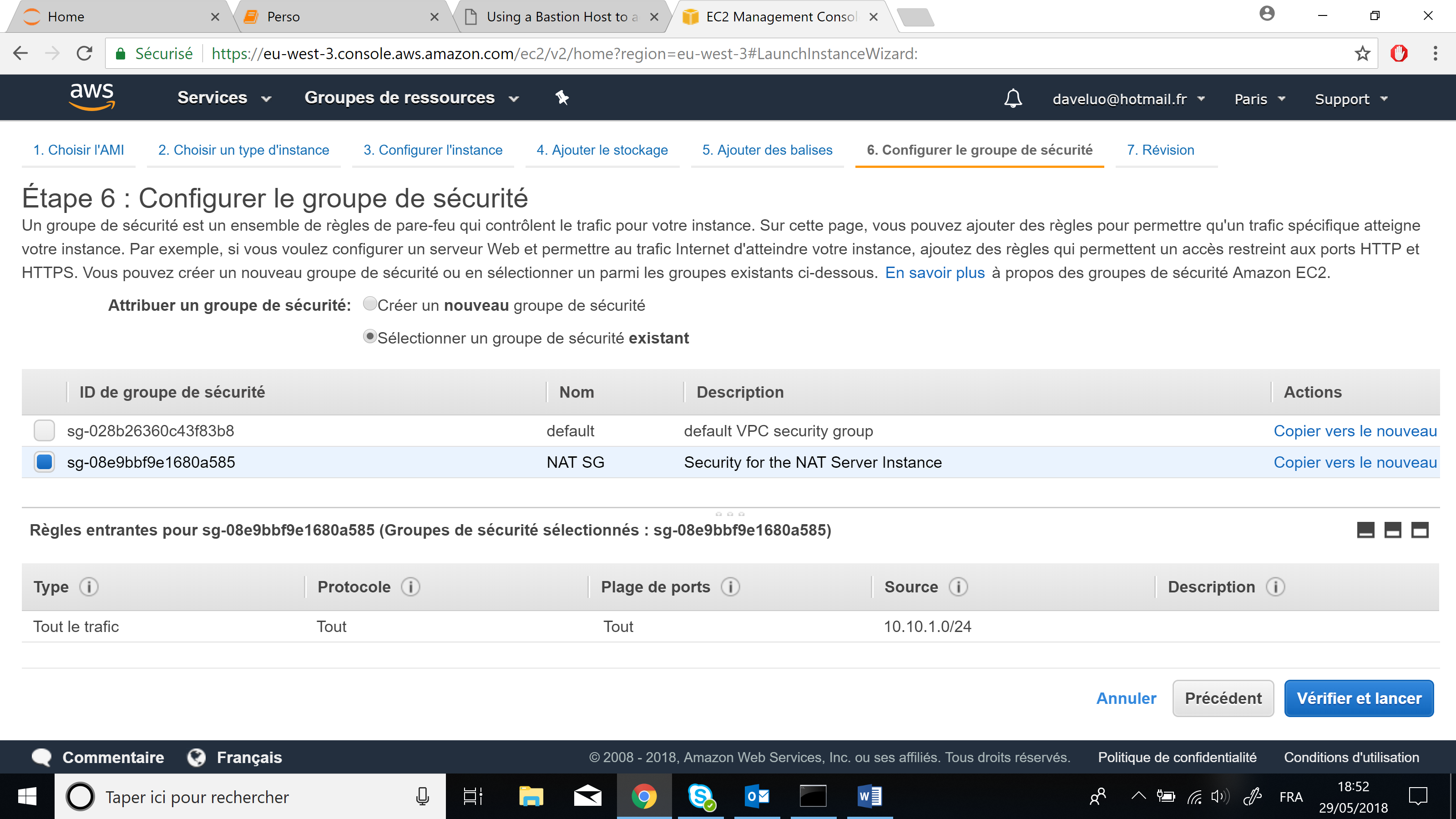
On crée la table de routage privée qui autorise le réseau privé à se connecter au serveur NAT : on associe la table à Private Subnet. Et on associe le sous-réseau Private Subnet avec Private Route Table.

Ensuite on crée le NAT Server Instance Security Group : celui-ci restreint le NAT à recevoir du trafic uniquement du réseau privé.

Dans le menu EC2, on va dans Security Groups. On crée un groupe de sécurité configuré comme suit :

Security group name : NAT SG

VPC : TestVPC



On ajoute une règle Inbound :

Type : All traffic

Source : 10.10.1.0/24 (CIDR du réseau privé)

On crée ensuite l’instance NAT EC2 : Amazon Linux AMI (t2.micro).

Network : TestVPC, Subnet : Public Subnet, Auto-Assign Public IP: Enable (automatic)

Dans la section Advanced Details, on ajoute le code suivant :

#!/bin/sh

echo 1 > /proc/sys/net/ipv4/ip\_forward

echo 0 > /proc/sys/net/ipv4/conf/eth0/send\_redirects

/sbin/iptables -t nat -A POSTROUTING -o eth0 -s 0.0.0.0/0 -j MASQUERADE

/sbin/iptables-save > /etc/sysconfig/iptables

mkdir -p /etc/sysctl.d/

cat <<EOF > /etc/sysctl.d/nat.conf

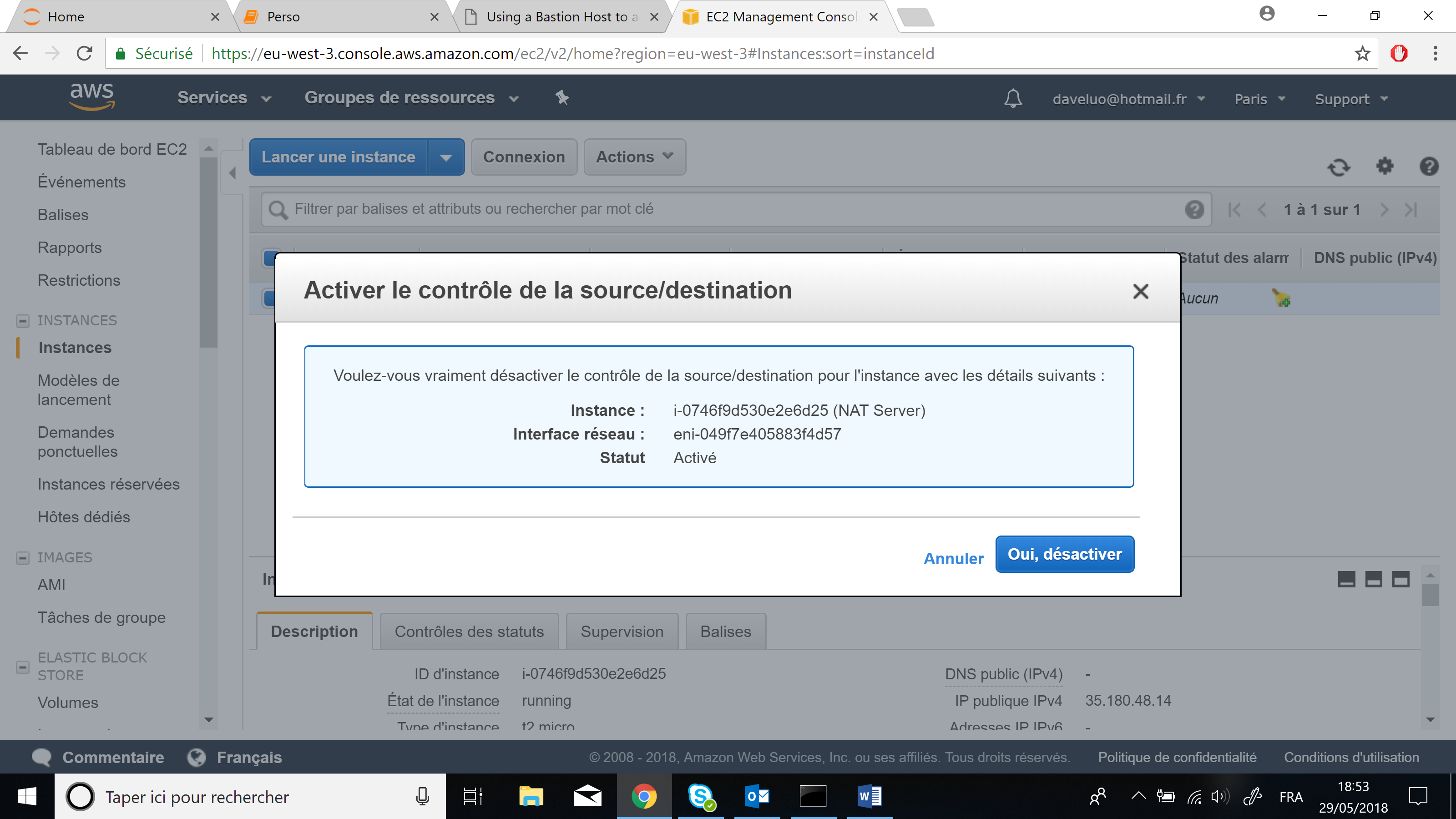
net.ipv4.ip\_forward = 1

net.ipv4.conf.eth0.send\_redirects = 0

EOF

Ce script configure le serveur comme un NAT de sorte qu’il puisse rediriger les requêtes IP vers la machine interne et faire des requêtes externes au nom du serveur interne.

Après avoir fini de configurer le serveur, on va dans le Dashboard EC2 et on fait clic droit sur le NAT Server. Sous Networking, on clique Change Source/Destination et on désactive.



On relie le réseau privé au serveur NAT en créant une route privée dans la table de routage privée : Dans le menu VPC, on clique Route Tables et on choisit Private Route Table. Dans l’onglet Routes, on modifie : Destination : 0.0.0.0/0, Target : NAT Server.

On crée ensuite le bastion hôte. Dans le menu EC2, on va dans Security Groups et on clique sur Create Security Groups :

Security group name : Bastion Security Group

VPC: TestVPC

Dans Inbound Tab, on ajoute Type : SSH, Source : Custom et l’adresse IP personnelle.

On crée l’instance : Amazon Linux AMI (t2.micro) : Network : TestVPC, Subnet : Public Subnet, Auto-Assign Public IP : default

Dans la section Advanced Details, on ajoute le script suivant :

#!/bin/sh

yum update -y

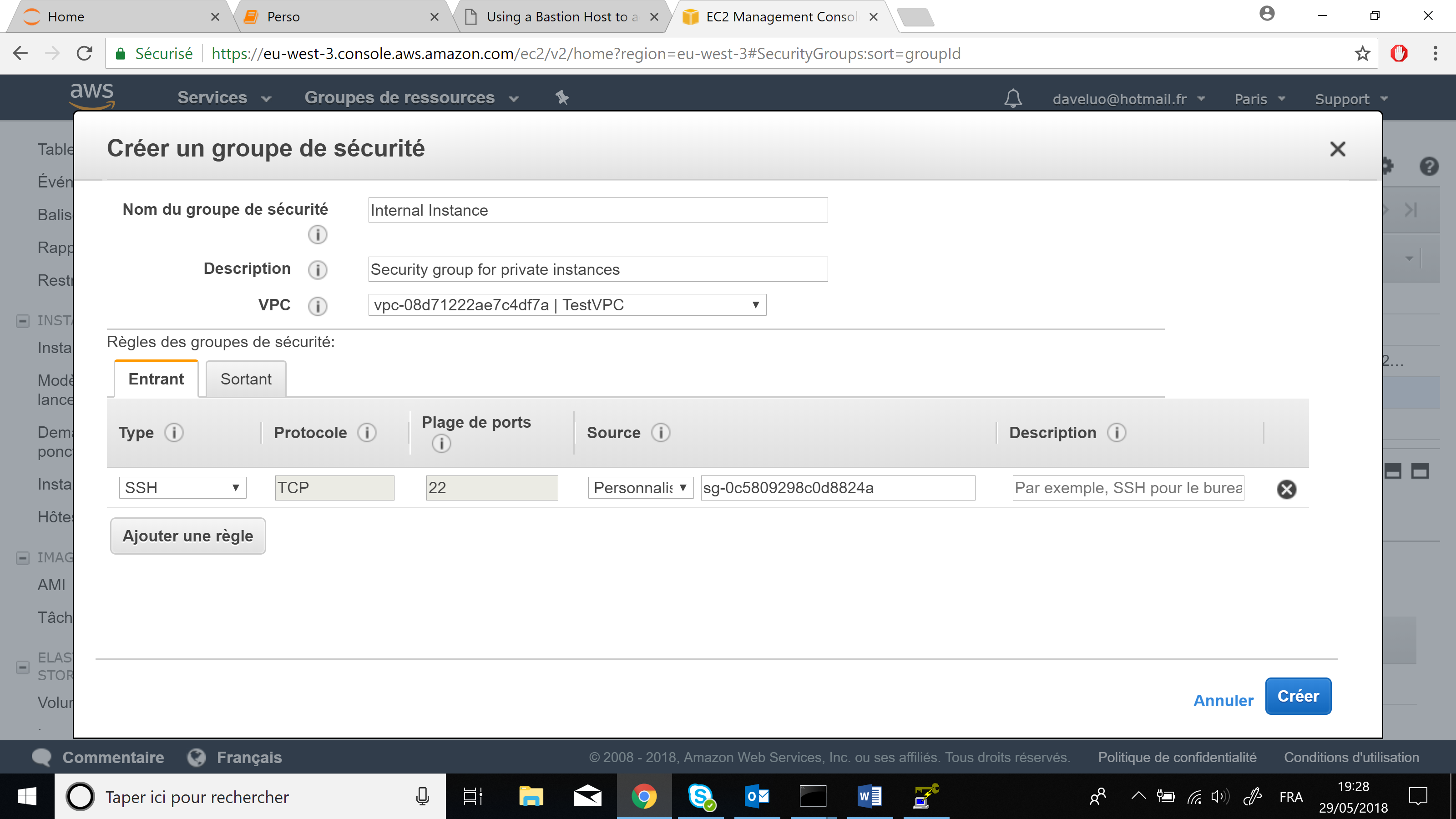
Ce script permet au serveur de télécharger les mises à jour sécurité.

Dans Configure Security Group, on choisit Bastion Security Group.

Maintenant, on crée une instance EC2 dans le réseau privé.

On crée d’abord une nouvelle paire de clé, uniquement pour l’instance privée. Le groupe de sécurité du réseau privé accepte uniquement les connexions SSH du bastion hôte. Pour se connecter à l’instance, il faut d’abord se connecter au bastion puis à l’instance privée. Dans la console EC2 Management, on clique sur Key Pairs et on crée une nouvelle paire. Avec Putty, on convertit le fichier PEM en clé PPK.

Dans la console EC2, on clique sur Security Groups. On crée un nouveau groupe de sécurité : Name : Internal Instance, VPC : TestVPC. On ajoute comme règle : SSH, Source :Custom avec le Group ID du Bastion Security Group. Ainsi, seules les instances appartenant au groupe de sécurité du bastion peuvent se connecter à l’instance interne.

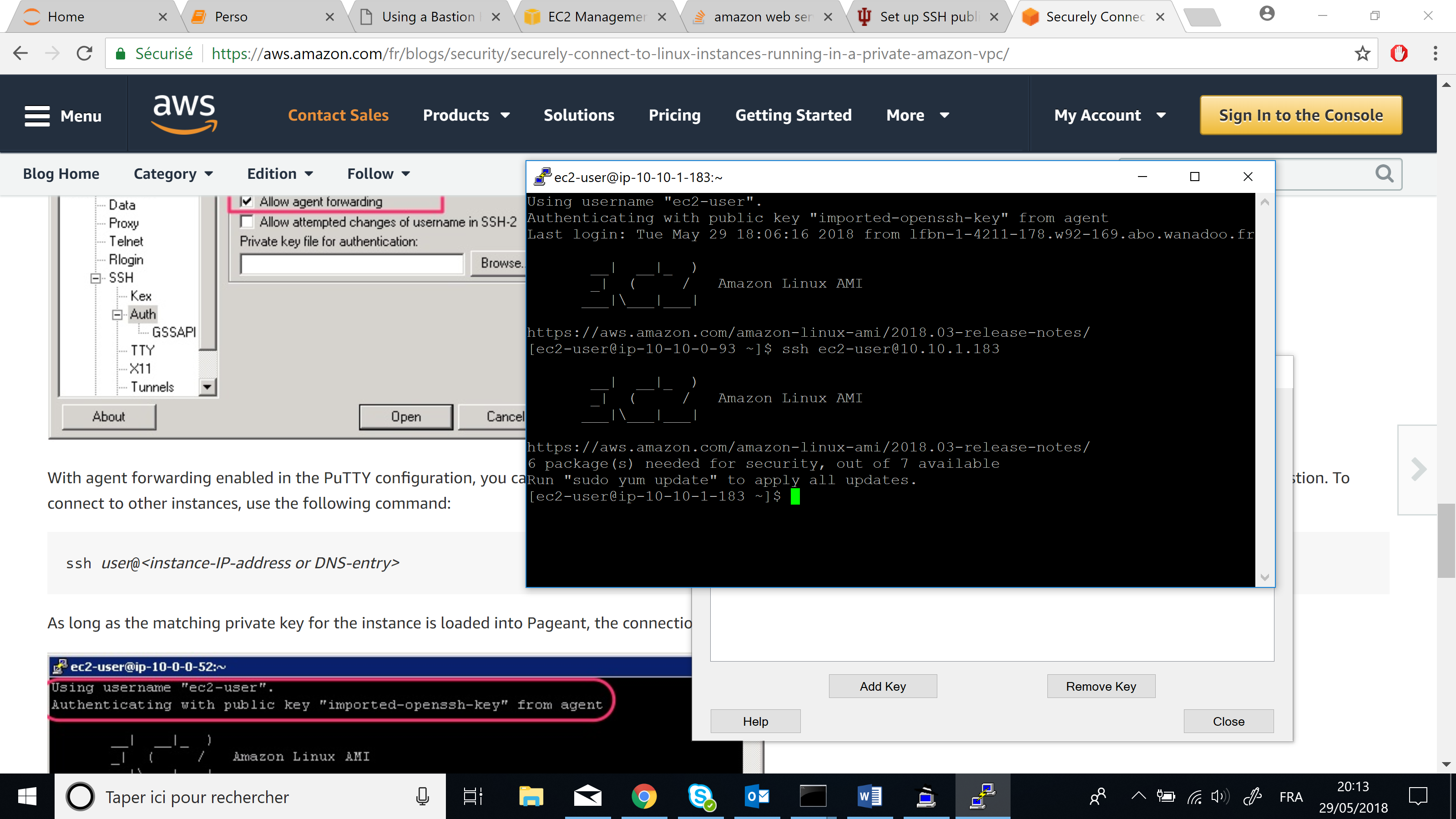


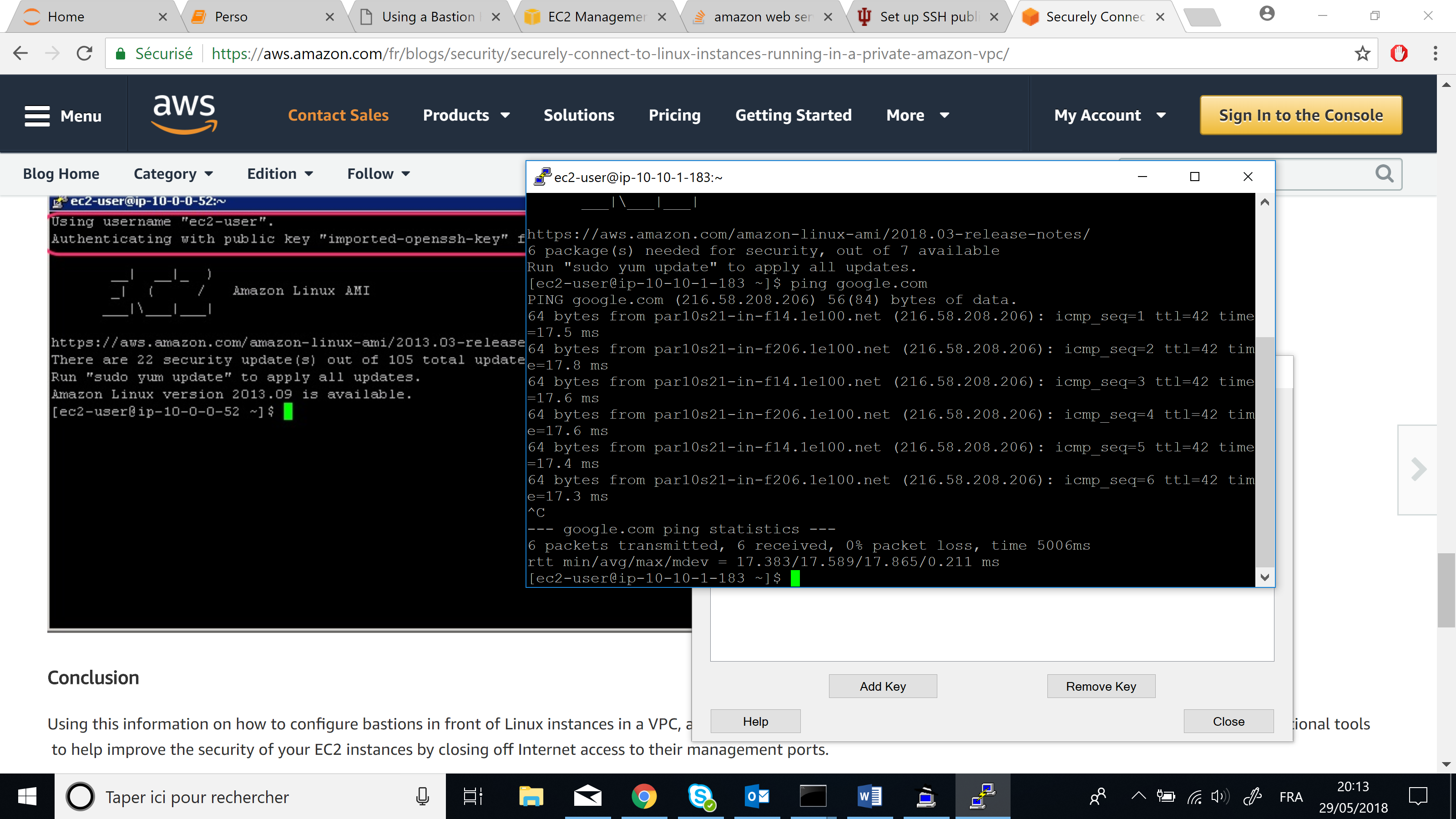
On crée l’instance privée, on lui associe le groupe de sécurité précédemment crée et on lui associe la nouvelle paire de clé.

Il faut maintenant configurer le ssh-agent. Pour pouvoir utiliser SSH-agent, on peut utiliser Pageant. Puis on utilise l’option agent forwarding dans PUTTY pour se connecter à des instances dans des réseaux privés. Sur Pageant Key List, on ajoute le fichier PPK. Sur Putty, on coche la case qui correspond à Allow agent forwarding et on laisse le champ Private Key file for authentication vide.

Une fois connecté, on tape ssh accompagné de ec2-user@private-ip-adress.

Une fois connecté à l’instance privée, on peut pinger google.com





Ci-dessous se trouve un aperçu du Dashboard final.

