ACORUS NETWORKS

L’automatisation, un outils indispensable à la cybersécurité

Alexandre Corso et Remy Pouppeville

Le 13 décembre 2018

QUI SOMMES NOUS

- Alexandre Corso (aka Master Minion), ingénieur de formation, anciennement chez France-IX et depuis 1 an chez Acorus Networks, s'assure du fonctionnement du backbone Acorus Networks, de son automatisation et de la R&D réseau.
- Remy Pouppeville (aka Minion), ingénieur de formation, anciennement chez Blade Shadow et depuis peu chez Acorus Networks, venu renforcer l'équipe réseau et permettre son déploiement à l'international.

*Nous recrutons

ACORUS NETWORKS

ACORUS NETWORKS

Acorus Networks est une entreprise Française qui fournit des services de protection DDoS réseau et applicatif. Elle possède son propre réseau d'opérateur en Europe, en Amérique du Nord et bientôt en Asie du Sud-est, ce qui lui permet de filtrer plusieurs Térabits de DDoS.

Acorus Networks protège des clients dans le domaine du Cloud, SaaS, Web, e-commerce, jeux en ligne, la santé, la finance, etc.

Nous mettons en place un système de protection robuste et à grande échelle personnalisable pour chacun de nos clients. Chaque client peut contrôler sa protection en amont de son infrastructure réseau ou web sans avoir à investir dans des boîtiers et liaisons internet à haute capacité.

ACORUS NETWORKS

WORKSHOP - LES PRE-REQUIS

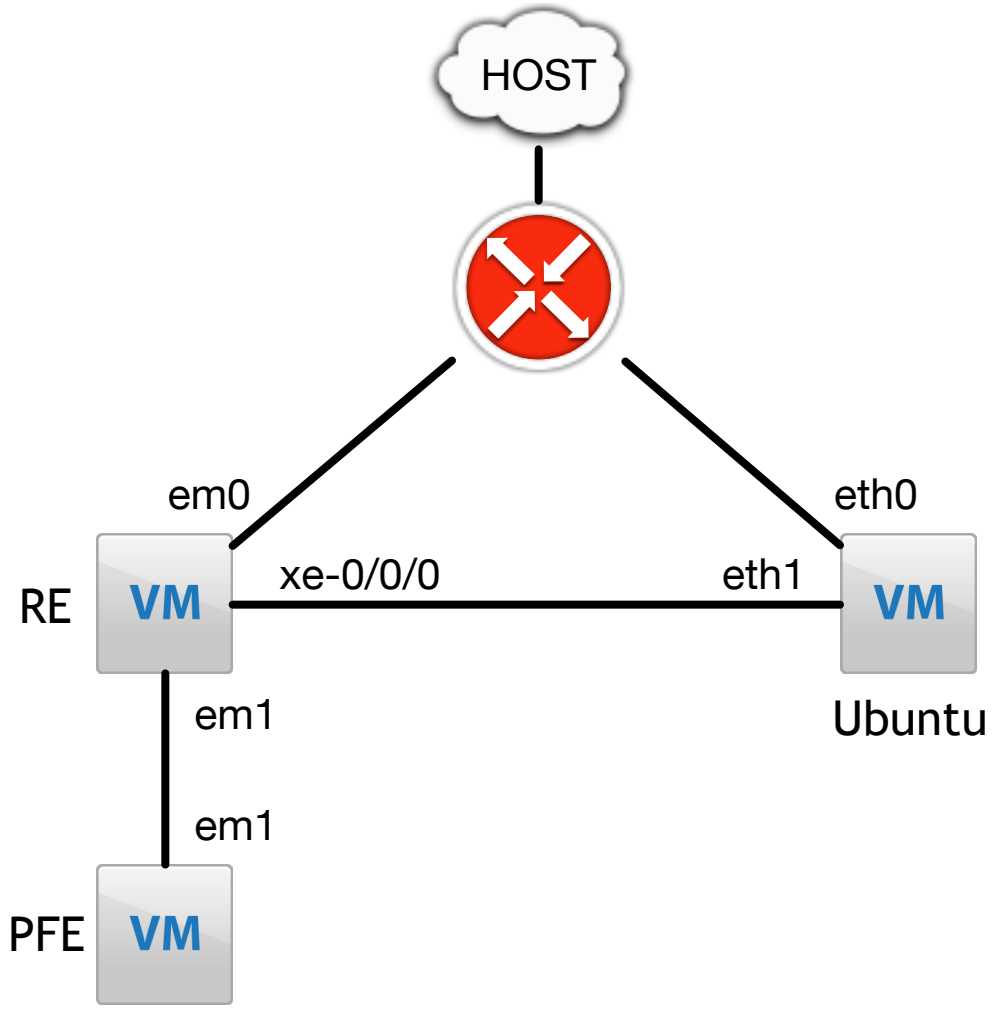
- Vagrant (min 2.2)
- Virtual Box (min 5.2)
- Les images de Junos et Ubuntu (via internet / clé USB)
- Compréhension de BGP (routage principalement)
- Connaissance d'Ansible

ACORUS NETWORKS

TOPOLOGIE PHYSIQUE

Vagrant contrôle VirtualBox pour lancer 3 machines virtuelles:

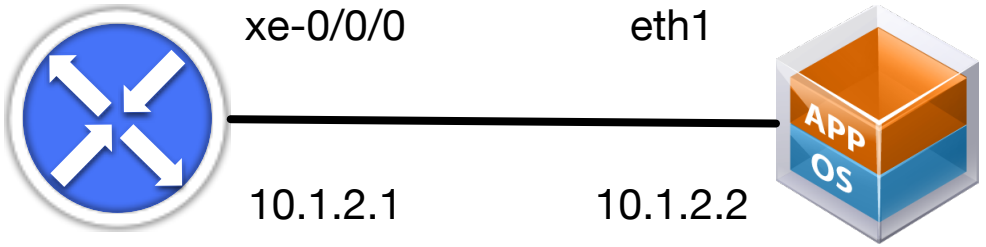
- Ubuntu (xenial)
- vQFX-RE
- vQFX-PFE



ACORUS NETWORKS

TOPOLOGIE LOGIQUE

- Un routeur JunOS avec une interface UP
- Un serveur Ubuntu avec une interface connectée au routeur
  - Un Ansible
  - Un BIRD



ACORUS NETWORKS

DÉMARRER LE LAB

- Démarrer les VMs

```
vagrant box add vqfx10k-re.box --name juniper/vqfx10k-re
vagrant box add vqfx10k-pfe.box --name juniper/vqfx10k-pfe
vagrant box add xenial64.box --name ubuntu/xenial64

vagrant up
```

- Test de connectivité

```
vagrant ssh vqfx
        show configuration
vagrant ssh srv
        ping 10.1.2.1
        ssh vqfx
```

- Test des outils

```
vagrant ssh srv
        ansible-playbook -i inventories/hosts pb.test.netconf.yaml
```


ACORUS NETWORKS

TUTORIAL 1

Nous allons ajouter un nouveau utilisateur sur le routeur Juniper

- Pour des raisons de sécurité, nous ne stockons que le HASH du password qui est lui-même chiffré dans un coffre fort (vault)

- Pour créer le hash du mot de passe, nous utilisons le vqfx (pour des raisons de simplicité):

```
vagrant ssh vqfx
        edit
        set system login user {YOUR_USER} class read-only authentication plain-text-password
        show | compare
```

Le HASH ressemble à 6…..

ACORUS NETWORKS

TUTORIAL 1

- Edition du fichier

vagrant ssh srv

```
EDITOR=nano ansible-vault edit inventories/group_vars/all/users.yaml
```

Password : gN4PFTz5nmWWqpiYzmrcdSwHif6ePkYy7zwyhfkeFAQW9HwAVM3edKjDAmM5nKa

- On applique la configuration sur le routeur via Ansible

vagrant ssh srv

```
ansible-playbook -i inventories/hosts pb.juniper.users.yaml --vault-id ~/.vault_pass.txt
```

- Vérification

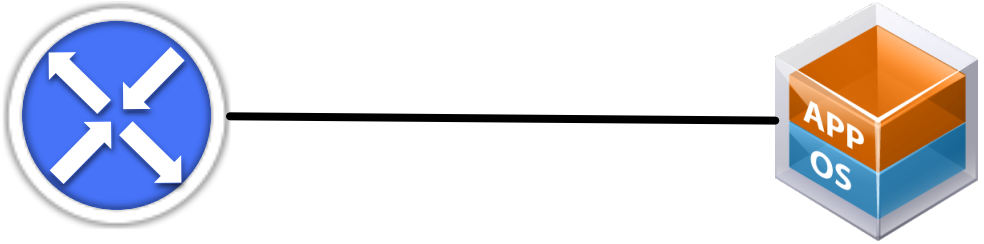
vagrant ssh srv

```
ssh {YOUR_USER}@vqfx
```


ACORUS NETWORKS

TUTORIAL 2

Nous allons configurer une session BGP et filtrer les annonces reçues



- Le routeur annonce 1 route 0.0.0.0/0 (par defaut)

Le serveur annonce 2 routes
1.1.1.0/24
2.2.2.0/24

ACORUS NETWORKS

TUTORIAL 2

- On applique un template pour configurer la session BGP

vagrant ssh srv

```
ansible-playbook -i inventories/hosts pb.juniper.bgp.yaml --vault-id ~/.vault_pass.txt
```

- Vérification

vagrant ssh vqfx

```
show bgp summary
```

- Routes reçues

vagrant ssh vqfx

```
show route receive-protocol bgp 10.2.1.2
```


ACORUS NETWORKS

TUTORIAL 2

- Modification de la “policy” d’import

vagrant ssh srv

```
nano ~/ansible/inventories/group_vars/all/bgp_transit_filter.yaml
ansible-playbook -i inventories/hosts pb.juniper.bgp.yaml --vault-id ~/.vault_pass.txt
```

- Vérification

vagrant ssh vqfx

```
show route receive-protocol bgp 10.2.1.2
```


ACORUS NETWORKS

TUTORIAL 3

- Comment supprimer un filtre via Ansible ?

- Une solution ?

ACORUS NETWORKS

CONCLUSION

- L’automatisation est nécessaire pour être réactif et surtout proactif
  - Optimiser les tâches répétitives
  - Règles de sécurité homogènes sur toute une infrastructure
  - Transmettre rapidement les informations de sécurité
  - Limiter les erreurs humaines

ACORUS NETWORKS

Alexandre Corso
alexandre@acorus.net
@CorsoAlexandre

Remy Pouppeville
remy@acorus.net
@RemyPouppeville

https://github.com/alexandrecorso/nsd2018

THANK YOU

K e e p y o u r b u s i n e s s o n

info@acorus.net www.acorus-networks.com @acorusnetworks