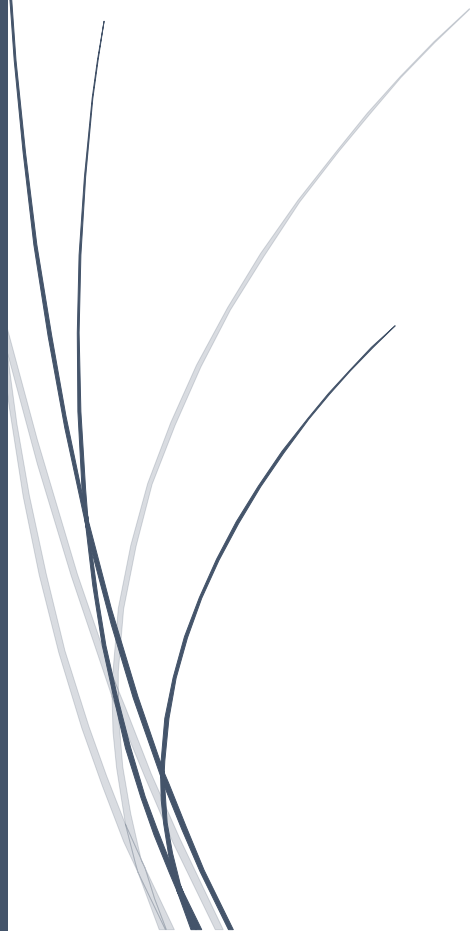


A dark blue vertical bar on the left side of the page. A blue arrow points to the right from the bar, containing the date.

20/01/2024

TP IPSEC

Rapport de TP

Several thin, curved lines in dark blue and light grey originate from the bottom left and sweep upwards and to the right.

Jules AMELOT, Carole GAREL, Léo DONATH-ILIC,
Erwann GASCHET
ESAIP

Table des matières

Rappelle Consigne	2
Document à rendre.....	2
Technologie Utilisée	3
Docker	3
Strongswan.....	3

Rappelle Consigne

Utiliser strongswan et docker pour créer un réseau sécurisé entre deux sites

Document à rendre

- Un zip avec les fichiers docker
- Un fichier avec les commandes pour mettre en place la connexion sécurisée.
- Une explication sur les algorithmes cryptos utilisés.

Technologie Utilisée

Docker

Docker est une plateforme de virtualisation légère qui permet d'emballer des applications et leurs dépendances dans des conteneurs portables. Ces conteneurs sont des unités d'exécution isolées qui encapsulent une application avec toutes les bibliothèques et configurations nécessaires, assurant ainsi une portabilité entre différents environnements. Docker facilite le déploiement, la gestion et la mise à l'échelle des applications, tout en offrant une efficacité de ressources accrue par rapport aux machines virtuelles traditionnelles.

Strongswan

StrongSwan est une solution open-source de réseau privé virtuel (VPN) basée sur le protocole IPsec (Internet Protocol Security). Il offre une sécurité robuste en permettant l'authentification et le chiffrement des communications réseau. StrongSwan est conçu pour établir des connexions VPN sécurisées, assurant la confidentialité, l'intégrité et l'authenticité des données échangées sur des réseaux non sécurisés, tels qu'Internet.

Préparation de l'environnement

Pour faire ce TP, nous avons commencé par créer un docker pour conteneuriser nos machines.

Nous avons choisi de les nommée Alice et BOB.

Nous leur avons attribué une adresse IPv4 à la main dans leur configuration directement

```
networks:
  syd_tp_001_ipsec_network:
    ipv4_address: 10.0.0.101
```

Et nous avons aussi créé un fichier partagé entre nos 2 machine pour plus de simplicité

```
volumes:
  - "./exchange/:/exchange_alice/"
```

Une fois nos machine prête a l'emploi, nous avons paramétré des commandes qui s'exécute automatiquement au lancement de celle-ci

```
FROM ubuntu:bionic

RUN apt-get update \
    && apt-get install -y net-tools iputils-ping iproute2 nano strongswan \
    && cd / && mkdir exchange_alice \
    && cd / && mkdir alice \
    # && echo "route add default gw 192.168.111.3 eth0" > /alice/add_default_gateway.sh \
    # && chmod +x /alice/add_default_gateway.sh
    && mkdir /ca
```

Nous retrouvons le système d'exploitation, Ubuntu, mais nous avons ici l'installation de plusieurs logiciels comme strongswan. Nous avons aussi créé des dossier et d'autre petit paramètre.

Nos machines sont prêtes, nous pouvons les lancer.

```
PS C:\Users\JulesAMELOT\OneDrive\ESAIP\chiffrement et VPN\TP IPSEC\TP IPSEC> docker-compose up -d
[+] Building 0.0s (0/0)                                                                                               docker:default
[+] Running 5/5
✓ Network tpipesec_syd_tp_001_open_vpn_network_1 Created 0.1s
✓ Network tpipesec_syd_tp_001_open_vpn_network_2 Created 0.1s
✓ Container tp_ipsec_eve Started 0.1s
✓ Container tp_ipsec_alice Started 0.1s
✓ Container tp_ipsec_bob Started 0.1s
PS C:\Users\JulesAMELOT\OneDrive\ESAIP\chiffrement et VPN\TP IPSEC\TP IPSEC> docker exec -ti tp_ipsec_alice /bin/bash
root@936f9b9c42c8:/exchange_alice# ls
```

Génération des certificats

Pour mettre en place notre IPsec, nous avons besoin de certificat valide, nous allons donc en créer un pour bob et un pour Alice.

On commence par créer une clé de certificat

```
root@326825d793c3:/exchange_bob# openssl genpkey -algorithm RSA -out CA-root-key.pem -pkeyopt rsa_keygen_bits:4096
.....+++++
.....+++++
```

Et ensuite on génère notre certificat

```
root@326825d793c3:/exchange_bob# openssl req -new -x509 -days 3650 -key CA-root-key.pem -out root-ipsec-ca.pem
Can't load /root/.rnd into RNG
139725036900800:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/root/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:VPN Ipsec
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:VPN Ipsec Root CA
Email Address []:
root@326825d793c3:/exchange_bob# ls
CA-root-key.pem  root-ipsec-ca.pem
root@326825d793c3:/exchange_bob# |
```

On retrouve notre certificat sous le nom de CA-root-key.pem .

On répète le même procédé sur l'autre machine

```
root@326825d793c3:/exchange_bob# openssl req -new -key bob-key.pem -out bob-CA.csr -config myserverCA.conf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:FR
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organizational Unit Name (eg, section) []:VPN Ipsec
Common Name (eg, your name or your server's hostname) []:VPN Ipsec Bob CA
Email Address []:
root@326825d793c3:/exchange_bob# |
```

Une fois nos certificats générés il faut les signer grâce au certificat root

```
root@326825d793c3:/exchange_bob# openssl x509 -req -days 365 -in bob-CA.csr -CA root-ipsec-ca.pem -CAkey CA-root-key.pem -CAcreateserial -out bob-CA.crt -extensions req_ext -extfile myserverCA.conf
Signature ok
subject=C = FR, OU = VPN Ipsec, CN = VPN Ipsec Bob CA
Getting CA Private Key
root@326825d793c3:/exchange_bob# |
```

Et on voit nos certificats en mode « ok ». Ce qui veut dire que nos certificats son actif.

Ensuite on met les bons fichiers à leur place

```
root@326825d793c3:/exchange_bob# cp bob-CA.crt /etc/ipsec.d/certs/
root@326825d793c3:/exchange_bob# cp bob-key.pem /etc/ipsec.d/private/
```

Cela est plus simple que d'aller changer dans la configuration de ipsec le dossier dans laquelle il doit chercher ces informations, on lui met les informations dont il a besoin dans les dossiers qu'il prévoit pour cette effet.

Configuration de Strongswan

Dans un premier temps nous allons créer la configuration de base de notre ipsec.

```
root@936f9b9c42c8:/etc# cat ipsec.conf
config setup
    charondebug="ike 1, knl 1, cfg 0"
conn ikev2-vpn
    ike=aes256-sha1-modp1024,3des-sha1-modp1024!
    esp=aes256-sha1,3des-sha1!
    left=%any
    leftid=192.168.111.2
    leftcert=/etc/ipsec.d/certs/alice-CA.crt
    leftsendcert=always
    leftsubnet=10.0.0.100/24
    right=%any
    rightid=%any
    rightauth=eap-mschapv2
    rightsourceip=10.0.0.0/24
    rightdns=8.8.8.8,8.8.4.4
    rightsendcert=never
    eap_identity=%identityroot@936f9b9c42c8:/etc#
root@936f9b9c42c8:/etc#
```

On retrouve dans cette capture plusieurs information plus ou moins simple, nous avons le serveur DNS, l'IP, mais aussi le certificat utilisé pour la configuration et son chemin.

Ensuite nous mettons en place nos clé privé dans la configuration de chaque utilisateur

```
root@936f9b9c42c8:/etc# cat ipsec.secrets
192.168.112.2 : RSA "/etc/ipsec.d/private/bob-key.pem"
```

On peut voir ici que ipsec vas chercher la clé privée dans le fichier bob.key

Du coté de Alice cela marche aussi de la même façon, les clés sont automatiquement récupérées.

Mise en place de la connexion

La première étape pour mettre en place la connexion est de vérifier les routes par défaut, si elles ne sont pas paramétrées, il faut les paramétrer à la fois sur bob et Alice

Bob: `/bob/add_default_gateway.sh`

Alice `/alice/add_default_gateway.sh`

Cela configurera les routes par défaut de nos 2 clients.

Conclusion

Nous n'avons malheureusement pas réussi à mettre en place l'IPsec dans le temps imparti, nous avons eu beaucoup de mal à créer notre docker proprement et nous avons aussi eu des problèmes différents sur chaque pc que nous utilisions.

Chaque PC lançait la même configuration docker, mais certain le pouvais pas la lancer, d'autre la lançais mais elle plantait etc...

Nous avons fini par réussir à faire une configuration docker mais trop tard par rapport a l'échéance du projet et nous n'avons donc pas eu le temps de trop explorer la partie strongswan du projet.

Nous continuerons dans les prochaine semaine à essayer de le faire fonctionner pour avoir la satisfaction d'avoir réussi.