# Scénario 1 - Epreuve E4

Mise en place d'un tunnel VPN

## Objectif

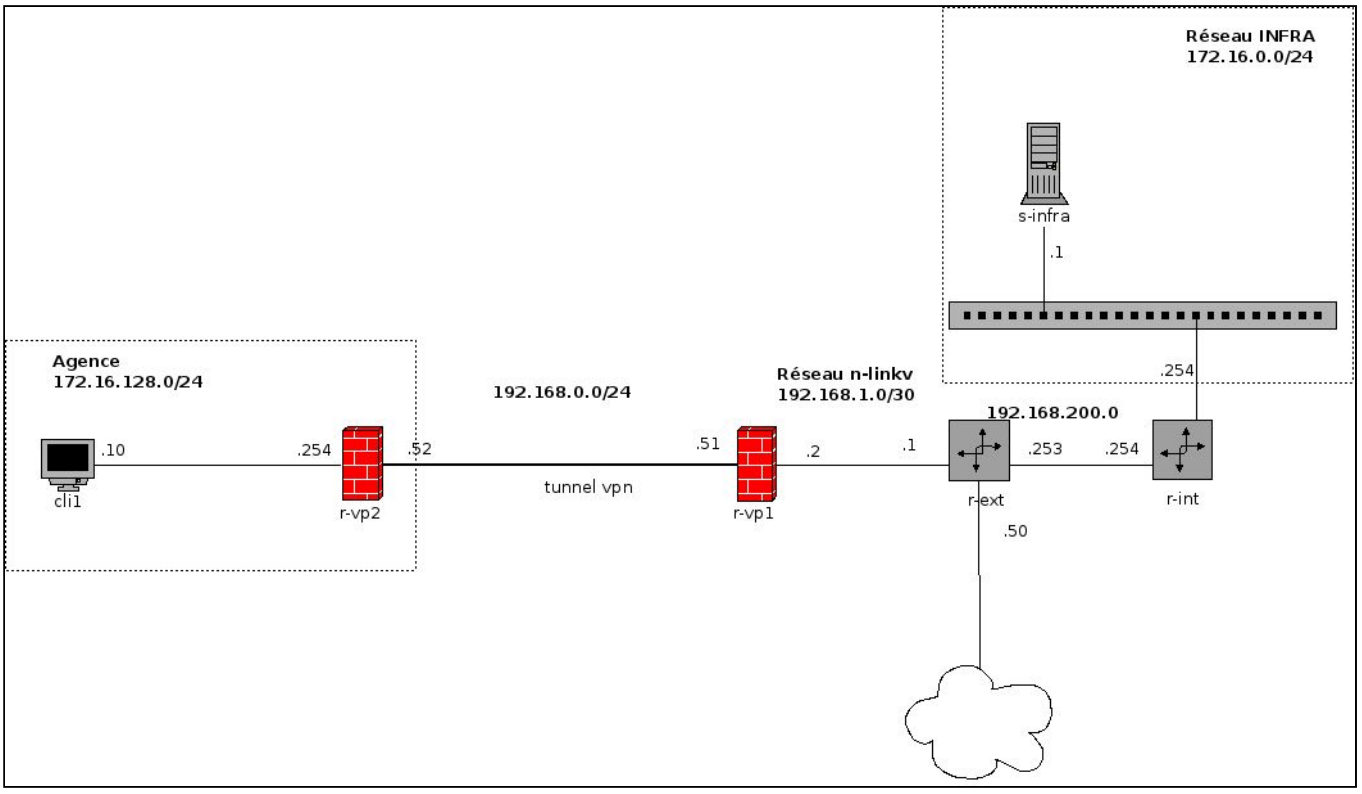
L'agence échange des données confidentielles avec le serveur s-infra situé dans le réseau n-infra. Il a été décidé que celles-ci communiqueraient désormais impérativement en utilisant un tunnel chiffré VPN afin que les informations transmises ne soient pas disponibles en clair pour toute personne cherchant à les pirater. Il faudra pour cela mettre en place deux serveurs VPN qui établiront une connexion entre les machines grâce à des certificats X509. Un pare-feu situé sur les deux serveurs VPN filtre les connexions pour plus de sécurité. Les machines seront configurées avec des playbooks Ansible.

## Choix effectués

- **ipsec** : Un ensemble de standard de chiffrement des connexions, utilisé notamment dans les tunnels VPN. Bien que plus compliqué à utiliser que d'autres standards VPN, il est largement utilisé depuis 15 ans et considéré comme le standard lorsqu'on veut mettre en place un VPN. Le fait d'effectuer le chiffrement par les couches basses du modèles OSI est préférable.
- **Strongswan** : Paquet utilisant ipsec afin de mettre en place du VPN.
- **Certificats X509** : Standard utilisé pour identifier les serveurs VPN. On peut également utiliser un secret partagé, c'est-à-dire un mot de passe utilisé pour relier les deux serveurs. Contrairement aux certificats, ils ne sont pas révocables. Dans le cas où un serveur VPN serait volé ou piraté par un tiers, un secret partagé lui permet d'accéder librement au VPN sans qu'on puisse lui interdire l'accès. Les certificats sont ainsi beaucoup plus sécurisés que le secret partagé, et indispensable dès que le nombre de machines devient assez important.
- **Ferm** : Ce service simplifie les règles de filtrage iptables et vide la table iptables lorsqu'il est stoppé, ce qui peut être très pratique pour les tests.

## Infrastructure à mettre en place

- **r-vp1, r-vp2** : serveurs VPN principaux
- **r-ext, r-int** : les deux routeurs qui séparent le réseau n-agence et n-infra
- **cli1, s-infra** : les deux machines qui souhaitent communiquer entre elles




*Les serveurs et les routeurs seront connectés à s-adm afin de procéder à leur installation. La connexion à cette machine ne sera plus effective dès la fin de l'installation.*

- r-vp1 :

### Interfaces

- **enp0s3** dhcp **n-adm**
- **enp0s8** 192.168.0.51/24 **bridge** (tunnel)
- **enp0s9** 192.168.1.2/24 **n-linkv** (liaison avec r-ext)

### Routes

- Par défaut: 192.168.1.1 (r-ext, interface enp0s9)
- Statique : 172.16.128.0/24 (r-vp2 enp0s8)

- r-vp2 :

### Interfaces

- **enp0s3** dhcp **n-adm**
- **enp0s8** 192.168.1.2/24 **n-ag**
- **enp0s9** 192.168.0.52/24 **bridge**

### Routes

- Par défaut: 192.168.99.99

    - Statique : 192.168.1.0/24

- r-ext (uniquement ip utiles pour le vpn)
- r-int (idem)
- client XP

# Tâches à effectuer

## Notes importantes

- Installer par playbook r-vp2 avant r-vp1 et pas en même temps
- Désactiver les pare-feux en cas de problèmes non-résolus

Création des playbooks `vpn-l.yml` (pour la partie gauche) et `vpn-r.yml` (pour la partie droite). Ils devront automatiser les taĉhes suivantes :

## Installation d'ipsec sur les deux serveurs et configuration

- Choix du paquet strongswan qui utilise ipsec pour sa documentation fournie
- Installer le paquet tcpdump
- Activer le routage

Tâche à effectuer à la main :

- **Génération d'une clé publique liant r-vp1 à r-vp2, utilisé pour récupérer les certificats de r-vp2 depuis r-vp1**
- **Désactiver le pare-feu de la machine XP**

~~Il faut ajouter l'interface d'écoute du DHCP.~~

## Génération d'un secret partagé pour vérifier le fonctionnement du VPN, avant de passer aux certificats

- Dans le playbook, commenter le rôle x509 et voir si le VPN fonctionne. Le rôle vpn-stg-x automatise les tâches suivantes :
    - Modification du fichier `/etc/ipsec.conf` afin d'ajouter les adresses IP des serveurs VPN et des réseaux correspondants, et d'indiquer que l'on utilise un secret partagé en ajoutant ou décommentant la ligne `authby=secret`
    - Modification du fichier `/etc/ipsec.secrets` qui contient le secret partagé, en indiquant les adresses des machines et le mot de passe utilisé
      `192.168.0.52 192.168.0.51 : PSK 'root'`
    - Relancer le service ipsec

### Génération des certificats et configuration

- Dans le playbook, décommenter le rôle x509, qui automatise les tâches suivantes :
    - Modification du fichier `/etc/ipsec.conf` pour indiquer l'utilisation d'un secret partagé en commentant la ligne `authby=secret`
    - Ajout des lignes suivantes (issues de r-vp1):
        - `leftcert=r-vp1Cert.pem` ; permet d'indiquer le nom du certificat
        - `leftid="C=CH, O=GSB, CN=r-vp1"` ; Indiquer le serveur VPN sur lequel on modifie le fichier et l'Unité Organisationnelle utilisée
        - `rightid="C=CH, O=GSB, CN=r-vp2"`; Indiquer l'autre serveur VPN et l'Unité Organisationnelle utilisée
    - Modification du fichier `/etc/ipsec.secrets` qui contient la ligne suivante qui indique le nom du certificat utilisé :
    - `: RSA r-vp1Key.pem`
    - Les certificats sont générés grâce à un script sur r-vp1, qui récupère en même temps les clés de r-vp2.
    - Relancer le service ipsec

### Mis en place, sur les serveurs, d'un pare-feu n'autorisant que les ports correspondant au VPN et autres types de connexions utilisés

- Ports autorisés :
    - SSH serveur
    - DHCP serveur (sur r-vp2 uniquement)
    - DNS client et serveur
    - ipsec
    - nat-t-ike
    - SNMP (utilisé pour la supervision)
    - NTP
    - ping (sauf depuis l'extérieur)
- Installation du service ferm visant à simplifier l'utilisation de règles iptables
- Modification du fichier de configuration `/etc/ferm/ferm.conf` afin d'ajouter des règles de filtrage

# Tests à effectuer

### Fonctionnement du VPN

- DHCP, DNS actifs
- **Liste des pings à effectuer**
    - **172.16.128.254** (r-vp2 côté agence)
    - 192.168.0.52 (tunnel vpn côté r-vp2)

- **192.168.0.51** (tunnel vpn côté r-vp1)
- 192.168.1.2
- **192.168.1.1**
- 192.168.200.253
- 192.168.200.254
- **172.16.0.254**
- 172.16.0.1

- **Envoyer un ping vers s-infra depuis cli1 et dans l'autre sens** (situé dans l'agence) et voir dans les logs si le paquet passe dans le VPN. Dans ce cas, on ne verra que l'entrée et sortie du tunnel par le paquet, sans savoir ce qui se passe entre.
- Stopper le service ipsec sur un serveur et vérifier que le ping de s-infra depuis cli1 ne fonctionne plus. Si c'est le cas, cela veut dire que la paquet passe bien par le tunnel et est donc chiffré.

## Fonctionnement du pare-feu

- Depuis cli1, envoi d'un ping vers s-infra pour vérifier que le VPN n'a pas été bloqué par le pare-feu.
- Tests des autres règles de pare-feu : lancement d'une commande `host` pour le DNS client, `ifconfig /renew` depuis le client Windows XP pour tester le DHCP serveur, entre autres.
- Effectuer la commande `ipsec status`
- Depuis un client extérieur, lancer un nmap qui scanne les ports ouverts. On ne devra pas voir la majorité des ports ouverts.