# Mise en place d'un réseau « d'entreprise »

## Objectif

L'objectif de ce projet est la bonne compréhension des principaux protocoles et mécanismes que l'on rencontre dans le réseau Internet classique de faible échelle : réseau domestique, réseau d'entreprise, etc... Un aspect n'est pas du tout traité par ce projet : la supervision du réseau, et nous éviterons d'utiliser des techniques de niveau technologique (Ethernet en particulier) pour répondre au cahier des charges. Le but est alors de monter un réseau dit d'entreprise en utilisant une démarche incrémentale pour illustrer le cours et le compléter par une partie pratique et des aspects manquants.

## Organisation

Le projet est avant tout un projet individuel. Toutefois, pour l'interconnexion de votre réseau d'entreprise, nous vous proposons de travailler par groupe de 3 à 4 personnes. Chaque groupe aura en charge la réflexion sur l'adressage public que leurs réseaux, l'architecture de l'interconnexion, la mise en place de cette dernière, les tests des réseaux des autres et enfin la rédaction d'un bref rapport sur leur travail.

## Outils

Le réseau d'entreprise est à réaliser individuellement sur machine virtuel. Pour ce qui est de l'outil de machine virtuel vous êtes libres d'utiliser VirtualBox ou VMware.
Il est préférable d'installer un Linux mais vous êtes libre quant à l'OS utilisé, du moment qu'il est assez léger pour avoir 3-4 VM sur votre machine en parallèle.
Pour le reste des outils, il est requis[1] un serveur web (apache2), un navigateur web, un proxy web (squid), l'accès aux iptables, un serveur DNS (bind), et un serveur dhcp (gdhcpd).

## Evaluation

L'évaluation de ce projet s'effectue sur plusieurs points :

- une démonstration de chaque étudiant de leur réseau,
- une démonstration de chaque groupe de l'interconnexion de leurs réseaux,
- l'autonomie et la motivation de l'étudiant,
- un rapport final comprenant l'architecture mise en place par le groupe, la réponse aux différentes questions, les observations et tests effectués ainsi que toute remarque pouvant apporter des évolutions au projet.

## Partie I Mise en place du réseau sur les VMs *(individuel)*

Le réseau d'entreprise est constitué de deux réseaux distincts : d'une part un réseau privé, caché du reste du monde, et d'autre part, d'un réseau public dénommé DMZ (zone démilitarisée) où les services publiques du réseau sont déployés, ici le DNS et le serveur web.

### Etape 1.1 – *Réseau privé*

Mettre en place le réseau privé d'un point de vue logique (plan d'adressage) comme physique.
Vérifier la communication au sein du réseau.
Compétences : Prise en main des VMs, configuration d'une interface, test de communications (ping), configuration de lien virtuel sur une VM.

[1] En parenthèse, il s'agit d'un exemple d'application, si vous en préférez une autre, c'est tout à fait possible.

**Etape 1.2 – *Réseau public***

Mettre en place le réseau public d'un point de vue logique comme physique.
Vérifier la communication
Mettre en place d'un serveur web (on pourra utiliser le serveur apache2) avec une page d'accueil simple qui est propre à votre entreprise (on pourra laisser dans un premier temps la page par défaut d'apache2)
Vous pouvez mettre en place d'autres services Internet en supplément si vous le souhaitez.
Compétences : Installation de logiciel sur des VMs, compréhension du protocole applicatif http

**Etape 1.3 – *Interconnexion***

Interconnecter réseau privé et réseau public.
Compétences : activer et configurer un routeur, ajouter des routes

***Question 1.1***

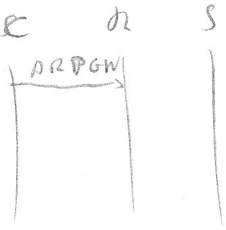
*Faut-il mettre en place du NAT pour la communication entre la DMZ et le réseau privé ? Pourquoi ?* ✓

***Question 1.2***

*Décrire l'enchainement des messages d'une communication entre un client Web et un serveur de la DMZ. ?* ✓
*Quelles sont les caractéristiques de la communication ?*
*Quelles sont les étapes de la communication ?*
*Que manque-t'il par rapport à un cas classique ? (chez vous par exemple)*

***Question 1.3***

*Quelles sont les routes*
- *d'une machine du réseau privé ?* ✓
- *du serveur de la DMZ ?* ✓
- *du routeur ?* ✓




**Partie II** **<u>Interconnexion avec le « reste du monde »</u>** ***(en groupe)***

**Etape 2.1 – *Mise en place d'un routeur vers l'extérieur***

Mettre en place un routage vers l'extérieur.
Faire en sorte que chaque serveur web puisse être consulté par toute entité des réseaux publics.
Compétences : Faire communiquer des VMs avec le monde réel, approfondir sa maîtrise du routage

***Question 2.1***

*Quelles routes doivent être rajoutées et où ?*

***Question 2.2***

*Qu'est-ce qui ne communique pas avec le reste du monde et pourquoi ?*

**Partie III** **<u>Communication du réseau privé avec les serveurs web</u>** ***(mixte)***

**Etape 3.1 – *Réseau privé***

Permettre la communication du réseau privé avec les DMZ des réseaux extérieurs en utilisant le NAT.
Compétences : Utiliser iptables pour faire du NAT, reconnaitre le NAT

***Question 3.1***

*Expliquez comment fonctionne le NAT sur une machine Linux.*

***Question 3.2***

*Peut-on communiquer partout à présent ? Pourquoi ?*

**Partie IV** **Mise en place de la sécurité** ***(mixte)***

**Etape 4.1 – *Politique de sécurité***

Définir une politique de sécurité pour votre réseau. On différenciera la protection du routeur, du réseau et des machines.

Compétences : Avoir une première idée des politiques de sécurité

**Etape 4.2 – *Mise en place de la politique choisie***

Mettre en place la politique de sécurité en utilisant les tables ip (iptables) de Linux.

Compétences : Savoir configurer un parefeu, affiner sa connaissance d'iptables, comprendre le statefull.

***Question 4.1***

*Comment mettre en place les règles pour permettre les communications web entrantes sur la DMZ venant de l'extérieur? Expliquez les règles à mettre en place.*

***Question 4.2***

*En quoi l'état d'une connexion TCP peut nous être utile pour le filtrage ?*

**Partie V** **Configuration automatique** ***(individuel)***

**Etape 5.1 – *DHCP sur réseau privé***

Pour une administration plus facile, utilisez une configuration automatique des machines du réseau privée en utilisant le protocole DHCP.

Compétences : Mise en œuvre du service DHCP, comprendre les étapes du protocole.

***Question 5.1***

*Quelles sont les informations à renseigner ? Quelles sont les informations à véhiculer ?*

***Question 5.2***

*Expliquez le fonctionnement de DHCP.*

***Question 5.3***

*En quoi ce protocole présente-t'il un danger ?*

*Commandes utiles en salle de TP*

*gdhcpd -> interface graphique*

*dhclient <-r> <eth>*

**Partie VI** **Mise en place d'un proxy web** ***(individuel)***

**Etape 6.1 – *Proxy cache web***

Mettre en place un proxy cache web explicite et le configurer pour être utilisé par les navigateurs web du réseau privé.

Compétences : Configurer un proxy, configurer un navigateur pour utiliser un proxy.

**Etape 6.2 – *Proxy cache tranparent***

Mettre en place un proxy transparent à la place.
Compétences : Configurer un proxy transparent, rediriger du trafic.

***Question 6.1***

*Expliquez le fonctionnement et l'intérêt d'un proxy web.*

***Question 6.2***

*Quelles sont les raison de l'utilisation d'un proxy web transparent à la place d'un proxy web classique et explicite ?*

***Question 6.3***

*Expliquez en quoi un proxy transparent est plus complexe d'un point de vue réseau. Expliquez comment mettre en place ce type de proxy transparent ainsi que les configurations réseaux à effectuer.*

*Commandes utiles en salle de TP*

*Squid = proxy cache http/https/ftp + accélérateur web*
*Fichier de conf /etc/squid/squid.conf*
*Port d'écoute par défaut 3128 (http_port)*
*Mode transparent à activer*
*Démarrage : /etc/init.d/squid start*

**Partie VII DNS *(mixte)***

**Etape 7.1 – *Espace de nommage***

Mettre en place un système de nommage.
Compétences : Savoir utiliser des noms à la place d'adresse IP.

**Etape 7.2 – *Serveur DNS***

Mettre en place un serveur DNS pour votre domaine.
Compétences : Mettre en place un serveur DNS, configurer un domaine, comprendre les requêtes.

**Etape 7.3 – *Service global***

Etendre le service à une solution globale.
Compétences : Hiérarchie DNS, utiliser les redirections.

***Question 7.1***

*Tracez l'enchainement des messages DNS dans le réseau et observer l'évolution des caches.*

***Question 7.2***

*Un système de nommage par dépendant des FAIs est-il une bonne solution pour des réseaux d'entreprises ? Une autre solution est-elle possible ? Pourquoi ?*