TP4 : SERVICE DHCP & DNS

OBJECTIFS

A l'issue de ce TP, vous serez en mesure de :

a. Créer une maquette simple
b. Comprendre le fonctionnement de DNS.
c. Comprendre DHCP, configurer un serveur DHCP et un serveur DHCP de relai.

A. OUTILS D'INTERROGATION ET D'ANALYSE DNS

1. Quel est le rôle du service DNS dans Internet ?
2. Utiliser le site **https://zonemaster.net/domain_check** pour vérifier la conformité des domaines DNS de votre choix (tester par exemple **efrei.fr**, **fr.** et **gouv.fr.**).
3. Installer l'outil **whois** sur une machine Linux connectée à Internet, puis afficher les informations administratives du domaine de votre choix.
4. Sur Linux, Quel est le rôle de chacun des fichiers **/etc/hosts**, **/etc/host.conf** et **/etc/resolv.conf** ?
5. La commande **dig** (à effecturer sur une machine Linux connectée à Internet) :
   a) Installer le package **dnsutils**
   b) A l'aide de la commande **dig** du package dnsutils, répondre aux questions suivantes (alternativement, vous pouvez utiliser sa version en ligne www.digwebinterface.com/) :
      - Lister les *serveurs racines*. C'est quoi leur rôle ? Combien de serveurs racines existent-ils aujourd'hui ? Où se trouvent-ils ?
      - Quels sont les serveurs DNS du domaine **efrei.fr.** ?
      - C'est quoi un serveur autoritaire ? comment récupérer une réponse DNS autoritaire ?
      - Quel est le nom et l'adresse IP du serveur de messagerie de l'Efrei ?
      - En utilisant l'option +trace de dig, quels sont les serveurs DNS participant à la résolution du nom **www.efrei.fr.** ?

B. CREER LA MAQUETTE

La maquette à réaliser est illustrée dans la figure 1.

PC1, FW1, FW2, et les Serveurs DHCP, HTTP et DNS sont des machines Linux.

1. Créer la maquette de la figure 1 et connecter virtuellement les différentes machines.
2. Configurer les adresses IP en respectant le plan d'adressage indiqué sur le schéma. PC1 utilise DHCP pour obtenir son adresse IP dynamiquement.
3. Faites les configurations nécessaires pour que les machines DNS, HTTP et DHCP accèdent à Internet.

Il faut noter que les serveurs DNS et HTTP sont accessible depuis l'extérieure. Une bonne pratique est de les mettre dans un segment séparé protégé par des parefeu : c'est la notion de DMZ (zone démilitarisée). L'utilisation de deux parefeux en cascade est une bonne pratique qui est très répandue dans les entreprises.

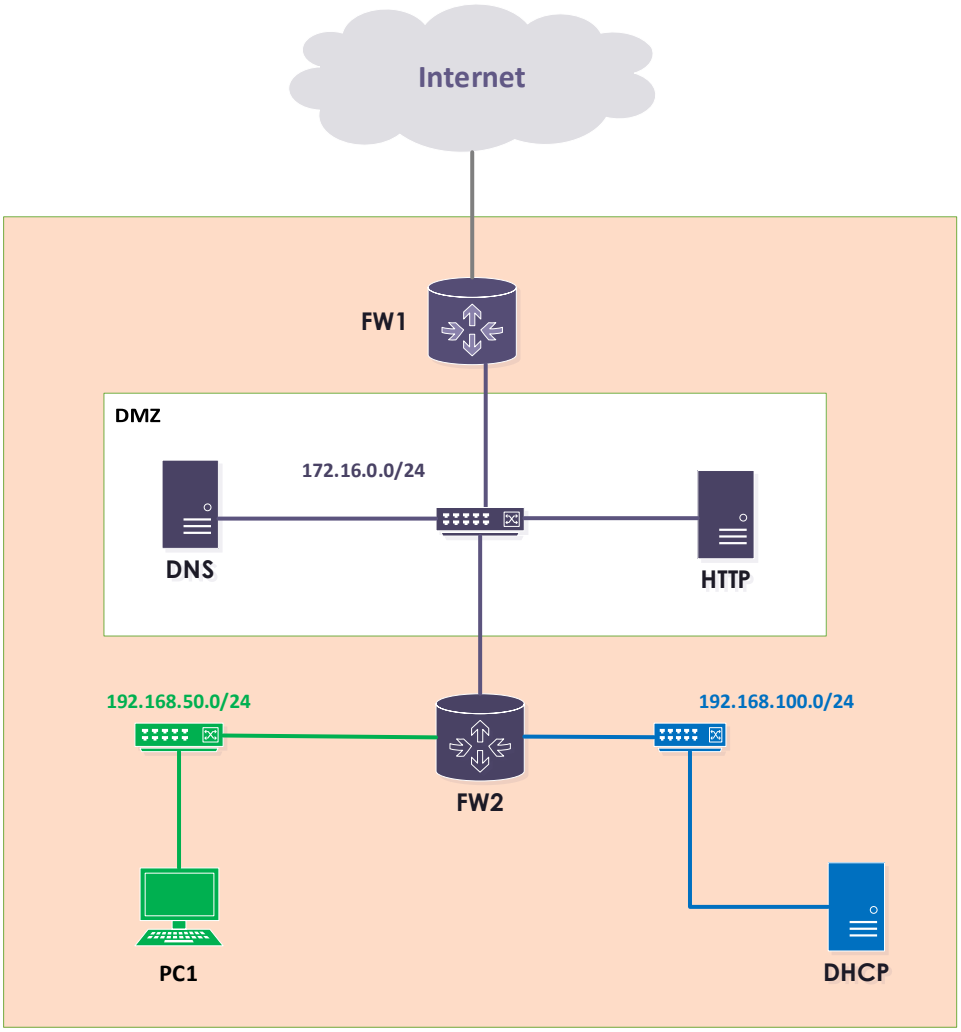

FIGURE 1 : MAQUETTE RESEAU A REALISER

C. INSTALLATION DU SERVEUR BIND9

BIND9 est une implémentation très répandue du service DNS sur Internet. Dans cette section, vous allez l'installer et le configurer. Utiliser au maximum des fichiers déjà existants dont vous pouvez faire une copie pour les modifier ensuite en fonction des configurations que vous aurez à mettre en place.

1. Installation de BIND9 sur DNS1 :

- Installer le serveur BIND9 (nom du package bind9). Vérifier qu'il a été correctement installé. Vérifier sous quel compte système il est lancé et sous quel port il écoute les requêtes.
- Identifiez le répertoire des configurations de BIND9 ainsi que les éléments principaux de ce fichier de configuration (man named.conf)
- Identifier le répertoire où se situent les fichiers de zone. Quels sont les fichiers dans lesquels sont définis les différents enregistrements du domaine ?
- Vérifier s'il résout bien les requêtes en lui adressant directement une requête DNS avec la commande :

```
user@debian$ dig @localhost www.efrei.fr
```

2. Sur le serveur HTTP, configurer l'adresse du serveur DNS que vous venez d'installer comme serveur DNS principal (rajouter la ligne `nameserver @IP_serveur DNS` dans le fichier /etc/resolv.conf du serveur HTTP). Assurez-vous que le serveur HTTP peut toujours pinguer www.google.fr.

D. SERVEUR DHCP

1. Sur la VM serveur DHCP :

   - Vérifiez que le résolveur DNS déclaré dans /etc/resolv.conf exploite votre serveur DNS (à déclarer dans /etc/resolv.conf)
   - Installez le service DHCP issu du consortium ISC (isc-dhcp-server). Acceptez les options par défaut. Si le démarrage du service échoue, pas d'inquiétude. Les choses iront mieux après la configuration.
   - Dans le fichier **`/etc/dhcp/dhcpd.conf`**, déclarez un réseau correspondant à l'adresse de réseau 192.168.50.0/24. Au sein du subnet, déclarez une plage d'adresses allant de 192.168.50.50 à 192.168.1.99, déclarez l'adresse de la passerelle par défaut, déclarez votre serveur DNS actif, configurez la durée des baux par défaut à 24h.
   - Déclarer la carte réseau d'écoute des requête et d'envoie des réponses dans le fichier **/etc/default/ isc-dhcp-server**
   - Redémarrer le service DHCP

2. Le PC1 ne peut pas contacter votre serveur DHCP car PC1 et le serveur DHCP ne sont pas sur le bon segment réseau. C'est pourquoi nous devons configurer FW2 comme **relai DHCP**. Mettre le serveur DHCP dans la zone des serveurs internes est une bonne pratique de sécurité, en plus ceci permet de centraliser la gestion et l'attribution des adresses IP dans l'entreprise.

3. Installe un serveur DHCP relai (package isc-dhcp-relay) sur **FW2** et configurez-le afin qu'il redirige les requêtes DHCP du PC1 vers le serveur DHCP.
4. Sur PC1 :
   - Assurez vous qu'il est configuré pour récupérer l'adresse IP en DHCP.
   - Redémarrer le service réseau (**systemctl restart networking**) ou bien lancer la commande **dhclient** afin de récupérer une adresse DHCP.
   - Vérifier maintenant que PC1 a obtenu sa configuration IP dynamiquement.
5. Identifier la commande et le fichier dans lequel sont sauvegardés les baux en cours.
6. Capture des trames sur PC1 :
   - Depuis votre terminal, libérez l'adresse IP précédemment obtenue.
   - Depuis un autre terminal, capturez les paquets échangés sur les ports 67 et 68 (échanges DHCP). Utilisez la commande **tcpdump** avec les privilèges administrateur en sauvegardant la capture dans un fichier **dhcp.cap**.
   - Depuis le premier terminal, provoquez une requête DHCP (commande **dhclient**).
   - Ouvrez le fichier **dhcp.cap** avec Wireshark.
   - Analyser le fonctionnement du protocole DHCP en vous appuyant sur le résultat de la capture.
7. Rajouter des règles sur FW1 et sur FW2 pour n'autoriser que votre serveur DNS à résoudre les noms DNS (un dig @8.8.8.8 www.efrei.fr depuis PC1 sera bloqué par le parefeu).
   C'est quoi l'intérêt de ce choix ?