SAÉ 21

Construire un réseau informatique pour une petite structure

A FAIRE PAR GROUPE DE DEUX ETUDIANT·E·S

Encadrants :

Michael Lance - Michael.Lance@eurecom.fr

Guillaume Urvoy-Keller - guillaume.urvoy-keller@univ-cotedazur.fr

Objectif SAÉ (suivant Programme pédagogique National) : Le professionnel R&T (vous!) peut être sollicité pour construire et mettre en place le réseau informatique d'une « petite » entreprise. L'objectif est alors de répondre aux besoins de commutation, de routage, de services réseaux de base et de sécurité formulés pour la structure. Ce réseau s'appuie sur des équipements et des services informatiques incontournables mais fondamentaux pour fournir à la structure un réseau fonctionnel et structuré.

Notation : Cette SAÉ est constituée de :

- 6h de TP en mode projet avec GNS3 et des équipements physiques
- Un projet individuel sous Packet tracer avec rendu d'un rapport (/5), du fichier pkt global et d'une vidéo de 3 à 5 min (/3)

Instructions :

- Pour chaque partie du rapport, vous devez inclure les configurations des équipements réseaux et équipement d'accès. Mettre seulement les configurations ne suffit pas, il faut les commenter. Ne garder les parties pertinentes des configurations.
- Pour la vidéo, vous devez utiliser le mode Simulation de Packet tracer pour démontrer le bon fonctionnement aux différentes étapes de la construction du réseau.

- Production de la vidéo : Vous êtes libre d'utiliser le logiciel de capture vidéo d'écran (*screencast*) de votre choix, tel que Kazam sous Ubuntu. Une fois la vidéo produite, il vous est demandé de la ré-encoder avec l'outil open source https://handbrake.fr/, ce qui va vous permettre de réduire significativement sa taille, comme expliqué sur https://theshiftproject.org/guide-reduire-poids-video-5-minutes/.
- Dépôt des rendus : Les dépôts des fichiers pdf de compte-rendu, du fichier pkt et du .mp4 de vidéo se font sous Moodle : https://lms.univ-cotedazur.fr/course/view.php?id=15655&section=0

Cahier des charges

L'objectif est de construire un réseau d'entreprise typique d'une PME avec :

- Un cœur de réseau comportant un multi-layer switch (MLS), appelé switch de niveau 3 qui est capable de switcher ou router suivant les besoins

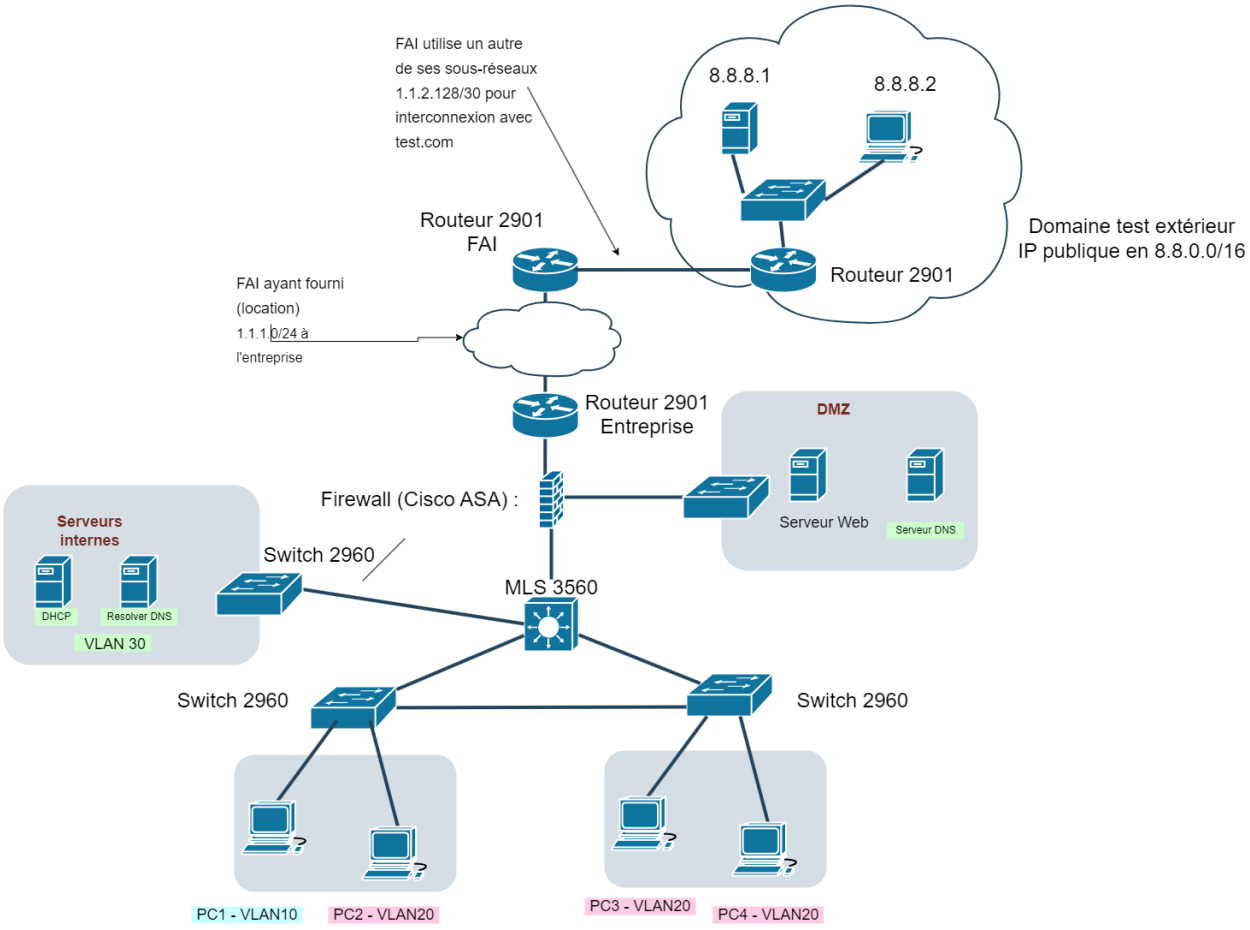
- Ce MLS sert plusieurs VLANs :
    - Deux VLANs correpondant à deux groupes de travail dans l'entreprise (par exemple service RH et service ingénierie)
    - Le VLAN des serveurs internes

- Ce MLS est ensuite raccordé à un pare-feu (CISCO Asa) qui offre les services ci-après :
    - Il permet les machines sur Internet d'accéder au serveur Web de la DMZ uniquement sur les ports 80 et 443 en TCP dans les deux cas
    - Il contrôle que les paquets reçus par les clients internes correspondent à des connexions initiées par les clients internes.

- Un FAI qui :
    - fournit un range d'adresse publique au routeur de bordure de l'entreprise etoffre les services de NAT :
        - NAT (overloading en langage CISCO) pour les machines des VLAN 10 et 20 lorsqu'elles accèdent à Internet
        - NAT statique pour le serveur Web de la DMZ lorsqu'on y accède depuis l'extérieur.
    - s'interconnecte avec un autre réseau dans lequel se trouvent un serveur Web, pour tester que les machines internes de l'entreprise, en adressage privé, peuvent accéder à des resources « sur Internet » et un client pour tester l'accès au serveur Web de l'entreprise qui est dans la DMZ.

Un schéma complet du réseau avec des indications du type d'équipement à utiliser est disponible dans la figure suivante.

Schéma global



Plan d'adressage (/5) :

Voici des élements sur le plan d'adressage qu'il faudra compléter. Les adresses IPs de tous les élements (routeurs, serveurs, MLS sur certaines interfaces spécifiques) doivent apparaître sur vos schémas dans votre rapport et dans le .pkt.

- VLAN 10 et VLAN 20 et VLAN serveurs : vous avez le droit d'utiliser les adresses privées en 172.16.0.0/12 en faisant des sous-réseaux en /24, ce qui permettra d'avoir 254 IPs dans chaque réseau client. La passerelle de chaque VLAN doit être la dernière ou la première adresse IP du sous-réseau. Le VLAN Serveur sera un sous-resseaux en /24 de la plage 10.0.0.0/8.

- Le réseau entre le MLS et l'ASA sera un 192.168.10.x/y où y doit être choisi de manière à avoir uniquement les deux adresses nécessaires. 'x' est choisi de manière à être compatible avec y.

- Le réseau entre l'ASA et le routeur de sortie est 192.168.11.252/30.

- La DMZ est sur un réseau dédié en 192.168.1.0/24.

- Le fournisseur d'accès internet de l'entreprise opère localement sur les adresses publiques 1.1.1.1.0/24 qu'il dédie au réseau de notre entreprise. C'est la pratique habituelle et l'extension naturelle de l'octoi d'une adresse du FAI pour votre box.

- On suppose l'existence d'un réseau public test en 8.8.0.0/16 qui va contenir un serveur Web et un client.

- L'interconnexion entre le réseau 8.8.0.0/16 et 1.1.1.0/24 se fait avec un second réseau 1.1.2.128.0/30 qui appartient au fournisseur d'accès Internet qui sert l'entreprise.

Etape 1 : Construction de coeur de réseau avec les switches d'accès et le Multi-layer switch (/5)

La première étape est de construire le cœur du réseau avec les trois switchs qui servent les VLANs et le MLS. Mettez des adresses statiques pour les machines clients dans cette étape et montrez que tout fonctionne bien avec des pings et la fonction simulation de Packet Tracer dans la vidéo. Cette fonction vous sera aussi utile pour le debug. Il faut donc montrer que :

- Le ping est possible entre deux machines du même VLAN
- Le ping est possible entre deux machines de VLANs différents.
- La configuration STP est bonne et que le switch racine pour les 2 Vlans est bien le MLS. Forcez la configuration dans ce sens.
- Les notions de trunk et d'access VLAN sont bien comprises. Des trunk mis inutilement seront sanctionnés.

Il faudra donner la configuration d'un des switchs et du MLS et commenter, dans le rapport.

Le site (https://polar91.wordpress.com/2017/09/27/configure-multilayer-switch-on-packet-tracer/) devrait être une aide précieuse.

Etape 2 : Ajout de l'ASA et du service DHCP (/5)

Interconnectez l'ASA et le MLS. Il va falloir modifier l'interface correspondante du MLS de manière à ce qu'on puisse lui donner une adresse IP (de base, ses interfaces sont de niveau 2 et non 3 !!) (/1)

Si ce n'était pas fait à l'étape 1, activez le service DNS sur le serveur dans le VLAN serveurs. En théorie, ce dernier devrait être capable de dialoguer avec d'autres serveurs DNS sur Internet mais on va faire simple ici (on est limité par Packet Tracer) : il faut seulement ajouter un enregistrement du bon type (A? NS? MX?) pour que www.test.com corresponde à l'IP du serveur externe. Mais aussi un enregistrement pour que www.entreprise.com coresponde au serveur dans la DMZ. Pas de points partiel ici. Soit votre configuration est 100% bonne soit vous n'avez pas les points. (/2)

Ajouter dans le VLAN serveur (VLAN 30) un serveur DHCP en utilisant le serveur DNS interne comme resolver DNS. Il faudra configurer les "IP helper address" au niveau du MLS de manière à ce que les requêtes DHCP des deux VLANs soient redirigés sur le serveur DHCP. Cela permet d'avoir un unique serveur DHCP pour tous les VLANs ; sinon, il en faudrait un par VLAN. Attention au nombre d'adresse à mettre dans le pool DHCP. Pas de points partiel ici. Soit votre configuration est 100% bonne soit vous n'avez pas les points. Faites bien attention aux adresses dans vos pools. (/2)

Etape 3 : Ajout de la DMZ et du routeur du FAI (/10)

Il faut configurer le routeur externe pour que le serveur Web de la DMZ soit accessible sur l'adresse externe 1.1.1.253 (/2) et que les clients locaux de l'entreprise sortent en NAT dynamique (overload en langage CISCO)(/2). (/4)

Il faut ensuite configurer les règles du pare-feu (serveurs de la DMZ accessibles sur les bons ports uniquement et trafic venant de l'extérieur envoyé aux clients uniquement si ils l'ont initié précédemment). (/4)

La licence pour le pare-feu ASA dans PT ne permet que d'avoir 2 interfaces VLAN qui communique sans restriction. La 3ème ne peut discuter qu'avec un seul autre VLAN. C'est celle-là qu'il va falloir utiliser pour la DMZ avec le mode no foward. (/2)

Les livres de la collection ENI (voir Biblio à la fin) devraient vous aider.

Etape 4 : Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI (/5)

Dans cette étape, commencez par construire le réseau 8.8.0.0/16 (domaine test.com) avec des adresses IP statiques pour le serveur et le routeur en internes, puis ajouter l'interconnexion avec le réseau.

C'est le FAI qui fournit les adresses IP (1.1.2.128/30) pour l'interconnexion avec le domaine test.com. Le routage se fera en EIGRP pour l'échange des réseaux, à savoir 1.1.1.0/24 d'un côté et 8.8.0.0/16 de l'autre.

Le site (https://polar91.wordpress.com/category/networking/routing/) devrait être une aide précieuse.

Rajoutez un serveur DNS dans le réseau externe qui permettra à votre client externe de résoudre l'IP publique du serveur web de l'entreprise : www.entreprise.com.

Une fois tout cela fait, vous pouvez maintenant faire les tests ultimes, c'est à dire montrer que les clients internes de l'entreprise peuvent accéder à www.test.com (la correspondance entre www.test.com et l'adresse IP est faite par le resolver DNS interne à l'entreprise) et que le client dans le réseau test.com peut accéder au serveur Web de l'entreprise sur les ports 80 et 443, mais pas sur les autres. Sa

résolution est faite par le serveur DNS dans le réseau externe. Il faut aussi montrer que les clients en interne peuvent communiquer avec le serveur web en DMZ sur l'adresse : www.entreprise.com(/12)

Bibliographie et webographie utiles

- Les livres de l'éditeur ENI (des livres sur CISCO et sur les ASA) pour lequel UCA à un accès via le login habituel de l'université : https://www-eni-training-com.proxy.unice.fr/instant-Connection/Default.aspx?WSLogin=ZX9dGKhciKOt7Mbu0vZQbA%3d%3d&WSPwd=fz40h%2fY4B%2bLAiCsI%2b6O3SA%3d%3d&IdDomain=4400&IdGroup=905542

- https://polar91.wordpress.com/2017/09/27/configure-multilayer-switch-on-packet-tracer/ et les autres rubriques sur ce site
- https://www.youtube.com/watch?v=SLZS1mSc_VY&list=PLK-Bs6BGQBEP4HUmB1g27aIL4EPyXeLNx

- https://itexamanswers.net/21-7-5-packet-tracer-configure-asa-basic-settings-and-firewall-using-the-cli-answers.html

- https://www.ccri.edu/faculty_staff/comp/jmowry/Security/ASA5506%209-3-1-2%20Lab%20-%20Configure%20ASA%20Basic%20Settings%20and%20Firewall%20Using%20CLI.pdf

- https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html