Quelques éléments d'architecture réseau et de sécurité

Année 2025-2026

Enseignants :

Gilles Guette gilles.guette@imt-atlantique.fr

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Contents

1 Présentation de la séance

Lors de cette séance de TP, vous allez progressivement mettre en place une infrastructure réseau avec différents services ainsi que les règles de filtrage permettant de mettre en place un contrôle des flux réseaux autorisés à passer. La figure 1 présente la topologie finale. La partie "Internet" et la partie "DMZ" vous est fournie dans le fichier `Internet-DMZ.fls`.

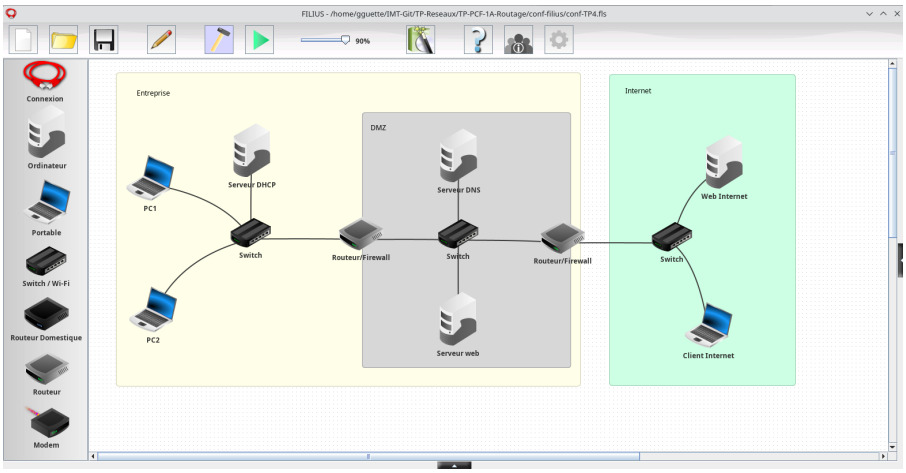

Figure 1: Topologie finale du TP

2 Mise en place du réseau interne et du serveur DHCP

Nous allons mettre en place la partie "réseau interne" de l'entreprise. Pour notre manipulation, cette partie sera constituée de deux portables et d'un serveur DHCP raccordés par un switch. Ce même switch étant raccordé à un routeur ayant deux interfaces.

Pour faciliter la gestion d'adressage IP dans les réseaux locaux, on se base généralement sur le service DHCP. Un service DHCP permet dans un premier temps de pouvoir, selon sa configuration, distribuer des adresses IP aux machines ayant besoin de configurer la carte réseau. Le DHCP permet entre autres de fournir à une machine, son adresse IP et son masque de sous-réseau, mais aussi sa passerelle par défaut, son serveur DNS, *etc.*

Question

Mettez en place PC1 et PC2 du réseau interne ainsi que le switch. Pour la configuration des PC, cochez la case sur la droite "Configuration automatique par serveur DHCP"

Question

Ajoutez un "ordinateur" connecté à votre switch, nommez-le "Serveur DHCP". Pour configurer le service DHCP, en bas à droite, cliquez sur "Configuration du service DHCP". Dans la boîte de dialogue qui s'affiche, vous allez pouvoir spécifier la plage d'adresses disponibles pour numéroter les machines de votre réseau interne. Choisissez une plage d'adresse de votre choix, par exemple entre 192.168.0.1 et 192.168.0.100. Vous pouvez aussi renseigner la passerelle par défaut (cochez la case config manuelle) qui sera l'adresse que vous souhaitez mette sur votre routeur. Cochez la case "Activer le service DHCP". Ça y est, votre serveur est prêt.

Finalisez votre réseau interne en ajoutant la bonne adresse à votre routeur.

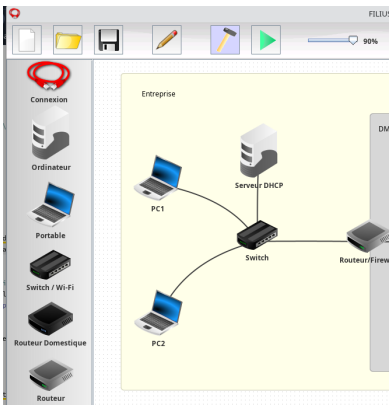

Figure 2: Réseau Interne avec DHCP

2.1 Observation de l'échange DHCP

Question

Passez en mode simulation, afficher le trafic étant passé par le serveur DHCP, analysez/expliquez ce qu'il s'est passé en regardant les adresses de destination et le contenu des paquets. Par exemple, pourquoi les paquets DHCP DISCOVER partant des PC ont une adresse de destination en 255.255.255.255 ? Pourquoi l'échange nécessite-t-il 4 paquets ?

3 Mise en place de la DMZ

La DMZ ou *De Militarized Zone* (figure 3) est un sous-réseau de l'entreprise hébergeant généralement les serveurs publics ainsi que les proxys et reverse proxy. Cette zone hébergeant des services devant être accessibles depuis l'extérieur, elle est naturellement la plus proche de l'extérieur et donc la "plus exposée". Notre DMZ contient un serveur Web et un serveur DNS.

Question

Ces serveurs doivent avoir une adresse IP fixe (pas d'attribution par DHCP). Pourquoi ?

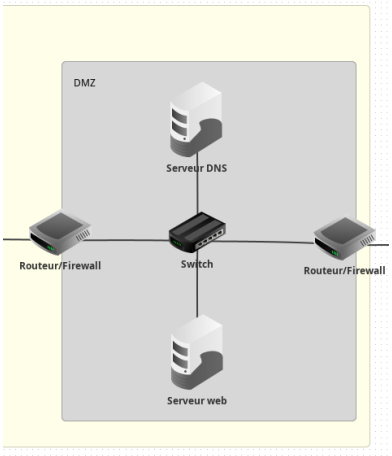

Figure 3: Réseau DMZ

Question

Les équipements de la DMZ sont pré-configurés et disposent d'une adresse IP fixe (pas de DHCP). Depuis PC1 et PC2, vérifiez l'accessibilité à toutes les machines du réseau de l'entreprise.

3.1 Observation du DNS

Sur le serveur Web, depuis le bureau, cliquez sur l'icône "Serveur Web" et activez le service web. Sur PC1, ajoutez sur le bureau un navigateur web et, à partir de ce navigateur, essayez de joindre votre serveur en utilisant son IP.

Question

Est-ce que tout se passe correctement ? Essayez de le joindre en utilisant le nom monbeauserveur.com, pourquoi cela ne fonctionne-t-il pas ? (Regardez la capture de trafic.)

Pour pouvoir résoudre un nom en adresse IP, il faut que PC1 connaisse un serveur DNS à qui poser la question et que ce serveur soit configuré correctement.

Question

Ajoutez l'adresse IP de votre serveur DNS dans la configuration de PC1. Comme la configuration de PC1 est faite par DHCP, c'est sur le serveur DHCP qu'il faut agir.

Question

Sur le serveur DNS, ajouter l'association d'adresse : monbeauserveur.com 192.168.1.2 et démarrez le serveur DNS. Dans le navigateur Web de PC, entrez dans la barre d'URL : `http://monbeauserveur.com`. Pourquoi cela fonctionne maintenant ? Justifiez à partir de la capture de trafic.

4 Mise en place du filtrage de flux

En préliminaire, vérifiez que PC1 et PC2 ont bien accès à toutes les machines, y compris celle sur "Internet". Comme vous pouvez le constater, tout le monde a accès à tout, ce qui n'est pas très sûr. Nous allons donc dans la suite, commencez à restreindre les accès en appliquant une politique de sécurité. Cette politique sera matérialisée par des règles de filtrage posées dans les routeurs.

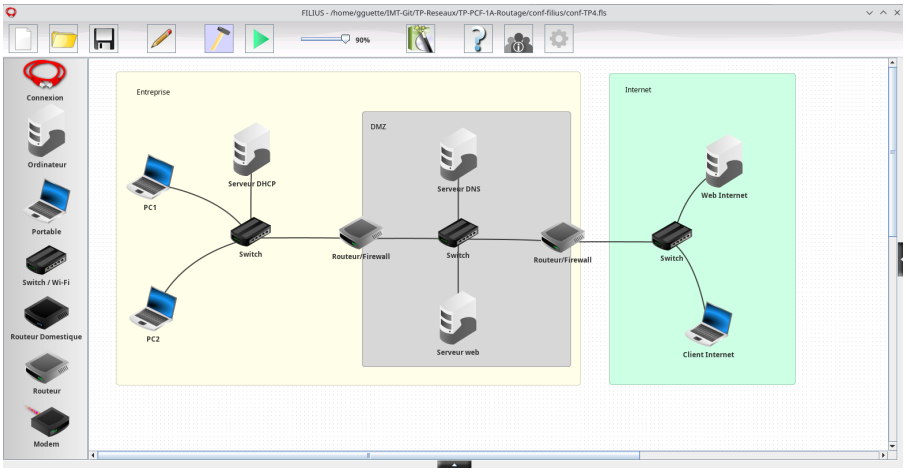

Figure 4: Topologie sur laquelle effectuer le filtrage

4.1 Fermeture des accès

4.1.1 Premier filtrage

Par précaution, on va commencer par bloquer tous les accès entrants et sortants sur le routeur d'entrée de l'entreprise. Pour cela, dans le routeur, cliquer sur configurer le "pare-feu", cocher les cases "Filtrer les paquets ICMP" et "activer le pare-feu" (figure 5), puis passer sur l'onglet "Règles du pare-feu" (figure 6).

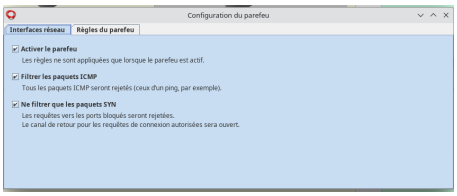

Figure 5: Activation du pare-feu

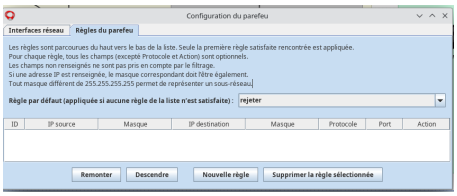

Figure 6: Visualisation de la politique et des règles

Comme vous pouvez le constater ce pare-feu exerce un contrôle à deux niveaux. Tout d'abord en regardant si une règle correspond au paquet analysé (pour le moment, nous n'avons pas de règle) et si aucune règle n'est déclenchée, il applique la politique par défaut qui est ici : "rejeter". C'est bien ce que nous souhaitons faire. Et c'est la bonne pratique pour un pare-feu de réseau local, on ferme tout et on ouvre petit à petit selon le besoin réel. L'idée est simple, un employé qui ne peut pas travailler à cause du filtrage viendra râler et vous serez au courant. Un employé pouvant télécharger n'importe quoi et regarder Netflix, ne viendra pas vous informer qu'il y a un trou dans votre politique de sécurité.

Note : Le pare-feu que vous manipulez ici, contrairement à d'autres équipements, garde un état des connexions, vous n'avez donc qu'à écrire la règle "aller" et il s'occupe de la règle "retour" tout seul.

Question

Votre pare-feu étant activé, testez que votre réseau interne n'a plus accès à la machine Web Internet

grâce à un client Web ni à Client Internet grâce à un `ping`.

Question

Vérifiez aussi que Client Internet n'a pas accès au serveur Web de l'entreprise.

4.1.2 Deuxième filtrage : accès Web

Question

Avoir un serveur Web d'entreprise non accessible depuis Internet n'est pas très utile. Vous allez donc ajouter une règle dans le pare-feu pour qu'il laisse passer les accès à votre serveur Web depuis Internet. Si vous laissez une case vide, cela veut dire qu'elle peut prendre toutes les valeurs possibles, si vous précisez une valeur, la règle sera déclenchée si le champ du paquet réseau vérifie cette valeur. Si vous voulez indiquer une adresse de machine le masque est 255.255.255.255, si vous voulez spécifier un réseau tout entier, il suffit de jouer avec la valeur du masque. Votre serveur Web écoute sur le port TCP 80. complétez une règle acceptant les paquets provenant d'Internet (toutes les valeurs possibles en source) à destination de votre serveur Web (IP 192.168.1.2), protocole TCP, port 80. Vérifiez que Client Internet a bien accès à votre serveur Web.

4.1.3 Troisième filtrage : accès Internet

Question

Nous allons maintenant permettre à vos postes internes d'aller surfer sur Internet. Écrivez une règle permettant de laisser passer tout le réseau interne (celui de PC1 et PC2) vers des serveurs Web de l'Internet.

4.1.4 Quatrième filtrage : et la DMZ dans tout ça ?

Les premières règles permettent de mettre un premier filtre à l'entrée pour pouvoir donner accès à la DMZ, néanmoins pour le moment rien n'a été fait pour séparer la DMZ du réseau interne, donc un accès à la DMZ équivaut à un accès au réseau interne et ça, c'est mal !

Question

Activez le pare-feu sur le routeur liant le réseau interne et la DMZ. Par défaut tout est bloqué. Ajoutez-y aussi une règle pour continuer de pouvoir aller sur Internet depuis le réseau interne. Vérifiez que tout fonctionne comme prévu. Et bien sûr qu'Internet a toujours aussi accès à votre serveur web.

4.1.5 Cinquième filtrage : l'ordre c'est important

Dans le pare-feu reliant le réseau interne à la DMZ, ajoutez une règle pour empêcher le PC2 d'avoir accès au serveur web de la DMZ. Que se passe-t-il ? Pourquoi ? Corrigez.

Question

Activez le pare-feu sur le routeur liant le réseau interne et la DMZ. Par défaut tout est bloqué. Ajoutez-y aussi une règle pour continuer de pouvoir aller sur Internet depuis le réseau interne. Vérifiez que tout fonctionne comme prévu. Et bien sûr qu'Internet a toujours aussi accès à votre serveur web.