Présentation SAE21: Firewalling

Présentation du contexte:
cette sae à pour but de recréer un réseau d'entreprise. ce réseau serait consituté en pratique de 2 partie, un réseau de PC qui seraient séparés avec des VLANS. Ce réseau comprendrais un serveur d'adressage ainsi qu'un serveur web. cet intranet serait séparé par un routeur qui reliait cet intranet à un extranet qui contiendrait un serveur DNS et un site WEB. enfin cette infrastructure serait reliée à internet par le biais d'un routeur qui comprendrait aussi un firewall.
Dans la pratique le réseau intranet sera fait sur GNS3, le serveur DNS/WEB sera un pc de salle réseau et le firewall routeur sera un routeur mikrotik.

Lors de ce travail de groupe je me suis penché sur la mise en place du routeur mikrotik ainsi que de la mise en place du firewall.

Présentation des étapes
Il a d'abord fallu configurer l'adressage des pâtes du routeur en suivant le plan d'adressage précédemment donné par mes camarades.
on utilise la commande:
[admin@MikroTik] ip address> add address=<adresse>/<masque> interface=<interface>
pour ajouter une adresse aux 2 pâtes de communication.
La pâte interne est relié au pc et à la maquette GNS3 la pâte interne au réseau de la salle réseau.

Maintenant passons au firewalling

petite explication préalable
Il existe 2 types de firewall, les firewall stateless et stateful. La différence majeure est que les firewall dit stateful analysent la connexion entière. il y a 2 états principaux new, established. Le premier symbolise les filtres arrivés sur les paquets initiateurs d'une connexion, les seconds représentent les paquets faisant partie d'une connexion déjà établie.

mise en place
Dans le cas de cette SAE j'ai adopté la stratégie suivante

- appliquer une restriction stricte sur les paquets new afin de filtrer toute connexion indésirable
- n'appliquer aucune restriction sur les paquet established car pour que l'état soit considéré established il faut pour cela que le paquet new ai été accepté au préalable

j'ai donc appliqué créé comme politique par défaut "drop" puis j'ai ajouté des exceptions pour:

- les connection sortante à destination du port tcp 80
- les connection sortante à destination du port udp 53
- le trafic ICMP
- les états established

en pratique on utilise la commande
[admin@MikroTik]ip firewall filter print
pour afficher les filtres existants
et
[admin@MikroTik]ip firewall filter add aciton=<action> chain=forward dst-port=<port de destination> ou src-port=<port source> si on veut appliquer une règle sur le port tcp source.

On applique cette configuration et on vérifie qu'elle fonctionne bien.

conclusion
Pour conclure je peux dire que c'est la lecture et la compréhension de la documentation qui m'a pris le plus de temps. Par exemple, comprendre les tenants et aboutissants du suivis des trames pour créer une stratégie cohérente de firewalling à été une source importante de réflexion et débats au sein du groupe.