

Configuration

Plan d'adressage

Opérateur

Entre deux routeurs ou entre un routeur et le serveur web externe, j'ai décidé de créer des sous-réseaux du réseau 10.0.0.0/24 avec des masques en /30. Par exemple, le premier réseau sera 10.0.0.0/30, le second 10.0.0.4/30 etc... Un réseau avec un masque en /30 permet d'accueillir deux machines ce qui suffit pour connecter deux routeurs par exemple. Par conséquent, on économise des adresses IPv4.

Réseau interne

En ce qui concerne le réseau interne, les machines doivent avoir des adresse privées. Dans ce contexte, j'ai décidé de que les réseaux de chaque VLAN seraient définis de cette manière en respectant la RFC 1918: 192.168.VLAN.MACHINE. Par exemple, la première machine recevant une adresse IP appartenant au VLAN 10 possède cette adresse IP: 192.168.10.1/24. Par ailleurs, j'ai mis en place un serveur DHCP qui attribue des adresses IP à toutes les machines de tous les VLANs sauf celui dans lequel il se situe.

Routage opérateur

J'ai décidé de mettre en place du routage dynamique pour avoir une configuration modulaire. Parmi les protocoles de routage que je connais se trouvent RIP, OSPF et BGP. Pour choisir entre ces trois protocoles, j'ai procédé par élimination. RIP n'est pas recommandé en raison de son temps de convergence élevé et des problèmes de bouclage. Par ailleurs, BGP est un EGP (Exterior Gateway Protocol) c'est-à-dire qu'il est utile pour du routage inter-AS (Autonomous System). Or, nous voulons mettre en place du routage à l'intérieur d'un réseau opérateur donc à l'intérieur d'un AS. Ainsi, le protocole de routage le plus adéquat à mettre en place est OSPF qui est une IGP (Interior Gateway Protocol) et qui a un faible temps de convergence.

Parler du point-à-point

Sécurité

Réseau interne

Pour répondre aux besoins de sécurité au niveau du réseau interne, j'ai mis en place des VLANs. En effet, ces derniers permettent de segmenter le réseau interne et d'instaurer des règles de sécurité. Pour ce faire, j'ai attribué un VLAN par service:

Nom	Numéro
Commercial	10
Administration	20
SI	30
Services_internes	40

Après avoir configuré les deux switchs, je me suis occupé de l'interface interne du routeur de telle sorte que les machines des différents VLANs puissent communiquer. Ensuite, j'ai pu instaurer des règles de sécurité. Par exemple, pour faire en sorte que les administratifs aient accès au serveur interne, à la DMZ et à Internet mais qu'ils ne puissent pas avoir accès aux autres réseaux internes, cette règle a été mis en place:

Extended IP access list administration

```
deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
permit tcp 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255 established
permit icmp 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255 echo-reply
permit ip any any
```