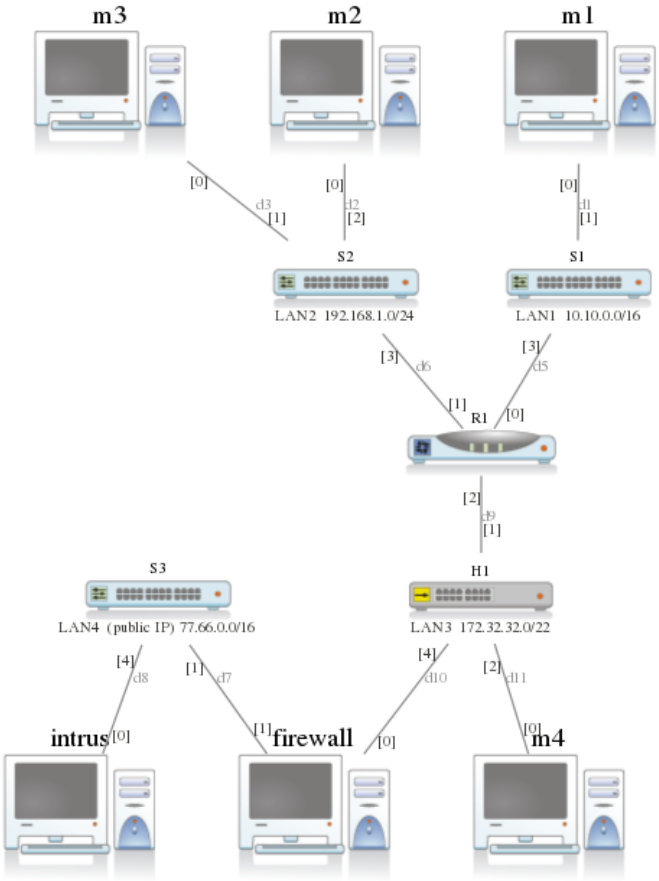
Contrôle Réseaux

Lic. Pro R&T-FC ASSUR, IUT de Villetaneuse

15 Novembre 2018

Partie II. Contrôle pratique

Documents autorisés - Durée 1h45



Configuration à réaliser

1. $LAN_1 = \{m_1, R1[0]\}$ en 10.10.0.0/16 ; la machine m_1 offre un service SSH
2. $LAN_2 = \{m_2, m_3, R1[1]\}$ en 192.168.1.0/24 ; la machine m_2 offre un service HTTP
3. $LAN_3 = \{m_4,\ R1[2],\ firewall[0]\}$ en 172.32.32.0/22 ; la machine m_4 offre un service HTTP
4. $LAN_4 = \{firewall[1],\ intrus\}$ en 77.66.0.0/16
5. La machine *firewall* a **l'unique adresse IPv4 publique** du réseau, c'est-à-dire 77.66.0.15 (sur `eth1`, c'est-à-dire le LAN_4). Elle **protège** toutes le machines qui se trouvent derrière son interface `eth0` (LAN_1, LAN_2 et LAN_3) et leur **prête** l'adresse publique pour sortir sur Internet (dont fait partie le LAN_4). Elle donne aussi accès depuis l'extérieur (par exemple à *intrus*) au service SSH de m_1, au service HTTP de m_2 et au service HTTP de m_4 (pour ce dernier, *firewall* "propose" à l'extérieur le service sur le port fictif 8080).

Note pour les points 1., 2. et 3. : le routeur $R1$ doit être configuré comme toutes les autres machines, c'est-à-dire en supposant d'y avoir accès par un terminal Unix (`ifconfig`, ...).