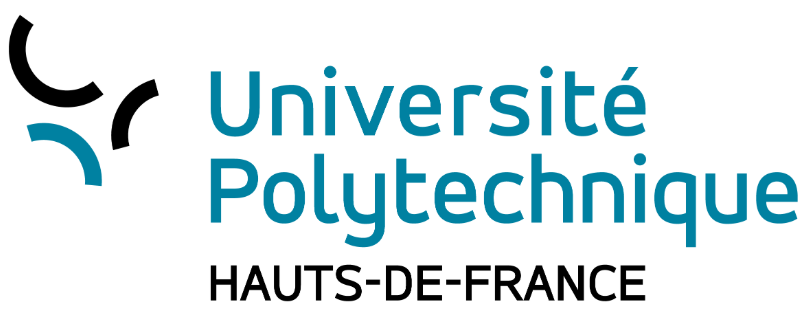
****

****

**Privacity**

**Sommaire**

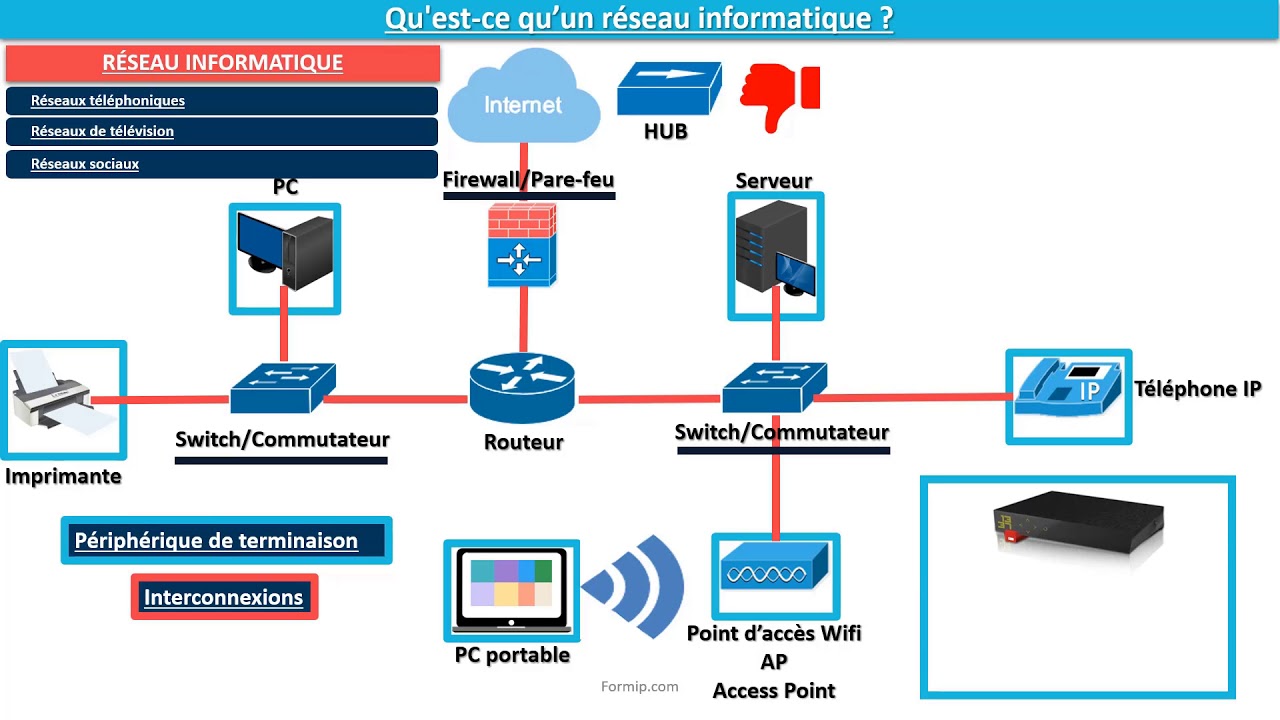
1. Un réseau classique ?
2. SDN (Software Defined Network)
3. Mininet
4. Architecture
5. la définition d’architecture
6. Les fonctions des nœuds
7. Générateur de trafic
8. Fonction du switch
9. Simulation (VM)

Un réseau classique ?

Un réseau informatique est un ensemble d’équipements reliés entre eux qui communique des informations

Les Nœuds sont reliés entre eux avec des équipements d’interconnexion :

* Switch
* Router
* FireWall
* ETC…



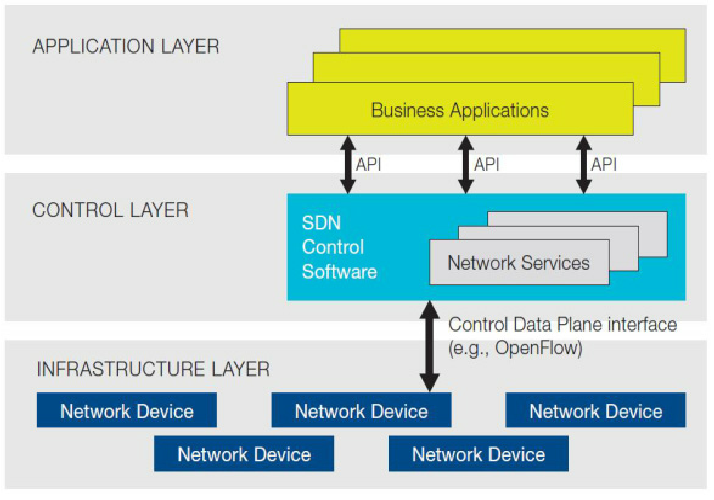
La puissance de calcul et la prise de décision sont distribués sue les différents équipements

SDN (Software Defined Network)

SDN est une architecture émergente qui est dynamique, gérable, rentable et adaptable, ce qui est idéale pour la nature dynamique des applications

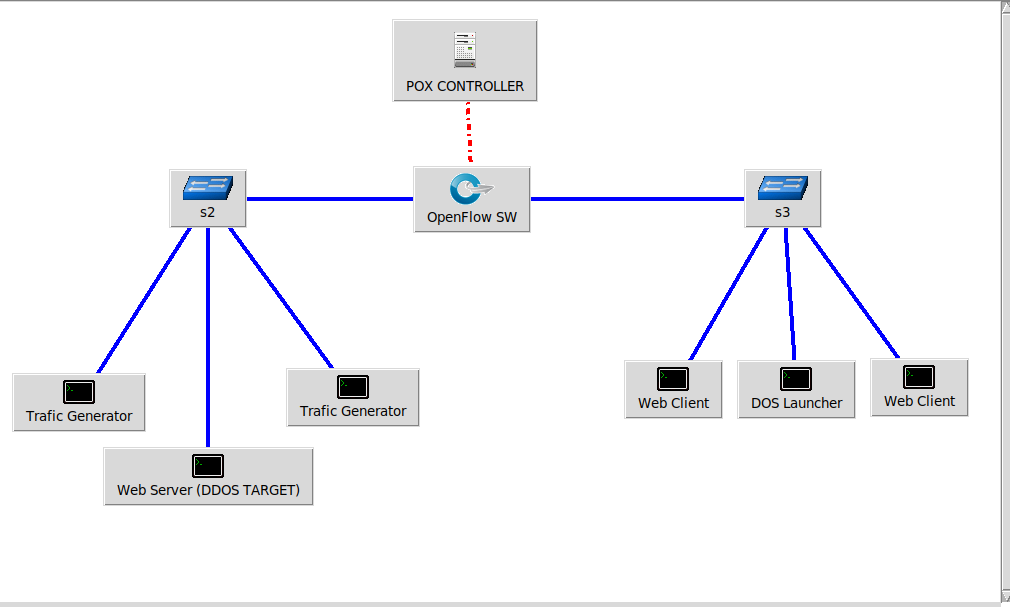
Cette architecture décuple les fonctions :

* Control plan
* Data plan



Mininet

Architecture :



Mininet est une solution qui va nous permettre de mettre en place des architectures réseaux au plus près des besoins de nos tests.

Plus concrètement, Mininet nous permet de déployer sur une seule machine, des réseaux, commutateur, routeurs, FW ou tous autres équipements réseau

On peut utiliser Mininet via deux moyens :

1. En ligne de commande
2. Via une librairie python

Mininet offre beaucoup classe pour construire des architectures

La définition d’architecture



Nous commençons la création de notre architecture par la création de notre des objets qui représente les nœuds et les équipements réseau.

* 2 Clients web
* 1 serveur
* 2 générateurs de trafic
* 2 commutateurs
* 1 contrôleur Openflow

Ensuite, il faut créer les liaisons entre les équipements.

Les fonctions des nœuds



Pour donner aux nœuds des rôles il faut :

* Utiliser des commandes natives
* Utiliser des librairies python

Générateur de trafic

Pour générer le trafic réseau nous avons utilisé la librairie Scapy pour créer des paquets et les envoyer.

Ont généré le trafic de différents protocoles :

* TCP
* UDP
* ICMP



On utilise scapy pour créer des paquets et les envoyer dans une boucle infinie.



POX est un Framework pour communiquer avec les switch SDN en utilisant le protocole Openflow.

Nous pouvons utiliser POX pour créer un contrôleur SDN en utilisant le langage Python.

Fonction du switch

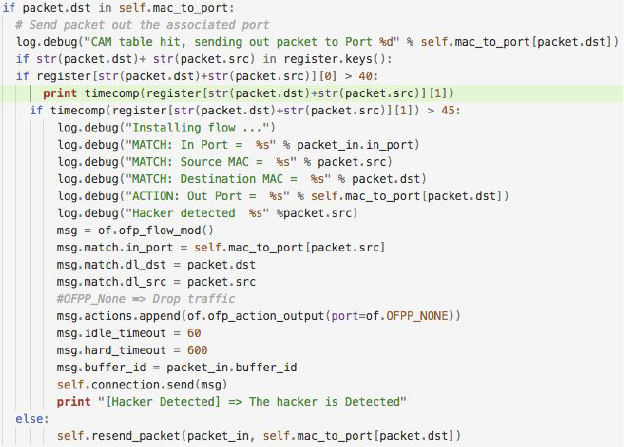


Pour garder des traces des connexions et détecter les attaques nous allons parser les paquets et enregistrer les informations d’émetteur et le récepteur dans le registre qui contient :

* Le nombre de connexion
* Le timetamp de la première connexion

Détection :

Nous allons vérifier dans un premier temps qu’un host a envoyé plus que 40 paquets en 45 secondes, le contrôleur envoie un msg OpenFlow au switch pour droper tout le trafic réseau entre la source et la destination



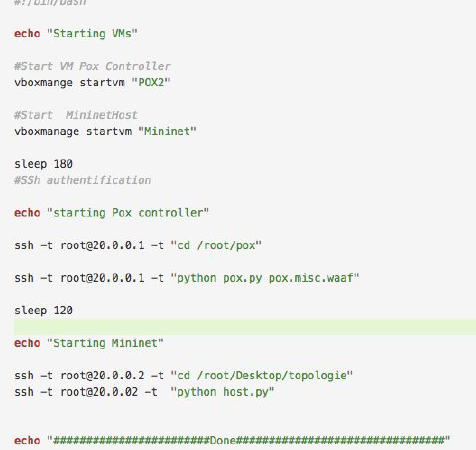
Simulation

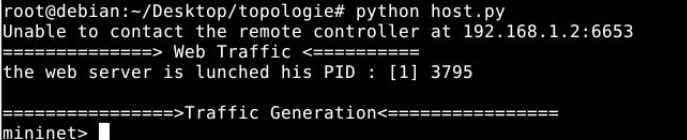
Ce script va lancer les deux machines virtuelles :

* POX
* Mininet

Et lancer les scripts :

* POX
* Topologie





Détection d’attaque

