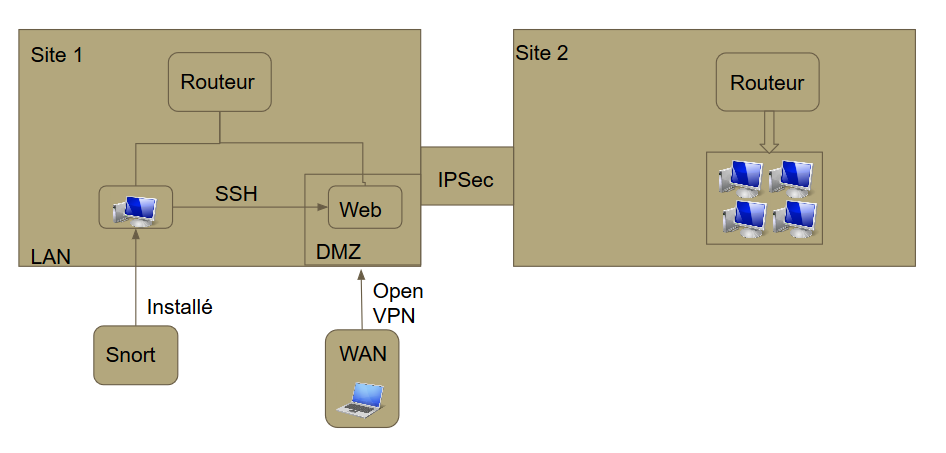
Projet Sécurité

## Alves Vincent, Luce Gatien, Rasamoelison Lawrencio, Demailly Benjamin, Ariiotima Vaiani

# Structure du réseau



Les deux sites sont reliés par un tunnel IPSec. Chaque site est géré par un routeur pfSense, qui utilise trois interfaces :

* LAN – Les machines en réseau privé, non accessibles de l’extérieur mais pouvant communiquer entre elles
* DMZ – Les machines du réseau privé accessibles de l’extérieur et depuis la LAN.
* WAN – L’internet extérieur.

Ici, on a placé un serveur Web Apache2 dans la DMZ, accessible en SSH depuis les machines de la LAN.

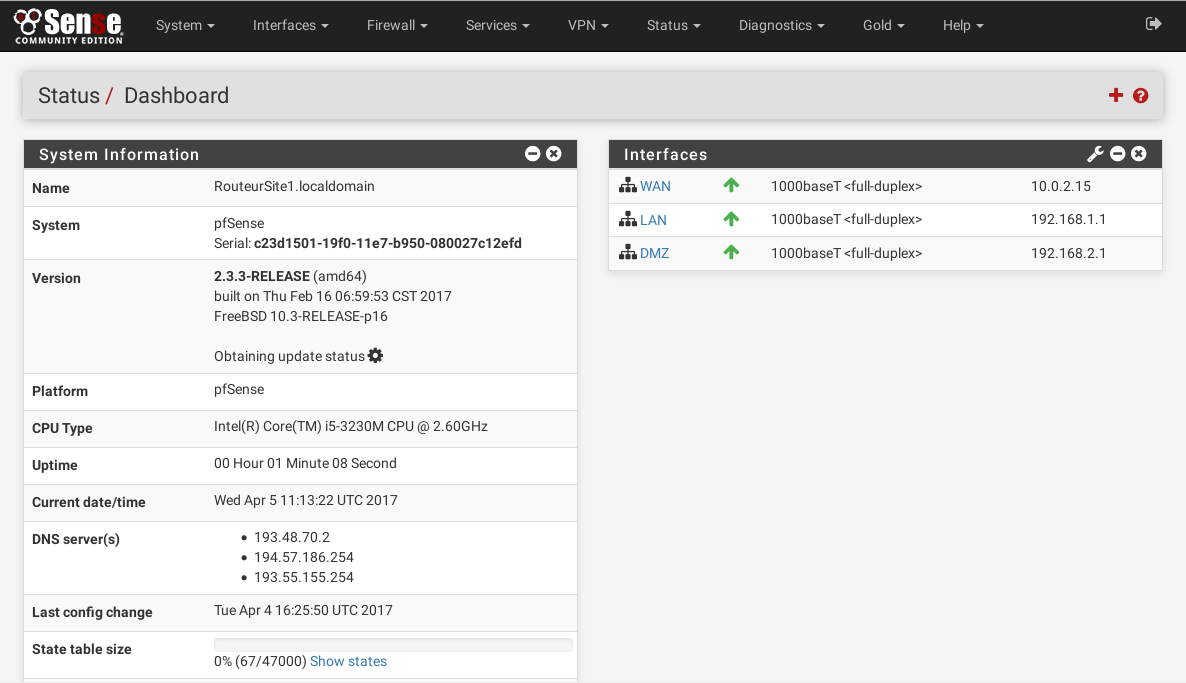
Le Site 1 est également accessible via un tunnel OpenVPN.

# Notre implémentation

Pour simuler ce réseau, nous avons pris plusieurs machines virtuelles :

* Deux VMs pfSense pour les routeurs
* Deux VMs Debian, une en DMZ pour le serveur Web et une autre en LAN pour gérer le pfSense du site 1

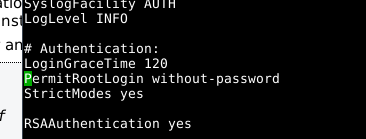
Les VMs pfSense ont trois interfaces : Une en NAT reliée à la connexion internet standard (WAN), et deux réseaux virtuels pour simuler LAN/DMZ.



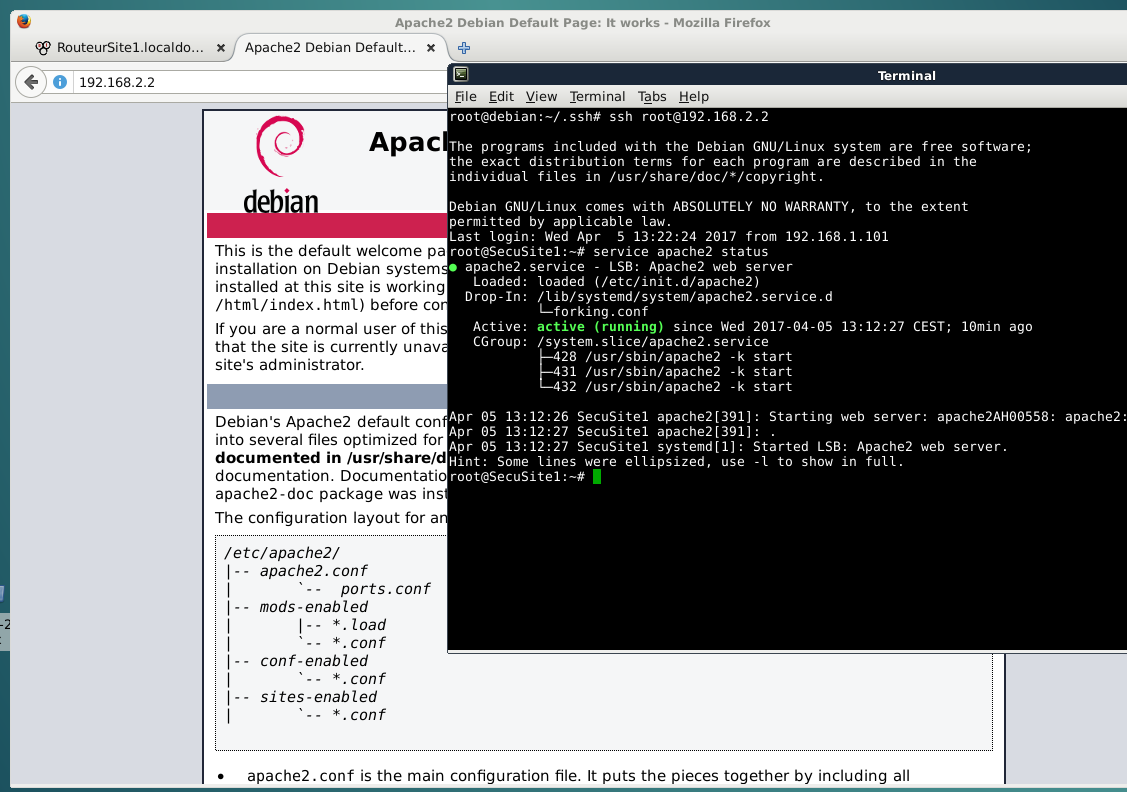
Interface Web de pfSense

La VM sur le LAN a pour IP 192.168.1.101, et la VM sur le DMZ 192.168.2.2.

En copiant la clé ssh publique de la machine LAN sur la VM en DMZ, on peut se logger dessus sans entrer de mot de passe, puis désactiver le login via password sur la machine DMZ.



Désactivation de l’authentification sur la machine DMZ



Accès au serveur web de la machine DMZ depuis la machine LAN et connexion en SSH sans password

Nous avons essayé d’installer snort sur une autre VM pour la brancher sur le LAN, mais ce ne fut pas très concluant.

Quant à OpenVPN, le setup côté routeur fut facile grâce à pfSense, mais nous n’avons pas eu le temps de setup un client pour le tester correctement.