Atelier Pro

Mise en place d’un firewall avec PfSense

RASCLE Rémi

Sommaire

Description du laboratoire GSB

Le secteur d'activité :

L’industrie pharmaceutique est un secteur très lucratif dans lequel le mouvement de fusion acquisition est très fort. Les regroupements de laboratoires ces dernières années ont donné naissance à des entités gigantesques au sein desquelles le travail est longtemps resté organisé selon les anciennes structures. Des déboires divers récents autour de médicaments ou molécules ayant entraîné des complications médicales ont fait s'élever des voix contre une partie de l'activité des laboratoires : la visite médicale, réputée être le lieu d' arrangements entre l'industrie et les praticiens, et tout du moins un terrain d'influence opaque.

L'entreprise :

Le laboratoire Galaxy Swiss Bourdin (GSB) est issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui-même déjà union de trois petits laboratoires . En 2009, les deux géants pharmaceutiques ont uni leurs forces pour créer un leader de ce secteur industriel. L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris. Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis. La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

Description du laboratoire GSB

Le système informatique :

Sur le site parisien, toutes les fonctions administratives (gestion des ressources humaines, comptabilité, direction, commerciale, etc.) sont présentes. On trouve en outre un service labo-recherche, le service juridique et le service communication.

La salle serveur occupe le 6ème étage du bâtiment et les accès y sont restreints (étage accessible par ascenseur à l'aide d'une clé sécurisée, portes d'accès par escalier munies d'un lecteur de badge, sas d'entrée avec gardien présent 24h/24).

Les serveurs assurent les fonctions de base du réseau (DHCP, DNS, Annuaire et gestion centralisée des environnements) et les fonctions de communication (Intranet, Messagerie, Agenda partagé, etc.).

On trouve aussi de nombreuses applications métier (base d'information pharmaceutique, serveurs dédiés à la recherche, base de données des produits du laboratoire, base de données des licences d'exploitation pharmaceutique, etc.) et les fonctions plus génériques de toute entreprise (Progiciel de Gestion Intégré avec ses modules RH, GRC, etc.).

Un nombre croissant de serveurs est virtualisé.

Constitué autour de VLAN, le réseau segmente les services de manière à fluidifier le trafic.

Les données de l'entreprises sont considérées comme stratégiques et ne peuvent tolérer ni fuite, ni destruction. L'ensemble des informations est répliqué quotidiennement aux Etats-Unis par un lien dédié. Toutes les fonctions de redondances (RAID, alimentation, lien réseau redondant, Spanning-tree, clustering, etc.) sont mises en œuvre pour assurer une tolérance aux pannes maximale.

L'équipement :

L'informatique est fortement répandue sur le site. Chaque employé est équipé d'un poste fixe relié au système central. On dénombre ainsi plus de 350 équipements terminaux et un nombre de serveurs physiques conséquent (45 en 2012) sur lesquels tournent plus de 100 serveurs virtuels.

On trouve aussi des stations de travail plus puissantes dans la partie labo-recherche, et une multitude d'ordinateurs portables (personnels de direction, service informatique, services commerciaux, etc).

Les visiteurs médicaux reçoivent une indemnité bisannuelle pour s'équiper en informatique (politique Swiss-Bourdin) ou une dotation en équipement (politique Galaxy). Il n'y a pas à l'heure actuelle d'uniformisation des machines ni du mode de fonctionnement.

Segmentation du réseau :

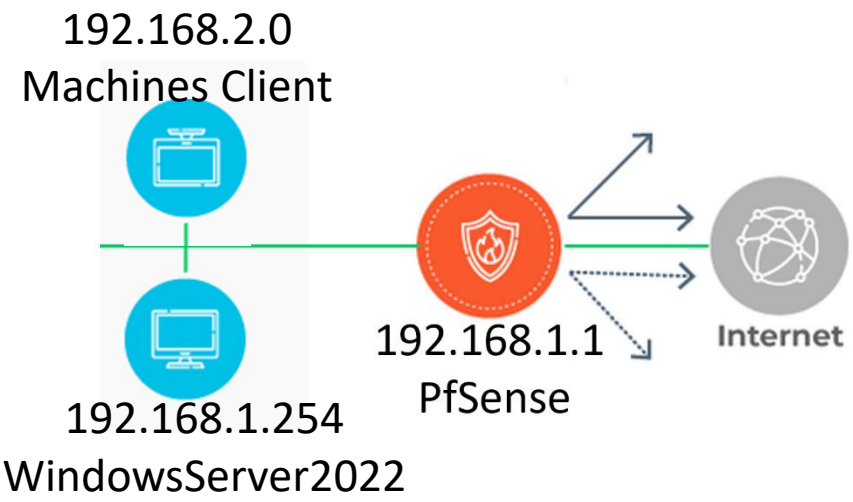
L'organisation des VLAN et de l'adressage IP est la suivante :

N° VLAN	Service(s)	Adressage IP
210	Serveur	192.168.1.0
211	Clients	192.168.2.0

Salle serveur et connexion internet :

L'organisation des serveurs et des équipements réseaux est la suivante :

- Le serveur principal est virtualisé sous le système Vmware Vcenter 7.0
- Un Commutateur Multicouche Cisco permet l'interconnection du serveur principal et la liaison vers le firewall de proximité (Internet).
- L'environnement Virtuel et réseau des Projets d'Atelier de Professionnalisation sont référencées ci-dessous :

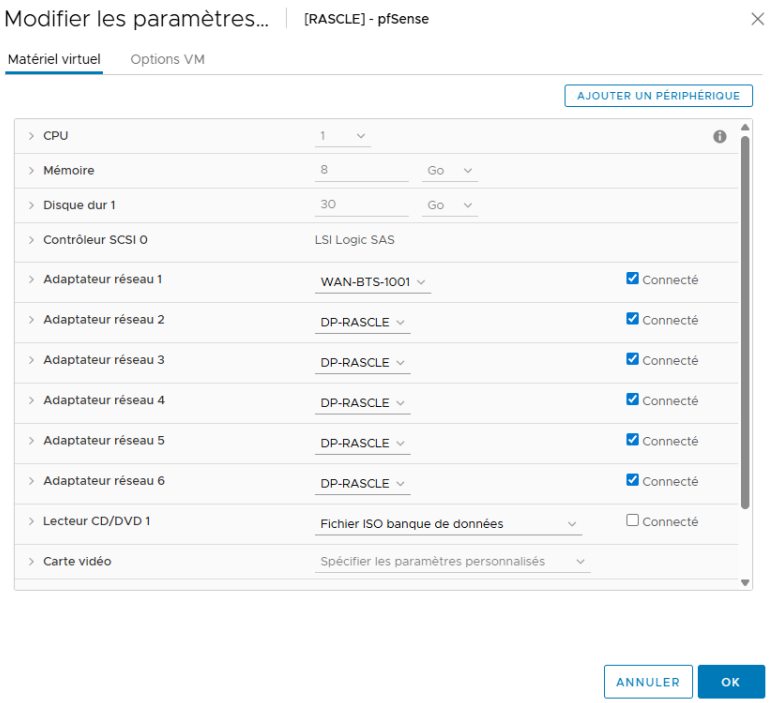


Cahier des Charges

- Créer un machine Firewall (Pfsense)
- Faire passer chaque échange par le Firewall
- Accéder au Firewall par une interface web
- Filtrer les échanges grâce à des règles

Ajout des cartes réseaux à la machines PfSense :

[RASCLE] PfSense > Clic droit > Modifier les paramètres > Matériel virtuel > Ajouter un périphérique > Adaptateur réseau > DP-RASCLE > OK



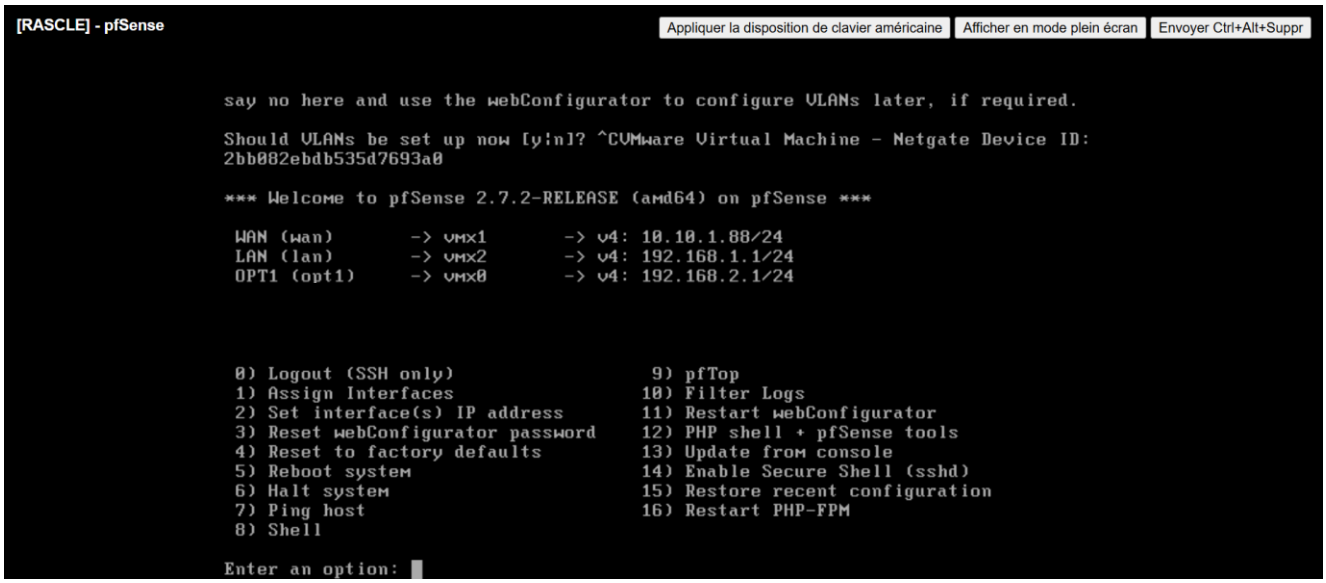
Redémarrer la Machine PfSense

Configuration des cartes réseaux :

vmx1 : WAN, 10.10.1.88

vmx2 : LAN, 192.168.1.1 VLAN 210

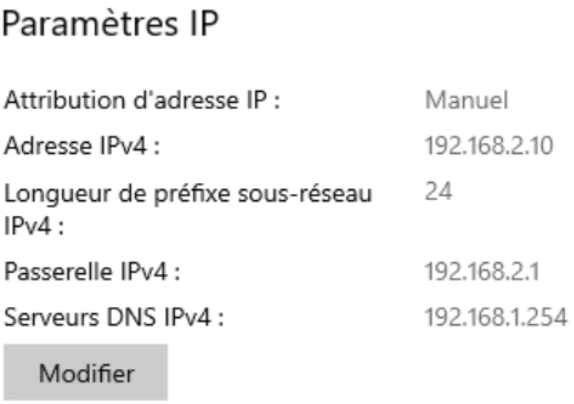
vmx0 : OPT1 (Machines client), 192.168.2.1 VLAN 211



Mettre en place les passerelles sur les machines :

Dans les paramètres réseaux des machines, mettre l'ip du firewall en passerelle.

Pour le serveur

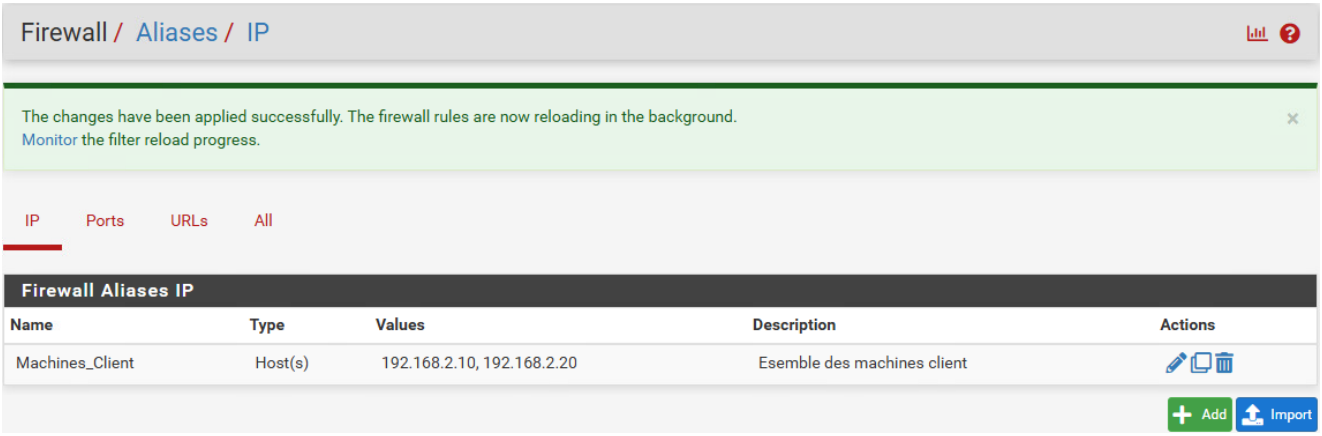


Pour les Machine clients (IP fixes différentes pour chaque machines)

Les Aliases :

Les alias regroupes un ensemble d'IP, de ports ou d'URLs pour faciliter la création de règles.

Ici je regroupe dans un alias mes machines client.



Règles de Firwall :

- Première ligne pour ne pas perdre l'accès à l'interface web du PfSense.
- Deuxième permet à tous le réseau LAN d'accéder à toutes les destinations en IPv4
- Troisième en IPv6