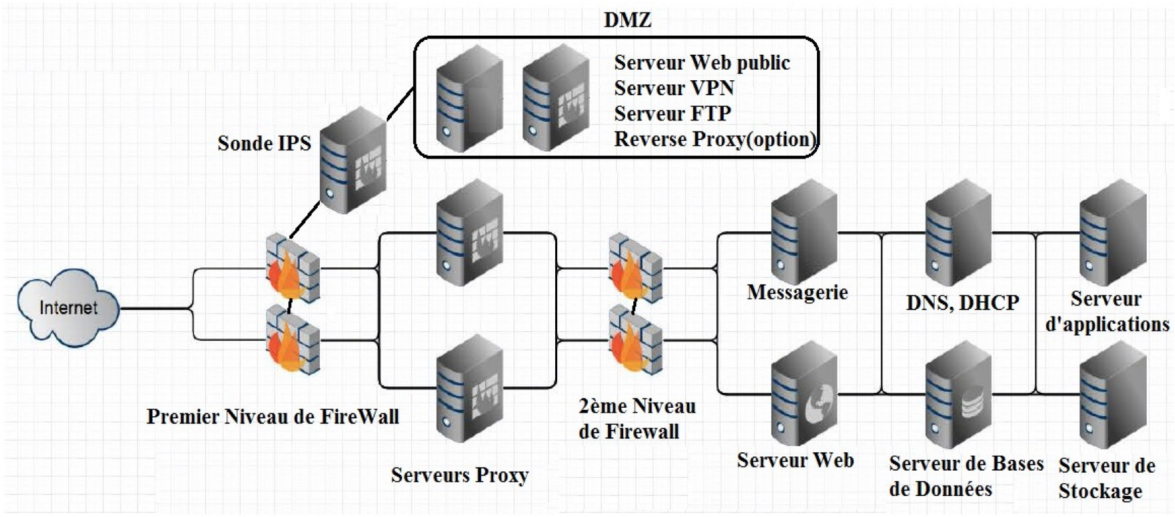
Mathieu BOISNARD
Valentin FRIES
Vincent MILANO

ENOVATIVE keys

école supérieure de génie informatique

1 - Détail des besoins de l'architecture

Rappelons d'abord brièvement l'architecture réseau demandée par le client lors de la mission 3 du projet Webex :



Architecture réseau Webex

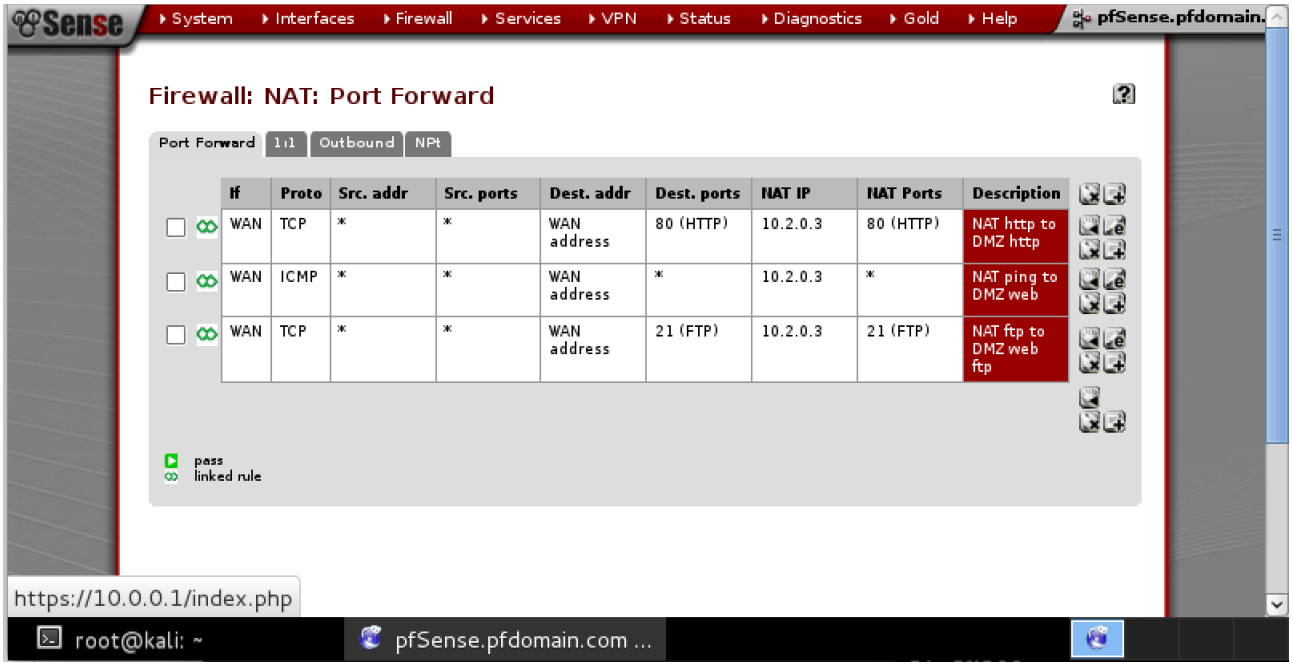
Cette architecture complète nécessite différentes configurations au niveau des règles appliquées sur le firewall et au niveau de la redirection des connexions rentrantes en amont au niveau du WAN.

C'est pour cela qu'il nous faut :

- Permettre à toute personne venant du WAN (en http aussi bien qu'en ftp) d'être redirigé automatiquement vers la DMZ (et non le LAN /!\ - formellement interdit)
- Permettre au Cloud, situé dans la DMZ, de passer des données en http au WebService, qui se trouvera sur le serveur web de la LAN. Ce WebService communique facilement avec la BDD qui est elle-même située dans le LAN, mais nous devons également permettre aux données de passer dans le sens inverse, c'est à dire autoriser le passage de données en http du WebService dans la LAN vers la DMZ.
- Interdire à tout employé à l'intérieur de la LAN d'accéder au serveur web de la DMZ, en effet nous ne voulons pas que les employés et développeurs puissent se permettre de changer la configuration ou quoi que ce soit à l'intérieur de notre DMZ.
- Interdire à tout employé à l'intérieur de la LAN d'accéder à une liste précise de sites internets considérés comme non sécures (téléchargement, contenu adulte, violence...). Il est évident que l'accès à un maximum de ces sites soient bloqués.

2 - Configuration adaptée aux besoins

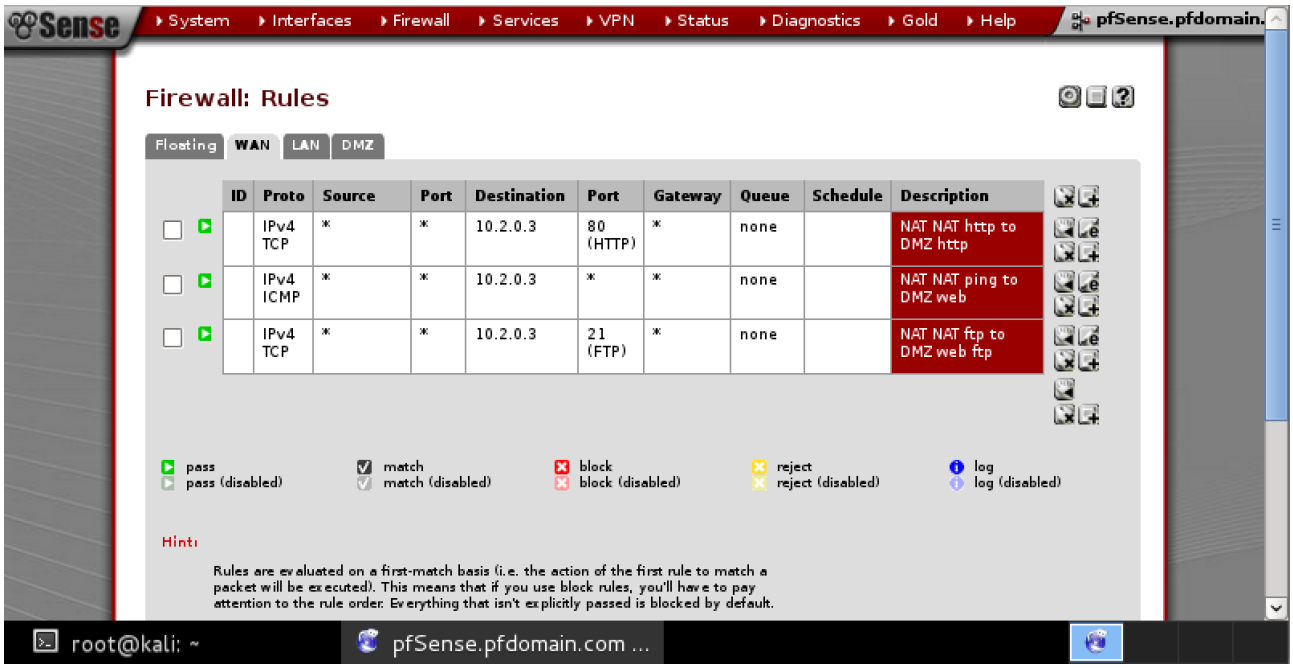
Nous montrerons dans cette partie la mise en place adaptée des règles, dont celle de redirection, directement sur le firewall pfsense à partir des screenshots suivants :



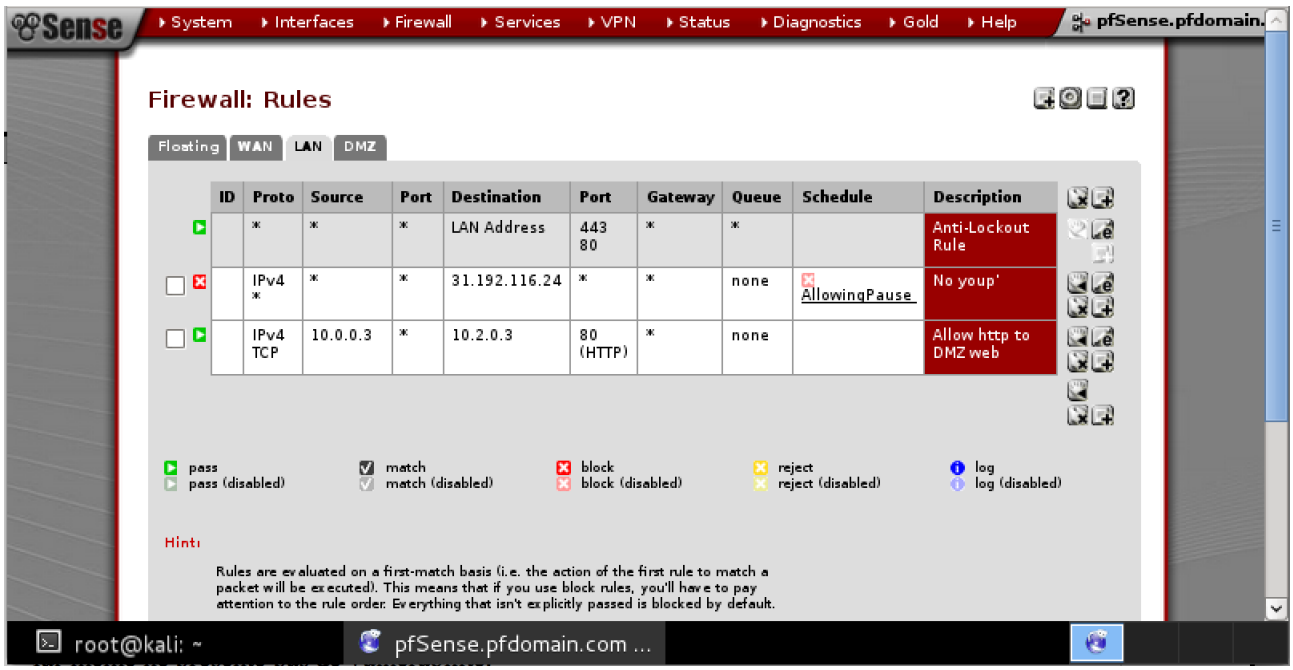
Règles NAT de redirection (port forwarding) à l'arrivée depuis le WAN

→ http to DMZ http (accès au Cloud utilisateur)
→ icmp to DMZ web (simple précaution)
→ ftp to DMZ ftp, bien qu'on remarquera que le ftp ne serrait utilisé qu'avec une configuration en réel

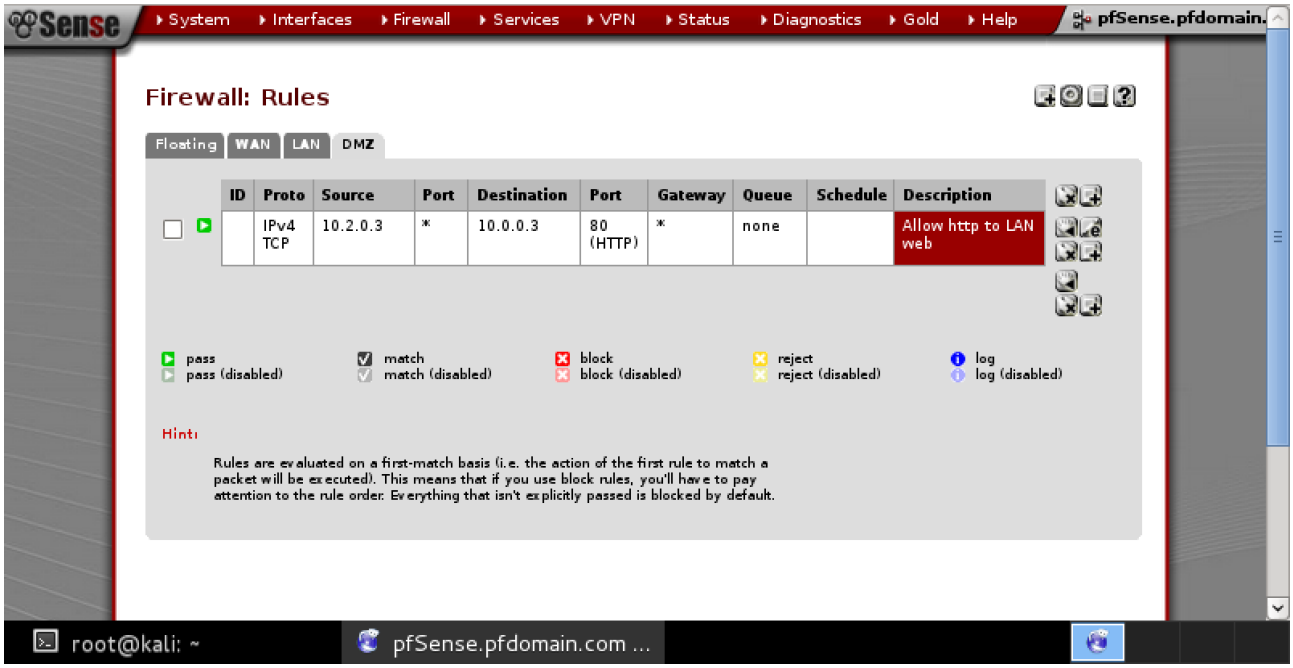
A la création de ces règles, des règles automatiques sont créées sur le WAN :



Il reste ensuite les règles appliquées sur le LAN et la DMZ :



Règles appliquées sur le LAN



Règle appliquée sur la DMZ

Remarquons tout d'abord que la règle placée sur la DMZ, permettant au Cloud de communiquer des données HTTP au service web de la LAN, possède une règle correspondante dans le LAN, permettant à ce dernier de lui renvoyer également les résultats de ses requêtes en HTTP.

La règle de Block sur le LAN, ayant pour but de bloquer une adresse bien précise, illustre que nous pouvons appliquer une liste de Block bien spécifique nous permettant de restreindre l'accès aux sites internet dangereux pour le LAN de Webex. On remarquera, dans la colonne Schedule (emploi du temps), la mise en place d'une « AllowingPause » : nous pouvons en effet désactiver une règle sur des périodes données, à l'exemple d'un cron, ce qui nous permet d'affiner la restriction et ainsi sécuriser le LAN.

3 - Vulnérabilités constatées

Tout d'abord, après avoir effectué un scan Nessus sur l'interface WAN de la pfsense, nous pouvons affirmer que l'entrée extérieure ne présente pas de vulnérabilités. Ceci étant en partie dû au fait qu'aucun service n'est pour l'instant actif derrière le firewall, il est possible que nous constations des évolutions dans les configurations prochaines. Cependant nous pouvons affirmer que le firewall lui-même ne présente pas de vulnérabilité.

Pourtant, en nous intéressant aux derniers patchs de pfSense (source : https://blog.pfsense.org/?p=1661), nous remarquons qu'il continue d'existe sur cette distribution des vulnérabilités, à savoir un Integer overflow dans le protocole IGMP utilisé par pfSense, ou encore de multiples failles XSS dans l'UI. On dénote également des failles dues directement à OpenSSL...

Par ailleurs, listons quelques services principaux actifs sur notre Debian 7 présente dans la DMZ : Apache, vsftpd, OpenVPN.

Le second service possède une Backdoor Command Execution, comme en témoigne le lien suivant : http://fr.1337day.com/exploit/description/16466. Il nous est particulièrement compliqué de nous en prémunir même si l'exploitation de cette faille semble particulièrement rare et complexe.

La faille récente 'HeartBleed', qui consiste pour un attaquant à lire la mémoire d'un serveur ou d'un client afin de récupérer par exemple les clés privées utilisées lors de l'échange, à également été repérée récemment sur OpenVPN mais à bien été patchée et nous avons pu garder notre service à jour grâce au lien suivant : https://openvpn.net/index.php/access-server/heartbleed.html.

Finalement, nous pourrons dans les douze prochaines heures affirmer si nos machines sont vulnérables aux différentes vulnérabilités Shellshock, grâce à la simple ligne de commande trouvée sur le site suivant : https://shellshocker.net/.

4 - Stockage des données

Comme nous pouvons le voir sur le schéma présenté plus haut, le stockage des données va s'effectuer au niveau de la LAN, directement sur le serveur Zentyal. Une taille maximale à été définie via Apache afin qu'un utilisateur ne puisse pas uploader un fichier d'une taille supérieure à 1Mo sur le Cloud.

Une sécurité supplémentaire est mise en place au niveau du serveur Zentyal pour vérifier qu'un utilisateur ne prend pas plus de place qu'il ne peut en posséder. Ainsi, s'il cherche à uploader de nouveau fichiers alors que son Cloud est déjà rempli, il devra d'abord procéder à un nettoyage de ses données actuelles afin de se libérer de la place dans la zone de stockage. Cette limite sera fixée à 2Go dans un premier temps, et pourra être augmentée si nous constatons que les utilisateurs nécessitent plus d'espace de stockage.

Dans le cadre d'une installation non virtuelle, c'est-à-dire avec différents serveurs physiques comme proposé dans le « Choix du matériel réseau », nous utiliserions le serveur suivant

Serveur	**Dell PowerEdge T320**
Processeur	Intel Xeon E5-2420
Mémoire	8Go
Disque dur	1To *(extensible sur 4 fiches SATA 3,5")*
Garantie	Garantie support pro. 3 ans
Prix	**2027€**

Serveur de Stockage Dell PowerEdgeT320 configurable

Après un calcul rapide on voit qu'à l'utilisation de ce serveur, et considérant que l'on laisse 2Go de stockage par utilisateur, cela nous donne 4000 utilisateurs. C'est un chiffre correct en terme de sécurité au niveau stockage, et nous pouvons facilement augmenter l'espace de stockage par utilisateur à 5Go, ce qui nous laisserait 800 utilisateurs.