Mathieu BOISNARD
Valentin FRIES
Vincent MILANO

ENOVATIVE keys

école supérieure de génie informatique

Choix du matériel réseau

1. LAN

1.1 SAN

Serveur	**Synology RackStation RS2414RP+**
Processeur	Intel Atom D2700
Mémoire	2Go *extensible 4Go*
Disque dur	*12 baies, jusqu'à 24 avec unité d'expansion.* *Pris en charge :* *HDD 3.5" SATA III/II* *HDD 2.5" SATA III/II* *SSD 2.5" SATA III/II* *Remplaçables à chaud*
Garantie	Garantie 3 ans
Prix	**2125€**

Le serveur de stockage doit permettre la mise en place aisé d'un RAID5 sur une grande capacité de stockage. Ainsi nous avons fait le choix d'un NAS Synology, permettant une gestion simple et efficace des disques et volumes ainsi que des dossiers partagés.

1.2 Serveur Web

Serveur	**IBM System x3500 M4**
Processeur	Intel Xeon E5-2603
Mémoire	4Go *extensible 384Go*
Disque dur	500Go *extensible 32To* *Remplaçable à chaud*
Garantie	Garantie 3 ans sur site
Prix	**1445€**

Ce serveur dispose d'un bon processeur pouvant accueillir de nombreux clients connectés simultanément ; d'une mémoire moyenne (4Go sont suffisants pour faire tourner un serveur Apache) mais pouvant être augmentée jusqu'à 96fois, d'un espace de stockage de base de 500Go pouvant eux aussi être étendus jusqu'à 32To, ainsi que d'une garantie IBM de 3 ans sur site. Pour

un prix de 1445€, ce serveur semble le compromis parfait pour la configuration Webex : une configuration de base standard, mais pouvant être améliorée au fil du temps en fonction de l'utilisation faite de la machine.

1.3 Serveur de messagerie

Serveur	**HP ProLiant ML350e Gen 8**
Processeur	Intel Xeon E5-2403
Mémoire	2Go *extensible 8Go*
Disque dur	500Go
Garantie	Remplacement : 3 ans Intervention : 1 an
Prix	**957€**

Le serveur de messagerie sera chargé de faire tourner un logiciel de discussion interne à l'entreprise ou un Webmail. Disposant d'un processeur pouvant prendre en charge la connexion de nombreux clients ainsi que de 2Go de RAM (ce qui est largement suffisant pour faire fonctionner un logiciel de messagerie), il est par ailleurs équipé de 500Go de stockage – utiles pour l'enregistrement des logs de discussion ou des e-mails reçus. La mémoire est extensible jusqu'à 8Go. Fourni avec une garantie de remplacement sur 3 ans le tout pour 957€, ce serveur de messagerie saura répondre aux attentes de Webex.

14 Serveur d'applications

Serveur	**IBM System x3630 M4**
Processeur	Intel Xeon E5-2400
Mémoire	16Go *extensible 384Go*
Disque dur	1To *extensible 32To*
Garantie	Garantie 3 ans sur site
Prix	**2964€**

Sur le serveur d'applications devront être installées toutes les applications qui seront atteintes depuis les différents postes de l'entreprise par le réseau. Le processeur Intel Xeon E5 de ce serveur IBM System x3630 M4 lui permettra de prendre en charge les requêtes de lancement d'applications des différents clients. Équipé de 16Go de mémoire extensibles jusqu'à 384Go, il ne devrait pas souffrir d'un trop grand nombre de programmes exécutés simultanément. Son stockage de base de 1To peut être également étendu à 32To, pouvant ainsi héberger de nombreuses applications réseaux.

1.5 Serveur DNS/DHCP

Serveur	**Dell PowerEdge R810**
Processeur	Intel Xeon E7-2830
Mémoire	8Go *extensible 1Go*
Disque dur	500Go *extensible 6To*
Garantie	Dell full support, services & advices 3 ans
Prix	**5995€**

Le serveur DNS devra gérer les tentatives de connexion à un nom de domaine donné, l'analyser et renvoyer la connexion du client vers l'adresse IP correspondante, tout cela dans le laps de temps le plus court possible. Avec son processeur ultra- performant, sa mémoire et sa capacité de stockage extensible, ce Dell PowerEdge R810 pourra traiter en un temps record les requêtes des clients et mettre en cache les associations DNS/IP pour encore améliorer son temps de traitement.

1.6 Serveur de stockage

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€**

Le serveur de stockage sera chargé d'héberger les contenus partagés sur le réseau, aussi avons-nous orienté notre choix vers le Dell PowerEdge T320 pour remplir ce rôle. Son processeur Intel Xeon E5 sera suffisant pour gérer un grand nombre d'accès aux répertoires partagés, il dispose également de 8Go de mémoire lui permettant de mettre en cache lors des copies distantes ou des écritures de fichiers sur ses disques. Il est de plus équipé des 4 fiches SATA 3,5'' accompagnées de base par un DD de 1To.

1.7 Serveur de base de données

Serveur	**IBM System x3300 M4**
Processeur	Intel Xeon E5-2420
Mémoire	8Go *extensible 192Go*
Disque dur	500Go *extensible 8To* *Remplaçable à chaud*
Garantie	Garantie 3 ans sur site
Prix	**1759€**

Equipé d'un processeur Intel Xeon E5 ce serveur sera également en mesure de traiter de nombreuses requête simultanément. Disposant également de 8Go de RAM – bien plus qu'il n'en faut pour faire tourner MySQL ou SQL Server – et de 500Go de stockage – les deux extensibles – ce serveur proposera lui aussi une grand adaptabilité dans son fonctionnement et son évolution en fonction des besoins.

1.8 Serveur proxy

Serveur	**HP ProLiant ML350e Gen 8**
Processeur	Intel Xeon E5-2403
Mémoire	2Go *extensible 8Go*
Disque dur	500Go
Garantie	Remplacement : 3 ans Intervention : 1 an
Prix	**957€**

Le serveur Proxy servira d'intermédiaire entre les postes clients et Internet, filtrant les requêtes sortantes du réseau LAN et mettant en cache les sites atteints de manière à accélérer l'accès aux ressources déjà consultées. À cette fin, nous avons choisi un serveur HP simple.

2. DMZ

2.1 Serveur Web

Serveur	**IBM System x3500 M4**
Processeur	Intel Xeon E5-2603
Mémoire	4Go *extensible 384Go*
Disque dur	500Go *extensible 32To* *Remplaçable à chaud*
Garantie	Garantie 3 ans sur site
Prix	**1445€**

Nous conseillons d'utiliser ici le même serveur web que pour le LAN étant donné que ses caractéristiques très adaptables peuvent être configurées pour répondre aux besoins spécifiques de la DMZ.

2.2 Serveur FTP

Serveur	**IBM System x3500 M4**
Processeur	Intel Xeon E5-2603
Mémoire	4Go *extensible 384Go*
Disque dur	500Go *extensible 32To* *Remplaçable à chaud*
Garantie	Garantie 3 ans sur site
Prix	**1445€**

Le serveur Web et le serveur FTP allant souvent de paire, et aux vues de l'adaptabilité de cette machine, il serait possible de faire cohabiter les deux sur un seul serveur quitte à y ajouter dès son acquisition de la mémoire RAM et quelques To de stockage.

3. Connectivité

3.1 Routeur

Cisco ASA 5506-K9

- Routeur de sécurité avec protection avancée contre les menaces système et les malwares, filtrage d'URL, et gestion du nouveau mode IPS (NGIPS)
- Petit format pour une installation et intégration en toute simplicité
- Fonctions VPN avancées
- 8 ports Gigabit LAN + 1 port Gigabit LAN management
- Prise en charge du Wi-Fi AC
- Système de cryptage : 3DES/AES

Avec son pare-feu et son service VPN intégrés, le routeur Cisco ASA 5506-K9 correspond parfaitement aux besoins de l'entreprise Webex. Il intègre également un mode IPS et des fonctions VPN avancées, à un coût plus abordable de 699,95€.

3.2 Switchs

Switch	**Netgear ProSafe JGS524**
Ports	24 ports
Protocoles	Ethernet/Fast ethernet/Gigabit ethernet
Vitesse	10/100/1000 Mbps
Garantie	Garantie à vie
Prix	**185,26€**

Ce switch 24 ports est le parfait compromis performance/prix : prenant en charge les trois grand protocoles internet aujourd'hui en fonctionnement, il propose de plus un choix de trois vitesses de transfert. Il est livré pour le prix de 185,26€ l'unité avec une garantie à vie.

Choix des logiciels de l'architecture

1. Zentyal

Zentyal est un serveur de réseau unifié particulièrement destiné aux petites et moyennes entreprises. Il est utilisé principalement pour gérer l'infrastructure réseau mais peut également servir de passerelle internet ou de serveur de communications. Ses fonctions comprennent pare-feu et routage, NAT, DNS, DHCP, Proxy, Serveur mail, de fichiers, internet, VoIP... Et est donc ainsi un compromis parfait à la nécessité de Webex en termes réseau. Ce serveur pourra remplir un grand nombre des fonctionnalités principales des zones DMZ et LAN, et ce tout en même temps, ce qui permet une centralisation (unification) et donc de nombreux avantages techniques et autres.

2. Squid

Un serveur Squid est un serveur mandataire (proxy), capable d'utiliser les protocoles FTP, HTTP et HTTPS. Squid gère toutes les requêtes en un seul processus d'entrée/sortie non bloquant, ce qui fait sa particularité. Squid est un logiciel libre distribué sous licence GNU GPL. Son installation se fait de manière classique : installation du package puis définition des réseaux clients et ACL d'accès HTTP. Squid répond aux attentes technologiques sécuritaires logicielles de Webex grâce à son avancée et sa malléabilité qui permettront l'installation d'un proxy efficace.

3. pfSense

pfSense est un routeur / pare-feu opensource basé sur FreeBSD (système d'exploitation UNIX libre). Il peut être installé aussi bien sur un ordinateur de bureau que sur un serveur. PfSense est réputé pour sa fiabilité, ce qui fait de lui la technologie idéale pour permettre à Webex de bénéficier de firewalls efficaces. Une fois installé en mode console pfSense s'administre simplement depuis un panel Web, ce qui se montrera extrêmement pratique dans la maintenance du système réseau. Tout comme Zentyal, pfSense gère les VLAN. PfSense dispose notamment d'autres fonctionnalités, tout comme la possibilité d'installer un VPN (IPSec, OpenVPN ou PPTP).

4. Snort_inline

Snort_inline est un IPS (Intrusion Prevention System – Système de Prévention d'Intrusion), version améliorée de Snort, qui est un IDS (Système de Détection d'Intrusion). Contrairement à Snort qui se base sur la librairie pcap (libpcap), Snort_inline se sert des iptables (et de la libnetfilterqueue). Snort_inline est donc une solution capable de bloquer les intrusions/attaques réseau, nécessaire à la sécurité de Webex.

Audit réseau

L'installation de ce réseau à été prévue spécifiquement pour répondre aux besoins de l'interface client/employé, comme nous allons le détailler ci-dessous.

Une DMZ contient le serveur qui se chargera d'accueillir le Cloud. Celle-ci est uniquement accessible depuis internet ou depuis une unique machine sur le LAN (qui y a accès à des fins de maintenance, mise à jour...) dont l'adresse est 10.0.0.8/16.

Cette zone contient également un serveur Postfix utilisé comme relais SMTP afin de permettre une communication par mail entre le client et les employés. Bien que les employés situés dans le LAN n'aient pas accès à l'intérieur de la DMZ, il est intéressant de préciser que les fichiers envoyés au WebService situé dans le LAN depuis le Cloud seront stockés sur le Synology placé dans le LAN.

La zone LAN, beaucoup plus large, voit l'accueil de plus de 240 machines, qui se voient distribuer une adresse IP entre 10.0.0.10/16 et 10.0.0.253/16. Comme précisé précédemment, une machine statique placée en 10.0.0.8/16 permet à un administrateur d'avoir accès à l'intérieur de la DMZ directement dans le LAN. C'est la seule machine qui possède un accès DMZ.

En entrée du LAN nous avons donc une machine Zentyal, dont le détail technique est fait ci-dessous, et le DHCP pfSense distribue aux machines internes du LAN une adresse sur la bonne plage. Une configuration à été préparée en amont sur les pfSense afin de systématiquement distribuer la même adresse IP à certaines adresses MAC. Ainsi le serveur Zentyal est en 10.0.0.4, le Synology en 10.0.0.6 et l'utilisateur gérant la DMZ en 10.0.0.8/16.

Un Synology à été installé dans le but de stocker efficacement les données clients : un RAID5 à été mis en place afin de garantir la sécurité des données enregistrées.

Dans le LAN, l'accès des clients à internet est filtré par l'utilisation de Squid comme proxy sur notre système de firewalling. Squid est configuré afin de limiter l'accès aux sites violents, à contenu adulte ou encore traitant de drogues ou de paris. Cette configuration peut être changée selon les besoins de l'entreprise.

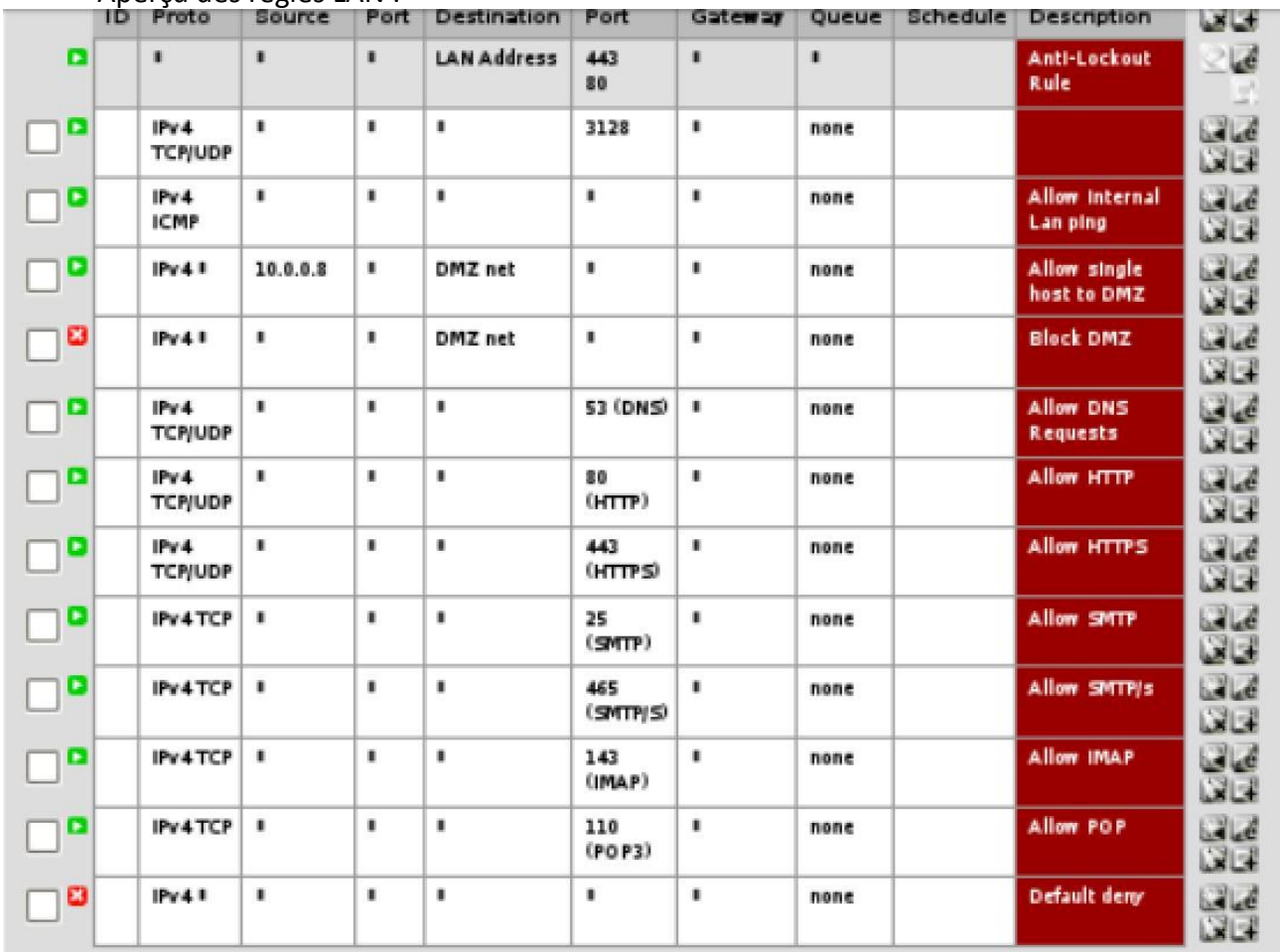
Enfin il nous faut détailler l'interface de firewalling, qui est le cœur de l'architecture réseau proposée. Une redondance à été mise en place au niveau du firewall pfSense via CARP, via l'import de la configuration de la pfSense maître sur la pfSense esclave. Ainsi, il faut se représenter le deuxième niveau de routeurs (au centre gauche du schéma) comme représentant simplement des IP virtuelles, sur lesquelles communiquent le LAN et la DMZ. Tout l'adressage LAN est en 10.0.0.*, avec la pfSense maître en .1, l'esclave en .2 et l'IP virtuelle en .254. Le principe est le même pour la DMZ, dont l'adressage est en 10.2.0.*. Les deux firewalls communiquent sur une carte réseau à part entière. Lorsque la maître, située en 12.0.0.1, devient incapable d'assurer le service, l'esclave située en 12.0.0.254 reprend le service avec exactement les mêmes configurations des services que sur la pfSense précédente.

Afin de compléter ce système de firewalling, Snort à été installé puis placé en mode IPS afin de prévenir d'éventuelles intrusions (voir détail Snort). Squid, accompagné de Squid3 et Squidguard ont également été rajoutés comme précisé précédemment lors de l'explication LAN, afin de contrôler toutes les sorties des machines de cette dernière zone vers le web.

La mise en place d'outils efficaces et de la configuration adaptée de ces outils nous permet d'assurer le bonne fonctionnement du réseau et la sécurité de son intégrité.

Une problématique reste cependant en suspens par rapport à l'accès à la DMZ et l'intégrité du réseau par rapport à cet accès. En effet, comme il n'y à aucune machine physique utilisée dans le réseau interne à la DMZ (si ce n'est celle qui héberge le Cloud), nous avons pu configurer les règles de la DMZ sur notre pfSense de sorte à ce qu'elle ait énormément de droits quant à ses accès au web mais également au LAN. Nous nous sommes donc demandé si cette configuration n'était pas faillible, et il se trouve qu'elle pourrait l'être, dans l'optique où un attaquant, placé sur le Cloud, change la configuration de sa machine afin de faire croire à notre système de firewall qu'il vient du LAN. Ceci pourrait être rendu possible par l'analyse des adresses se connectant au Cloud, et permettrait à un attaquant de se rendre alors à l'intérieur du réseau LAN alors qu'il vient de l'extérieur. Cela pourrait être résolu par la mise en place en réseaux virtuels (VLANs), nous permettant alors de créer deux réseaux virtuels, indiscernables l'un de l'autre. Un attaquant n'aurait alors pas d'accès au LAN.

Aperçu des règles LAN :



	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
		IPv4 TCP/UDP	*	*	*	3128	*	none		
		IPv4 ICMP	*	*	*	*	*	none		Allow Internal Lan ping
		IPv4 *	10.0.0.8	*	DMZ net	*	*	none		Allow single host to DMZ
		IPv4 *	*	*	DMZ net	*	*	none		Block DMZ
		IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		Allow DNS Requests
		IPv4 TCP/UDP	*	*	*	80 (HTTP)	*	none		Allow HTTP
		IPv4 TCP/UDP	*	*	*	443 (HTTPS)	*	none		Allow HTTPS
		IPv4 TCP	*	*	*	25 (SMTP)	*	none		Allow SMTP
		IPv4 TCP	*	*	*	465 (SMTP/S)	*	none		Allow SMTP/s
		IPv4 TCP	*	*	*	143 (IMAP)	*	none		Allow IMAP
		IPv4 TCP	*	*	*	110 (POP3)	*	none		Allow POP
		IPv4 *	*	*	*	*	*	none		Default deny

Exemple de Squid en action :