Volet technique

En réponse à votre appel d'offre, nous détaillons ici les possibilités techniques que nous avons retenues afin de satisfaire au mieux votre demande d'informatisation de la société Fub-Kurcz. Nous avons décidé d'utiliser un ensemble de solutions dont certaines sont payantes et d'autres libres.
L'architecture que nous vous proposons se base sur la virtualisation, qui permet d'utiliser un même serveur physique pour l'installation de plusieurs systèmes d'exploitation et donc d'un grand nombre de services différents. Ce choix permet non seulement de réaliser des économies importantes, mais aussi d'apporter plus de souplesse, d'évolutivité et de sécurité à votre futur SI.
La virtualisation est basée sur des produits propriétaires édités par la société VMware, actuellement leader de ce secteur. L'installation et la configuration de cette solution sont expliquées dans ce document.
En ce qui concerne les systèmes d'exploitation (OS) payants, nous utilisons Microsoft Windows Server 2012 R2 pour la partie serveur, couplé à Windows 10 pour les clients. L'écosystème Microsoft assure une compatibilité élevée avec toutes les applications métiers et les périphériques que vous pourriez être amené à utiliser, et Windows Server 2012 R2 comme Windows 10 sont sur le marché depuis suffisamment longtemps pour que leur fonctionnement ne souffre aujourd'hui d'aucun problème critique.
La partie dite 'libre' donc gratuite des OS est basée sur plusieurs distributions Linux : Debian, Ubuntu, CentOS et FreeBSD. Ici aussi, nous utilisons des versions récentes mais robustes de ces systèmes, reconnues pour leur fiabilité et ne présentant aucun défaut majeur.
Le reste de votre infrastructure reposera notamment sur du matériel du constructeur Cisco pour toute la partie réseau : les commutateurs qui permettent de connecter vos postes de travail et serveurs, les routeurs / pare-feu qui assurent le transit de vos données et leur sécurité contre les attaques externes.
Pour ce qui est de la téléphonie, nous utilisons la VoIP, qui vous permet de passer par votre connexion Internet pour l'ensemble de vos communications téléphoniques internes. Les téléphones sont aussi conçus par Cisco. La VoIP présente plusieurs avantages, dont une réduction des coûts, une augmentation de la flexibilité et une facilité de gestion accrue. Le système est d'autre part 'ouvert' puisqu'il est basé sur le protocole SIP, qui n'est pas propriétaire.
Cette partie introductive n'est en rien exhaustive, vous trouverez tous les détails sur les autres aspects de votre SI dans la suite de ce document.

Contents

1. Infrastructure du réseau Fub-Kurcz

1.1 Généralités

➔ *Voir schéma infrastructure en annexe* **'architecture polfran.pdf'**

Les 3 sites seront reliés entre eux par VPN via le protocole IPSec. Ce sont les pare-feu ASA qui se chargent de cette interconnexion.

Cela permet d'avoir un grand réseau global : à l'utilisation et l'administration, le VPN est quasi transparent tout en assurant une liaison inter-sites très sécurisée. La principale faiblesse de ce mode d'interconnexion est le fait que les sites de France et de Rzeszow dépendent de l'état et de la qualité de la connexion au WAN (internet) pour accéder aux ressources de l'infrastructure. Ceci explique en grande partie pourquoi il y a deux connexions distinctes, provenant de deux fournisseurs d'accès internet (FAI) sur les sites de Krakow et Rzeszow. Nous avons décidé de ne pas mettre de deuxième connexion sur le site de France, qui est moins critique, de par son nombre d'utilisateurs réduit.

Les différents sites de l'infrastructure disposent de plusieurs « zones » :

LAN

La zone LAN contient toute la partie « cliente » de l'infrastructure. C'est-à-dire les postes clients, imprimantes/copieurs et les téléphones IP. Il est intéressant de soumettre cette zone au filtrage des sites web (intranet et extranet) via pfSense.

Depuis cette zone, les machines peuvent atteindre les postes des zones SRV et DMZ.

SRV

La zone SRV contient toute la partie « serveurs et ressources » de l'infrastructure, elle contient donc principalement les serveurs, hyperviseurs et SAN.

Depuis cette zone, les machines peuvent atteindre les machines des zones LAN et DMZ.

DMZ

La zone DMZ, zone démilitarisée, peut être vue comme un sous-réseau de la zone SRV. Elle contient les serveurs devant être accessible depuis internet. Les serveurs de cette zone ne peuvent pas initier de connexions vers les zones LAN et SRV. Ainsi, en cas de compromission d'un des serveurs de la DMZ, l'attaquant n'aura pas accès aux autres zones de l'infrastructure. Pour atteindre cette zone de l'extérieur, il faut mettre en place du NAT statique PAT (Port Address Translation).

Dans notre infrastructure, la DMZ est tout de même accessible de l'intérieur. C'est-à-dire qu'une machine de la zone LAN ou SRV peut atteindre une machine de la DMZ. Le contraire n'est pas possible (et c'est le premier but d'une zone démilitarisée).
Ceci est rendu possible par pfSense, car ce dernier est un pare-feu à états. Pour simplifier, seuls les paquets qui correspondent à une connexion active connue (et donc précédemment autorisés via les règles de filtrage) seront autorisés par le pare-feu.

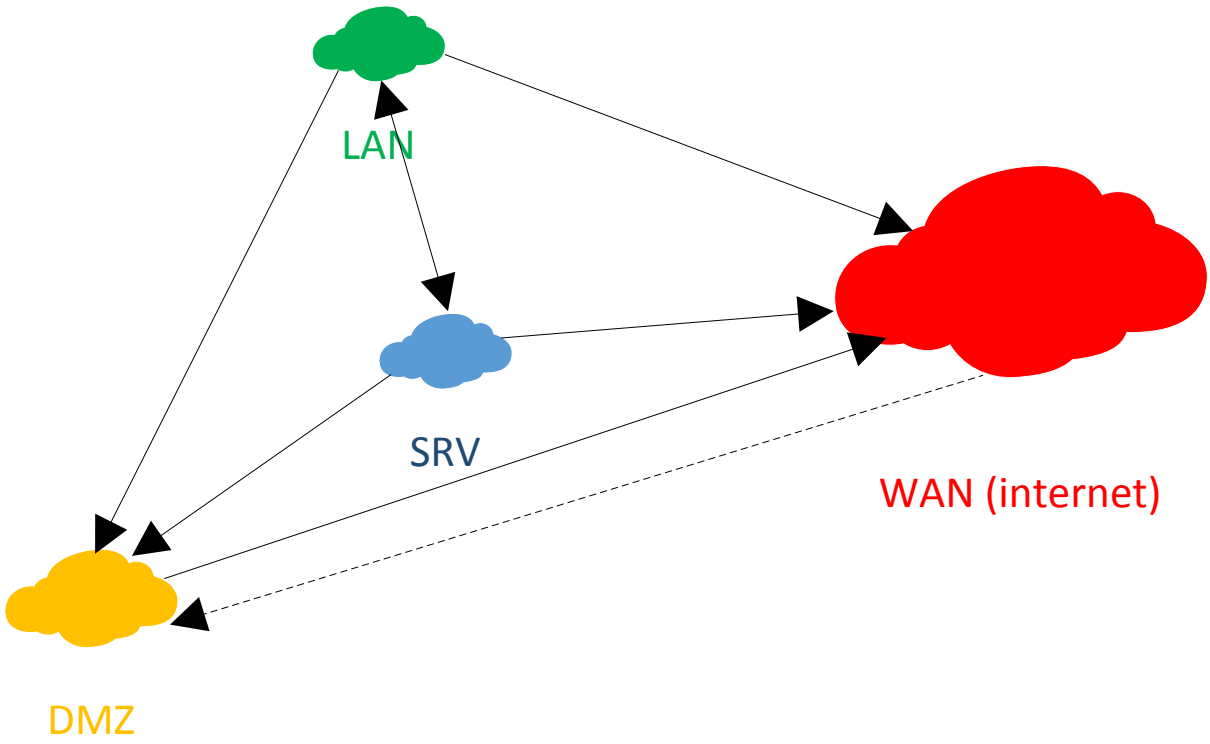


Schéma logique du filtrage du réseau

1.2 Réseaux locaux virtuels (VLANs)

Il existe plusieurs VLAN dans l'infrastructure :
VLAN 10 (VoIP) : Il s'agit du VLAN de la téléphonie VoIP. Ce type de réseau ne supportant pas les grandes latences, nous mettons en place du QoS (Quality of Service) sur les commutateurs afin que les paquets de ce VLAN soit transmis avant ceux des autres VLAN. Il s'agit d'un VLAN de niveau 2 (par adresse MAC). On aurait également pu utiliser un VLAN de niveau 3 (par adresse IP), mais cela demande quelques ajustements, notamment au niveau de la configuration des serveurs DHCP.
VLAN 20 (DMZ) : Il s'agit du VLAN de la zone démilitarisée. Ce VLAN est nécessaire afin de pouvoir séparer le flux de ce VLAN des autres réseaux (et VLAN). Il s'agit d'un VLAN de niveau 1 (par port)
Nous avons aussi la possibilité de créer des VLAN spécifiques à chaque service de l'infrastructure (par ex. : secrétaires, techniciens, responsables etc.) mais nous préférons, pour l'instant, n'utiliser que les

deux VLANs décrits ci-dessus. En effet, nous n'avons pas d'information quant à l'organisation des différents services dans l'appel d'offre et de plus, nous pensons qu'une gestion des droits et accès depuis les ressources réseaux (serveurs, partages etc.) est suffisante.
Les commutateurs s'inter-changeront leurs VLANs via le protocole propriétaire de Cisco : **VTP** (**V**LAN **T**runking **P**rotocol).

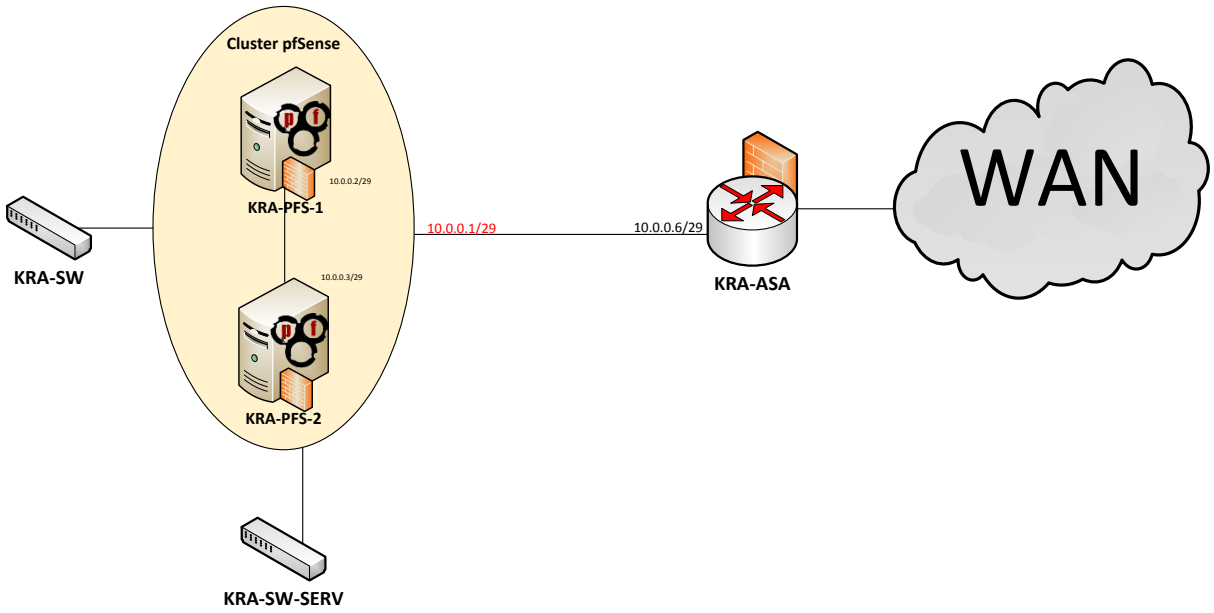
1.3 pfSense

pfSense est un routeur & pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter et assure diverses fonctions comme le routage, le NAT, les VLAN, le filtrage des sites internet etc.

Dans votre infrastructure, il se situe derrière le pare-feu Cisco ASA. Cet emplacement assure un deuxième niveau de sécurité. En effet, en cas d'intrusion dans l'infrastructure par le Cisco ASA (faille de sécurité, mauvais paramétrage etc.), l'intrus sera également confronté à ce pare-feu.

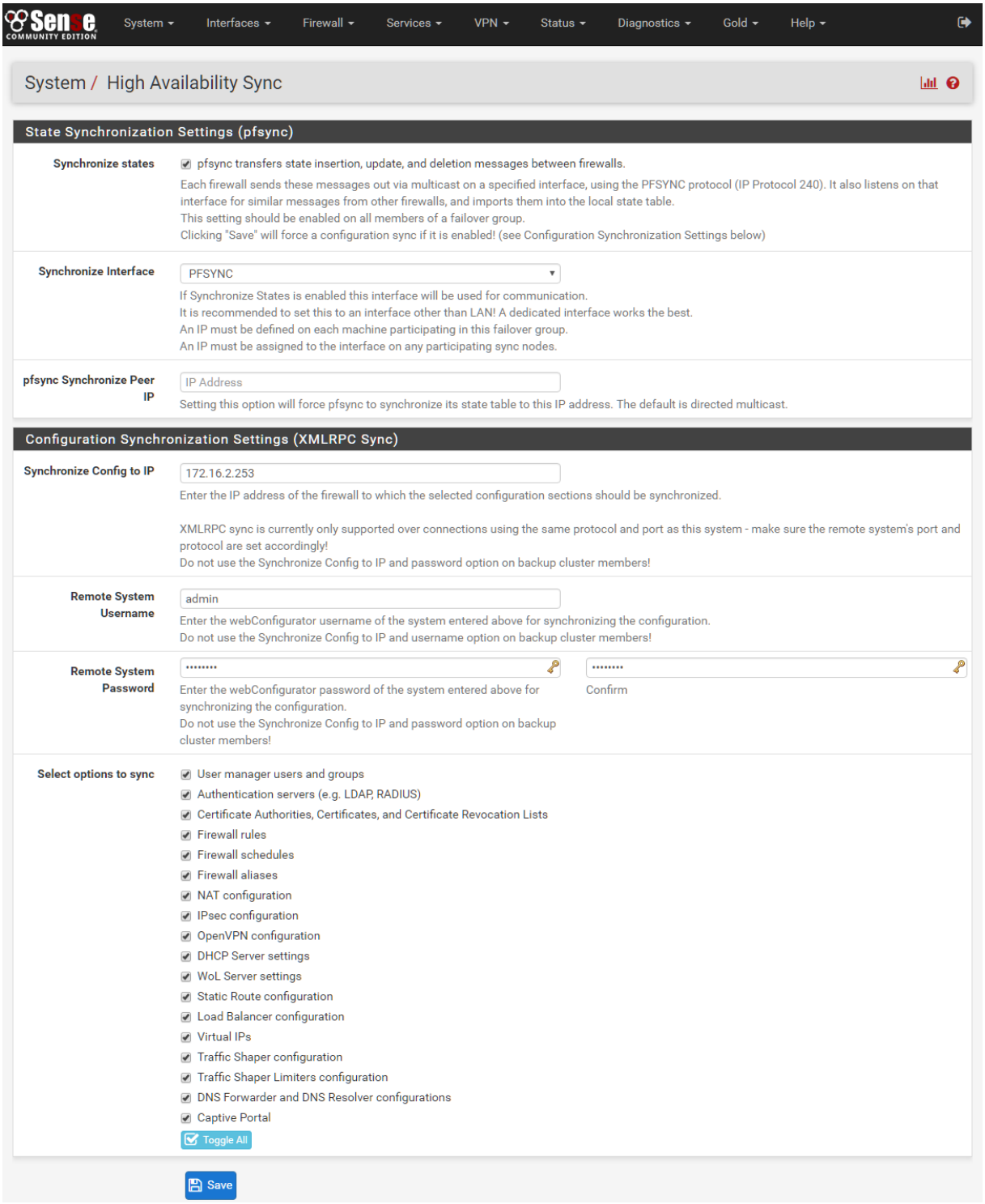
Aussi, afin d'augmenter la résilience de l'ensemble, nous en mettons un deuxième de secours, synchronisé avec le premier, qui prendra le relais en cas de défaillance de ce dernier. Les protocoles CARP et PFSYNC sont entre-autres mis en œuvre pour assurer ces fonctions.

Schéma simplifié du site de Kraków



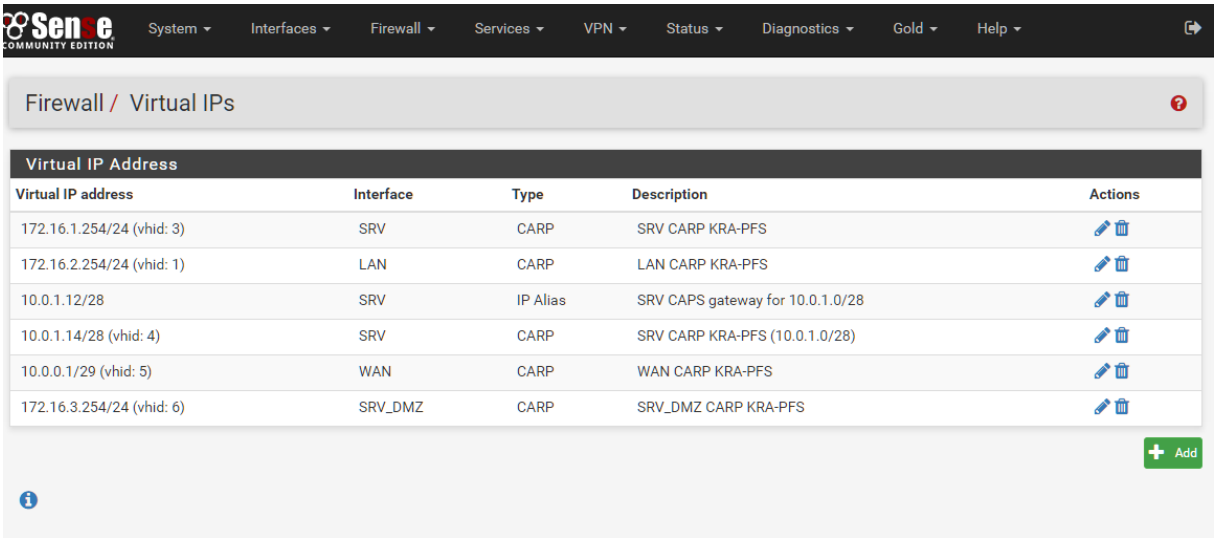
Pour cela, une fois les interfaces réseaux des pfSense correctement affectées et configurées, nous mettons dans un premier temps en place les synchronisations PFSYNC et XMLRPC entre les deux pfSense.

System -> High Avail. Sync



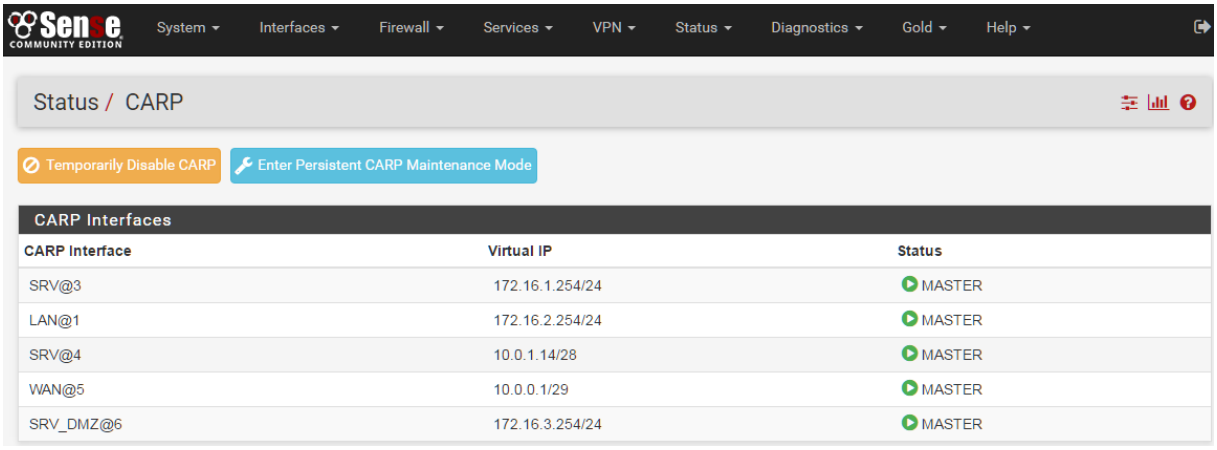
Une fois les synchronisations totalement opérationnelles, nous mettons en place les adresse IP virtuelle CARP.

Firewall –> Virtual IPs

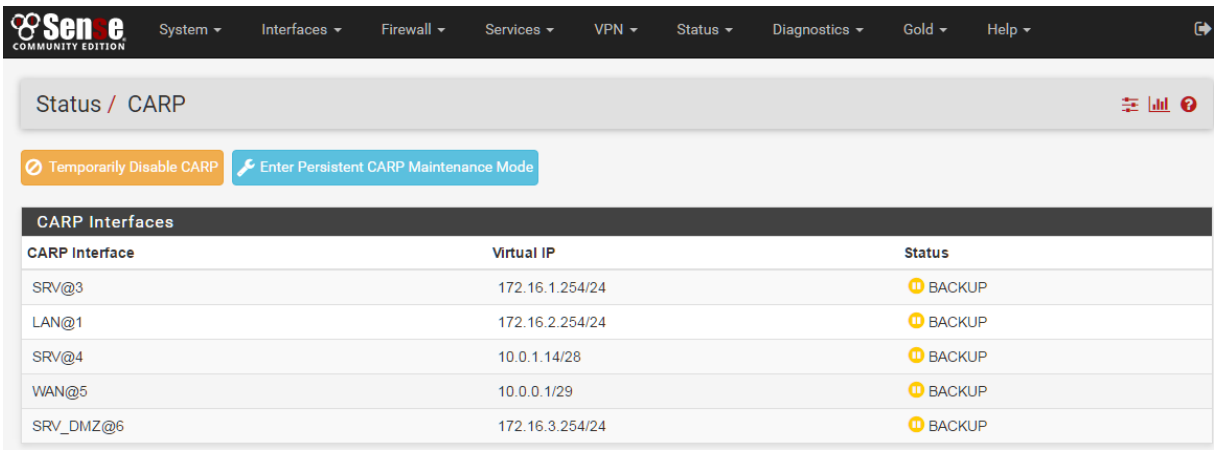


Grâce aux synchronisations, cette étape s'est répliquée sur le deuxième pfSense. Nous pouvons vérifier l'état des adresses IP CARP via le menu **Status** -> **CARP (failover)** sur chacun.

Statut CARP depuis le 1er pfSense



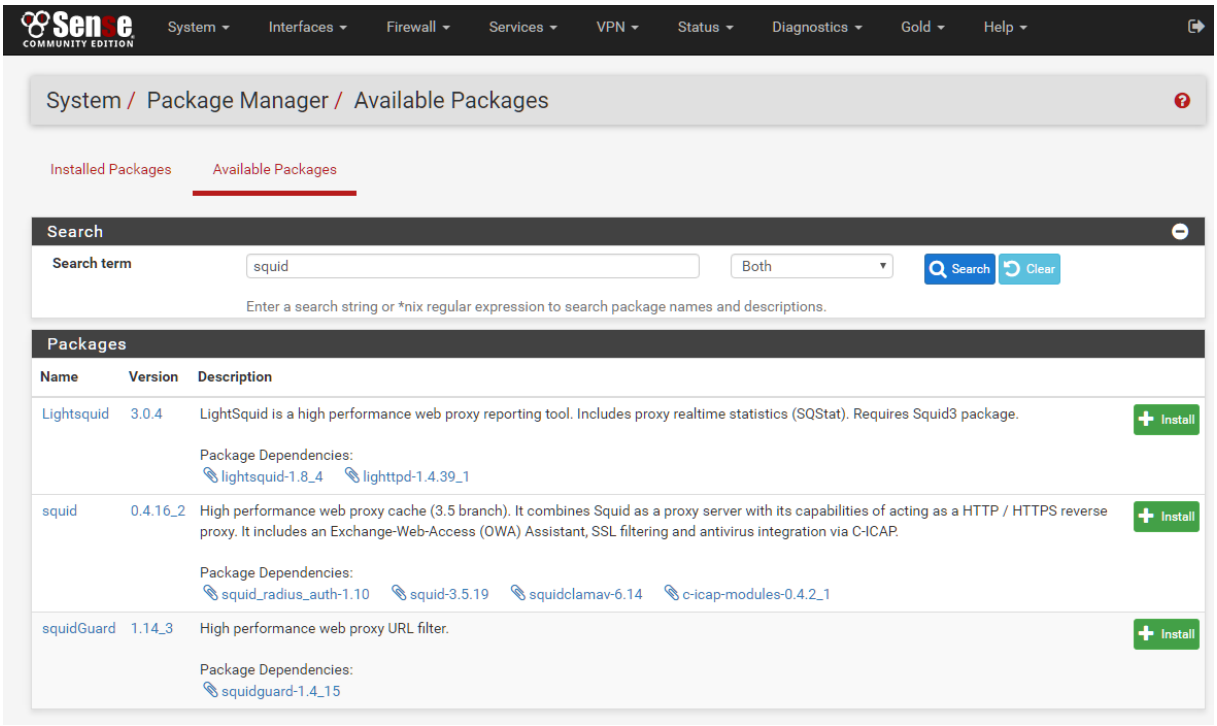
Statut CARP depuis le 2ème pfSense



Ainsi, si le premier pfSense (MASTER) est injoignable, le second pfSense (BACKUP) jouera le rôle MASTER et prendra le relais tant que le pfSense principal est indisponible. Une fois que ce dernier redevient accessible, les rôles sont de nouveau inversés et la situation initiale est automatiquement restaurée.

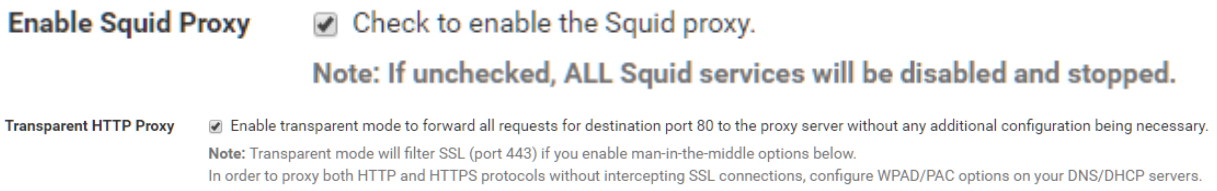
1.4 Filtrage des sites web intranet/extranet

Le filtrage des sites se fait via un serveur Squid par le biais d'un serveur mandataire (proxy). pfSense permet la gestion total de Squid via les packages **squid** et **squidGuard** installables depuis **System** -> **Package Manager** -> **Available Packages**.

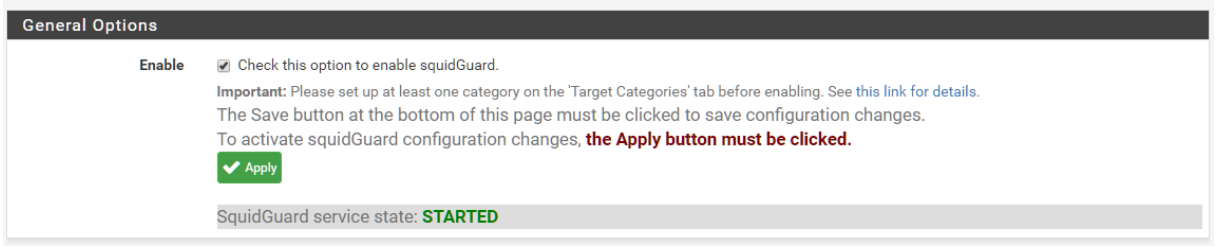


Une fois installés, la configuration de Squid se fait via le menu **Services** -> **Squid Proxy Server**.

Via ce menu, nous activerons le proxy Squid (**Enable Squid Proxy**) en mode transparent (**Transparent HTTP Proxy**) sur l'interface **LAN** de pfSense. Nous laisserons les autres options avec leurs paramètres par défaut.

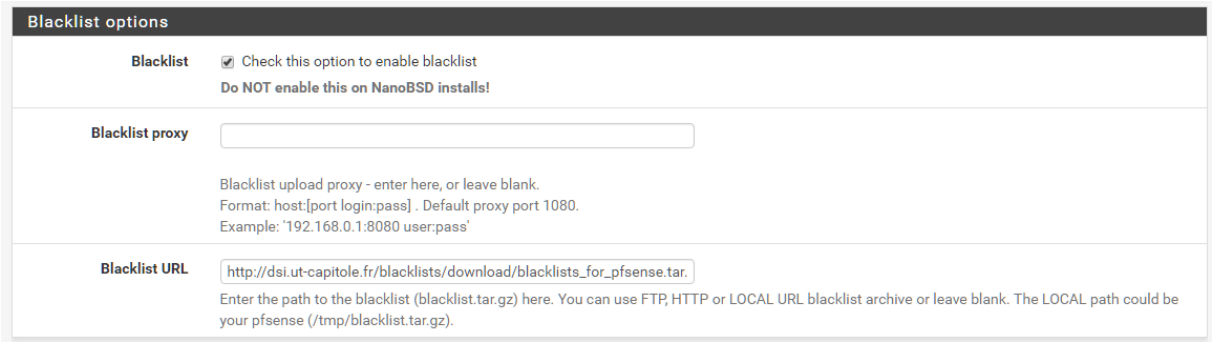


Une fois fait, nous pouvons maintenant utiliser le service **SquidGuare Proxy Filter** en complément de Squid. Pour cela, on se rend dans **Services** -> **SquidGuard Proxy Filter** et l'on active squidGuard.



Une fois ce filtre activé et après avoir démarré le service correspondant, il faut lui indiquer le chemin d'une liste noire (blacklist) à utiliser. Ici, nous utilisons la liste noire de l'Université Toulouse 1 Capitole (https://dsi.ut-capitole.fr/blacklists/) mise à disposition sous contrat *Creative Commons*.

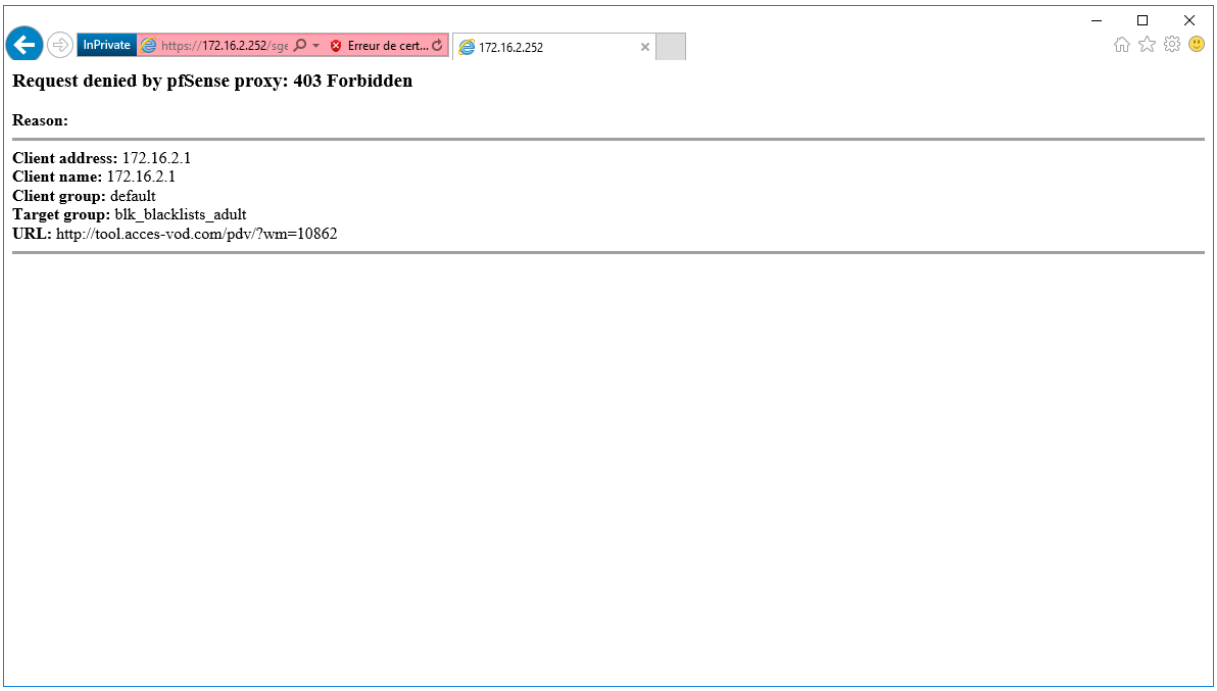
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz



Cette liste contient diverses catégories de sites telles que :

Catégorie	Nombre	Description
adult	1104537	Des sites adultes allant de l'érotique à la pornographie dure.
agressif	358	Quelques sites racistes, antisémites, incitant à la haine.
arjel	69	Sites de pari en ligne certifiés par l ARJEL
associations_religieuses	1	Sites d'associations religieuses
astrology	29	Astrologie
audio-video	3396	Quelques sites orientés vers l'audio et la vidéo.
bank	1697	Banque en ligne
bitcoin	254	Sites de bitcoin
blog	1471	Quelques sites hébergeant des blogs.
celebrity	672	Tout ce qui concerne l actualité dite people
chat	227	Site de dialogue et conversation en ligne.
child	43	Tout ce qui est autorisé pour des enfants
cleaning	173	Sites pour désinfecter et mettre à jour des ordinateurs.
cooking	16	Sites de cuisine
dangerous_material	49	Sites décrivant des moyens de créer du matériel dangereux (explosif, poison, etc.).
dating	3571	Sites de rencontres
ddos	61	Sites de déni de services
dialer	0	Sites de dialer
download	66	Sites qui permettent de télécharger des logiciels
drogue	1055	Drogue.
educational_games	10	Sites de jeux éducatifs
filehosting	833	Sites qui hébergent des contenus (vidéos, images, sons)
financial	80	Informations financières, bourses.
forums	209	Forums.
gambling	1114	Sites de jeux en ligne, casino, etc.
games	11131	Sites de jeux, en ligne, ou de distributions de jeux.
hacking	301	Sites de piratage et d'agressions informatiques.
jobsearch	385	Site pour trouver un emploi
lingerie	69	Sites de lingerie
liste_bu	2782	Une liste très "univ-tlse1.fr" de sites éducatifs pour notre bibliothèque.
malware	27865	Tout site qui injecte des malwares
manga	729	Tout ce qui est lié à l'univers des mangas et de la bande dessinée
marketingware	820	Sites de marketing très spéciaux
mixed_adult	152	Sites qui contiennent des portions adultes non structurés
mobile-phone	46	Sites pour les mobiles (sonneries, etc.).
phishing	63508	Sites de phishing, de pièges bancaires, ou autres.
press	4451	Tout site de presse d'information
publicite	1429	Publicité.
radio	491	Sites de radio sur Internet
reaffected	8	Sites qui ont changé de propriétaire et donc de contenu
redirector	124266	Quelques sites qui permettent de contourner les filtres.
remote-control	42	Site permettant la prise de contrôle à distance
sect	144	Secte
sexual_education	18	Sites qui parlent d éducation sexuelle et qui peuvent être détectés comme pornographiques
shopping	36397	Sites de vente et achat en ligne
shortener	262	Raccoursisseur d'URL
social_networks	636	Tous les sites de réseaux sociaux
sports	2275	Sports
strict_redirector	123985	Comme redirector, mais avec les moteurs de recherche classiques.
strong_redirector	123985	Comme strict_redirector, mais, pour google et autres, on ne bloque que certains termes.
translation	170	Sites de traduction
tricheur	46	Sites qui expliquent comme tricher aux examens.
update	5	Sites d'update
warez	878	Sites distribuant, entre autres, des logiciels ou vidéos pirates.
webmail	341	Webmail que l'on trouve sur internet (hotmail, webmail.univ-tlse1.fr, etc.)

Lorsqu'un utilisateur essayera d'accéder à une catégorie bloquée, une page internet lui expliquera pourquoi l'URL a été bloquée et par quel filtre.



Il est possible de personnaliser cette page, ou encore de créer une redirection vers une autre page.

1.5 Filtrage des flux réseaux

Afin d'accroître la sécurité de l'infrastructure, nous filtrons les paquets IPv4 et IPv6 sortant vers le WAN depuis l'ASA.

Via ce dernier, nous autorisons uniquement les paquets utilisant ces ports à sortir de l'extérieur (WAN) :

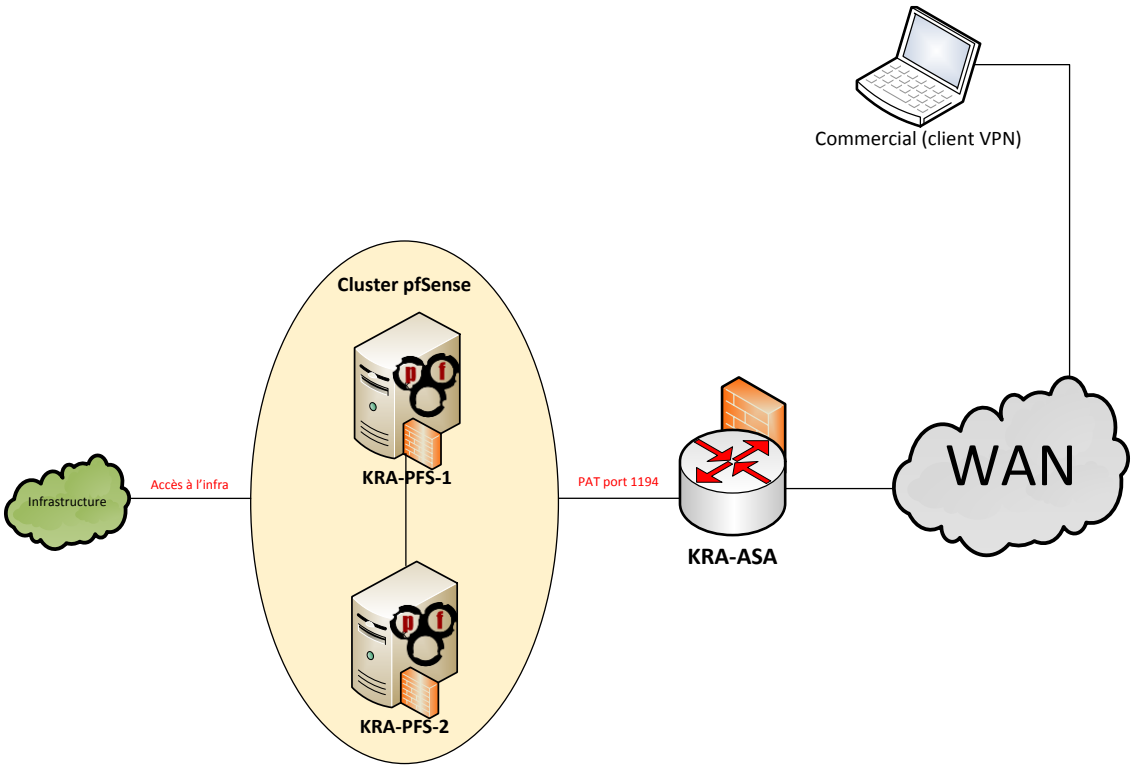
- **TCP 20/21**, pour l'échange de fichiers via FTP
- **TCP 22**, pour l'accès à un shell sécurisé Secure SHell, également utilisé pour l'échange de fichiers sécurisés SFTP
- **TCP 25** & **465**, pour l'envoi d'un courrier électronique via un serveur dédié SMTP
- **UDP 53**, pour la résolution de noms de domaine en adresses IP : DNS
- **TCP 80** & **443**, pour la consultation d'un serveur http(s) par le biais d'un navigateur web
- **TCP 110** & **995**, pour la récupération de son courrier électronique via POP (+SSL)
- **TCP 143** & **993**, pour la récupération de son courrier électronique via IMAP (+SSL)
- **UDP 123** pour la synchronisation de l'horloge : Network Time Protocol (NTP)

L'intérêt de filtrer les paquets sortants de l'infrastructure réside dans le fait que cela ajoute une couche de sécurité, car il est aujourd'hui très difficile pour un « spécialiste » de pénétrer une infrastructure, surtout si comme la vôtre, elle est composée de plusieurs pare-feu 'en chaine'. Par contre, il est tout à fait envisageable qu'un logiciel de type « backdoor », introduit par un tiers en interne, puisse mettre en place une porte dérobée (en réalité, une machine cliente accédant à internet, ouvrant ainsi les ports nécessaires par lesquels le trafic retour serait possible). De plus, cela permet de connaitre précisément la nature des paquets sortants de l'infrastructure, tout en bloquant certains usages tels que le P2P. Pour rappel, vous êtes responsables des attaques initiées depuis votre infrastructure vers l'extérieur.

Bien entendu, tous les paquets entrants du WAN vers l'infrastructure sont par défaut bloqués, sauf cas particuliers (notamment en cas de **NAT/PAT vers la DMZ**).

1.6 Connexion à distance (OpenVPN)

Pour que les commerciaux puissent accéder à l'infrastructure à distance, depuis un hôtel par exemple, nous utilisons un VPN OpenVPN géré par pfSense. Nous aurions aussi pu utiliser le VPN du Cisco ASA, mais après réflexion, il apparait que cela pourrait poser des problèmes de sécurité. Nous préférons passer par le pfSense, car ce dernier permet de gérer finement les règles d'accès et de filtrages de ces clients via une zone « OpenVPN » créé spécifiquement pour eux. Nous mettons ainsi en place du PAT (**P**ort **A**ddress **T**ranslation) depuis l'ASA vers le cluster pfSense.



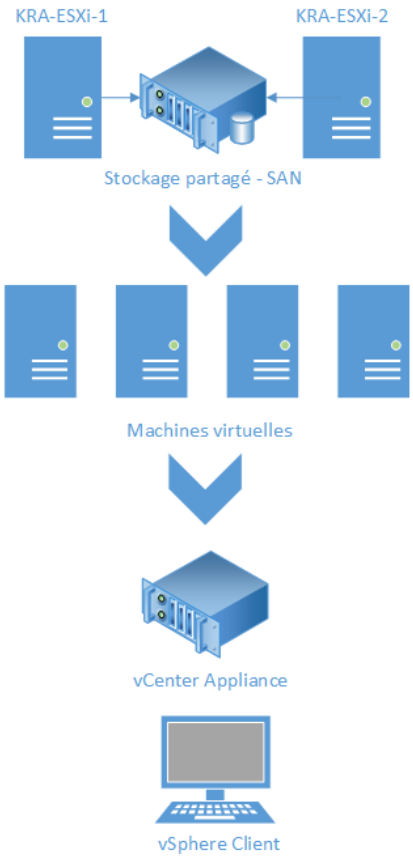
Pour accéder au VPN, le client doit installer le client OpenVPN (disponible sur https://openvpn.net/index.php/open-source/downloads.html) et importer les fichiers de configuration pour la connexion au serveur OpenVPN qu'on lui aura préalablement transmis.
Une fois connecté au VPN, le commercial a accès aux mêmes ressources qu'en interne.
Les clients OpenVPN sont dans le réseau **10.0.1.128/29** , ce qui permet la connexion de 6 clients en même temps. Pour des raisons évidentes de sécurité, chaque client se verra attribuer un certificat SSL, qui lui servira de clé pour se connecter (pas besoin de login/password) au serveur OpenVPN. Un client ne peut se connecter avec sa clé que depuis un PC portable / smartphone à la fois.
Etant donné qu'il n'y a pas de serveurs sur les sites de Rzeszów de France, nous installons le serveur OpenVPN uniquement sur celui de Kraków.

2. Virtualisation

Comme indiqué en introduction, la virtualisation permet une mutualisation des ressources. Un même serveur physique peut donc héberger plusieurs machines virtuelles (VM). Ce mécanisme optimise grandement l'utilisation de la puissance disponible et offre la possibilité d'ajouter rapidement de nouveaux serveurs, donc des services supplémentaires. Son fonctionnement se base sur l'installation d'hyperviseurs dont le rôle sera d'accueillir les VMs, qui se verront attribuer une certaine quantité de ressource : RAM, CPU, Espace disque etc. VMware propose un ensemble d'applications destinées à la virtualisation, dont des hyperviseurs appelés ESXi. L'autre brique la plus importante se nomme vCenter Server. Cette solution, qui prend ici la forme d'une *appliance,* permet de gérer ces hyperviseurs et les VMs qui y seront installées. Concrètement, ce système offre la possibilité de faire transiter les machines d'un serveur à un autre, ce qui permet notamment :

- L'équilibrage de charge entre les serveurs
- La possibilité d'effectuer des opérations de maintenance à chaud
- Une tolérance de panne : en cas de défaillance d'un des serveurs, les VMs sont automatiquement prises en charge pas le second

Cette redondance est un élément clé de la stabilité de votre infrastructure et de la qualité de service que vous pouvez offrir aux utilisateurs de votre SI.



➔ 2 ESXi sont installés sur 2 serveurs physiques distincts

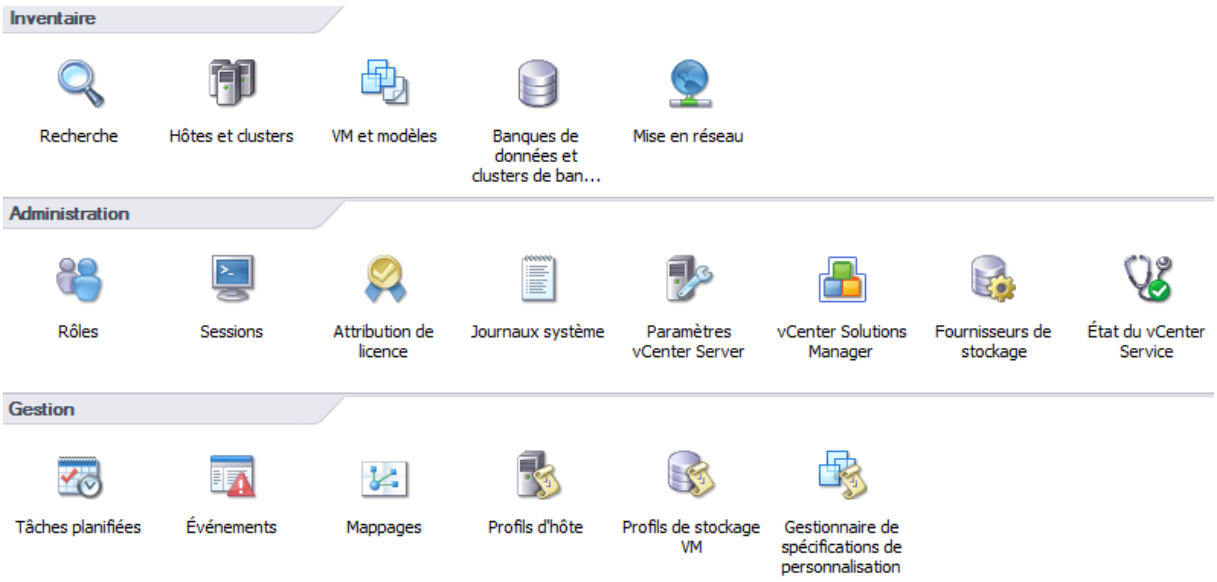
➔ Le stockage se fait via un système centralisé appelé SAN

➔ Vos serveurs virtuels sont ainsi hébergés sur les ESXi

➔ vCenter Server permet de manager les ESXi et VMs associées

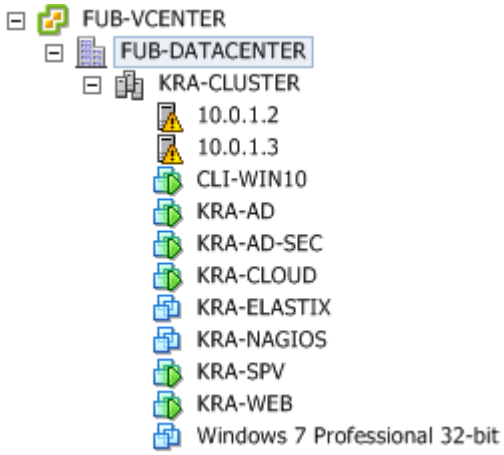
➔ vSphere client permet d'accéder à vCenter pour le piloter

Pour Fub-Kurcz, ces 2 EXSi (version 6) sont installés sur des serveurs rackable Dell, sur votre site principal de Krakow. Ces serveurs sont largement dimensionnés et offre plus que la puissance nécessaire à votre infrastructure actuelle. Le but est bien sûr de garantir l'évolutivité de votre parc, qui se verra adjoindre de nouveaux services au fil du temps. Ces serveurs sont connectés à un commutateur sur le réseau 10.0.1.0 /29 en parallèles du SAN et de l'appliance vCenter. L'ensemble de la configuration est managé via vSphere Client, qui permet de prendre la main sur vCenter et d'avoir une vision globale des VMs de votre infrastructure. Vous pouvez donc effectuer des snapshots de ces machines pour les opérations de maintenances, gérer l'allocation de la puissance disponible, ajouter ou supprimer des serveurs etc.
Une technique appelé HA, pour High Availability, autorise la perte temporaire d'un de vos ESXi : Les VMs associées à cet hôte seront automatiquement déplacé sur le second, le temps de la restauration du premier. Cela est rendu possible par l'utilisation de vMotion, une autre technologie VMware, qui assure la migration des serveurs virtuels à chaud.
La configuration de votre PRA, dont nous parlerons plus loin dans ce document, sera claquée sur ce principe, afin de vous assurer une reprise d'activité rapide en cas d'incident majeur sur le site de Krakow.



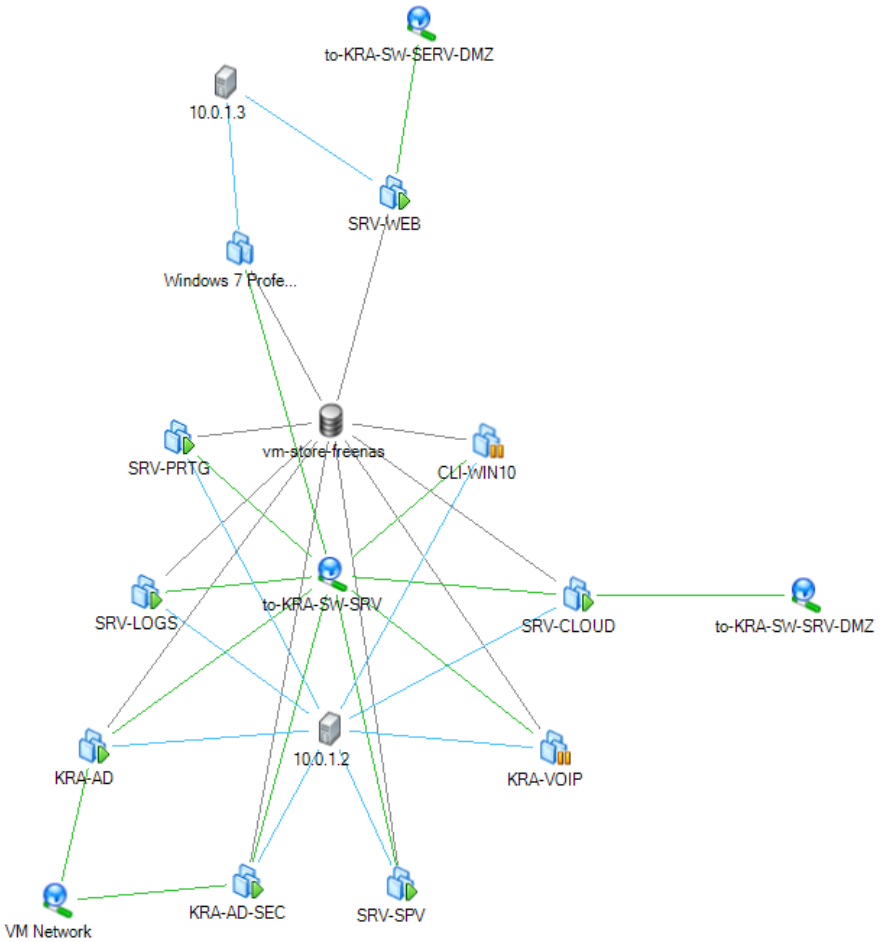
Votre interface d'administration vCenter Server.

Dans un premier temps, les VMs installées sur les ESXi sont les suivantes :



- KRA-AD & KRA-AD-SEC, vos contrôleurs de domaines principal et secondaire
- KRA-CLOUD, un Cloud personnel et libre basé sur Owncloud
- KRA-ELASTIX, votre serveur de VoIP
- SRV-WEB, qui héberge votre site en interne ainsi que le serveur FTP attenant
- SRV-LOGS, pour la gestion des fichiers de logs
- SRV-SPV, qui assure la supervision de votre infrastructure via Centreon
- CLI-WIN7, CLI-WIN10, CLI-Lubuntu, des clients de tests

Nous avons réalisé des *images* de ces serveurs et des OS au format OVF, afin que leur déploiement soit le plus rapide possible. L'idée est de ne pas perdre de temps à réinstaller complètement un système à chaque fois que vous souhaitez ajouter un nouveau serveur. Ces modèles sont donc à votre disposition et seront mis à jour périodiquement.



3. Redondance / Protection

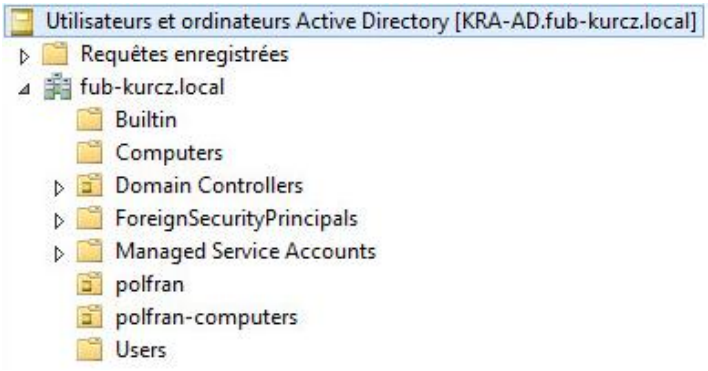
La redondance de l'infrastructure se fait à plusieurs niveaux :

- Comme expliqué plus haut, toutes les VMs installées au sein des ESXi sont protégées par HA / vMotion, et pourront passer d'un serveur physique à un autre en cas de défaillance.
- Ces serveurs sont eux même protégés par des onduleurs, qui assureront leur alimentation pour quelques minutes en cas de coupure de courant. Si celle-ci venait à durer trop longtemps, les serveurs seraient automatiquement éteints pour préserver leur intégrité.
- Vos contrôleurs de domaine KRA-AD & KRA-AD-SEC sont configurés pour la tolérance de panne et l'équilibrage de charge nous y reviendrons plus tard. Un autre contrôleur de domaine (RZE-AD) en lecture seule est installé sur le site de Rzeszow, pour éviter un trafic inutile entre les 2 villes.
- Les pare-feu utilisent le protocole CARP, si l'un tombe, l'autre prend le relais.
- Les serveurs de VoIP sont installés à la fois sur les sites de Krakow et Rzeszow, afin que la téléphonie reste accessible en toutes circonstances.
- Une connexion Internet de secours, utilisant un provider différent, est installée en cas de problème avec le lien principal.
- Vos données sont sauvegardées en Cloud.
- Un PRA, basé sur la réplication de votre infrastructure dans un Datacenter externe, permet la reprise de votre activité, même en cas d'incident majeur.

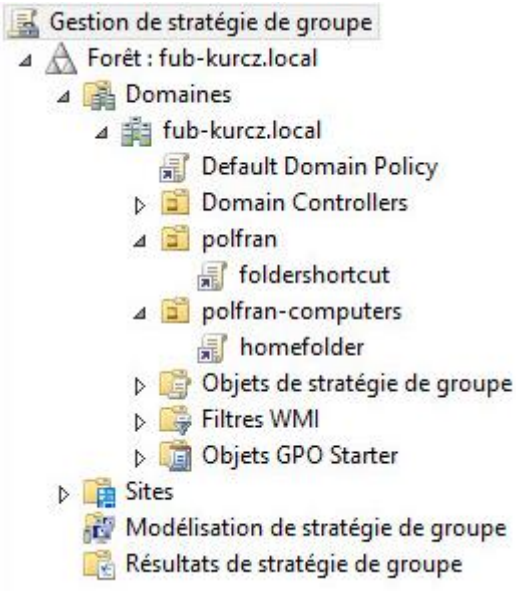
4. Domaine

4.1 Généralités

La mise en domaine du parc avec Active Directory (AD) permet de gérer efficacement vos machines et vos utilisateurs. Active Directory repose sur le protocole LDAP (Lightweight Directory Access Protocol), largement utilisé et compatible avec de nombreux services. Vos postes clients et vos utilisateurs sont donc membres de ce domaine dont voici les principales caractéristiques :



- Nom de domaine local : **fub-kurcz.local**
- Nom de domaine externe : **fub-kurcz.pl**, hébergé une société partenaire de Google, nous y reviendrons plus tard
- Mise en réseau :
    - KRA-AD : 172.16.1.1
    - KRA-AD-SEC : 172.16.1.101
    - RZE-AD : 172.17.1.1
- Utilisation de groupes de sécurité pour réguler l'accès aux données partagées
- Utilisation de GPO, pour l'administration des postes, la gestion des droits etc.



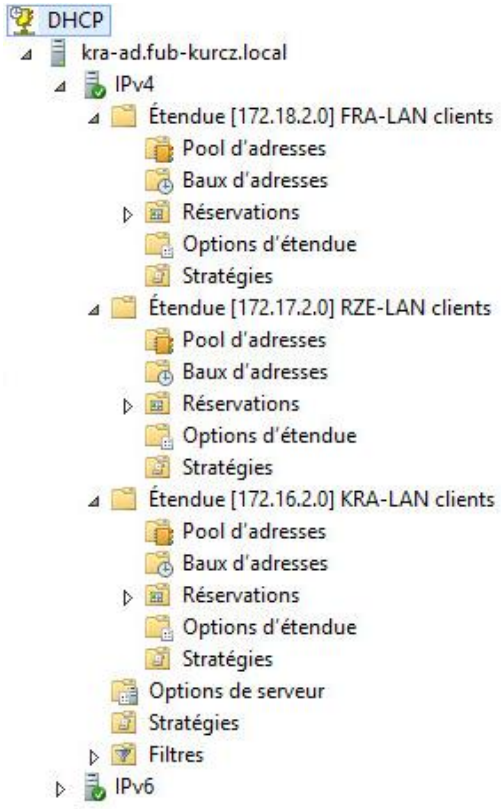
4.2 Contrôleurs de domaine : KRA-AD & KRA-AD-SEC

Dans cette partie, nous décrivons le fonctionnement de ces serveurs et les principaux rôles qu'ils prennent en charge.

KRA-AD est le PDC (Principal Domain Controler), il est totalement synchronisé avec KRA-AD-SEC. Ces 2 serveurs sont accessibles en lecture / écriture, les modifications touchant à l'AD, aux GPO et aux autres services généraux peuvent donc être effectuées sur l'un ou l'autre sans distinction. Cette synchronisation, bien que rapide, peut ne pas être immédiate dans certains cas, ce qui pourrait entrainer quelques secondes de latence entre les changements que vous apportez et leur réplication.

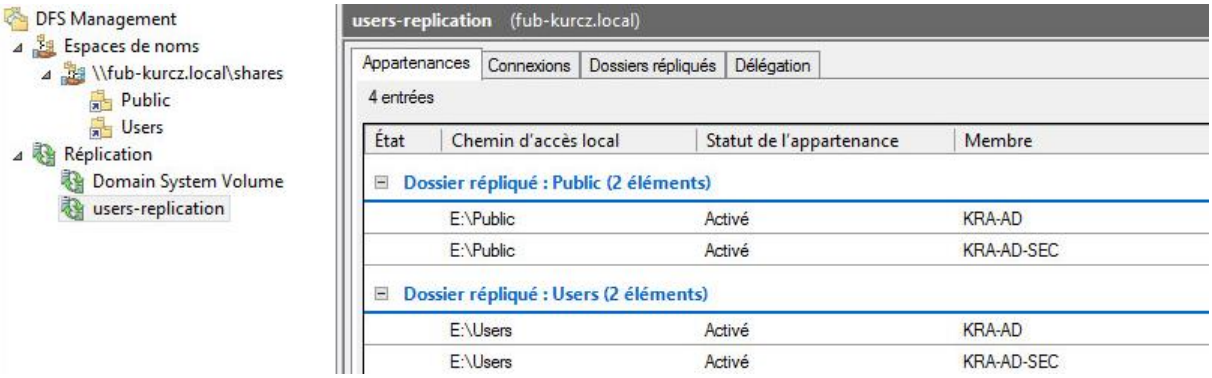
Voici la liste et la fonction des rôles de ces serveurs :

- **Active Directory** : pour la gestion du domaine (service d'annuaire)
- **DNS** : (obligatoire dans le cas d'un contrôleur de domaine), pour la résolution des noms des postes, périphériques et sites web. A noter que toutes nouvelles machines Windows qui adhèrent au domaine est automatiquement ajouté dans la liste des hôtes du DNS. Ce principe ne s'applique pas aux serveurs/clients Linux dont il faut renseigner le nom manuellement dans le DNS afin qu'ils soient correctement répertoriés. Vos postes clients utiliseront KRA-AD en DNS primaire et KRA-AD-SEC en DNS secondaire sur le site de Krakow. A Rzeszow, RZE-AD fera office de DNS primaire.
- **DHCP** : pour la distribution des adresses IP dans votre parc. Ce service permet de gagner un temps considérable puisqu'il évite d'avoir à configurer chaque périphérique manuellement.



D'autre part les erreurs humaines inhérentes à ce type de manipulation sont également impossibles. Un processus appelé *basculement* permet à KRA-AD et KRA-AD-SEC de se répartir la distribution des IP sur votre réseau. Encore une fois, lors d'une opération de maintenance qui nécessiterait l'extinction / le redémarrage de votre serveur, ou s'il venait à subir une défaillance, la continuité de l'activité serait assurée.

- **Serveur de fichiers / DFS :** Le rôle de serveur de fichiers permet la centralisation et le partage de vos données pour qu'elles soient accessibles à tous les utilisateurs, sous réserve qu'ils possèdent les autorisations nécessaires. *Distributed File System* est un système de fichiers distribués. Grace à cette fonctionnalité, il est possible de créer des espaces de noms virtuels qui pointeront sur plusieurs serveurs simultanément.
  Votre espace de nom est accessible via : **\\fub-kurcz.local\shares**
  Les données qui y seront stockées sont répliquées sur les 3 contrôleurs de domaine. Cette répartition assure un accès aux données rapide et fiable quelles que soient les conditions ou le site concerné.



Espace de nom DFS pointant vers KRA-AD et KRA-AD-SEC. La réplication synchronise les fichiers créés, modifiés, supprimés entre les serveurs.

4.3 Utilisateurs, groupes et postes de travail

- **Utilisateurs** :

Vos utilisateurs sont regroupés dans l'AD dans des OU (Unités d'organisation) découpées en services. Elles vous permettent de gérer plus finalement (via GPO) les droits accordés à chacun sur son poste de travail et d'avoir un annuaire lisible et complet à disposition.

- **Login** :

Voici quelques informations concernant la gestion des connexions de vos utilisateurs sur les postes du domaine :

- L'utilisateur renseigne son login et son mot de passe
- Une GPO créée automatiquement son répertoire personnel sur l'espace de nom DFS \\fub-kurcz.local\shares\users. Ce répertoire est mappé à chaque ouverture de session sur le lecteur P : et c'est donc cet espace qui devra être utilisé pour le stockage des documents, afin qu'ils soient pris en compte dans la sauvegarde. Les emplacements locaux, tels que le *Bureau*, le répertoires *Mes Documents* etc. ne sont pas sauvegardés. Ce système simple et efficace évite d'avoir à utiliser une redirection de ces différents répertoires vers les serveurs de fichiers.
- Un raccourci vers P : est automatiquement ajouté sur le bureau
- Le dossier partagé *Public* est également mappé sur le lecteur Z :
- Les autres partages à ajouter seront créés au fil du temps et de vos besoins

- **Groupes** :

Nous utilisons les groupes de sécurité pour la gestion des accès aux ressources partagées. Ainsi, les répertoires possèdent un certain nombre de groupes associés à une série de permissions. Il suffit ensuite d'ajouter des utilisateurs dans ces groupes pour leur autoriser ou leur interdire l'accès aux différents répertoires.

- **Postes de travail / Serveurs** :

De la même manière, vos machines sont rangées dans des OU en fonction de leur type : client ou serveur. Elles remontent dans l'AD une fois leur adhésion au domaine effectuée et il est ensuite nécessaire d'effectuer un classement (dans les OU) manuellement.

5. Cloud

5.1 Google Apps for Work

Votre nom de domaine web est fourni par Google, qui sous traite cet abonnement auprès de la société Domaindiscount24. Il pourra être renouvelé automatiquement tous les ans sous réserve de votre acceptation. fub-kurcz.pl pointera donc vers une IP WAN côté Krakow : **164.132.93.169.** Vos services Web (site, FTP) sont liés à ce nom de domaine, dont tous le paramétrage peut se faire depuis l'interface de gestion Google Apps for Work sur l'URL https://apps.google.com.
Pour le moment, nous avons simplement ajouté votre adresse publique dans la section DNS de Domaindiscount24. Les utilisateurs de votre AD sont par ailleurs synchronisés avec votre compte Google, qui vous donne accès aux services suivants :


Gestion du domaine **fub-kurcz.pl**


Messagerie au format prenom.nom@fub-kurcz.pl pour l'ensemble des utilisateurs


Outils de travail collaboratifs en ligne : traitement de texte, tableur, présentation…


Espace de stockage en ligne illimité (Drive)

Calendrier partagé


Plateforme regroupant messagerie instantanée et visio-conférence (Hangouts)

Aucune configuration supplémentaire n'est nécessaire de votre part, nous utilisons GADS (Google Apps Directory Sync) pour que votre AD soit synchronisé en permanence avec votre compte Google Apps for Work.
Nous vous encourageons à utiliser les services de Google directement depuis le web, car ils ont été conçus dans cet optique. Toutefois, si vous souhaitez utiliser le client de messagerie Outlook, nous mettrons à votre disposition un outil développé par Google (Google Apps Sync), qui permet de synchroniser les contacts, calendriers, tâches sans qu'aucune action de l'utilisateur soit requise.

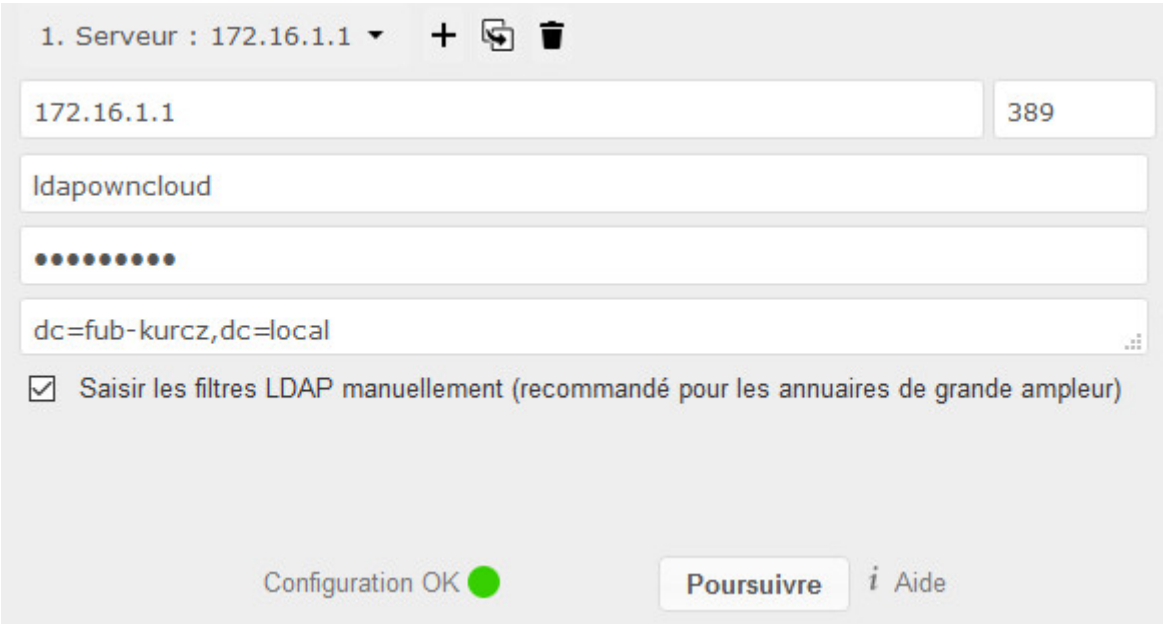
5.2 Cloud privé

Vous disposez également d'un Cloud privé basé sur Owncloud v9. C'est un produit libre qui a fait ses preuves, dont le développement remonte à début 2010. Il est installé sur le serveur KRA-CLOUD et est accessible via une interface web à l'adresse https://infra.fub-kurcz.pl/owncloud.

Le client de synchronisation doit être installé sur les postes de travail, mais aucune autre action complexe n'est requise de la part des employés. Les comptes AD remontent automatiquement dans l'annuaire du serveur et les utilisateurs n'auront plus qu'à renseigner leurs identifiants habituels pour commencer à partager leurs fichiers.

Pour le moment, nous n'avons ajouté aucune fonctionnalité particulière à Owncloud, mais un système de plugins permet d'ajouter des rôles que vous pourriez mettre en place à la suite de ce projet.

L'intérêt d'Owncloud est d'allié la simplicité d'un système tel que Google Drive, à la maitrise de l'emplacement de stockage de vos données. Vous pouvez donc les conserver au sein de votre site principal, ou décider d'installer ce serveur chez le prestataire de votre choix.



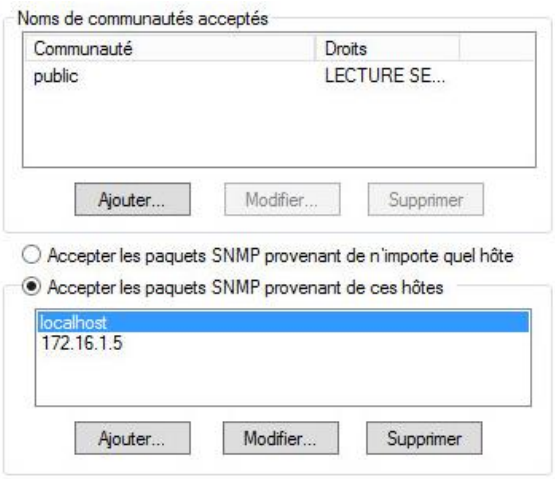
Connexion d'Owncloud au serveur LDAP (Active Directory) : L'utilisateur 'ldapowncloud' est utilisé pour effectuer la jonction. Le fait de placer un utilisateur dans le groupe de sécurité 'owncloud' entraine sa création dans l'arborescence du serveur Owncloud, ce qui lui permet d'accéder à ce service.

6. Supervision

6.1 Centreon

Le système de supervision utilisé est Centreon 2.7.4. Il s'agit également d'une solution gratuite basée sur CentOS, ici en version 6.8. A l'origine, Centreon était une interface graphique destinée à l'outil de supervision Nagios. L'application fonctionne aujourd'hui de façon autonome et l'ajout de plugins n'est pas nécessaire une fois l'installation terminée.

La supervision est basée sur le protocole SNMP (Simple Network Management Protocol), qui permet la récupération d'information sur toutes les machines ou périphériques compatibles. Sous Windows, SNMP est une fonctionnalité du système que nous avons installé et configuré via le gestionnaire de services :



Lors de la configuration de Centreon, la *Communauté* doit être définit pour chaque hôte ajouté. Nous utilisons ici la communauté 'public' pour établir la connexion avec ce serveur. Les requêtes SNMP ne seront autorisées que pour le serveur de supervision, dont l'adresse IP est 172.16.1.5.

Sous Linux, il est nécessaire d'installer un paquet supplémentaire (snmpd), puis le paramétrage se fait en modifiant les fichiers (textes) de configurations. Les informations remontent ensuite dans l'interface d'administration à l'adresse http://172.16.1.5/centreon et des mails sont envoyés à polfran@fub-kurcz.pl en cas de défaillance :

Hosts	Services	Status	Duration
Centreon-Server	Disk-/	OK	1w 4d 18h 52m 29s
	Load	OK	1w 4d 18h 53m 44s
	Memory	OK	1w 4d 18h 54m 59s
	Ping	OK	1w 4d 18h 56m 14s
KRA-AD	Check CPU	OK	1d 19h 37m 23s
	Check RAM	OK	18h 21m 3s
KRA-AD-SEC	Check CPU	OK	2h 17m 5s
	Check RAM	OK	2h 10m 16s
KRA-CLOUD	Check CPU	OK	13h 6m 19s
	Check RAM	OK	19h 26m 21s

6.2 Gestion des Logs

Nous utilisons Splunk Light pour la gestion des logs. Ce système permet de récupérer ces fichiers et de les analyser en temps réel. Sans cette solution, il serait nécessaire d'effectuer des contrôles manuels sur chaque serveur pour prendre connaissance des informations recensées par les logs.
Splunk est installé sur le serveur KRA-LOGS (Debian 7.11) et son interface d'administration est disponible à l'adresse http://172.16.1.3:8000.
Le moteur de recherche permet d'effectuer des requêtes très précises dans les fichiers et de nombreux filtres sont déjà configurés, par exemple l'affichage des erreurs sur les dernières 24H. Voici un exemple de requête :

Error OR failed OR severe OR (sourcetype=access_* (404 OR 500 OR 503))

Grace à cette syntaxe, on obtient un résultat de ce type pour un client Linux :

i	Période	Événement
>	15/07/16 05:54:25,000	Jul 15 05:54:25 KRA-LOGS kernel: [4.905923] Error: Driver 'pcspkr' is already registered, aborting... host = KRA-LOGS source = /var/log/kern.log sourcetype = syslog
>	15/07/16 05:54:25,000	Jul 15 05:54:25 KRA-LOGS kernel: [4.905923] Error: Driver 'pcspkr' is already registered, aborting... host = KRA-LOGS source = /var/log/syslog sourcetype = syslog
>	15/07/16 05:54:25,000	[4.905923] Error: Driver 'pcspkr' is already registered, aborting... host = SPLUNK source = /var/log/dmesg sourcetype = dmesg
>	15/07/16 05:53:55,000	parted_server: OUT: 0 (null) /lib/partman/commit.d/45format_swap: error_handler: exception with type Timer host = SPLUNK source = /var/log/installer/partman sourcetype = partman

Splunk utilise un client appelé UniversalForwarder pour l'indexation des données. Il peut être installé sur une machine distante (Windows, Linux…) et permet de sélectionner les données à renvoyer au serveur.

Hôtes		Nombre	Dernière mise à jour
KRA-AD-SEC		269	16/07/16 15:07:48,000
KRA-LOGS		3,202	16/07/16 15:04:47,000
SPLUNK		11,894	16/07/16 14:54:26,000
UTC		3	15/07/16 06:20:12,000
syslogd		1	15/07/16 06:20:12,000

>	16/07/16 15:07:48,000	07/16/2016 15:07:48.638 dcName=KRA-AD-SEC.fub-kurcz.local admonEventType=Update Names: objectCategory=CN=Computer,CN=Schema,CN=Configuration,DC=fub-kurcz,DC=local name=Splunk distinguishedName=CN=Splunk,CN=Computers,DC=fub-kurcz,DC=local cn=Splunk

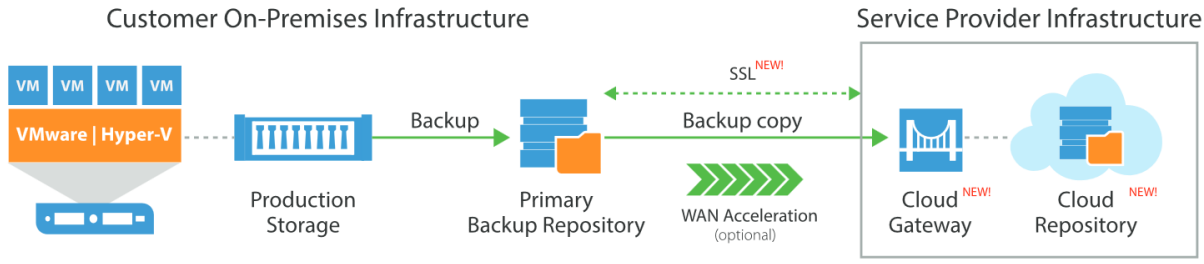
DC secondaire dans la liste des hôtes (capture 1). L'ajout du PC de test nommé 'Splunk' dans le dossier 'Computers' remonte immédiatement dans les logs (capture 2).

7. Plan de reprise d'activité

Bien que la redondance de votre infrastructure vous protège des interruptions de services au quotidien, nous nous devons aussi de prévoir ce qui pourrait se passer en cas de problème majeur, comme un incendie de vos locaux ou une catastrophe naturelle.

Il serait évidemment possible d'installer de nouveaux serveurs, de restaurer vos données, puis d'effectuer la reconfiguration de toutes vos VMs, mais cela prendrait plusieurs semaines et votre activité s'en trouverait très fortement impactée.

C'est dans cet optique que nous mettons un place un plan de sauvegarde de votre SI, qui s'appuie sur un produit de la société Veeam *: Availability Suite*. Cette solution s'inscrit dans un nouveau genre de service Cloud : le DRaaS (Disaster Recovery-as-a-Service). L'idée est de répliquer vos VMs vers un Datacenter situé dans un autre pays, afin qu'il soit possible de basculer sur une autre infrastructure en cas de perte de celle de Krakow. Afin de pouvoir couvrir des étendues plus importantes, Veeam s'appuie sur des providers comme OVH pour le stockage des VMs. Voici un schéma résumant le fonctionnement de ce PRA :



Nous insistons sur le fait qu'il ne s'agit pas d'une simple sauvegarde, mais bien d'une réplication en temps réel de toutes vos VMs. En résumé, ce système permet :

- De basculer sur votre infrastructure en Cloud à tous moments si votre site principal devient inaccessible.
- De restaurer tout ou partie des VMs sauvegardées sur les serveurs de votre Providers de Cloud.
- D'utiliser une VM distante le temps de remettre en état une VM locale qui ne fonctionnerait plus.

Outre la réplication de vos VMs, *Veeam Availability Suite* prend également en charge la sauvegarde de vos données.

8. Mises à jour / Masters / Déploiement

Cette rubrique concerne l'installation des mises à jour (MAJ) de vos postes clients et serveurs, mais touche aussi à la réalisation 'd'images' vous permettant de cloner ou réinstaller vos machines rapidement par l'intermédiaire du Multicast.

- **Mises à jour :**

  Une solution Microsoft intégrée à Windows Server est utilisée : *WSUS*. Son rôle est de télécharger toutes les mises à jours des produits recensés dans votre SI, c'est-à-dire Windows Server 2012 R2, Windows 10, et les éventuels logiciels Microsoft associés. Il vous sera ensuite possible de trier et sélectionner les MAJ que vous souhaitez installer. *A noter : Nous vous conseillons fortement d'utiliser un environnement de pré-production pour tester le bon fonctionnement des OS avant de déployer ces MAJ sur l'ensemble de votre parc.*

- **Réalisation de Masters :**

  La réalisation de ces images systèmes vous permettra de gagner un temps précieux lors de la réinstallation d'un ou plusieurs postes. Elle se base sur nouvelle fois sur 1 logiciel et 1 service Microsoft : *MDT* & *WDS*.

  MDT, pour Microsoft Deployment Toolkit, est constitué d'un ensemble de scripts qui permettent :

  - La capture d'une image via Windows PE (Preinstallation Environment)
  - La gestion de 'Task Sequence' qui permettent d'effectuer le déploiement de l'OS de façon automatisée, en spécifiant des actions pour chacune des étapes d'installation
  - L'ajout d'applications en fonction de différents profils (administration, compta etc.)
  - La gestion des pilotes, qui permet d'utiliser une seule image système pour n'importe quel type de machine, en y injectant uniquement les pilotes requis lors de l'installation de l'OS.

  WDS, pour Windows Deployment Services, qui prend en charge la distribution de l'image auprès des machines clientes. Après avoir configuré les postes pour un boot en PXE pointant sur le serveur WDS, il est possible de charger Windows PE en mémoire, puis d'effectuer la récupération de l'OS, des applications et des pilotes en Unicast & Multicast. Cela signifie que le temps nécessaire au déploiement sera à peu près le même, que le master soit appliqué à 1 ou 20 PC à la fois.

9. VoIP

Dans l'objectif de diminuer les frais de communications téléphoniques entre les deux sites principaux (Krakow et Rzeszow) et permettre une plus grande flexibilité de la téléphonie, nous installons des serveurs de téléphonie VoIP basé sur le logiciel libre d'autocommutateur téléphonique privé (PBX) Elastix, lui-même basé sur le logiciel libre Asterisk. Comme pour pfSense, son administration est entièrement réalisée depuis une interface web. Nous utilisons le protocole SIP.

Cisco 7811

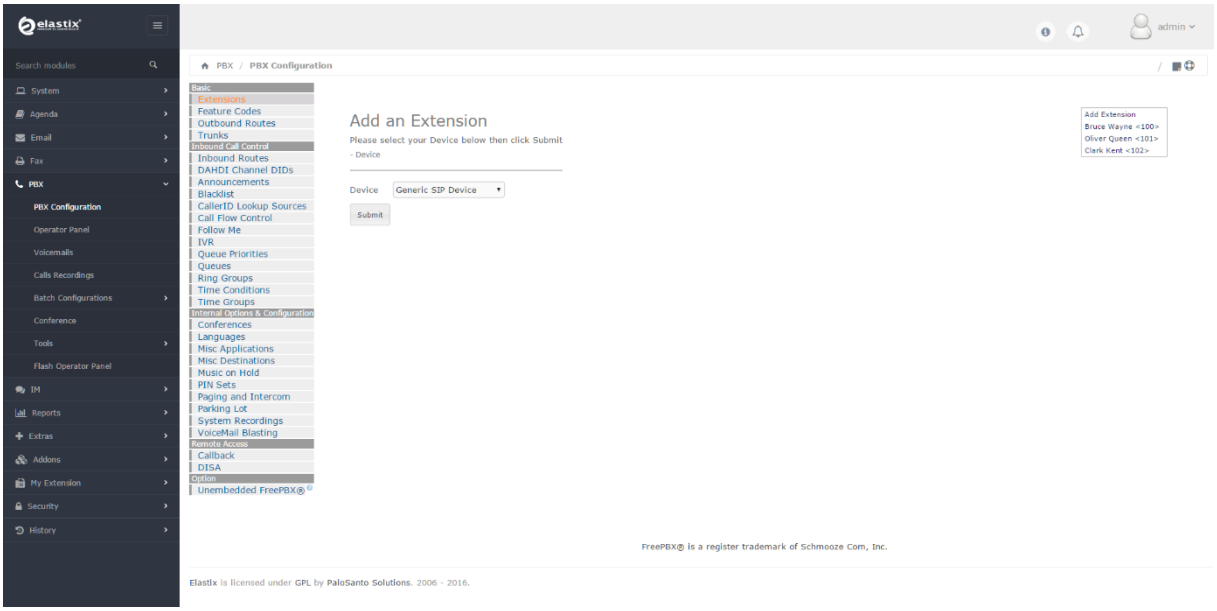
Les utilisateurs disposent d'un téléphone IP Cisco 7811. Leur ordinateur est connecté sur la prise Ethernet du téléphone, lui-même connecté à la prise Ethernet murale situé à proximité de leur bureau.

Pour assurer une qualité de service optimale, voire primordiale pour la VoIP, les téléphones IP sont dans un VLAN dédié et prioritaire (QoS).

Pour en revenir à Elastix, une fois connecté sur l'interface d'administrateur, la gestion des extensions (= ~ lignes téléphoniques) se fait via le menu **PBX** -> **PBX Configuration** -> **Extensions** .
Il existe une multitude d'options et de possibilités dans le menu **PBX** -> **PBX Configuration**, à adapter selon vos usages et souhaits.
Une fois les extensions créées, nous paramétrons les téléphones IP avec ces informations indispensables :

Registraire : **172.16.1.4**
Utilisateur : *<User extension>*
Mot de passe : *<secret >*

A noter qu'il est aussi possible d'utiliser ces extensions avec un softphone SIP tel que Ekiga, Linphone et X-Lite entre-autres. Si le client SIP est compatible, vous pourrez même passer des appels en visio-conférence.



*Menu **PBX** -> **PBX Configuration** -> **Extensions***