Open Knowledge Foundation

Dossier d'architecture technique

Bertrand Janvoie
Soule Ben namim
Faïze Madi

Contents

Avant propos

A. Présentation de l'entreprise

Open Knowledge est une jeune entreprise offrant des services de consulting et de formations sur les domaines des technologies de l'information. Afin de répondre à ces services, celle-ci à développer des modules d'e-learning.
Face à une augmentation de la demande de formation dans le secteur des technologies de l'information, le challenge d'Open-Knowledge est de répondre à ces besoins en étendant ses services au-delà de ses capacités actuelles, cela passera par une refonte de leur infrastructure et de ses services pouvant accueillir jusqu'à 20 formateurs et 800 étudiants à la fois.

B. Acteurs impliqués dans le projet

Afin de répondre à ses exigences, il convient de définir les parties prenantes impliqués dans le projet.

Acteur	Interne Externe	Description
Personnel administratif	Interne	Personnel qui gère le fonctionnement interne de l'entreprise.
Personnel technique	Interne	Personnel chargé du maintien en condition opérationnel du service informatique.
Formateur	Externe	Intervenant chargé de la formation des étudiants.
Etudiant	Externe	Etudiants impliqués dans un parcours de formation.

I. Architecture fonctionnelle

A. Besoins fonctionnels

Open-Knowledge est entrée dans une grande phase d'expansion et doit repenser son architecture et ses services.

Pour cela, une refonte de l'architecture du SI est nécessaire. Celle-ci devra inclure comme fonction :

- Des services de visioconférence.
- Un environnement de travail adaptés aux besoins de la formation, type machine virtuel.
- Une plateforme d'échange de fichiers et de documents nécessaires à l'apprentissage liés aux services de formation.
- Un environnement destiné à la gestion interne de l'entreprise.

Cette architecture devra répondre à des exigences de haute disponibilité afin de permettre aux différents acteurs des services formations et administratifs et techniques de composés à travers un environnement stable, fonctionnelle et maîtrisé.

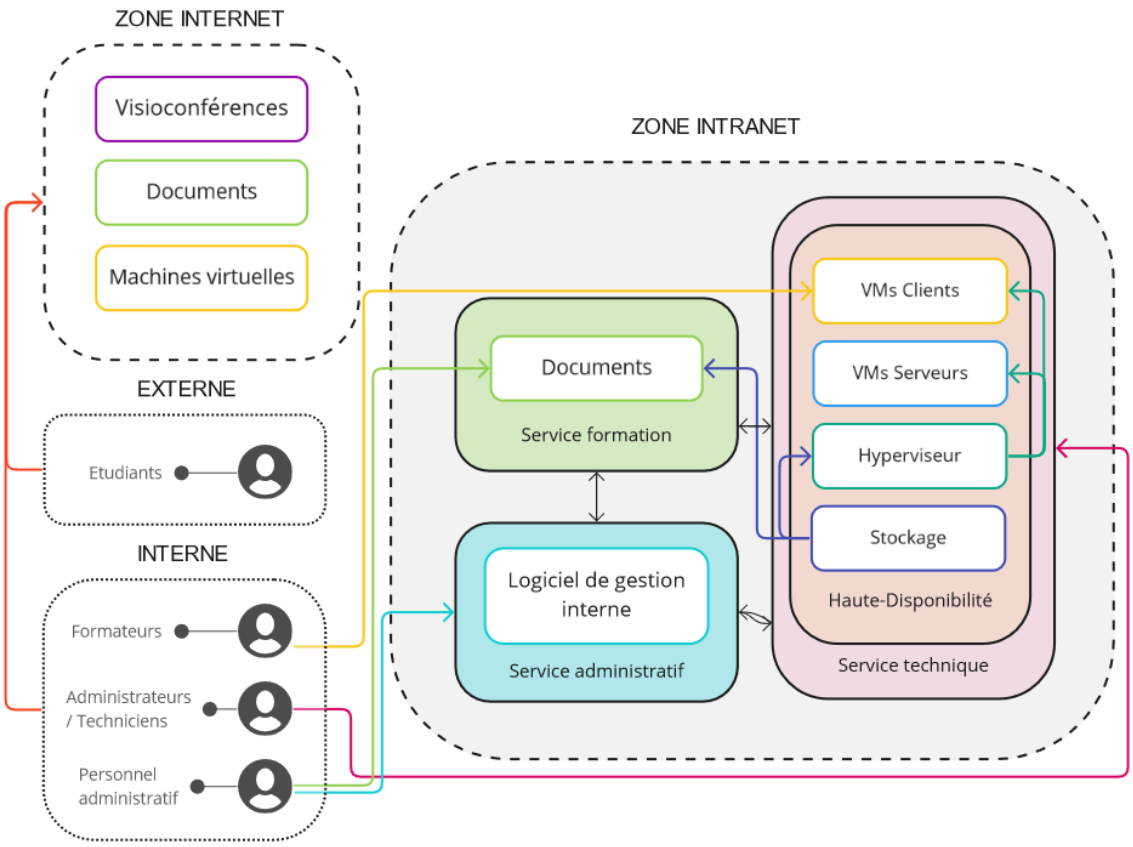
B. Besoins non fonctionnels

En plus des besoins exprimés dans le cahier des charges, la mise en place d'une telle infrastructure entraîne certaines contraintes imposées et indirectes liés aux choix architecturaux. Il convient de déclarer celle-ci afin d'en exposer clairement les différends critères afin de les traiter durablement lors de la mise en place de l'infrastructure.

Contrainte	Besoin
Imposé	L'architecture devra répondre à des exigences de haute-disponibilité.
Indirect	Il faudra assurer la redondance au niveau des serveurs /données.
Indirect	Les services déployés devront être réactif et tenir les monter en charge.
Indirect	Les serveurs devront être d'une exigence matérielle suffisante pour tenir les monter en charges et la redondance des données.
Indirect	Des choix architecturaux devront être effectué concernant les solutions de haute-disponibilité mise en place. Ex : Clustering, Load Balancer, Equilibrage de charge.
Imposé	Les classes virtuelles devront être privées/cloisonnées.
Indirect	Le service administratif devrait être indépendant du service de formation.
Imposé	Utilisation des solutions Microsoft pour les différents services implantés sur les serveurs (Impression, DHCP, DNS, Active Directory, Messagerie)
Imposé	Les services web devront utilisés un système d'exploitation GNU/Linux.

Indirect	Un choix applicatif devra être effectué concernant les services web.
Indirect	Il faudra prévoir des licences d'exploitation pour tous les services utilisés dans l'infrastructure.
Imposé	Les machines virtuelles des formateurs devront être fixes.
Indirect	Une capacité de stockage conséquentes devra être prévu pour le stockage des données et la virtualisation de machine virtuelle
Indirect	L'infrastructure devra être doté d'une connexion internet capable de supporter la charge concernant les accès distant, le déploiement de machines virtuelles ainsi que du potentiel traffic accédant au serveur web.
Indirect	L'infrastructure devra être capable d'accueillir de nouvelles fonctionnalités ou évolutions futures.
Indirect	L'infrastructure devra répondre à des exigences de scalabilité de part sa nature de plateforme d'e-learning.
Indirect	Il sera nécessaire de sécuriser hautement les différents flux de données.
Imposé	L'infrastructure devra suivre le modèle de cloud hybride.

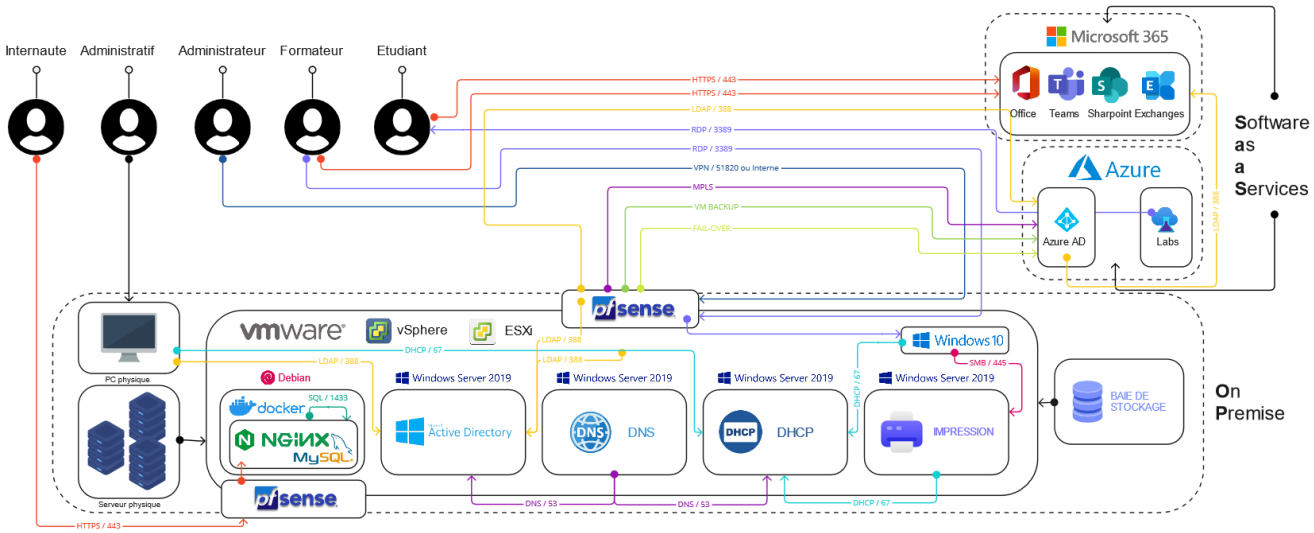
C. Représentation fonctionnelle



Représentation de haut niveau des fonctions du SI.

II. Architecture applicative

A. Schéma applicatif



En prenant compte les besoins et contraintes listés précédemment, il convient de lister les technologies utilisées en termes d'architectures applicative et de justifier leur choix.

- 3 x **Machines physiques** : le choix d'Open-Knowledge se porte sur l'environnement VMWare. Dans le cas de notre infrastructure, ce choix se traduit par une installation de vSphere et d'ESXi sur nos serveur physique.
    - 1 x **Vsphere**, aura pour fonction d'orchestrer de nos différends ESXi. (Clustering, Redondance, Migration)
    - 3 x **ESXi** aura pour fonction de virtualiser nos différents serveur et machines virtuelles.
- 6 x **Serveur virtualisés** : le choix d'Open-Knowledge privilégie l'environnement Microsoft pour différents services assurés par notre infrastructure.
    - 5 x **Windows Serveur 2019**, afin d'héberger un serveur assurant les services d'Active Directory, un serveur pour les services DNS, un pour les DHCP, un serveur d'impression et enfin un serveur servant de base de données et de stockage centralisé pour le reste des VM.
    - 1 x **Debian**, choisis pour sa stabilité afin d'héberger les services web de l'entreprise. Celui-ci devra utiliser le service Nginx, Docker et potentiellement une base de données dédié au web. Le serveur web devra être isolé du reste du réseau local dans une DMZ.
- 20 x **Machines virtuelles** : destiné aux formateurs, ses machines probablement sous Windows 10 ou 11 devront fournir une espace de travail pour les potentielles formateurs qui interviendront dans la formation.
- **Azure Cloud** : Un accès à Azure cloud afin de synchroniser l'active directory et potentiellement utilisé à des fins de réplication.

- Azure labs : Création de machines virtuelles à la demande pour les étudiants.

- M365 : Synchronisation de l'active directory local avec M365 afin d'associer les différents acteurs impliqués dans le projet à des groupes et leur fournir les outils nécessaires à l'apprentissage (Teams, Exchange, Sharpoint. Suite Office)

- 2xPfsense : Qui serviront de pare-feu et afin de mettre en place une DMZ.

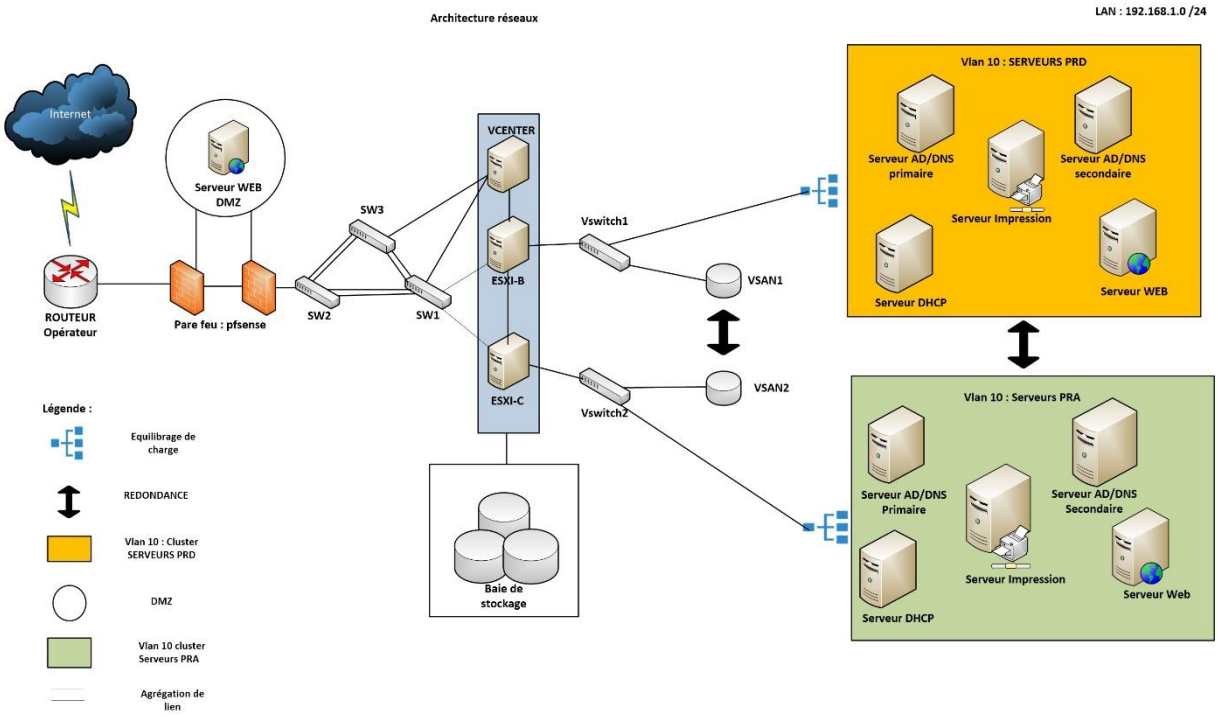
B. Liste des environnement

Convention de nommage:
[VM ou SRV][Description(2-4Lettres)][Numero](3Chiffres)

Env	Nom	Type	OS	vCPU	RAM	Stockage	réseau	
PRD	SRVHYP001	Physique	ESXi - vSphere		500Go	150Go	Interne	
PRD	SRVHYP002	Physique	ESXi		500Go	150Go	Interne	
PRD	SRVHYP002	Physique	ESXi		500Go	150Go	Interne	
PRD	REPLICATION	Physique	ESXI x3		1,5To	5To	Externe	=> Cloud
PRD	SRVNAS001	Physique	TrueNas		8Go	5To	Interne	
PRD	SRVDNS001	VM	Windows Serveur 2019	2	4Go	20Go	Interne	
PRD	SRVDHCP001	VM	Windows Serveur 2019	2	4Go	20Go	Interne	
PRD	SRVAD001	VM	Windows Serveur 2019	2	8Go	20Go	Interne	
PRD	SRVMAIL001	VM	Windows Serveur 2019	2	4Go	20Go	Externe	Cloud => Office365
PRD	SRVIMP001	VM	Windows Serveur 2019	2	4Go	20Go	Interne	
PRD	SRVFW001	VM	Pfsense	2	4Go	20Go	Interne	
PRD	SRVWEB001	VM	Debian	2	4Go	40Go	Interne	
FORM	VMFORM001	VM	Windows 10 Pro	2	16Go	500Go	Interne	
FORM	VMFORM...	VM	Windows 10 Pro	2	16Go	500Go	Interne	
FORM	VMLAB001	VM	Windows 10 Pro				Externe	
FORM	VMLAB...	VM	Windows 10 Pro				Externe	
FORM	VMLAB800	VM	Windows 10 Pro				Externe	

III. Architecture technique

A. Schéma technique



B. Choix des solutions technique.

- Le parefeu

Dans l'idéal deux pare feu (un dit principal dont le rôle est de filtrer le trafic entre la dmz est le réseau interne et un autre dit frontal qui n'autorise que le trafic réseaux destinée à la dmz)

- Pfsense

PfSense permet de mettre en place une connexion depuis l'extérieur vers le serveur web.
Il permet d'interdire le trafic réseaux du serveurs web vers internet (en filtrant les requêtes entrantes et sortantes depuis et vers internet)
Son principal atout est qu'il soit open source, gratuit, le fait aussi qu'il soit reçoi des mises à jour régulièrement pour combler les failles de sécurité connues, en plus la mise en place du pare feu au sein d'un réseaux est facilité par une gamme large de documentation technique, vidéo tutoriel dans divers à disposition de tous, partagé par une communauté fortement présente sur internet.

- DMZ

Offre la possibilité de mettre en œuvre un niveau de sécurité pour tous les services accessibles depuis un réseau externe, en limitant les

autorisations/communications d'accès à notre services web (protégé les hôtes les plus exposés aux attaques).

- Switch
    - sw1,sw2,sw3

Liées aux trois serveurs physiques qui vont accueillir les trois serveurs esxi leur rôle est d'assurer une liaison entre les routeurs et notre réseau notamment via la mise en place de la redondance au niveau des serveurs au routeurs (au cas où l'un est indisponible un autre prend le relais via l'agrégation de lien mise en place sur les trois switch) -> critères de haute disponibilité au sein de l'infrastructure.

- Stockage interne

Reliées à nos trois serveurs esxi , nous permet de réaliser de la sauvegarde , effectuer des backups en cas d'incident, stocké les données des différentes vms en mettant en place un san , assurer l'intégrité la pérennité des informations stocké et une meilleure centralisations des données dont le but est d'éviter des situations comme la perte ou le vol de données, de ce fait garantir une communication en interne plus optimale

- Équilibrage de charge (load balancing)

Utilise les ressources des différentes machines pour

- Serveur AD\DNS primaire

Organiser, mettre en place des règles de gestion, de déploiement au sein de nos différents réseaux.

- Serveur AD\DNS Secondaire

En cas de surcharge de notre serveur primaire, reprendre la charge en trop pour maintenir la disponibilité.

- Serveur d'impression

Gérer l'ensemble des imprimantes au niveaux des différents réseaux de openknowledge

- Serveur DHCP

Distribuer une configuration IP (adresse IP , masque , passerelle DNS aux différents machines de notre réseaux en fonction du Vlan (dans notre cas Formateurs)

C. Plan adressage IP des réseaux

Réseau lan serveurs :

192.168.1.0 / 24 -> permet d'accueillir 254 machines sur le réseaux (à revoir)

/24 -> 255.255.255.0

Broascast :192.168.1.255

L'ensemble des serveurs sera en adressage statique pour éviter les soucis de disponibilité de services

Plages IP utilisables : 192.168.1.1 à 192.168.1.254

Réseaux Formateurs interne :

172.16.10.0 / 27 pour accueillir 30 machines sur le réseau.

/27 -> 255.255.255.224

Broadcast : 172.16.10.31

Plages IP utilisables : 172.16.10.1 à 172.16.10.30

- L'Importance du choix d'adressage

  Eviter les problèmes liées à la distribution d'adresses ip(manque d'adresse IP sur un réseaux) mais aussi au niveau sécurité en ayant un réseaux défini adapté au besoin demandé ,nous offre la possibilité de mieux contrôler les activités liées à notre réseaux et d'identifier les machines ayant un comportement suspect ou d'identifier des anomalies au sein du réseaux.

IV. SWOT

SWOT	
POINTS FORTS (+)	FAIBLESSES (-)
• Stockage quasi illimité • Sécurité des flux de données • Coût des ressources cloud flexible • Mises à jour automatiques • Capacité d'innovation • Performances • Résilience des systèmes • Cloud hybride	• Dépendance vis à vis du fournisseur • Risque incident technique chez les utilisateurs distants utilisant leur matériel • Incapacité du fournisseur à garantir la localisation des données
OPPORTUNITÉS (+)	MENACES (-)
• Scalabilité de la solution cloud Azure • Redondance des éléments de l'infrastructure • Economies sur l'entretient du hardware • Possibilité d'automatiser des processus/taches	• Localisation des données stockées sur le cloud • Législations peu favorables en matière de stockage dans le cloud

V. Estimation des couts

Produits	Quantités	Prix en €	Total
Windows 10 pro	20	259€ /unités	5180,00 €
ESXI server	3	Compris dans la licence vcenter/vsphere	
Vcenter server	1	~12000 €	12000€
Azure labs services	30	8000€/mois	
Microsoft 365 Apps for entreprise offre E5	20	37,5€/utilisateurs	750,00 €
Fibres dédiées ou mutualisé		900€~/mois dédiée **ou** 85€/mois mutualisé	11000,00 €
Stockage interne		~5000 €	5000 €
Serveurs utilisés pour la virtualisation	3	5000 €	15000 €
Windows server 2019 datacenter	1	5000,00 €	5000,00 €
Switchs	3	2000,00 €	6000,00 €

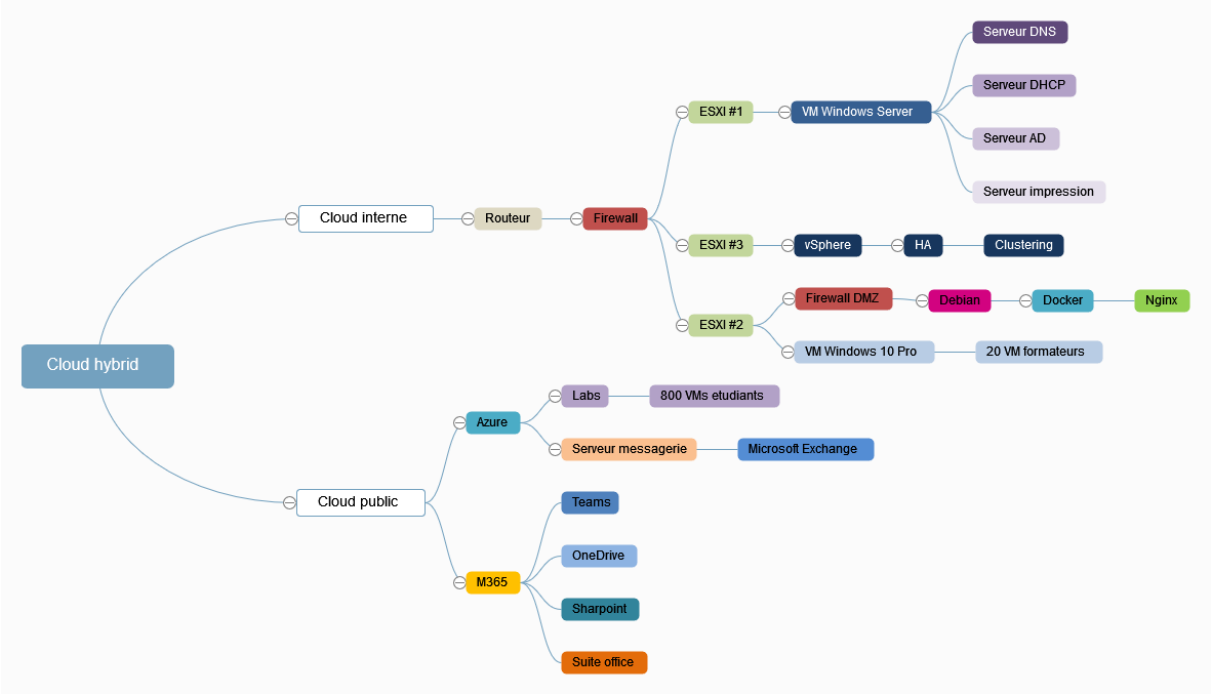
Charges fixe en €	Mois	Année
Fibres dédiées	900€	10800€
Total	**900€**	**10800€**

Cout variable en €	Mois	Année	
Azure labs services	213 333,33 €	2 559 996 €	⇨ MAX (800 utilisateurs)
Microsoft 365 Apps for entreprise offre E5	30 000 €	360 000 €	⇨ MAX (800 utilisateurs)
Total	**243 000€**	**2 919 996€**	

Cout d'investissement en €	Initial
Windows 10 Pro	5180,00 €
Vcenter + ESXI	12000 €
Stockage interne	5000 €
Windows server 2019 datacenter	5000,00 €
Switchs	6000,00 €
Total	**63000,00 €**

Annexe

Mind map de l'infrastructure



Tarification Azure Express route (MPLS)

Bande passante Circuit	Tarif Standard par mois	Tarif Premium par mois	Transfert de données entrantes inclus	Transfert de données sortantes inclus
50 Mbits/s	51,354 €	121,382 €	Illimité	Aucun
100 Mbits/s	102,708 €	186,742 €	Illimité	Aucun
200 Mbits/s	135,388 €	275,444 €	Illimité	Aucun
500 Mbits/s	270,775 €	644,258 €	Illimité	Aucun
1 Gbits/s	407,097 €	1107,377 €	Illimité	Aucun
2 Gbits/s	814,193 €	2 214,753 €	Illimité	Aucun
5 Gbits/s	2 035,481 €	4 836,602 €	Illimité	Aucun
10 Gbits/s	3 174,604 €	5 975,724 €	Illimité	Aucun