

Présentation de l'entreprise BookTic

Introduction :

Présentation de l'entreprise :

L'entreprise BookTic est un groupement d'établissements d'éditions informatique. Implantée partout en France depuis 1994 (Lille, Rennes, Bordeaux, Marseille, Lyon, Strasbourg).

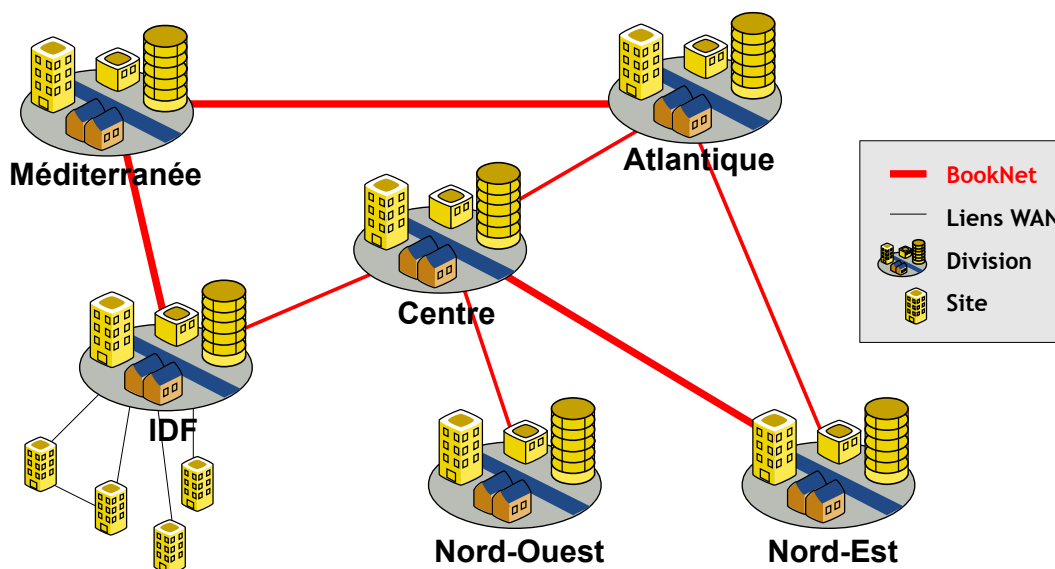
Leurs principaux ouvrages sont destinés, la plupart du temps à un usage pédagogique. Voici quelques exemples de titres les plus imprimés : C++ expliqué aux novices, La haute-disponibilité facile sous Linux, Windows Vista sans planter !, Mise en œuvre rapide Microsoft Windows 2008 Server...etc

Plusieurs centaines de personnes sont employées par les éditions BookTic.

Chacun de ces sites possède un réseau informatique connecté à Internet.

Tous les sites sont reliés entre eux par des liaisons WAN.

Les sièges sociaux de chaque division de BookTic sont reliés entre eux par un réseau indépendant à très haut débit nommé BookNet.



Centre administratif de Meaux :

Vous intégrez le service informatique du centre administratif de Meaux. Sur ce site sont effectuées toutes les opérations concernant la gestion du personnel, l'achats de fournitures, la facturation...etc. On y trouve 5 grands services :

- Les services économiques (Facturation, achat...)
- Ressources Humaines
- Service informatique
- Clientèle (SAV, relation clients...)
- Comité d'entreprise

Le centre de Meaux compte environ, 50 employés et une 10 permanents du comité d'entreprise. Chaque personne dispose d'un poste informatique sous Windows 7, Vista, ou XP pro. Selon la fonction et le service, les logiciels installés diffèrent mais ils sont tous dotés d'un navigateur, d'un client de messagerie, de la suite Microsoft Office ou Open Office. Les postes sont reliés en réseau via du câbles en paires torsadées catégorie 6 sur des prises murales les acheminant vers les baies de brassage de la salle informatique.

Des bornes WiFi sont aussi prévues pour la connexion des portables, des tablettes ou des smartphones de l'entreprise.

Le site de meaux dispose d'un service Active Directory, d'un service DHCP, et d'un DNS primaire sur une machine sous Windows 2008 Server. Celle-ci permet aussi le stockage des fichiers utilisateurs. Un serveur RSync et DNS Secondaire sous Linux Debian.

Le service informatique, afin de faciliter les opérations administratives des employés de BookTic IDF, installe un nouveau serveur LAMP qui permettra la publication de site HTTP et/ou HTTPS pour réservés aux employés.

La sécurisation des accès est assuré par un Pare-feu IPCOP sous Linux, il permet de gérer les accès au LAN ainsi qu'à la DMZ dans laquelle est situé le serveur LAMP. Des accès externes sont envisagés pour le télétravail, notamment. A cet effet, un serveur Windows 2008 server est prévu. Il hébergera un serveur de VPN. De plus, il devient nécessaire d'offrir des accès WiFi sécurisés sur le site, ceux ci seront dans un premier temps créés avec des bornes Cisco et isolés dans leur VLAN propre et les accès limités au protocole HTTP et HTTPS via un Proxy et le Pare Feu.

Afin de faciliter l'administration du site de Meaux, le service informatique dispose d'un serveur de supervision Zabbix, ainsi que d'un serveur GLPI.

Enfin le réseau de Meaux est divisé en cinq VLANs :

- 10 DATA → réseau des employés le 172.16.xxx.0/24
- 20 ToIP → réservé à la téléphonie IP 192.168.xxx.0/24
- 30 Admin → VLAN inter-routeurs 172.16.255.0/29
- 40 DMZ → VLAN accueillant la DMZ il est routé uniquement par le pare-feu.
- 50 WiFi → VLAN intégrant les accès WiFi

Configuration des services :

Paramétrage réseau général :

- Pare-feu IPCOP :
Adresses

Passerelle
DNS

- Serveurs :
AD/DHCP/DNS
OS
Adresse
Passerelle
DNS

VPN
OS
Adresse
Passerelle
DNS

DNS/FTP
OS
Adresse
Passerelle
DNS

ZABBIX/GLPI
OS
Adresse
Passerelle
DNS

LAMP
OS
Adresse
Passerelle
DNS

Proxy
OS
Adresse
Passerelle
DNS

Annuaire du site de Meaux :

Les utilisateurs sont authentifiés via le serveur Active Directory du domaine **booktic.local**. Il est configuré en regroupant les utilisateurs par service. Les UO suivantes sont présentes sur le serveur :

- ServEco
- CE
- Informatique
- RH
- Clientèle
- AccèsVPN

Chaque UO contient les utilisateurs du service concerné, un groupe d'utilisateurs dont le nom est au format G_xxx où xxx=le nom du service, un groupe regroupant les utilisateurs avec pouvoir du service GP_xxx (directeurs et responsables notamment) et une GPO permettant de d'imposer des contraintes d'utilisation et d'habilitations sur les machines du réseau.

Extrait d'une GPO : service RH → **gpo_RH**

- l'accès au panneau de configuration, aux paramètres réseau est interdit
- un script de démarrage **Rhstart.bat** permet la connexion des lecteurs réseaux accédant aux dossiers partagés.
- Les utilisateurs démarrent avec un bureau imposé (barre de menu, fond d'écran...)

...

Les utilisateurs ont des logins construits sur la base suivante - **pnom** - p=première lettre du prénom et nom=nom de famille. Si il y a homonymie un chiffre de 1 à 10 sera ajouté.

Chaque utilisateur possède un dossier personnel et un profil centralisé.

Une stratégie de complexité des mots de passe est définie au niveau domaine.

DNS :

Les serveurs DNS sont configurés pour résoudre la zone directe **booktic.local** et la zone inverse du 172.16.xxx./24

Le serveur primaire est hébergé sur une machine Windows 2008 Server et le DNS secondaire sur une Linux Debian.

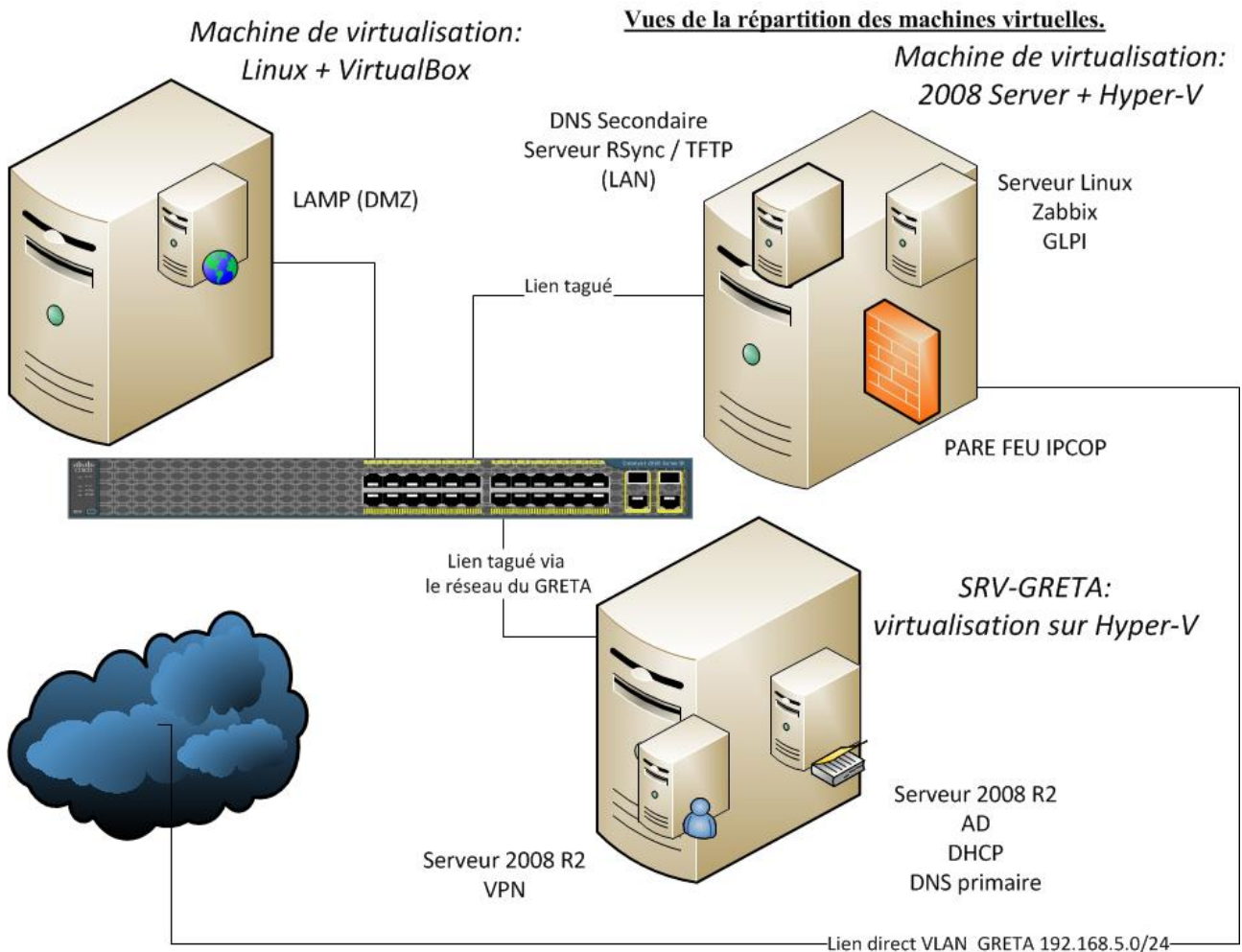
DHCP :

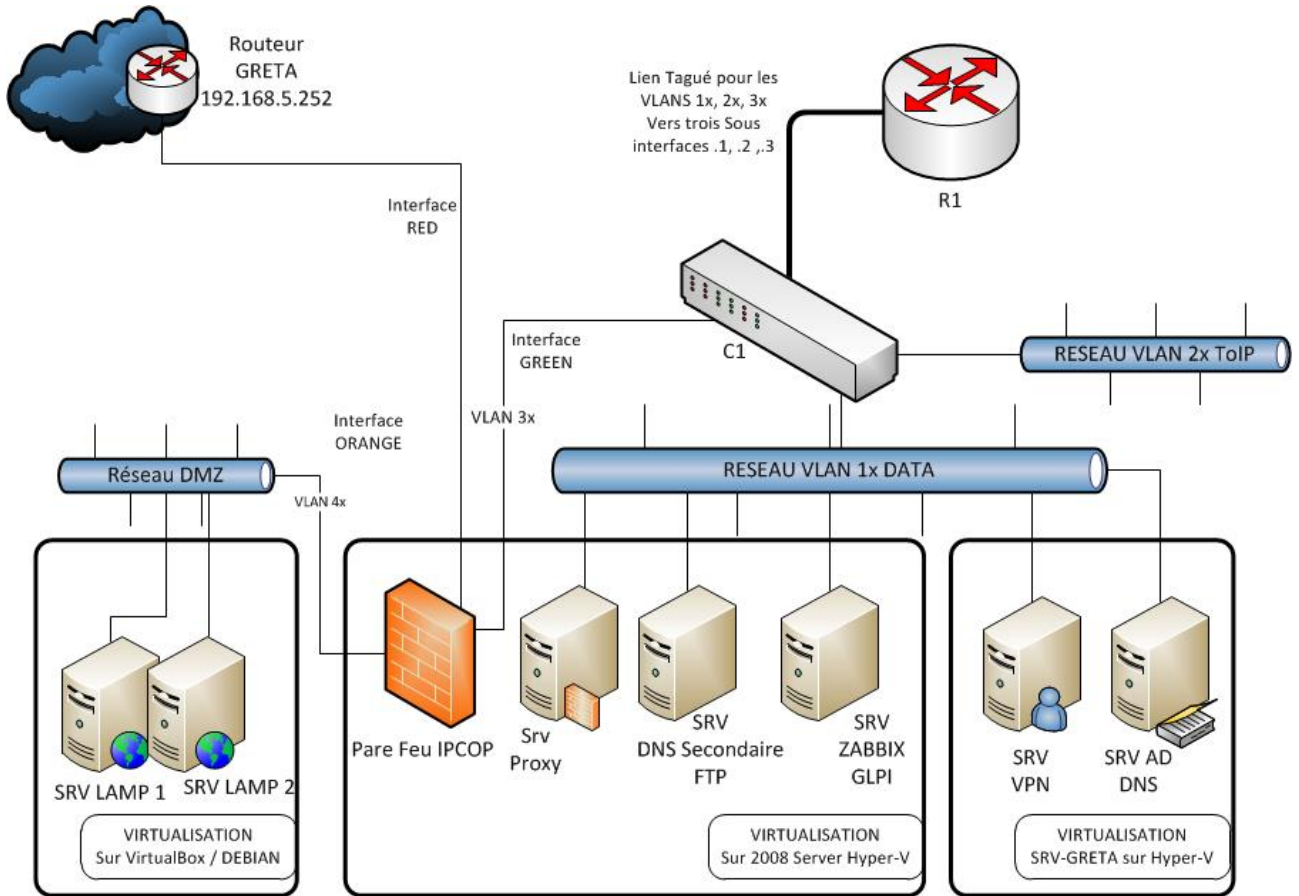
Une plage est définie sur le 172.16.xxx.0/24 avec des options de routeur renvoyant vers la passerelle/pare-feu IPCOP. Les serveurs DNS sont aussi transmis via les options DHCP.

Virtualisation du contexte :

L'ensemble des services sont virtualisés sur trois serveurs selon le schéma suivant :

Schéma logique et virtualisation des serveurs





Vue physique partielle

