

A dark blue vertical bar on the left side of the page. A blue arrow-shaped element points to the right from the bar, containing the date '01/09/2017'.

01/09/2017

SITUATION PROFESSIONNELLE 1.1

PROJET ARCHI-SITE / MISE EN PLACE DU
FIREWALL DES VLAN DU DHCP ET DE
L'ANNUAIRE

CAHIER DES CHARGES

Définition du besoin

Définition de l'objet

Point N°1 : Mise en place du firewall

Le laboratoire désire mettre à disposition des visiteurs médicaux une application Web permettant de centraliser les comptes rendus de visite et la gestion des frais engagés. Pour cela il faut tout d'abord mettre en œuvre une solution FIREWALL afin de créer une DMZ. En effet, les visiteurs (commerciaux de GSB) devront se connecter à distance aux serveurs WEBS afin d'alimenter une BDD.

Point N°2 : Mise en place des VLAN

Le laboratoire étant composé de plusieurs services (comptables/direction/visiteurs etc...), la DSI souhaite également diviser le LAN en VLAN afin d'améliorer la sécurité et la fluidité des échanges.

Point N°3 : Mise en place de l'annuaire

Le laboratoire a besoin d'un service d'annuaire pour son réseau d'entreprise. Il permettra donc de gérer les comptes des utilisateurs du réseau. Cette base d'annuaire doit être la base centrale et doit donc gérer les authentifications des différents services du réseau (WEB, INCIDENT, MESSAGERIE). Sur cet annuaire on trouvera également le service DNS du réseau. De plus, un serveur de fichier doit être présent dans le réseau afin d'accueillir les documents des utilisateurs.

Forme de l'objet et contraintes

Point N°1 : Mise en place du firewall

Le FIREWALL doit gérer 3 Zones, la **DMZ (zone orange)** où seront présent les serveurs WEBS, le **LAN de l'entreprise (zone verte)** où seront présent les serveurs et les postes clients des différents services, et **internet (zone rouge)**. Le laboratoire souhaite étudier une solution open source (PFSENSE par exemple) ou la mise en place d'un dispositif ROUTEUR/FIREWALL type ZYXEL USG40 fourni par l'environnement.

Point N°2 : Mise en place des VLAN

La création des VLAN se fera sur le switch fourni PLANET, le protocole 802.1Q doit être utilisé. Le plan d'adressage des VLAN doit être différent.

Le Switch PLANET est un Switch de niveau2, il faut alors que chaque VLAN est une passerelle défini sur le FIREWALL.

Point N°3 : Mise en place de l'annuaire

On souhaite un annuaire MICROSOFT, soit hébergé sur le système d'exploitation 2008R2 soit sur 2012R2.

L'annuaire doit être redondant et hébergé sur des machines virtuelles.

Le serveur de fichier doit également être une solution MICROSOFT. Il sera présent sur l'annuaire (disque dur supplémentaire partagé) ou directement sur un nouveau serveur (virtualisé).

Accessibilité/Sécurité/Fonctionnalité

Point N°1 : Mise en place du firewall

L'administration du FIREWALL ne peut se faire que depuis la zone verte.

Le FIREWALL doit sécuriser la zone verte grâce à des règles que vous aurez définies et mises en place. De plus certaines communications doivent s'effectuer de la DMZ vers la zone verte.

Concernant la DMZ, son plan d'adressage est défini en 172.31.0.0. Vous devez déterminer un masque pour ce réseau.

Vous étudierez et mettrez en place les fonctionnalités VPN et PROXY du firewall.

Le VPN doit permettre d'interconnecter des utilisateurs nomades au réseau de l'entreprise.

Le PROXY doit interdire la visite de site sensible pouvant altérer la sécurité du réseau ou consommer de la bande passante inutilement. Si le FIREWALL n'a pas de PROXY embarqué vous devez alors installer une solution open source virtualisé prenant en charge ce service.

Une documentation doit être fournie, expliquant les fonctionnalités mises en place. On ne souhaite pas de tutoriel d'installation du FIREWALL, mais les différents paramétrages (règles de sécurité, VPN, PROXY etc...).

Un schéma réseau au format VISIO doit être également réalisé.

Doit être présent en annexe les différentes procédures de mises en œuvre.

Point N°2 : Mise en place des VLAN

La configuration des VLAN est la suivante :

- Le VLAN 1 est celui de l'administration du switch la DSI souhaite une IP d'administration en 192.168.1.1.
- Le VLAN 10 est celui de la direction son adressage est 192.168.10.0/24.
- Le VLAN 100 est celui de l'interconnexion entre le switch et le firewall, son adressage est 10.10.0.0/30.
- Le VLAN 150 est celui des visiteurs son adressage est 192.168.150.0. Le masque est à définir en prenant compte que ce service dispose de 480 personnes. De plus, les postes de ce VLAN doivent être adressés dynamiquement.
- Le VLAN 300 est celui des serveurs son adressage est 172.16.0.0/24.

Les règles d'étanchéités sont les suivantes :

- Tous les VLAN peuvent communiquer avec le VLAN 300 et inversement.
- Les autres VLAN ne peuvent pas communiquer entre eux.
- Si possible, le VLAN 150 doit communiquer avec le VLAN 300, sauf avec le serveur de supervision qui s'y trouve.

Une documentation doit être fournie, expliquant le fonctionnement du SWITCH et des VLAN.

On ne souhaite pas de tutoriel d'installation, mais les différents paramétrages.

Doit être présent en annexe les différentes procédures de mises en œuvre.

Point N°3 : Mise en place de l'annuaire

Le domaine INTRANET ne doit être accessible que depuis l'intérieur de l'entreprise.

Vous devez définir les différentes conventions de nommages :

- Utilisateurs/groupes/PWD.
- Nom de domaine.
- Nom NETBIOS des postes clients et serveurs.

Vous devez également étudier et mettre en place des GPO afin d'automatiser certaines tâches ou d'interdire l'accès à certaines fonctionnalités des postes clients. A vous d'être le plus pertinent dans vos choix de stratégies.

Vous devez également administrer le DNS, création des alias nécessaires à certains services et enregistrement des serveurs spécifiques.

Concernant le serveur de fichier les règles sont les suivantes :

- Les visiteurs ont leurs dossiers partagés, un commun et un personnel pour chaque visiteur.
- Les comptables ont leurs dossiers partagés, un commun et un personnel pour chaque comptable.
- Les directeurs ont uniquement un dossier partagé commun à tous le service. Par contre ils n'ont pas de dossier personnel, ils doivent avoir un profil itinérant.
- Les directeurs peuvent voir les dossiers de tout le monde (les communs seulement).
- Les comptables peuvent voir les dossiers des visiteurs (les communs seulement) mais pas ceux des directeurs.
- Les visiteurs ne peuvent voir que leurs dossiers.

De plus, chaque partage est accessible via des lecteurs réseaux automatique pour l'ensemble du personnel de GSB.

Il faut impérativement une sauvegarde pour le service de fichier, vous justifierez sur la documentation le choix et la méthode de la sauvegarde.

Une documentation doit être fournie expliquant les différents paramétrages du service d'annuaire. On ne souhaite pas de tutoriel d'installation.

De plus, vous devez montrer la structure de votre annuaire (UO/groupe/utilisateurs) sous format VISIO.

Doit être présent en annexe les différentes procédures de mises en œuvre.