A) GESTION DE PROJET (Ce paragraphe concerne aussi les groupes SLAM).

Tâches à réaliser :

Le groupe SISR piloté par (_____) gèrera l'hébergement des deux groupes SLAM « _____/_____», et le groupe SISR piloté par (_____) gèrera l'hébergement des deux groupes SLAM « _____/_____».

Pour les groupes SISR et SLAM, il faut définir un nom de groupe, élaborer un logo d'entreprise, activer un portail collaboratif (partage de documents, affectation des tâches…).

Il faut un envoi par mail, chaque semaine (f.ramel@glpmr.info / s.pernelle@glpmr.info) d'un document de suivi type tableau de bord au format PdF (Présences, ce qui a été réalisé, par qui et en combien de temps, tâches à venir, % d'avancement, divers,…)

Rq : Tout groupe formé doit rester tel quel jusqu'à la fin du PPE2, cela fait partie du contrat de travaux en équipe.

B) HEBERGEMENT DU SITE «GESTIONNAIRE DE SANCTIONS » DANS LA DMZ REELLE DU LYCEE « Enseignement supérieur »

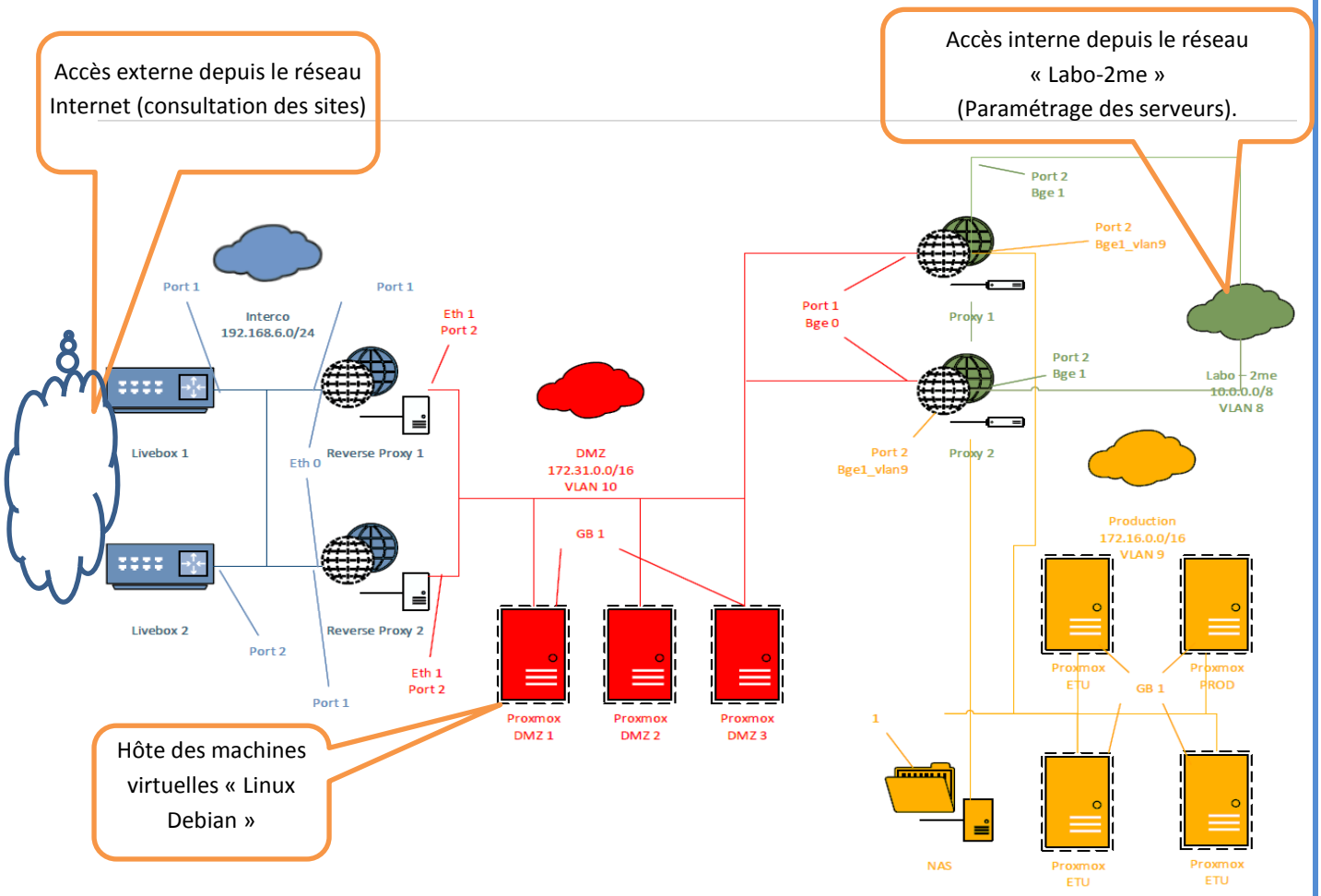
Objectif :Héberger les sites créés groupe développeurs (SLAM).

B.1) MISE EN SITUATION

Les différents sites créés par les développeurs (SLAM) seront hébergés au lycée sur des machines « Linux Debian » existantes créées au préalable par monsieur Bailly gestionnaire informatique. Ces serveurs étant dans la DMZ de l'enseignement supérieur du lycée, les élèves des groupes SISR pourront y accéder par liaison tunnel distante SSH, pour son paramétrage, à l'aide de Putty. Le logiciel WinSCP permettra de charger les fichiers (pages Web, images, base de données…)

A l'état initial du projet, ces machines sont vierges de tous services, seul le service SSH est déjà activé pour y accéder.

Schéma logique du réseau informatique « Enseignement supérieur » :



Légende :
DMZ (zone démilitarisée) : sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu.
NAS (Network Attached Storage) : serveur de stockage en réseau.
PROXY : le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges, généralement internet. Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau.
Proxmox : Ce système d'exploitation est utilisé pour virtualiser machine Linux.
VLAN : Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.
Firewall/Parefeu : bloque les ports réseaux, contrôles les accès aux machines d'un réseau.

B.2) MISE EN ŒUVRE DES SERVEURS LINUX DEBIAN DANS LA DMZ REELLE DU LYCEE « Enseignement supérieur »
(Echéance de l'envoi du lien du site attestant de sa mise en place pour le vendredi 14/04/16)
Contexte : Chaque machine Debian générée sur le serveur Proxmox du lycée est minimaliste et ne dispose donc que du service SSH activé.

Tâches à réaliser sur la machine virtuelle Linux Debian installée sur Proxmox dans la DMZ :
- faire une demande d'hébergement rapidement auprès d'Olivier Bailly par mail (2 X 2 serveurs au total).
- Accéder à la machine avec le logiciel gratuit « PUTTY » en utilisant la communication SSH qui est déjà installée par défaut.
- mettre à jour de la distribution Linux.
- paramétrer la base du serveur linux Debian afin de le convertir en serveur LAMP pour répondre aux contraintes du CDC.
- paramétrer la machine virtuelle Debian pour l'amélioration de la sécurité (sécurisation complémentaire possible en plus de l'existant...).
- transférer une page d'accueil provisoire pour tester rapidement la communication en utilisant par exemple le logiciel WinSCP qui évite de créer un accès FTP.
- mettre en place les sites respectifs avec leurs bases de données et vérifier le fonctionnement.
- envoyer les liens des sites par mail aux professeurs (s.pernnelle@glpmr.info et f .ramel@glpmr.info).

B.3) ELABORATION DU « *CAHIER DES CHARGES TECHNIQUE* » CONCERNANT L'HEBERGEMENT AU LYCEE DANS LA DMZ REELLE DU LYCEE « Enseignement supérieur »
(Dossier N°1 à rendre impérativement par mail le 14/04/17 dont une version intermédiaire le 17/02/17)

Rédiger un cahier des charges technique intégrant:
- le nom et une présentation succincte de tous les acteurs de la prestation réseau (SISR).
- le nom de tous les acteurs de la prestation développement (SLAM).
- les tâches initiales respectives des acteurs réseau.
- la présentation l'infrastructure du réseau de l'enseignement supérieur du lycée.
- le plan d'adressage IP, mots de passe pour la connexion de type SSH avec WinSCP,
N° de port SSH (accès interne et externe) des machines virtuelles Linux Debian (2 machines par groupe).
- le détail des services mis en place pour convertir la machine linux de base en serveur LAMP.
- le mode opératoire pour le transfert des données sur les serveurs respectifs (comment mettre en place les sites sur les machines distantes ?).
- une conclusion présentant un état des lieux de l'installation lors de la remis de ce rapport (ce qui fonctionne ou non, améliorations à envisager, etc…)

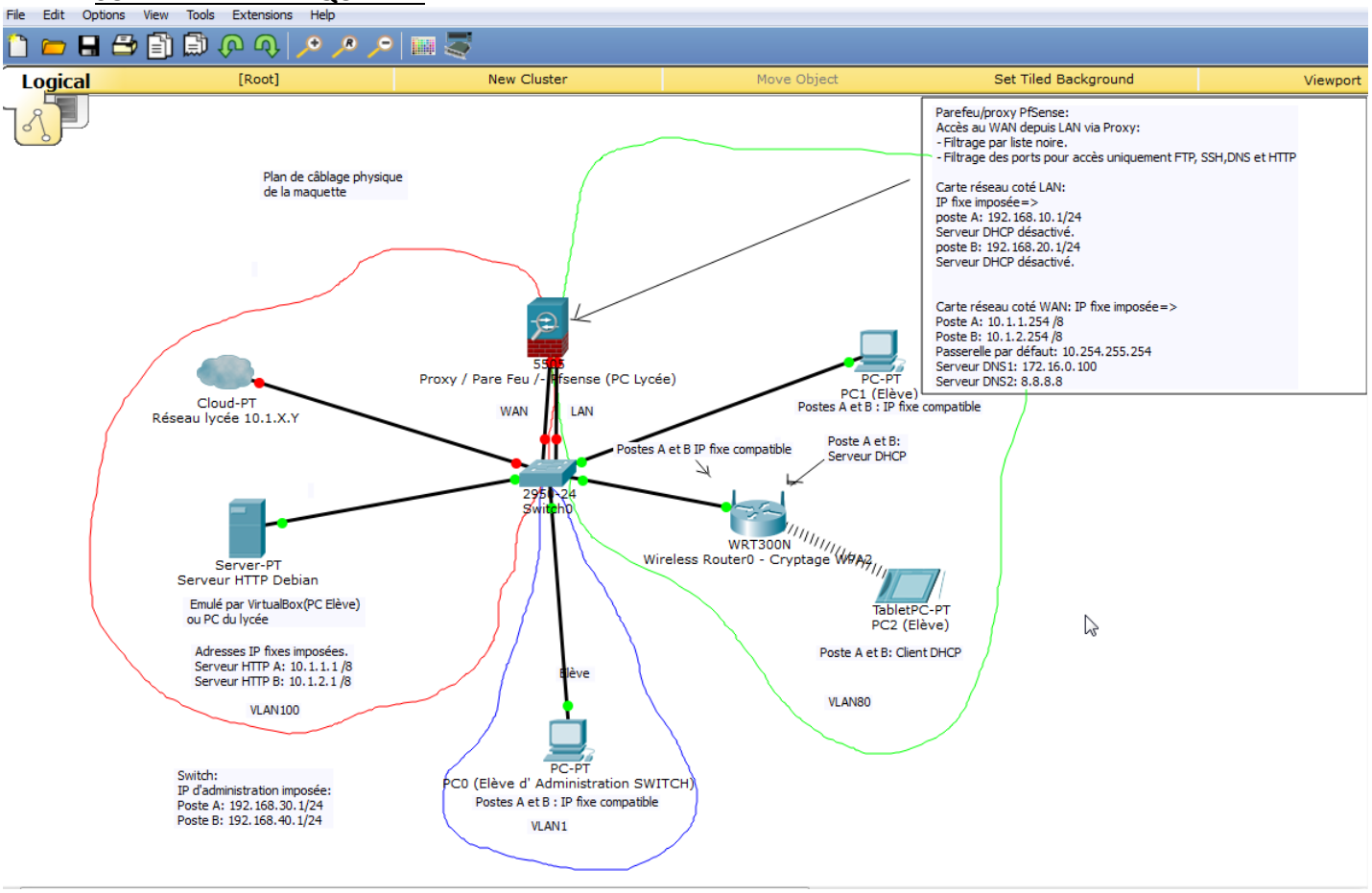
C) VALIDATION DE LA SECURISATION UTILISEE AU LYCEE (PFSENSE) SUR MAQUETTE

Objectif :
Créer une maquette proche du réel afin de valider la sécurisation du traffic via le proxy/parefeu Pfsense.

C.1) PRESENTATION DE LA MAQUETTE :

Le lycée utilise en autres le Proxy/Pare-Feu « **PfSense »** pour sécuriser l'installation.
On désire mettre à l'épreuve ce sous-ensemble pour conforter son choix.
Un banc de test de la sécurité informatique est mis en œuvre par groupe.
Chaque groupe utilise un poste de travail repéré A ou B.
Un affichage devra être apposé sur le matériel pour ne pas que les autres élèves modifient l'installation.

SCHEMA DE LA MAQUETTE :



C.2) MISE EN ŒUVRE DE LA MAQUETTE

Tâches à réaliser sur le serveur HTTP Debian :
- Installation, mise à jour, mise en service et paramétrage de base du serveur LAMP sur Debian (PC d'étudiant avec VirtualBox pour émuler Debian ou PC du lycée).
- Sécurisation complémentaire du serveur LAMP sur Debian en interne.
- Mise en ligne d'une page Web d'essai consultable via un poste client dans le VLAN 80.

Tâches à réaliser sur le Proxy/Pare-feu PfSense :
- Il est installé sur un ordinateur du lycée et mis à jour.
- Il doit respecter le plan d'adressage IP coté LAN et WAN au risque de perturber le réseau « labo-2me ».
- Il doit filtrer le transit LAN/WAN en autorisant uniquement des services FTP, SSH, HTTP et DNS.
- Il doit filtrer grâce aux modules SQUID3 et SQUIDGUARD l'accès à internet à l'aide des listes noires et blanches fournies sur le site : **https://dsi.ut-capitole.fr/blacklists/**
-Il doit permettre la consultation du serveur http Debian.
- Tous les serveurs DHCP LAN et WAN sont à désactiver pour ne pas perturber le réseau « labo-2me » existant.
- Le login d'administration du serveur est « admin » et le mot de passe « password_admin ».
Rq : nous utilisons ici des mots de passe simples, ce qui n'est pas conseillé pour une installation réelle.

Tâches à réaliser sur le switch :

- Attention ! Le switch pourra être raccordé à l'installation existante uniquement après vérification du cloisonnement des VLANs par ports physiques pour ne pas risquer de perturber l'installation existante.
- Reset du switch fourni.
- Paramétrage de l'adressage IP de switch fourni.
- Administration du switch par le VLAN1 de niveau 1 (port physique)=> Port N°1.
- Création des VLANs 80 et 100 de niveau 1 (ports physiques) => Ports 2 à 12 pour le VLAN80 et ports 13 à 23 pour le VLAN100.
  Rq : ces numéros de VLANs sont volontairement différents du réseau du lycée pour ne pas risquer de perturber son fonctionnement.

Tâches à réaliser sur le point d'accès Wifi :

Paramétrer la borne avec accès WPA2, serveur DHCP coté LAN, IP fixe coté WAN compatible avec le SWITCH. Vérifier l'accès au reste du réseau, internet etc…

Tâches à réaliser globalement pour tester la sécurité:

- Mise en place de phases de test de la sécurité du parefeu/proxy Pfsense en élaborant des phases d'attaques depuis le VLAN80 vers le serveur http, **sans pour autant mettre en danger le matériel des étudiants**.

C.3) ELABORATION DU « COMPTE RENDU TECHNIQUE » CONCERNANT LA MAQUETTE DE VALIDATION DE LA SECURISATION UTILISEE AU LYCEE (PFSENSE)

(Dossier N°2 à rendre impérativement par mail le 14/04/17 dont une version intermédiaire le 17/02/17)

On demande de rédiger un compte rendu **technique** de synthèse (Dossier N°2) précisant l'objectif de l'étude, le principe global, une description détaillée de la maquette, les schémas, plan d'adressage IP, les technologies mises en œuvre, les modes opératoires d'installation, les services utilisés, les stratégies de tests mises en place, les critiques par rapport aux résultats obtenus, améliorations possibles, conclusions…

D) SOUTENANCES :

Pour le BTS blanc du mois de mai 2017, il faudra prévoir :

- Une présentation collective par groupe de votre cahier des charges technique (Dossier N°1 concernant hébergement dans la DMZ réelle du lycée) et le rapport technique (Dossier N°2 concernant la mise en œuvre sur la maquette de teste de sécurité) avec un état des lieux, et la procédure de gestion de projet.
  Il est important de ne pas confondre les deux activités lors de la présentation (Distinction **Réel/Maquette**).

  Un questionnement suivra la présentation.
  Attention ! Ceci n'exclut pas des revues de projet qui peuvent être effectuées au cours du semestre.

- Une présentation individuelle de vos tâches au cours de l'année (projets, TP …) en relation avec votre portefeuille de compétences. Un questionnement suivra la présentation.
  On rappelle que le portefeuille de compétence avec les pièces justificatives est à mettre à jour progressivement au cours de l'année.

  Les grilles sont consultables en ligne et téléchargeables avec le lien suivant :

https://docs.google.com/spreadsheets/d/1APVKv1XynKGUl61hS3VuRUSQGaEUYXR8ec6AbKTkoXM/edit?usp=sharing