Projet Sécurité

Rapport

Groupe Defense

Novembre 2004

Membres: Audureau Nicolas
Begue Mathieu
Demblans Mathieu
Gidel Chales-Henri
Goffard Alexandre
Guillot Benjamin
Noiret Cathy

Table des matières

1)Introduction

Nous avons choisi, dans le cadre du projet Sécurité, de représenter le groupe Defense.
Notre objectif aura été de mettre en place une infrastructure réseau, et de la sécurisé.

Le projet Sécurité étant subdivisé en 3 groupes (Attaque, Observation et Défense), il aurait été ridicule de notre part de mettre en oeuvre dès le départ une infrastructure hautement sécurisée.
En effet, mettre en place directement une infrastructure hautement sécurisée nous aurait pris énormément de temps et aurait posé de gros problèmes aux équipes attaques et observations.

Ces raisons nous ont poussé à augmenter le niveau de sécurité de la maquette de manière progressive au travers d'étapes.
Nous avons retenu deux type d'étapes :

- Les étapes majeures qui représentent des modification importantes sur la maquette et qui sont misent en place en fonction du planning.
- Les étapes mineures qui représentent des modifications relativement peu importantes sur la maquette. Elles sont mise en place en fonction des remarques de l'équipe Observation.

Nous avons retenu 3 étapes majeurs :
- Etape 1 : Mise en place d'une maquette de base présentant un ensemble de service.
- Etape 2 : Mise en place de la technologie de VLAN et du routage Inter-VLAN.
- Etape 3 : Mise en place d'une FireWall.

Nous avons également retenu 3 étapes mineures :
- Mise en place d'un système d'antivirus sur la maquette.
- Mise en place de mise à jour.
- Mise en place de sécurisation au travers de préconisation de sécurité.

Nous avons fait infogérer la partie analyse de log et audit auprès de l'équipe Observation.
Nous avons donc tout au long du projet, travailler en coopération avec l'équipe Observation afin de lui laisser placer ses sondes et équipements au sein de notre infrastructure.

Nous allons maintenant vous décrire ce projet vu par le groupe Défense.
Nous commencerons par expliquer la répartition des rôles avant de nous intéresser au planning mis en place.
Une partie importante sera consacré au politiques de sécurité. Nous viendrons ensuite au différentes taches effectuées.
Chaque équipe a participé à ce rapports au travers des parties qui leur sont consacrées.

2)Distributions des rôles.

2.1)Brainstoorming des connaisances

Avant de rentrer dans la distributions des rôles, nous avons réalisé un petit brainsorming afin de connaître les compétences dont nous disposions au sein du groupe.

2.2) Division du groupe

Nous avons ensuite décidé de diviser le groupe en 4 équipes :

- Veille Technologique (VT) : Son rôle est de faire des recherches sur une thématique non maîtrisée et nécessaire pour l'avancement du projet. Au cours du projet, le rôle de l'équipe VT a été réorrienté vers l'étude et la préconisation de politique de sécurité. Les membres de cette équipe sont Cathy Noiret et Nicolas Audureau.

- Installation (INST) : Son rôle est de mettre en place logiciel et matériels retenus tout en ayant à gérer les contraintes lié à l'existant. Les membres de cette équipe sont Charles-Henri Gidel et Mathieu Demblans.

- Exploitation (EXPL) : Son rôle est double et se décompose d'une part en des taches de maintenance sur la maquette et d'autre part en la simulation d'utilisateurs actif lors des phase d'attaques. Les membres de cette équipe sont Mathieu Begue et Benjamin Guillot.

- Coordination (COO) : Vu le rôle central du groupe défense dans le projet Sécurité nous avons décider de diviser la coordination en deux afin de l'alléger.
  - Externe : Son rôle est de gérer les relations avec les autres groupes et gérer la synchronisation pour que l'on avance tous ensemble. Le membre de cette équipe est Nicolas Audureau.
  - Interne : Son rôle est de gérer l'avancement du projet du point de vue du groupe Défense. Il participe également, aux étapes critiques, d'un point de vue technique. Le membre de cette équipe est Alexandre Goffard.

Le fait d'avoir réalisé au préalable le brainstorming de compétences nous a permis de nous répartir plus facilement. D'autre part, ces connaisances ont constituées une base sur la quelle l'équipe VT est venue nous fournir les compétences manquantes.

Avec le recul, cette division du groupe en équipe nous a permi de bien répartir les responsabilités de chaque personne et ainsi de gagner en productivité.

3)Planning

3.1) Planning apriori

Nous avions convenu du planning prévisionnel suivant

Semaine 1 (11oct -> 15 oct) : Mise en place de l'étape 1
Semaine 2 (18oct -> 22oct) : Mise en place de l'étape 2
Semaine 3 (25oct -> 29oct) : Mise en place du FW
Semaine 4 (01nov -> 05nov) : pas cours (semaine tampon)
Semaine 5 (08nov -> 12nov) : prise en contact des conseils finaux de l'équipe observation.
Semaine 6 (15nov -> 19nov) : bilan au sein de l'équipe et préparation finale du rapport.

Comme on peut le voir, la semaine 4 sert de tampon afin rattraper d'éventuel retard pris sur les étapes techniques.

3.2) Planning apostériori :

Semaine 1 (11oct -> 15 oct) : Mise en place de l'étape 1
Semaine 2 (18oct -> 22oct) : Synchronisation Groupes et Accès distants
Semaine 3 (25oct -> 29oct) : Mise en place de l'étape 2
Semaine 4 (01nov -> 05nov) : Mise en place du FW (04nov)
Semaine 5 (08nov -> 12nov) : Préparation du rapport écrit
Semaine 6 (15nov -> 19nov) : Bilan au sein de l'équipe et préparation du rapport oral.
(Toutes les semaines nous avons pris en comptes les remarques et demmandes des 2 autres groupes)

Afin de laisser l'équipe Observation s'insérer dans notre maquette et ne pas modifier la maquette trop rapidemment, nous avons décidé de décaller la mise en place de l'étape 2 d'une semaine.
Cette semaine de latence a permi une meilleure synchronisation entre les groupes et nous a permis de régler les derniers petits problèmes comme par exemple la mise en place des accès distants.

Le reste du planning est similaire (à une semaine près) au planning prévisionnel.

4) Politique de Sécurité

4.1) Présentation générale :

Définir des règles d'accès aux systèmes d'informations d'une organisation :

La conduite à adopter
Les outils et les procédures utilisables
Sanctions en cas de non respect

Cette politique fixe un cadre dans lequel doivent évoluer les utilisateurs.

Nécessités de la politique de sécurité :

- Doit être :

Possible à mettre en place
Facile à lire et comprendre pour les utilisateurs
Bonne équilibre entre protection et productivité

- Doit pouvoir :

Expliquer pourquoi la politique est nécessaire
Expliquer qui est concerné par cette politique
Définir les contacts et les responsabilités
Définir les sanctions à apporter aux violations

Politiques de sécurité réalisées :

- Messagerie : Définir les critères d'utilisation et de non utilisation du système de messagerie.
- Règles de Filtrage : Définir les procédures à respecter en cas de modification des règles de filtrage.
- Mot de passe : Définir les procédures d'utilisation, et de stockage des mots de passe.
- Antivirus : Conduite à adopter face aux virus et à l'utilisation des antivirus.

4.2) Présentation détaillée

4.2.1) Point de vue de l'équipe VT

Le travail de l'équipe VT a consisté dans un premier temps à déceler les éléments susceptibles de répondre à une politique de sécurité, puis à créer ces politiques en accord avec le reste du groupe.
Le but de ces politiques était de définir un cadre strict dans lequel les utilisateurs et les administrateurs devaient travailler. Dans le cadre de la maquette réalisée, toutes les politiques mises en place n'ont pas pu être respectées précisément, notamment parce qu'il n'y avait pas d'utilisateurs 'classiques'.

4.2.2) Point de vue de l'équipe INST

4.2.2.1) Partie Systèmes

L'installation du serveur « mail-dns-active directory » a été faite avec le minimum requis par le système pour une installation de base afin que la machine soit suffisamment vulnérable pour l'équipe *attaque*. L'installation correspondait à une sécurisation datant d'octobre 2003. Le logiciel Tenable NeWT a recensé 39 failles dans la configuration de base.
Une image de l'installation a été faite afin de ne pas avoir à tout réinstallé après une attaque réussie. Cette installation s'est déroulée débranché de tout réseau afin d'éviter toute attaque pouvant venir de l'Internet.
Pour l'accès à distance, ce serveur dispose d'une combinaison « stunnel+vnc » afin de pouvoir administrer facilement la machine à distance. La partie « stunnel » sert à créer un tunnel sécurisé entre le serveur et le client, la partie « vnc » sert à visualiser le bureau du serveur et de l'utiliser comme si l'utilisateur était physiquement devant le serveur. Le mot de passe utilisé par vnc est composé de 16 caractères (lettres, chiffres et caractères spéciaux) afin d'éviter toute utilisation frauduleuse du serveur par ce moyen.

L'Active Directory a été configuré avec des comptes utilisateurs pour chaque membre de l'équipe avec un mot de passe basique de 4 caractères (même mot de passe pour tous les utilisateurs, aucune règle de changement de mot de passe appliquée). Un compte groupe a aussi été créé pour les envois groupés. Seul le mot de passe administrateur a été créé pour rendre plus difficile les attaques car il était composé de lettres et de chiffres sur 8 caractères. Celui ci n'a pas été changé au cours de l'exploitation. C'est ce compte qui est aussi utilisé pour administrer les machines qui appartiennent au domaine. C'est aussi le seul compte autorisé à accéder directement à ce serveur pour l'administrer ou effectuer des modifications.
D'autres comptes ont été générés automatiquement par Windows lors de l'installation et n'ont pas été supprimés afin de garder l'aspect « installation basique » du système.

Pour ce qui est du serveur Web-FTP, l'installation a suivi les mêmes règles de base, les mises à jour les plus minimales possibles ayant été effectuées.
Afin de garantir le contenu du site web, seul l'administrateur du serveur et celui du domaine ont un accès complet au serveur et à sa configuration et sont responsables des pages publiées.
Le serveur FTP était configuré de base avec un compte anonyme ayant accès en lecture et écriture sans limite. Suite à une attaque consistant à remplir au maximum le serveur de fichiers inutiles, ce compte a été supprimé et seules les personnes disposant d'un compte autorisé sur le FTP peuvent y avoir accès.
Le serveur dispose de vnc-serveur configuré pour n'accepter que les connexions venant du serveur mail. Toute connexion à distance sur ce serveur passe par un rebond sur le serveur mail. Le choix a été fait sur cette solution afin de limiter le nombre de tunnel vers l'extérieur.

En ce qui concerne le poste client XP, les règles ont été les mêmes que pour les serveurs.
Lors d'une première installation, le poste client n'était pas dans le domaine et ne comportait qu'un seul compte sans mot de passe.
Afin d'éviter tout accès abusif sur ce poste, il a ensuite été intégré au domaine.
Les utilisateurs accédaient d'abord à la machine par les comptes définis sur l'Active Directory. Suite à l'installation du firewall, des comptes locaux ont été créés sur le poste client. Aucune sécurité n'a été appliquée sur ce poste.

En ce qui concerne l'installation du firewall, les mises à jour les plus récentes ont été installées afin de garantir une sécurité maximale. Les règles de filtrage appliquées ont été choisi selon la politique « tout ce qui n'est pas autorisé est interdit ». Cette politique a pu être appliqué car le nombre de services utilisés était faible (web, ftp, mail).

4.2.2.2) Partie réseaux

4.2.2.2.1) L'administrateur réseau

Dans le carde d'une politique de sécurité réseau stricte, seul l'administrateur est en droit d'accéder de modifier au niveau logiciel ou physique les éléments réseau. De plus l'administrateur se doit d'être joignable a tout moment au cas ou une problème surgirai durant les périodes de travail. Celui-ci est joignable au sein de la structure, mais en dehors de ses horaires de travail, il doit être aussi joignable en permanence avec un numéro de téléphone dédié.

4.2.2.2.2) Les Documentations

L'administrateur se doit de réaliser des schémas réseau de toutes les architecture de l'entreprise au cas ou celui-ci viendrai a quitter l'entreprise ou même pour les autres administrateurs de la structure par exemple l'administrateur système. Mais il doit aussi réaliser des documentations d'usage des matériels qu'il met en place dans la structure Firewall ou proxy pour que ceux-ci puissent être modifiés ou consultés par les personnes concernées.

4.2.2.2.3) Sauvegarde des configurations

Toutes les configurations des éléments réseau doivent être sauvegardées et centralisée à 2 endroits différents : Une sauvegarde sur une machine et une sauvegarde en Dur par exemple sur CD-ROM en faisant attention bien sur que ces support soit éloignés dans l'espace sécurisé en cas de problème de type incendie. Pour effectuer ces sauvegarde l'utilisation d'un serveur TFTP est recommandée pour pouvoir par la suite redéployer les configurations le plus rapidement possible en cas de problème.

4.2.2.2.4) Les mots de passe

L'administrateur réseau est le seul a connaître les mots de passe des équipements réseau personne de doit les connaître car cela risquerai de mettre en péril la vie de l'entreprise. En revanche les mots de passe doivent être quand meme mis dans un espace sécurisé au cas ou il arriverait malheur à l administrateur. Cet espace sécurisé doit etre par exemple un coffre fort ou une machine isolé sur laquelle seuls les hauts responsables et l'administrateur système ont le droit d acces. Cette sécurité ne doit etre utilisée qu'en cas de problème majeur.
Au temps que possible il est conseillé de changer de temps à autres les mots de passe des machines car avec le temps les mots de passe finissent toujours par filtrer.

4.2.2.2.5) Migration de l'architecture

4.2.2.2.5.1) Les Test

Avant toute migration des tests doivent être fait sur le matériel pour s'assurer du bon fonctionnement de celui-ci. Et autant que possible, il est conseillé de se mettre dans la meme situation que celle de l'architecture finale. Dans notre cas lors de la migration sur les Vlans nous avons utilisés un switch 2924 identique a celui utilisé sur la maquette. Nous lui avons implanté la configuration, il en a été de même pour le routeur une fois que tous les test ont été vaidés sur la maquette de test.

4.2.2.2.5.2) Information

Lors d'une évolution majeure de l'architecture qui peut toucher au bon fonctionnement des utilisateurs finaux, il faut prévenir les utilisateurs concernés par mail et si cela est possible, passer les voir pour leurs expliquer qu'une intervention va être réalisée et qu'une interruption de service va avoir lieu. Dans un même temps il faut aussi faire suivre un mail a la coordination pour les informer des travaux en cours.

4.2.2.2.5.3) Quand faire la migration

Une fois que l'on s'est assuré que tout les utilisateurs et la coordination est prévenue et que l'intervention a été validée par ces derniers, on peut alors planifier la migration. Dans le cas de migration importante de l'architecture, comme nous avons réalisé a chaque évolution de la maquette, il conviens de planifier les intervention en dehors des heures d'utilisations des utilisateur, à la fin de la journée de travail ou un WE. Si l'évolution est minime et que elle ne comporte aucun risque de couper

les utilisateurs alors elle peut être planifiée en journée de préférence entre midi et deux pour pouvoir revenir en arrière le cas échéant.

4.2.2.2.5.4) La validation

Apres la mise en place il faut conjointement réseau et système pour valider les choses qui avaient été mise en place lors des tests. Une fois tout ça validé la migration est terminée

4.2.2.2.5.5) L'après migration

Apres la migration de l'architecture, il convient d'informer les utilisateurs concernée que la migration s'est bien déroulée et leur faire part des modifications dans leur habitudes si modifications il y a. De la même façon, il faut les inviter à faire des remarques s'ils rencontrent des problèmes qui n'auraient pas été soulevés après la mise en place.

4.2.2.2.5.6) La modification de la documentation

Il convient qu'une documentation qui n'est pas a jour est une documentation qui ne sert a rien. Donc dès que la migration est terminée et validée il faut modifier les documents adéquats pour les mettra à jour en tenant compte des modifications effectués.

4.2.2.2.6) Faire face aux problèmes

4.2.2.2.6.1) Coupure d'électricités

En temps normal les éléments réseau sont toujours ondulés. Comme les serveurs, ils ne craignent donc pas les coupures de courant. Si cela devait arriver qu'un équipement subisse une coupure de courant cela provoquerai une interruption du réseau momentanée.

4.2.2.2.6.2) Panne d'un équipement

Tous les équipements réseau doivent être redondés, on doit avoir un Spare pour chaque équipements avec la configuration adéquate de l'équipement correspondant installée dessus.

4.2.3) Point de vue de l'équipe EXPL

Pour permettre une bonne exploitation des services offerts par notre maquette, nous avons du mettre en place des politiques de sécurités efficaces. En effet ses politiques ont été utilisés jour après jour par l'équipe d'exploitation du groupe défense.

4.2.3.1) Gestion des comptes et mots de passe

4.2.3.1.1) Au niveau des utilisateurs :

Nous avons décidé de créer un compte Windows active directory pour chaque utilisateur de la maquette. Nous avons choisi de nommer les comptes de la manière suivante : prenom.nom . Par défaut, lors de la création, chaque compte est protégé par un mot de passe générique; il appartient ensuite à l' utilisateur de le changer lors de sa première connexion au système.
De plus, pour améliorer l'efficacité des mots de passe, le système demande à l'utilisateur de le changer tous les 14 jours.

4.2.3.1.2) Au niveau des machines :

Chaque machine installée, sous Windows, possède un seul compte local. Il s'agit du compte d'administrateur qui permet de se connecter sur la machine en ayant tous les droits sans passer par un compte d'active directory. Le compte d'administration possède un nom différent de « administrateur » ! Le mot de passe associé est différent sur chaque machine.

4.2.3.2) Gestion des mises à jour

Les machines qui ont été installées par l'équipe « installation » étaient fournies avec des versions de Windows non mises à jour. Il appartenait donc à l'équipe exploitation d'effectuer d'analyser les rapports générés par le groupe *analyse*.
En effet, une méthodologie d'exploitation à été mise en place : lors de la lecture des documents de synthèse nous fournissant les tentatives d'intrusion ou d'exploitation de failles effectuées par le groupe « attaque », nous effectuons les taches suivantes :

- Nous identifions les failles critiques exploitées;
- Nous recherchons les éventuels patchs et mises a jours publiées par Microsoft ;
  la faille est corrigée par l'installation des correctifs.
- Pour finir, nous vérifions avec l'équipe *analyse* que cette faille comblée n'est pas utilisée ultérieurement par l'équipe *attaque*. Cela prouve que le correctif est efficace.

4.2.3.3) Utilisation de la messagerie

Dans notre maquette, nous avons défini que chaque utilisateur possède un compte Email personnel accessible avec le même identifiant que celui du compte active directory personnel.
En ce qui concerne l'utilisation de ce service, le logiciel Outlook Express a été choisi, principalement pour sa grande simplicité de fonctionnement pour l'utilisateur lambda !
La politique de sécurité mise en place concernant la messagerie est la formation des utilisateurs de manière a se servir de ce logiciel de manière optimale. Par exemple le mot de passe du compte mail n'est pas mémorisé, c'est à l'utilisateur de le taper à chaque lancement du logiciel. Tout message dont la provenance ou le contenu est suspect ne doit pas être visualisé ; il en est de même pour les pièces jointes.

4.2.3.4) Traitement d'un incident

Les 2 personnes de l'équipe exploitation ont notamment pour charge de surveiller le bon fonctionnement du système et de prendre les mesures adéquates lorsqu'un incident survient.
Chaque jour, avec l'accès à distance VNC, nous pouvons vérifier que la maquette fonctionne correctement. En ce qui concerne l'accès à distance, nous avons décidé de mettre en place plusieurs accès VNC en parallèle, nous permettant ainsi de travailler sur les différentes machines d'une part de manière simultanée. D'autre part cela permet d'accéder à une partie de la maquette même si l'autre partie n'est plus accessible.
Lorsqu'un incident se présente, l'équipe exploitation a pour but de remettre en service le plus rapidement possible le bon fonctionnement de la maquette, puis d'analyser dans quelles conditions et pourquoi l'incident s'est produit. C'est ainsi qu'il faut prendre des mesures, comme par exemple mettre a jour une faille de sécurité s'il s'avère que celle-ci a été exploitée. (Voir paragraphe sur les mises à jour)

4.2.4) Point de vue de l'équipe COO

4.2.4.1) Externe

De façon un peu plus large, les politiques de sécurités s'appliquent tout autant au coordinateur externe qu'aux autres membres du groupe.
Notamment lors des échanges avec les autres équipes, il était important de connaître les informations 'divulgables' et à divulguer. D'autres part, l'utilisation de la maquette au meme titre que les autres utilisateurs impliquent une bonne connaissance et un bon respect des politiques de sécurité.

4.2.4.2) Interne

Les coordinateurs étant des utilisateurs normaux de la maquettes, ils sont soumis aux mêmes règles de politique de sécurité que ces derniers.

5) Taches et réalisations techniques

5.1) VT

5.1.1) But

L'équipe veille technologique avait un rôle de prévoyance sur la maquette. De plus, elle devait garder une vue globale du projet afin d'éviter des dérives.

Nous nous sommes donc attachés à prévoir les éventuels problèmes. L'objectif n'était pas de chercher à trouver les solutions de ces problèmes à l'avance (ce travail aurait été trop long et certainement peu utile). Nous avons plutôt cherché à disposer des moyens de trouver les réponses le plus rapidement possible.
Ainsi, nous avons essayé, dans chacun de nos travaux, de composer un panel de liens relatifs aux problèmes potentiels et solutions adaptées à ces derniers.

Nous avons pu dégager trois axes principaux dans nos études : une partie sur les serveurs, une partie sur les Antivirus et une partie sur les politiques de sécurité.

5.1.2) Serveurs

Nous nous sommes penchés sur les serveurs Mails et Web capables de remplir les fonctionnalités requises pour préparer notre maquette.
L'objectif n'était pas d'en choisir un mais plutôt de donner un panorama des offres actuelles, et surtout une manière de choisir les serveurs adaptés à nos besoins. Pour cela nous avons pris en compte les critères de sécurité, de niveau d'expertise pour l'installation et l'administration.

Une présentation des serveurs Mail et Web a été réalisée au cours de la seconde séance.
Ceux-ci ont été mis en place au cours de cette même séance.

Dans un premier temps, nous avons planifié les différentes étapes architecturales du réseau, ainsi que son plan d'adressage, en commun avec les autres équipes de la défense.

5.1.3) Antivirus

Par la suite, nous avons travaillé sur les antivirus, et les différentes solutions possibles répondant aux besoins de notre projet.
De la même façon que pour les serveurs, nous ne nous sommes pas contentés de lister les solutions en les comparant, nous avons préféré exposer la méthodologie à suivre pour choisir l'antivirus adapté à nos besoins. Il en résulte que nous avons privilégié les fonctions annexes de l'antivirus (fréquences des mises à jour, facilité d'administration, options) à sa « fiabilité ».

Une présentation sur les antivirus a été réalisée au cours de la troisième séance.
Ceux-ci mis en place par les équipes installation et maintenance lors des deux semaines suivantes (selon les attaques reçues).

5.1.4) Politiques Sécurité

Pour cette partie, nous nous sommes concentrés sur les politiques de sécurité.
Dans un premier temps, l'objectif a été de définir cette notion ainsi que les éléments qui s'y rattachent. En effet, la principale difficulté rencontrée a été de comprendre ce que devait être une politique de sécurité : les informations étant nombreuses, il a fallu retenir les plus pertinentes.

Ensuite, nous avons listé les points susceptibles de faire l'objet d'une politique de sécurité. Pour définir cette liste, nous avons regardé tout ce qui pouvait faire l'objet d'une politique de sécurité, et qui souvent semblait être trop évident pour en faire l'objet.

Enfin, nous avons apporté une politique claire pour chacun de ces points. Nous nous sommes basés sur les articles du SANS, ou encore créer ses propres politiques, cette partie a nécessité une concertation avec tous les autres membres de l'équipe.

5.2) INST

5.2.1) Partie Système

5.2.1.1) Le serveur mail-dns-active directory

L'installation du serveur mail-dns-active directory s'est déroulée comme suit :
- Installation du serveur Windows 2000 Serveur avec mises à jour SP3 (nécessaire à l'installation de Exchange 2003)
- Installation de Echange 2003 sans mise à jour
- Activation du serveur DNS
- Activation de l'Active Directory
- Création des comptes utilisateurs
- Paramétrage simple du DNS (serveur web ajouté en « www »)

- Activation des services pop, imap, smtp et webmail
- Création d'une image de l'installation en cas de corruption de l'installation par l'équipe attaque

Après s'être assuré que le serveur fonctionnait correctement (accès aux services mails, DNS), nous avons installé stunnel (version 4.05) afin de sécuriser l'accès à distance par vnc. Le schéma de fonctionnement est simple. Lorsqu'on veut accéder au serveur par vnc, on crée un tunnel sécurisé en faisant s'adresser le vnc-client à un port local écouté par stunnel. Celui-ci contacte le stunnel installé sur le serveur. Lorsque les échanges et les vérifications de clés de cryptage se sont bien passés, le tunnel créé fait passer les communications entre le vnc-client et le vnc-serveur. L'utilisation d'un tunnel sécurisé est totalement transparente pour vnc.
Nous avons eu quelques problèmes pour la mise en place de cette solution car les clés générées initialement pour le client et le serveur ne fonctionnaient pas dans la maquette. Une fois générée une même clé pour le client et le serveur, le système fonctionnait correctement.

L'installation s'est déroulée entièrement déconnecté de tout réseau afin de garantir le bon déroulement de l'installation. Lorsqu'une connexion réseau était nécessaire, le serveur était installé sur un réseau protégé par un firewall.
La dernière étape a été l'installation du serveur au sein de la maquette.

5.2.1.2) Le serveur Web-FTP

L'installation du serveur Web-FTP s'est déroulée comme suit :
- Installation minimale de Windows 2000 Serveur
- Activation des services Web et FTP
- Installation des dossiers utilisés par le Web et le FTP dans une autre partition que le système
- Création d'une image de l'installation en cas de corruption de l'installation par l'équipe attaque

Le serveur est configuré avec un compte administrateur local et les comptes du domaine auquel il appartient. Un compte anonyme était également présent pour le serveur FTP.
Il dispose également de vnc mais sans stunnel. Son accès à distance passe donc forcément par un rebond à partir du serveur mail.

Après quelques tests de bons fonctionnements, le serveur a été intégré au sein de la maquette.

5.2.1.3) Le client XP

Le poste client XP a été installé sans aucune mise à jour publiée depuis sa sortie.
Les comptes pour accéder à cette machine étaient initialement ceux du domaine auquel il appartenait. Suite aux problèmes rencontrés lors de l'installation du firewall, des comptes locaux à la machine ont été créés afin de garantir l'accès au client.
Ce poste est, comme le serveur mail, équipé de stunnel+vnc afin que l'équipe exploitation puisse simuler à distance l'utilisation par un utilisateur (navigation web, utilisation du mail,…).

5.2.1.4) Le Firewall

L'installation du firewall s'est déroulé comme suit :
- Installation d'une distribution Linux (Debian 3.0)
- Installation du paquetage Iptables
- Installation du serveur ssh afin de pouvoir configurer le firewall à distance
- Mises à jour de tous les paquets afin de garantir une meilleure sécurisation
- Mises en place de règles de filtrage adaptées

S'en est suivi une période de tests afin de valider les règles établies.

N'ayant pas réussi à mettre en place les règles nécessaires à l'utilisation de l'Active Directory derrière le firewall, et cette architecture ne correspondant pas à une architecture réelle (l'AD n'est jamais derrière un FW), il a été décidé d'abandonner l'utilisation de l'Active Directory par le client XP.

5.2.2) Partie Réseaux

Pour ce projet de sécurité réseau, l'architecture que nous allions choisir été primordiale pour le bon fonctionnement de la maquette. Nous avions le choix de l'architecture, mais certaines contraintes devraient être respectées : pour sortir de notre réseau local notre passerelle qui serai assimilable pour notre maquette a « l'extérieur » serait Cooper, la machine de M Latu. Le choix de notre réseau interne était à notre convenance.

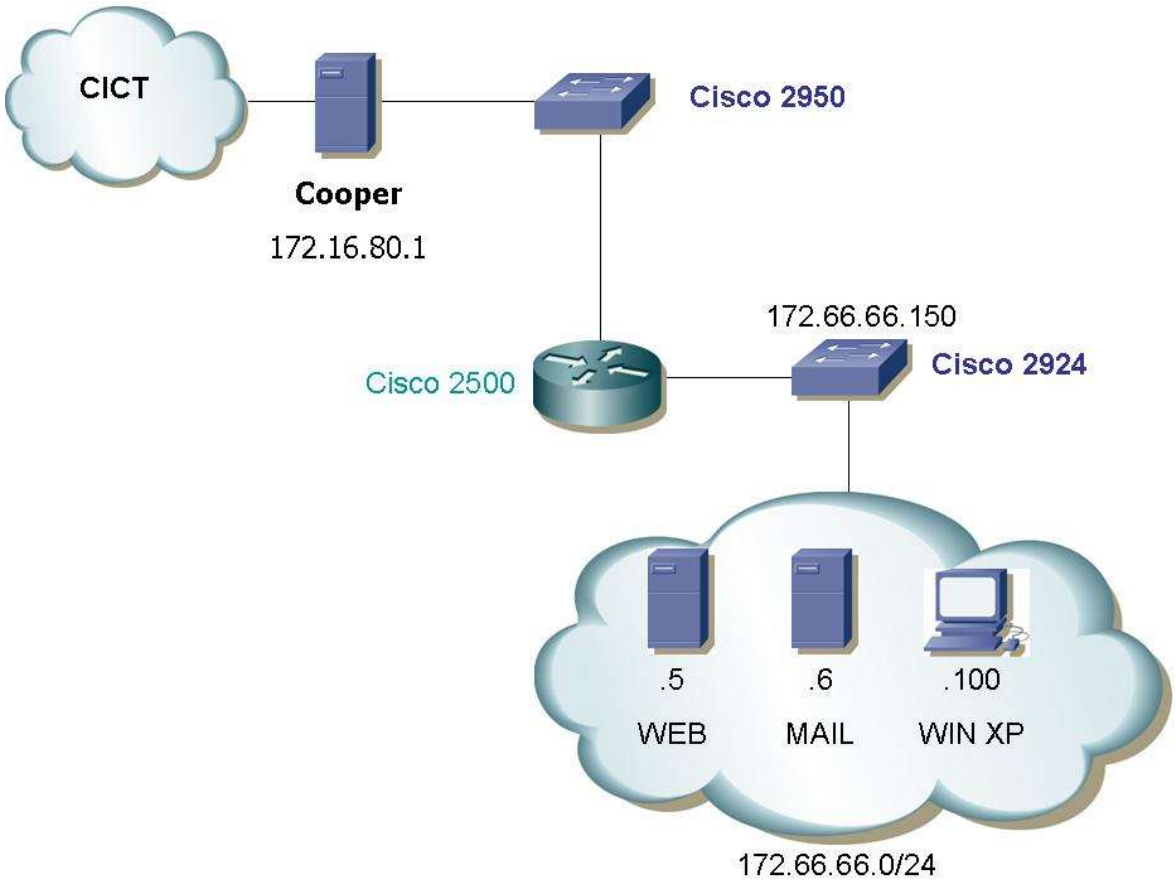
5.2.2.1) Architecture Etape 1

La première maquette est une maquette très simple et très peu sécurisée pour pouvoir permettre de mettre en évidence les failles d'une architecture faible.

5.2.2.1.1) Matériel utilisé

Pour cette architecture nous avons eu recours a un Routeur Cisco 2500 dont le rôle est d'assurer le routage entre notre réseau interne et l extérieur, et de deux switch Cisco 2924 un pour connecter notre routeur et Cooper et un autre pour nos 3 machines du réseau interne.

5.2.2.1.2) Schéma retenu



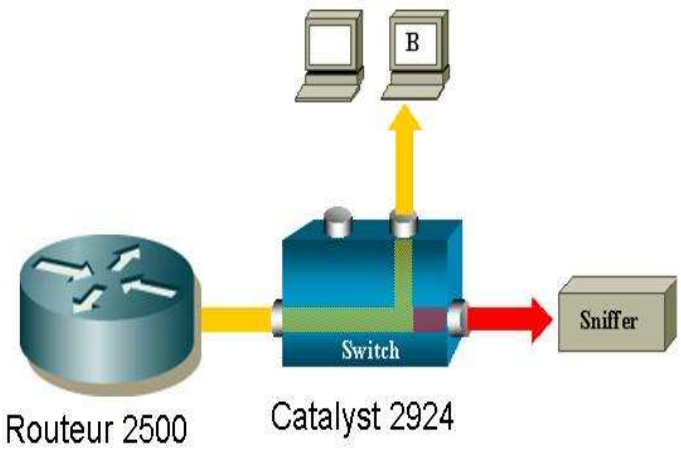
5.2.2.1.3) La mise en place

Nous avons tout d'abord effacé les précédentes configurations qui avaient été mises en place sur les différents équipements réseau (switchs et routeur) pour avoir une base de configuration seine. Nous avons ensuite implanté un switch Cisco 2950 sans aucune configuration spéciale. Sur ce switch nous avons branché Cooper et c'est aussi sur ce switch que vont se brancher les machines des attaquants. Ensuite nous avons configuré un des éléments clé de notre réseau le Routeur Cisco 2500 qui bien que d'une ancienne génération correspondra très bien à notre architecture. Ce routeur aura pour mission d'effectuer le routage entre le réseau 172.16.80.X /24de Cooper et notre réseau interne dont l'adresse arbitrairement choisie sera 172.66.66.0/24. Le 2500 aura pour passerelle par défaut Cooper pour sortir vers l'extérieur et le routage avec Cooper sera assuré par le protocole RIP Version2 (☹) Le routeur aura donc comme adresse 172.16.80.2 sur le réseau de Cooper et 172.66.66.1 sur le réseau interne.

Le reste de la configuration ne comporte rien de spécial elle est sécurisé comme celle de tous les équipements que nous avons mis en place sur la maquette :

- Mot de passe de login
- Mot de passe telnet
- Mot de passe Console
- Cryptage des mot de passe
- Désactivation de relais de messages ARP

Nous avons ensuite configuré le switch Cisco 2924 de notre réseau interne, nous lui avons attribué une adresse sur le réseau interne : 172.66.66.150 pour pouvoir l'atteindre et le configurer sans avoir à nous connecter en mode console. Le niveau de sécurité est le même que pour le Routeur tous les mots de passe sont activés et cryptés. Nous utilisons le Vlan1 qui est le vlan par défaut et tous les ports sont configurés sur ce Vlan. Il faut noter aussi que pour que l'équipe exploitation puisse recueillir les informations nécessaires nous avons dupliquer le port interconnectant le switch et le routeur grâce a la commande : « `port monitor` ».



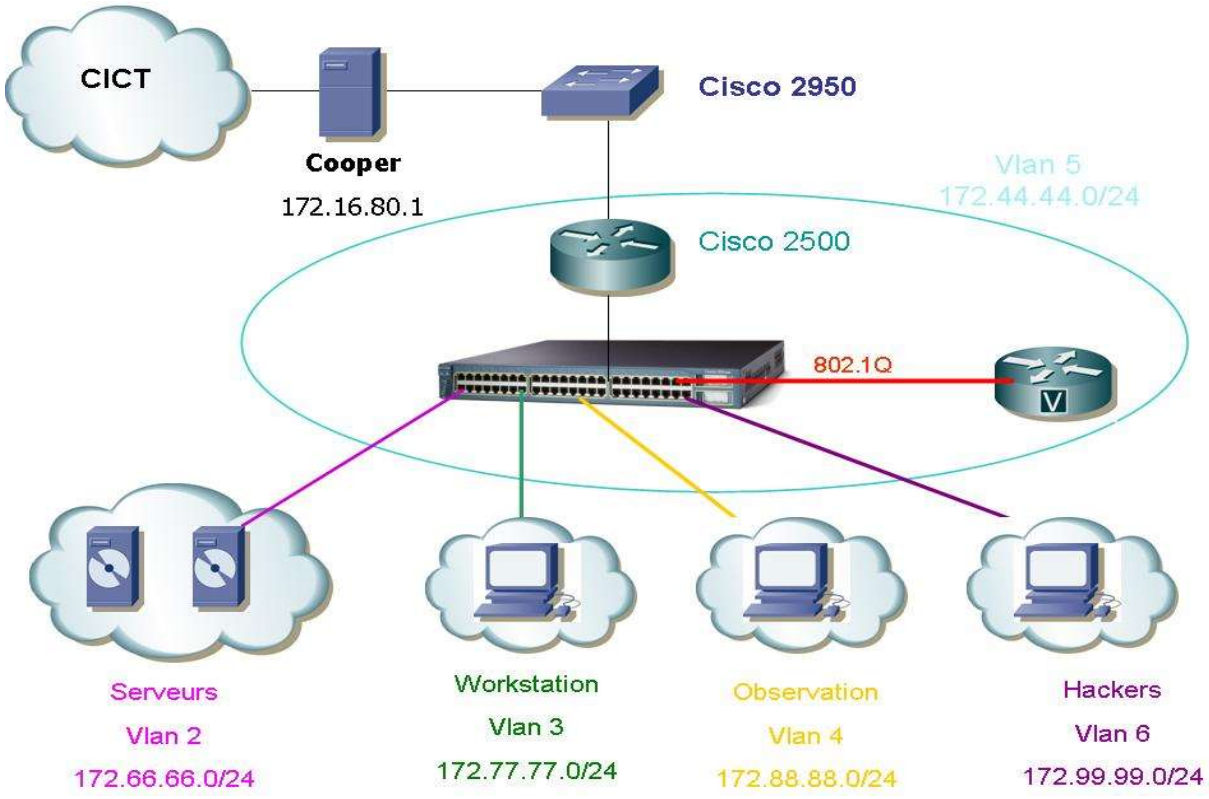
Ainsi tout le trafic entre notre réseau et le routeur 2500 été réplique sur le port de la machine Observation.

5.2.2.2) Architecture Etape 2

La seconde architecture a pour but de représenter une architecture plus réaliste se rapprochant d'une architecture d'une entreprise réelle. Pour répondre à ce besoin nous avons décidé de mettre en place une architecture s'appuyant sur des Vlan. Nous avons décidé de créer 5 Vlans.
-Un Vlan pour les équipements réseau le Vlan4
-Un Vlan pour les serveurs le Vlan3
-Un Vlan pour l'équipe observation
-Un vlan pour la Workstation
-Un vlan pour les hackers

Avec la création de ces Vlan, nous avons une segmentation des différents réseaux qui est proche de celle que l'on peut trouver dans une entreprise avec des Vlans pour les serveurs dans une DMZ et une segmentation des poste clients par services (comptabilité, administration..).Il conviens de noter aussi que nous avons introduis une machine contrôlées par l'équipe des hackers au sein même de notre architecture pour montrer qu'il est possible qu'une machine soit contrôlée dans l'entreprise et quelles peuvent en être les conséquences.
Pour cette architecture, nous n'avons en outre effectué aucun filtrage, les poste sont juste isolés par des vlans mais les flux transitent sans problèmes.

5.2.2.2.1) Schéma retenu



5.2.2.2.2) La mise en place

Pour la mise en place de ce réseau beaucoup de chose ont du être modifiée. C'est ici que s'est produit l'évolution de la maquette la plus importante. Toutes les adresses des postes de travail ont du être changés au prix de notre nouvel adressage.
Le routeur 2500 n'a pas subit de modification probante sur l'architecture, il est assimilable au routeur Internet de l'entreprise. Nous avons donc juste changé son adresse ip interne qui est passée a une adresse sur le réseau 172.44.44.0/24.Nous avons gardé le Routage effectué par du Rip V2 (☹).
Le switch 2924 a subit quand a lui des modifications importantes, nous avons crée tous les Vlans dans sa base de donnée et nous lui avons affecté une adresse sur le Vlan 4 qui sera le Vlan dédiée au équipement réseau pour ne pas risquer d'interférer avec les machines et pour sécuriser au maximum ces équipements. Ensuite nous avons attribués a chaque port le Vlan qui correspond à l'équipement branché dessus. Puis nous avons trunké le port 24 qui sera le port de communication inter vlan vers le routeur.
Pour effectuer ce routage entre les différents Vlans nous avons mis en place dans l'architecture un routeur Cisco 3620 capable d'effectuer ce type de routage. Le 3620 est connecté avec le switch sur un port en mode trunk ainsi tous les Vlans passe par ce port. Nous avons attribué au 3620 une adresse sur chacun des Vlans pour servir de passerelle de sortie a tous les équipements sur tous les Vlans. Par souci de simplicité et de communication, nous avons choisi la dernière adresse de chacun des Vlans soit « .254 ». On a donc 172.66.66.254 sur le Vlan2, 172.44.44.254 sur le 4 et ainsi de suite. Les machines mettent donc l'adresse du 3620 sur leur réseau comme passerelle de sortie pour atteindre les autres réseaux. Pour le routage extérieur nous avons utilisé du routage de type RIP Version2 entre le 2500 et le 3600 les routes se dupliquent ainsi jusqu'au Cooper qui permet la communication avec l'extérieur.
Pour la sécurité de la configuration du 3620, Nous avons mis en place tous les mots de passe et le login et en plus, nous avons rajouté pour chaque interface:
no ip proxy-arp qui désactive le relaye de messages ARP.
no ip redirects qui désactive l'envoi de messages ICMP Redirect.
no ip unreachables qui désactive l'envoi de messages ICMP Destination Unreachable.

Apres la mise en place de cette architecture l'équipe Observation a mis en place un serveur Syslog. Nous avons donc envoyés les logs du switch 2924 et ceux du 3620 sur leur serveur a hauteur d'un niveau assez faible grâce a la commande : « logging trap debugging ».

Pour l'équipe analyse nous avons remis le monitoring de port sur le port 24, celui de routeur 3620 pour qu'ils puissent a nouveau observer tout le trafic.

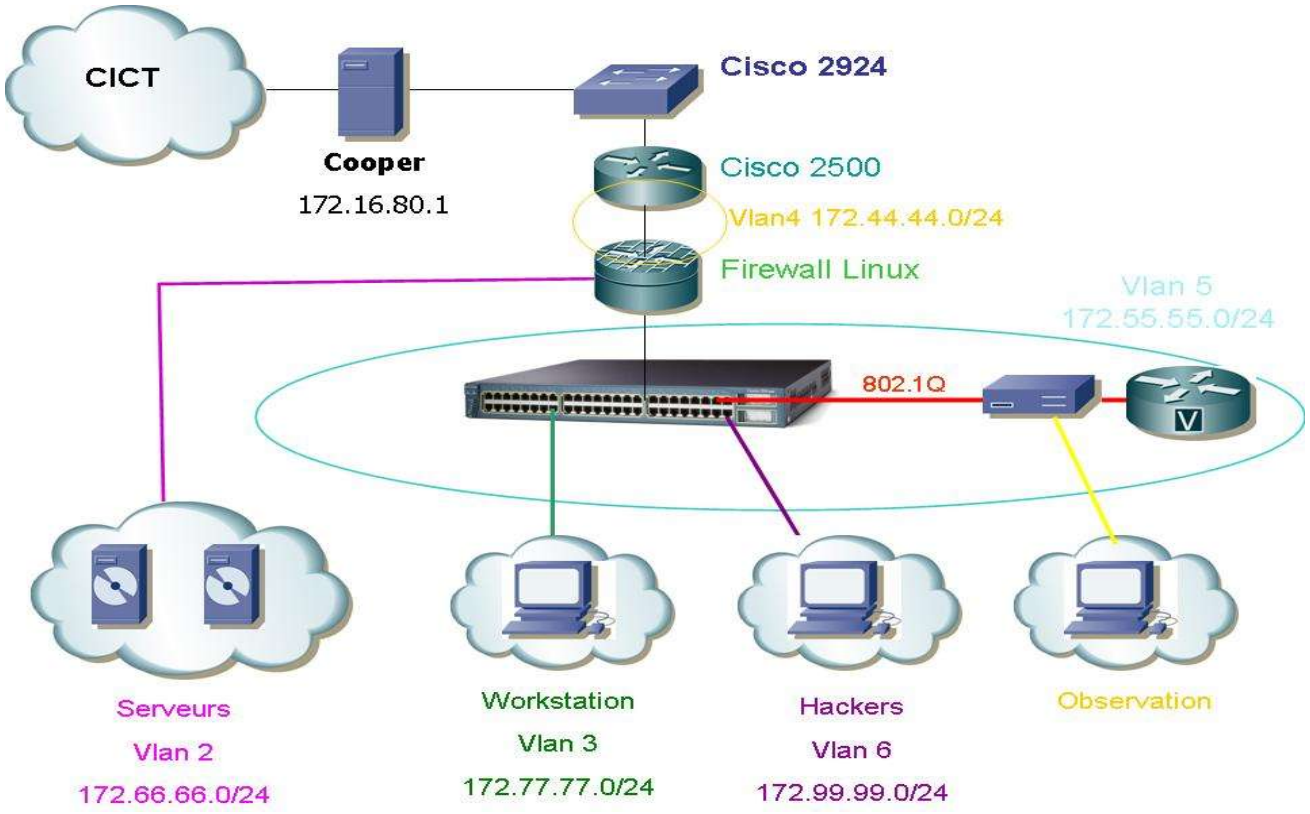
5.2.2.2.3) Problèmes rencontrés

Apres la mise en place de l'architecture, nous avons remarqué que la machine observation dédiée au monitoring du port 24 n'observais presque rien et pas de trames 802.1Q ce qui n'été pas normal. En réalité, le monitoring ne filtrais que les informations dédiée au port de la machine c'est-à-dire le Vlan4 et non pas les informations pour tous les Vlans comme prévu. Apres de multiples recherches, il s'est avérée qu'il est impossible de monitorer un port trunké ou différents Vlans en direction d'un autre sur un Catalyst 3620. Cette opération ne peut être effectué qu'avec des Châssis. Pour palier à ce problème, nous avons installé un hub entre le switch et le 3620 et branché une machine Observation dessus. Nous avons ensuite supprimé le Vlan4.

5.2.2.3) Architecture Etape 3 (initial)

Dans le but encore une fois de nous approcher le plus possible d'une architecture réaliste, nous avons décidé de séparer les serveurs sur une VRAI DMZ isolée du reste du réseau et contrôler les accès au réseau local grâce à Firewall évoluant sous linux. Nous avons ainsi une architecture très proche de celle d'une vrai entreprise avec Routeur Internet, Firewall, DMZ, et Vlan pour les workstations.

5.2.2.3.1) Schéma retenu



5.2.2.3.2) La mise en place

Pour le Firewall, nous nous somme procuré une nouvelle machine, avec 3 cartes réseau, sur laquelle nous avons installé un Distribution Debian. Au niveau réseau, nous lui avons attribué une adresse sur chacun des réseaux : Extérieur (172.44.44.0/24), DMZ (172.66.66.0/24), Interne (172.55.55.0/24). Au niveau du routage, le RIP V2 a été supprimé (☺) sur le 3620 et le Firewall assure le routage de façon statique ainsi que le NAT des adresses ip internes qu'il va Masquarade. Les redirections par ports ont été faites, ainsi une requête sur le port 80 envoie sur le serveur Web et une sur le 25 sur le serveur Mail. Apres nous n'avons pas mis en place de règles de filtrages particulières au niveau des iptables pour ne pas compliquer les choses.
Le Cisco 2500 a donc une nouvelle adresse interne sur le Vlan4 et continue d'utiliser le RIP V2 (☹) avec Cooper.
De son coté, le Cisco 3620 continue à assurer le routage inter vlan mais uniquement en interne puisque la DMZ est gérée par le Firewall.

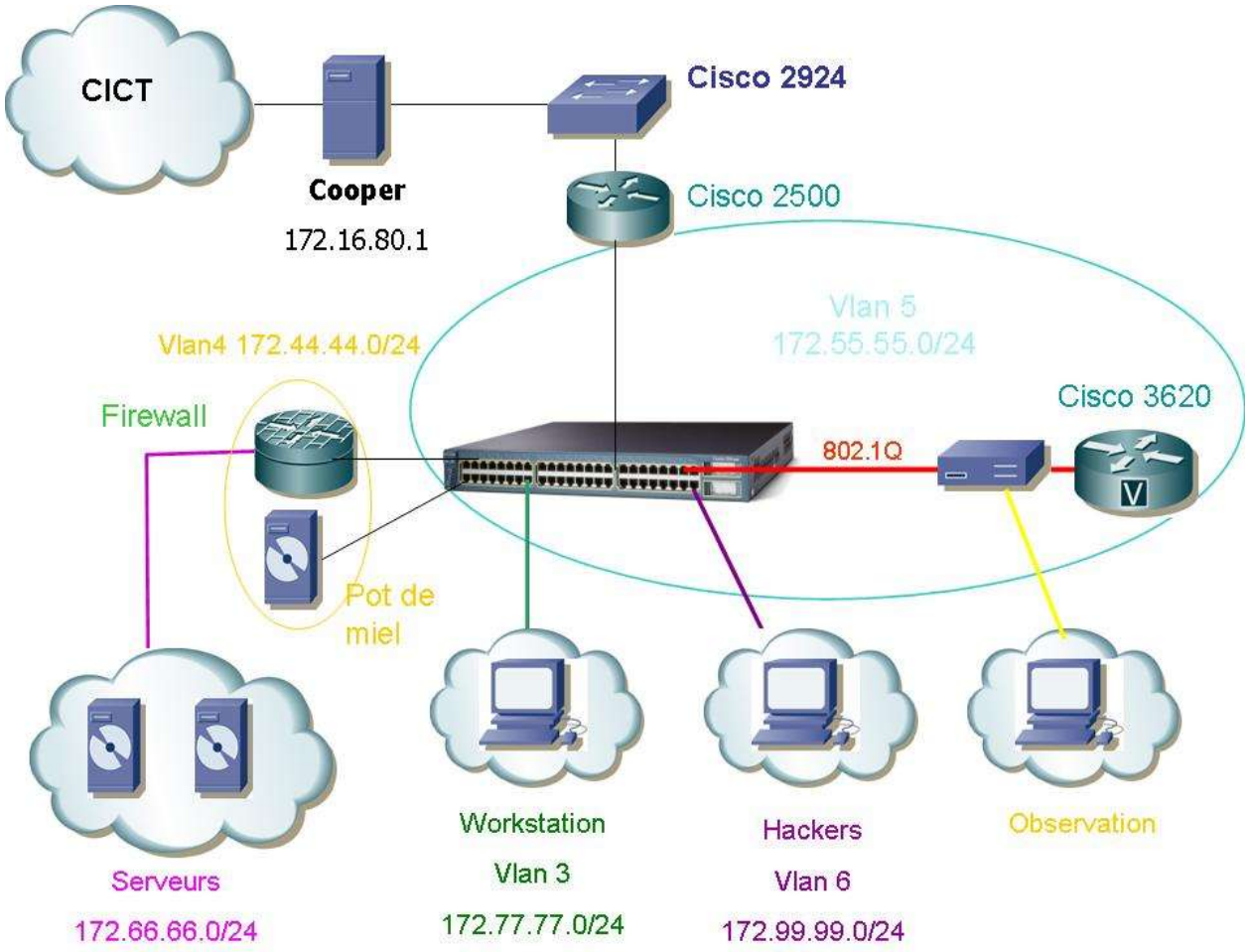
5.2.2.3.3) Problèmes rencontrés

Malheureusement, cette architecture ne s'est pas avérée concluante, en grande partie à cause des flux des autres groupes que nous ne maîtrisions pas (hackers et observation) et de tous les problèmes crées par la prise en main a distance sur les machines. Pour que cette architecture fonctionne il aurait fallu créer un nombre trop important de règles dans le Firewall pour permettre les accès et encore cela n'aurait pas garantie le bon fonctionnement. C'est pour cela que nous avons apporté une dernière modification à l'architecture de la maquette.

5.2.2.4) Architecture Etape 3 (réalisée)

Pour pallier aux problèmes rencontrés lors de la précédente architecture nous avons décidé de modifier notre maquette afin de permettre aux flux de traverser la maquette jusqu'au Workstation mais aussi de garder le Firewall, et en faire un Firewall de DMZ. Puis nous avons aussi conjointement a l'équipe observation ajouté un pot de miel (Honey pot) dans le Vlan4 du Firewall pour faire office d'appât.

5.2.2.4.1) Schéma retenu



5.2.2.4.2) Mise en place

Nous avons donc rebranché le Cisco 2500 comme il était initialement branché, c'est-à-dire directement sur le switch avec une adresse sur le Vlan5, le vlan des équipements réseaux. Puis nous avons réactivé le routage de type RIP Version 2 (☹) sur le 3620 qui communique donc les routes avec le 2500 qui les communique à Cooper. Nous avons ensuite branché le Firewall dans le Vlan4 qui lui était dédié et nous lui avons donné une adresse sur ce vlan ainsi que sur celui des serveurs. Il assurera donc le routage entre le vlan serveur et le Vlan4. De la même façon que précédemment le NAT a été mis en place avec des redirections de ports pour les services adéquats et une pour permettre la prise en main a distance. De plus nous avons ajouté sur le Valn4 un pot de miel géré par l'observation qui est la réplique exacte de nos serveurs sans aucune sécurité pour attirer les abeilles malveillantes.
Cette architecture fonctionne à l'heure actuelle sans aucun problème.

5.2.2.5) Conclusion partie Réseaux

L'évolution de l'architecture réseau c'est fait au fil des semaines avec une montée en puissance significative de la sécurité. Nous somme parti d'une architecture très simpliste avec un seul routeur pour arriver a une architecture multi vlan avec un routeur, un routeur inter vlan et un Firewall qui route aussi. Ce fut très intéressent pour nous de voir a quel point l'évolution du réseau vers une architecture sécurisée est difficile à mettre en place et a maintenir mais nous avons vu aussi que cette dernière architecture est aussi bien isolé contre les attaques.

5.3) EXPL

L'équipe d'exploitation avait en charge la surveillance du bon fonctionnement de la maquette, son exploitation d'un point de vue utilisateur ainsi que de son évolution au cours des différentes étapes.

5.3.1) Surveillance

Le travail de surveillance consistait à passer régulièrement sur les différentes stations pour regarder les journaux et tenter de déceler des traces d'attaque ou tout comportement anormal. Cette partie a révélé la limite de Windows à effectuer un traçage efficace des évènements. Ce travail a été effectué pendant les séances de TP. L'équipe analyse a fournie régulièrement des rapports qui nous ont permis de savoir ce qui s'était passé et ainsi en déduire ce que Windows n'avait pas vu. Le travail de mise à jour des stations découlait de ces rapports.

5.3.2) Simulation

Ensuite, la simulation du comportement d'utilisateurs lambda se faisait en accès distant via Stunnel et VNC. Cette phase avait pour objectif de générer du trafic récupérable par l'équipe d'analyse et celle d'attaque (en partie). Il s'agissait de consulter les mails (avec d'éventuels virus) comportant des pièces jointes à ouvrir. Ensuite, il fallait naviguer un peu sur Internet et simuler une activité pendant la tranche horaire allant de 21h à 0h.

L'équipe d'exploitation a aussi assisté l'équipe attaque au cours des tentatives afin de coordonner de façon plus efficace nos efforts. L'expérience la plus significative fut la tentative d'inondation de requêtes ARP. Le but était de faire passer une des machine de l'équipe attaque comme le serveur DNS. Ainsi, l'utilisateur, depuis son poste XP, tente d'accéder à www.google.fr. La requête DNS est alors dirigée vers le poste de l'équipe attaque ayant usurpée l'adresse de notre DNS. Elle renvoi au poste XP l'adresse IP de leur machine qui présente une page Internet totalement erronée, alors que la page de Google aurait du s'afficher. Cette attaque a été suivit. Sa réussite fut partielle puisque l'inondation fut efficace mais pas la redirection vers la page erronée.

5.3.3) Maintenance

Enfin, les configurations ont du évoluer au cours des séances. Des comptes utilisateurs on été crées sur le poste XP. :

administrateur (droits maximum)
Mathieu (droits limités)
Benjamin (droits limités)
STRI (droits limités)

Ces comptes se sont vu associé des comptes mails avec pour adresses respectives :

mathieu.begue@defense
benjamin.guillot@defense
stri@defense

Apres la mise en place de l'active directory sur notre réseau, ces comptes ont été supprimés pour bénéficier des comptes active directory. Chaque membre de l'équipe défense a obtenu un compte selon ce schéma : prenom.nom pour la session et prenom.nom@defense pour l'adresse mail.
Les mots de passe associés furent harmonisés au passage toujours en suivant le schéma de l'active directory. Ces comptes sont donc utilisables sur tout machine du réseau.

Enfin, les mises à jour logicielle ont principalement été les changements d'adresses IP suivant les configurations mise en place aux différentes étapes. L'antivirus a été mis en installé en fin d'étape puisqu'il inhibait toute attaque virale des le départ, ce qui ne correspondait pas à l'optique du projet.

6) Taches et réalisation de COO

6.1) Externe

Le but est de coordonner les efforts entre les groupes Attaques / Défense / Analyse pour éviter les dérapages du projet, les attaques à outrance ou le blocage complet de la sécurité de la défense.

Principales démarches :

Mise en place dans chaque groupe d'un coordinateur dédié à la communication intergroupe.
Synchroniser le départ des attaques
Faire en sorte que l'Analyse valide son système d'audit, et le cas échant, aider à la mise en place opérationnelle de l'architecture d'Analyse.
Définir des plages d'attaque fixes pour ne pas surcharger le travail d'Analyse.
Faire un 'reporting' auprès de la défense pour lui faire partager la vision de l'avancement global du projet.
Arriver à faire avancer le projet sans faire d'infogérance dans les autres groupes.
Mettre en place des utilisateurs 'lambda' : Définir les moyens de communications inter-équipe et les disponibilités.
Synchroniser les attaques entre Attaquant et Défenseur, superviser ces attaques en cas de problèmes, le but étant d'arriver à l'autonomie de l'organisation Attaquant-Utilisateur.

Continuer à informer les autres équipes (Attaque et Analyse) de l'évolution de l'architecture de la maquette et de sa répercution sur leurs machines.
Sélectionner et faire passer l'information pertinente aux autres équipes.

Elément clef dans le déroulement du projet, ce travail a permis d'avancer concrètement. Quelques difficultés ont été rencontrées quant à savoir si les requêtes effectuées par les autres groupes sont acceptables, ou non, ou bien encore, quant à définir les informations pertinentes à communiquer aux autres groupes.
En conclusion, la réussite de ce travail n'aurait pu avoir lieu sans la participation et le remarquable travail de coordination des autres équipes.

6.2) Interne

Je vais essayer de lister toutes les taches liées à la coordination que j'ai réalisé. Pour chacune d'elle, je m'efforcerai de donner un commentaire.

6.2.1) Gestion de projet :

- Proposition et mise en place du système d'étape : Le système d'étape a déjà été expliqué lors de l'introduction.
- Proposition et mise en place du brainstorming de connaissance.
- Proposition et mise en place du système d'équipe : Le système d'équipe a déjà été expliqué dans la partie distribution des rôles.
- Proposition, mise en place et maj du planning : Le planning a déjà été explique dans la partie planning.
- Gestion de “l'intendance” : J'entends par là que je me suis préocupé que les personnes de l'équipes aillent bien le bon matériel ou logiciel le jour nécessaire afin de les décharger de ces taches et améliorer leur productivité.
- Mise en place de la triade “programme de réunion” – “réunion” – “compte rendu de réunion” : Toutes les semaines cette triades a été mise en place afin de garder une cohérence entre le travail des équipes du groupes et afin de les faire participer au décisions.
- Mise en place de debriefing d'étape : Le but est que toute les personne du groupe comprenne bien ce qui vient de ce passé lors de la mise en place de la nouvel étape. Ici encore le but est de garder tout le monde concerné par le projet.
- Création des diagramme étape de la maquette : Ces diagrammes nous ont été fort utile lors des phases de mise en place (fourni en annexe).
- Mise en place du travail à faire : J'ai précisé pour chaque semaine et chaque équipe le travail qu'il avait à réaliser.
- Proposition du plan du rapport et coordination liée à la réalisation de ce dernier.

6.2.2) Management du groupe :

- Animation et motivation du groupe : Cette tâche consiste à motiver les gens lorsqu'ils sont face à des problèmes et essayer de les aider. Par animation, j'entend l'animation de la liste et des réunions.
- Aménagement et Encouragement d'une utilisation intensive de la liste : J'ai aménagé la liste afin que chaque équipe aille son répertoire “personel”. Considérant que la communication permetrait de nous faire gagner en productivité, j'ai poussé tout le monde à utiliser le plus possible la liste et moi en premier (Il suffit de regarder le nombre de message poster sur la liste...).
- Encadrement des équipes : Le but était que chaque équipe se rende compte qu'il y avait quelqu'un derrière pour les pousser à travailler mais aussi les aider en cas problèmes.
- Gestion des conflicts : J'ai essayé de calmer les tensions dans le groupe au travers notemment de modération sur la liste, etc...
- Rappel à l'ordre : J'ai du faire des rappels à l'odre pour les gens qui ne travaillais pas afin de les remotiver et de les faire avancer dans le projet.

- Mise en place d'un bilan de projet au sein du groupe. : Ce bilan a pour but de nous faire tirer les enseignement à tout niveau de ce projet.
- Responsabilisation et leading sur le projet : Difficile à définir si ce n'est que j'ai participé à toutes les décisions et j'ai essayé de leader le projet de la meilleure mainière pour le faire aboutir.

6.2.3) Renfort technique

Participation technique sur les étapes critiques suivantes :

- Etape 1 : Aide à la mise en place et configuration des équipement réseau et des accès distants.
- Etape 2 : Aide à la mise en place et configuration des équipement réseau.
- Etape 3 : Mise en place des règles de FireWall avec l'aide de Mr Latu.

7) Bilan

Pour écrire ce bilan, nous avons commencer par réaliser un bilan de projet. Nous nous sommes assis autours d'une table et nous avons discuté des points positifs et négatifs de ce projets. Nous ne rentrerons pas ici dans des conclusions ni techniques ni organisationnelles mais nous nous intéresserons de façon plus large au projet dans son ensemble.

Ce qu'il résulte de cette réunion, c'est qu'il aurait été intéressant qu'au départ, les groupes soient plus pris en charge notemment au travers de certaines figures imposées et de certains conseils tant organisationnel que technique.

Il aurait été également intéressant que à chaque scéance, chaque groupe présente en 5min les actions effectuées durant la semaine afin de garder la cohésion et la synchronisation entre les groupes.

D'autre part, dans l'intéret du projet, nous avons jugé inutile, les tentatives de monter les groupes les uns contre les autres. En effet, si les groupes ne travaillent pas main dans la main, ce projet ne peut aboutir.

En ce qui concerne les problèmes techniques, les accès distants sont un problèmes assez délicat à traiter et récurent tout le long du projet.

Concernant nos regrets, nous pensons que nous n'avons pas eu assez de scéances de cours. Nous déplorons le fait (sans accuser aucunement l'équipe Attaque) que nous n'avons finalement pu rebondir que sur un nombre restreint d'attaques réussies. Une aide plus importante auprès de l'équipe Attaque serait peut-être à prendre en considération.

En ce qui concerne notre organisation, avec le recul, il aurait été préférable de prévoir seulement 2 étapes afin de ne pas remettre en cause à chaque fois l'architecture,ce qui à posé des problèmes aux 2 autres groupes.

Il n'en demeure pas moins que ce projet est un excellent projet probablement un des meilleurs que nous aillons eu l'occasion de réaliser lors de notre formations. Les points forts sont les libertés tant organisationnelles que techniques qui sont laissées aux étudiants. Pour résumé, nous pensons qu'il faut bien evidemment garder cette liberté tout en l'encadrant un peu plus afin d'éviter les dérives.

Annexes

Politique de Sécurité

Antivirus

Procédure Antivirus - Définit les directives pour réduire efficacement la menace de virus informatiques sur le réseau de l'organisation.
Directives sur les Procédures Antivirus

Processus recommandés pour empêcher des problèmes viraux :

- Toujours utiliser le logiciel antivirus standard disponible sur le site de téléchargement de l'entreprise. Télécharger et exécuter la version actuelle; télécharger et installer les mises à jour du logiciel antivirus quand ils sont disponibles.
- Ne jamais ouvrir les fichiers ou macros attachés à un email d'une source inconnue, soupçonneuse ou douteuse. Supprimez ces pièces jointes immédiatement, et supprimez les définitivement en vidant la corbeille.
- Supprimer les Spams, les chaînes et autres messages suspects sans retransmission.
- Ne jamais télécharger les fichiers provenant de sources inconnues ou douteuses.
- Eviter le partage de disque en accès lecture/écriture sans une autorisation spéciale.
- Toujours scanner à l'antivirus une disquette d'une source inconnue avant son utilisation.
- Sauvegarder régulièrement les données critiques et la configurations de système sur un support et dans un lieu sur.
- Si une utilisation entre en conflit avec le logiciel antivirus, exécuter l'antivirus afin de s'assurer que la machine est saine, désactiver le logiciel antivirus, et exécuter le travail. Une fois effectué, activer le logiciel antivirus. Quand le logiciel antivirus est désactivé, ne pas exécuter d'applications qui pourraient amener un virus (email ou partage de fichier par exemple).
- De nouveaux virus sont découverts presque chaque jour. Vérifier périodiquement la *Politique Antivirus* et la liste de procédures recommandées pour les mises à jour.

Messagerie

Politique d'utilisation de la messagerie

But

Eviter de ternir l'image de la compagnie, quand les messages sortent de l'enceinte de la compagnie, en effet, le grand public aura tendance à interpréter ces messages comme des messages reflétant la politique de la compagnie.

Couverture

Cette politique décrit l'utilisation appropriée de tous les messages envoyés par une adresse de la compagnie et s'applique à tous les employés, commerciaux, et techniciens au service de l'entreprise.

Politique

Utilisation proscrite.

Le système de messagerie de la compagnie ne doit pas être utilisé pour la création ou la distribution d'un quelconque message offensant ou diffamant, ceci incluse les propos offensant au sujet de la race, le genre, les cheveux, la couleur, les incapacités, l'age, l'orientation sexuelle, la pornographie, la religion, la politique ou les origines. Les employés qui reçoivent un message avec ce type de contenu envoyé par un employé de la compagnie doivent immédiatement rapporter ce problème à leur supérieur.

Utilisation personnelle.

L'utilisation raisonnable des ressources de la compagnie pour des messages personnels est acceptable, mais ces messages à caractère non productif devront être stockés dans un répertoire séparé des messages à caractères professionnels. L'envoi de chaîne ou de plaisanterie par l'intermédiaire de la messagerie de la compagnie est interdit. Ces restrictions s'appliquent aussi au transfert de messages reçus par un employé de la compagnie.

Surveillance

Les employés de la compagnie ne doivent pas s'attendre à un quelconque caractère privé de leur stockage, envoi, ou réception de message. La compagnie peut surveiller tous les messages sans aucune justification préalable. La compagnie n'est pas tenue de surveiller tous les messages.

Sanctions

Un employé pris en violation de cette politique peu faire l'objet d'une sanction disciplinaire allant jusqu'à la rupture de son contrat.

Mots de passes

Politique des mots de passe

1.0 Vue générale

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of <Company Name>'s entire corporate network. As such, all <Company Name> employees (including contractors and vendors with access to <Company Name> systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Les mots de passe sont un aspect important de la sécurité informatique. Ils sont la première protection pour les comptes d'utilisateur. Un mot de passe mal choisi peut aboutir au compromis du réseau entier de l''entreprise <Nom entreprise>. Comme tel, tout les employés <de Nom de compagnie> (incluant les entrepreneurs et les vendeurs avec l'accès aux systèmes de < Nom de compagnie >) sont responsables de réaliser les étapes suivantes et de sécuriser leurs mots de passe.

2.0 Objetif

L'objectif de cette politique est d'établir un standard pour la création de mots de passé compliqués, pour la protection des mots de passe et pour la fréquence de changement.

3.0 Portée

La portée de cette politique inclus tout le personnel qui a ou est responsable d'un compte (ou de toute forme d'accès à des supports nécessitant un mot de passé) sur tout système résidant à <Nom de la Compagnie>, qui a accès au réseau de <Nom de la compagnie> ou stockant des informations non publiques.

4.0 Politique

4.1 Générale

.

- Tous les mots de passe de niveau de système (par exemple : racine, NT admin, etc) doivent être changés sur au moins une base trimestrielle.
- Tous les productions de mots de passe de niveau système de production doivent faire partie de

la base de donnée InfoSec.

- Tous les mots de passe de niveau utilisateur (par exemple : email, web, bureau,etc.) doivent être changés au moins tous les six mois. L'intervalle recommandé est tous les quatre mois.
- Les mots de passe ne doivent pas être transmis par email ou par toute autre forme de communication électronique.
- Lorsque SNMP est utilisé, les login et mots de passes par défaut ne doivent pas être utilisés.
- Tout les mots de passe de niveau utilisateur et de niveau de système doivent se conformer aux directives décrites ci-dessous.

4.2 Directives

A. Directives générales de Construction de Mot de passe

Les mots de passe sont utilisés à différentes fins à <Nom de la compagnie>. Certains des usages communs sont inclus : comptes de niveau utilisateur, comptes web, comptes mail, protection de l'écran de veille.

Puisque très peu de systèmes utilisent des mots de passe jetables) (c'est-à-dire, les mots de passe dynamiques qui sont seulement utilisés une fois), chacun devrait être conscient de la façon de choisir des mots de passe forts.

Des mots de passe pauvres, faibles ont les caractéristiques suivantes :

- Le mot de passe a moins de 8 caractères.
- Le mot de passé est un mot du dictionnaire (toutes langues)
- Le mot de passe est du type usage commun :
- Nom de famille, surnom, amis, collègue, etc.
- Termest et noms d'ordinateur, commandes, sites, entreprises, hardware, software.
- Les mots "<Company Name>", "sanjose", "sanfran" ou toute dérivation.
- Anniversaires ou toute autre information personnelle comme une adresse ou un numéro de telephone.
- Les mots ou les numéros (nombres) comme aaabbb, qwerty*
- N'importe lequel des mots précédés ou suivis par un chiffre (par exemple, secret1, 1secret).

Les mots de passe forts ont les caractéristiques suivantes :

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]: ";'<>?,./)
- Are at least eight alphanumeric characters long.
- Ils contiennent des majuscules et des minuscules (par exemple, a-z, A-Z),
- Ils contiennent des chiffres et des caractères de ponctuation aussi bien que des lettres par exemple, 0-9! *$ % ^* * () _ + | ~-= \ ` { } [] : "; ' < > ?./) ·
- Ils ont au moins huit caractères alphanumériques,
- Ils ne sont pas un mot dans aucune langue, argot, dialecte, jargon, etc ·

- Ils ne sont pas basés sur des informations personnelles, les noms de famille, etc
- Les Mots de passe ne devraient jamais être notés ou stockés en ligne. Essayer de créer les mots de passe dont il est facile de se souvenir. Une façon de le faire est de créer un mot de passe basé sur un titre de chanson, l'affirmation, ou d'autre expression. Par exemple, l'expression pourrait être : "cela Peut Être Une Façon de Se souvenir" et le mot de passe pourrait être : "cpE1F2s!" ou une autre variation.

NOTE: Ne pas utiliser les mots de passé cites en exemple !!

B. Password Protection Standards

Ne pas utiliser les meme mots de passe pour les comptes de la société <Nom compagnie> et les comptes personnels. Où cela est possible, n'utilisez pas le même mot de passe pour des besoins d'accès divers de <de Nom de compagnie>. Par exemple, choisissez un mot de passe pour les systèmes Techniques et un mot de passe séparé pour des systèmes d'information. De même, choisissez un mot de passe séparé pour un compte de NT et un compte UNIX.

Ne partagez les mots de passe <de Nom de compagnie> avec personne, y compris avec des aides administratifs ou des secrétaires. Tous les mots de passe doivent être traités comme sensibles et Confidentiels.

Voici une liste d'interdictions :

- Ne reveler à personne un mot de passé par telephone
- Ne pas reveler un mot de passé par mail
- Ne pas reveler un mot de passe au patron
- Ne parler d'un mot de passe devant personne
- Ne faites pas allusion au format d'un mot de passe (par exemple, "mon nom de famille")
- Ne revelez pas un mot de passe sous forme de questionnaire
- Ne partagez pas un mot de passé avec des member de votre famille
- Ne révélez pas de mot de passe aux collaborateurs pendant vos vacances

Si quelqu'un exige un mot de passe, referez le à ce document ou appelez quelqu'un du Département de la Sécurité Informatique.

N'utilisez pas la fonction "Se rappeler du Mot de passe" dans les applications.

Ne notez pas de mots de passe et ne les stockez pas n'importe où dans votre bureau. Ne stockez de mots de passe dans un fichier sur AUCUN système informatique (incluant des Palm Pilots ou des dispositifs semblables) sans chiffrage.

Changez de mot de passe au moins tous les six mois

Change passwords at least once every six months (sauf les mots de passe de niveau de système qui doivent être changés tous les trimestres). L'intervalle de changement recommandé est tous les quatre mois.

Si un compte ou un mot de passe sont soupçonnés d' avoir été compromis, annoncer l'incident à InfoSec et changer tous les mots de passe.

Si un mot de passe est deviné ou piraté l'utilisateur doit le changer.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the <Company Name> Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms Definitions

Application Administration Account Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

FireWall

Politique de modification des règles de filtrage du FireWall

But

Pour éviter de dégrader les relations entre employés à l'intérieur de la compagnie. Toute modification des règles de filtrage au niveau du FireWall devra respecter la politique suivante.

Couverture

Cette politique décrit les procédures à effectuer lors de l'ajout, du retrait ou de modification de règles de filtrage sur le FireWall. Elle s'adresse aux administrateurs du réseau informatique.

Politique

Ajout, suppression ou modification de règle.

Toute modification ne pourra être réalisée qu'en accord avec son équipe et son supérieur, la seule exception restant l'ajout d'une règle temporaire (voir plus loin). Une fois la règle clairement définie, l'ensemble des utilisateurs du système devront être mis au courant de l'intervention sur le FireWall au moins une journée à l'avance.

Règle temporaire.

En cas d'impératif précis et temporaire (virus exploitant une nouvelle faille pouvant être bloquée par l'ajout d'une règle), et si cela n'entraîne pas de gêne majeur pour le système, les administrateurs sont autorisés à mettre en place des règles de filtrage rapidement. Ils devront tout fois en référer dans la journée à leur supérieur.

Référencement.

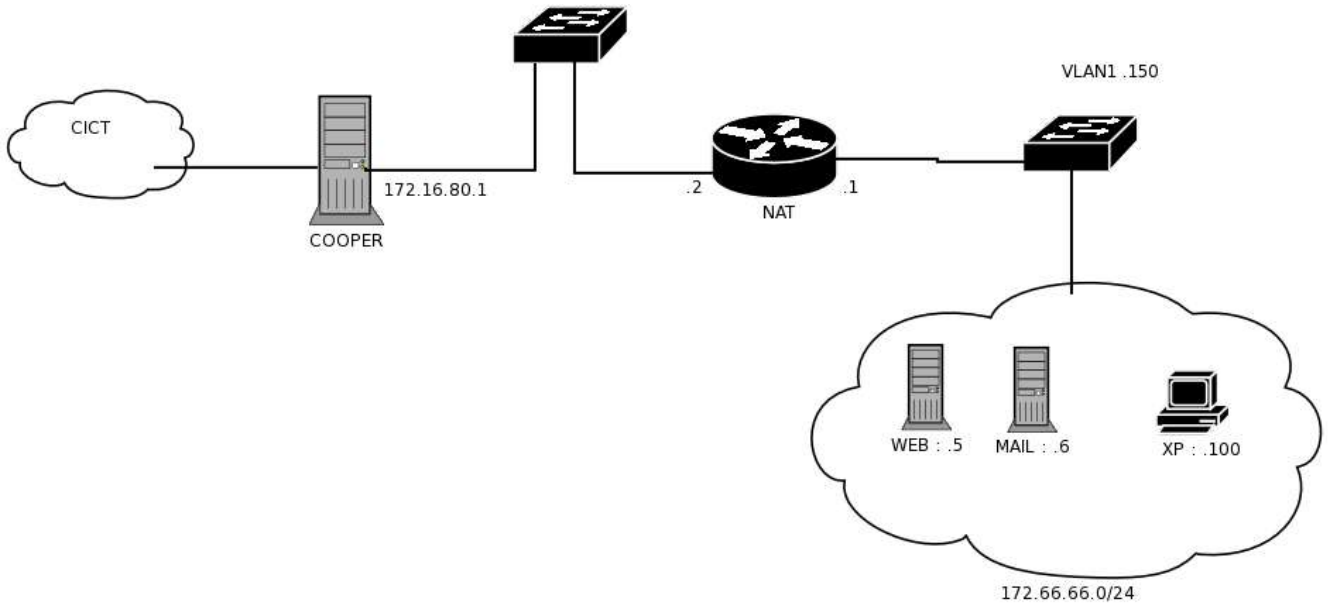
Toute modification devra être référencée dans l'espace réservé à cet effet par la compagnie.

Tests.

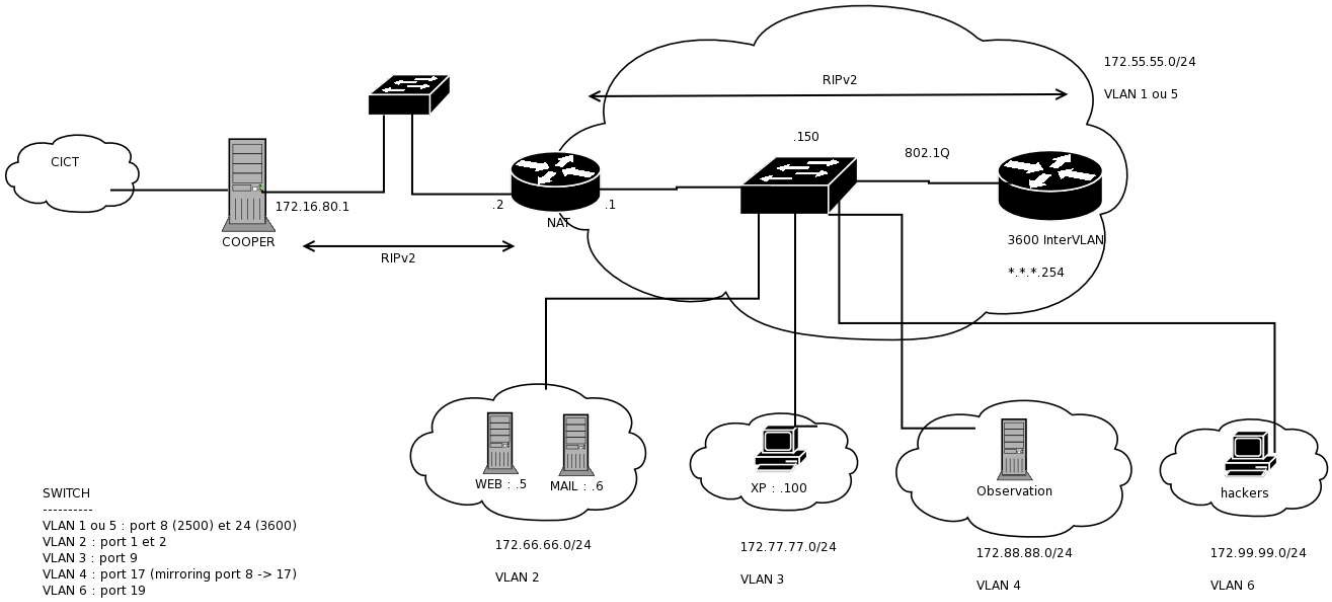
Avant la mise en place d'une règle de filtrage 'critique', risquant d'engendrer de lourdes conséquences sur l'utilisation du système, une maquette de test devra être mise en place, et l'utilisation courante du système devra être testée.

Diagrammes Reseaux produits par la COO Interne

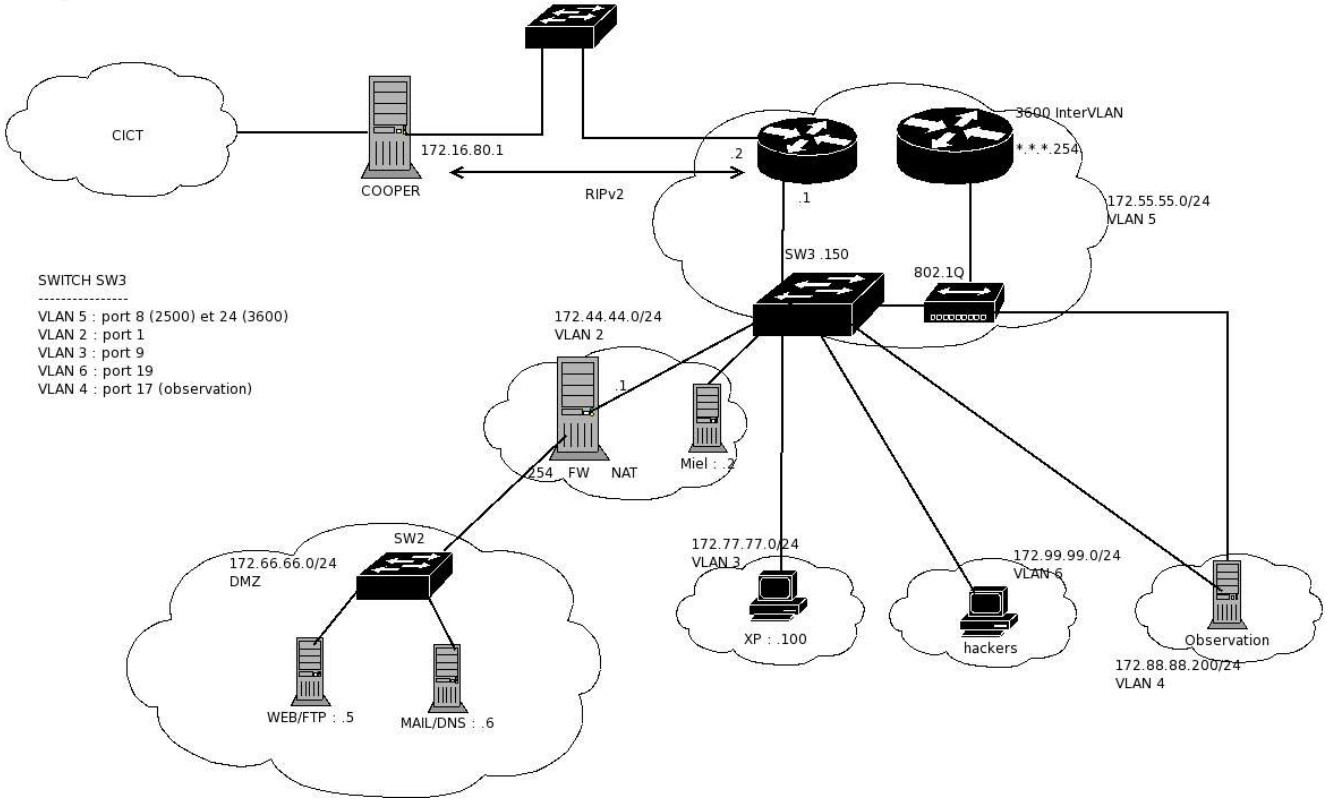
Etape 1



Etape 2



Etape 3


CICT
COOPER
172.16.80.1
RIPv2
.2
.1
3600 InterVLAN
..*.254
172.55.55.0/24
VLAN 5
SW3 .150
802.1Q
SWITCH SW3
VLAN 5 : port 8 (2500) et 24 (3600)
VLAN 2 : port 1
VLAN 3 : port 9
VLAN 6 : port 19
VLAN 4 : port 17 (observation)
172.44.44.0/24
VLAN 2
.1
.254 FW NAT
Miel : .2
SW2
172.66.66.0/24
DMZ
WEB/FTP : .5
MAIL/DNS : .6
172.77.77.0/24
VLAN 3
XP : .100
172.99.99.0/24
VLAN 6
hackers
Observation
172.88.88.200/24
VLAN 4