Sécurité d'un système d'information groupe défense

Benjamin Aguila
Cindy Candiago
Ibrahim Manroufou
Nordine Medjadj
Marc Moisand
Romain Montoya
Christophe Ortiz
Laurent Perarnaud
Yannick Poirier
Julien Puntus
Pierre Quentel
Peno Heriniaina Rajaonarison
Enrique Renard
Nicolas Robert
Lionel Rouvellat
Charlie Salvan
Willy Wong

SOMMAIRE

1. PRÉSENTATION DU PROJET

L'objet de ce projet de sécurisation d'un système d'information d'une entreprise est de diviser la promotion en différents groupes ayant chacun un rôle bien définit.

- **Groupe attaque** : Ce groupe est chargé de rechercher toutes les possibilités d'intrusion et de compromission les plus efficaces et les plus faciles à mettre en œuvre. Ils sont totalement étrangers à la structure de l'entreprise. Les 2 autres groupes ne sont pas sensés leur communiquer la moindre information. Bien entendu, les membres du groupe «attaque» ne doivent pas se limiter aux moyens techniques pour collecter leurs informations.

- **Groupe analyse :** Ce groupe est chargé de collecter un maximum d'informations et de les analyser pour identifier les actions entreprises aussi bien en défense qu'en attaque. Au début du projet, ils sont étrangers à la structure de l'entreprise. Par la suite, ils ne disposent que des informations et/ou des accès que leur fournissent les membres du groupe «défense».

- **Groupe défense :** Ce groupe est chargé de mettre en place l'infrastructure des services du scénario d'entreprise. Il doit rechercher les moyens les plus simples possibles pour se défendre contre les tentatives d'intrusion et de compromission entreprises par le groupe «attaque».

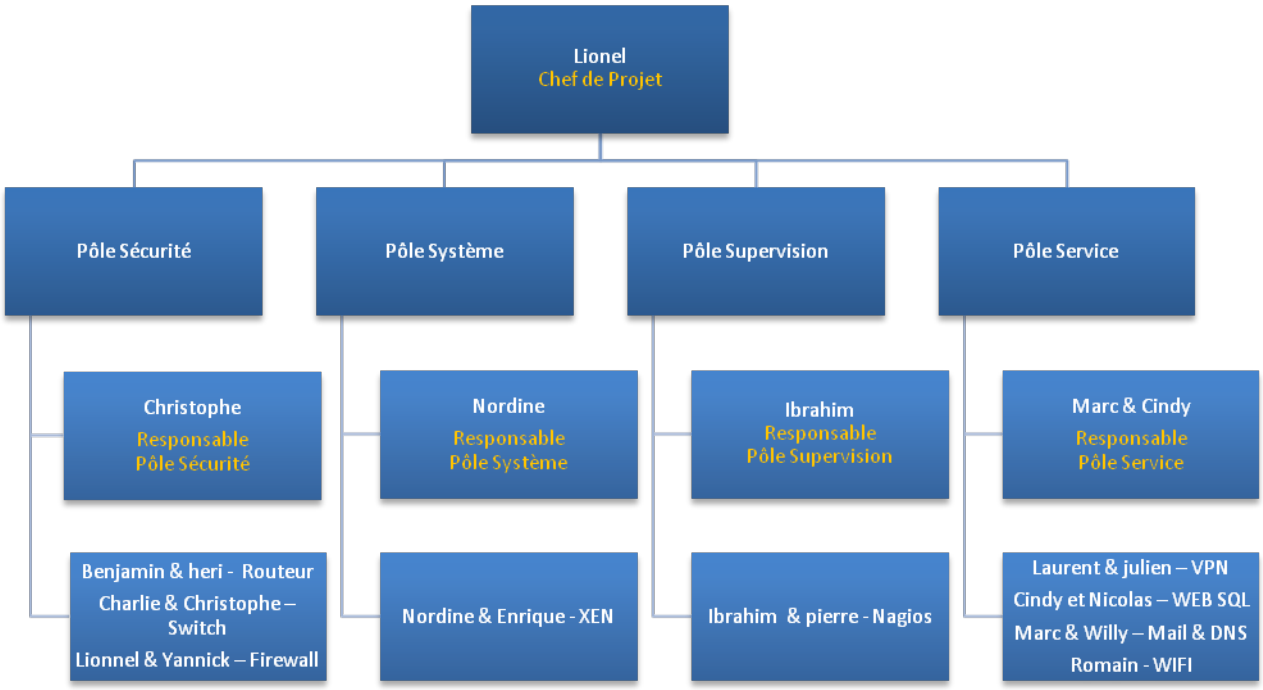
Chaque équipe s'est vu attribuer le matériel informatique nécessaire pour mener à bien son projet. Nous étudierons par la suite les moyens informatiques mis à notre disposition. De même chaque équipe a obtenu un accès sécurisé VPN afin de pouvoir réaliser les opérations le concernant. Enfin une mailing list a été mise à disposition pour que chaque groupe puisse correspondre de manière efficace.

2. ORGANISATION DE L'EQUIPE DEFENSE

Comme énoncé ci-dessus l'équipe défense s'est vue attribuer le rôle de mettre en place un système d'information complet et sécurisé, se rapprochant au plus d'un cas de figure d'une entreprise classique. Nous avons découpé le projet en différentes phases dont nous prendrons soin de détailler par la suite.

2.1 Les différents membres

2.1.1 Organigramme



2.1.2 Chef de projet

Son rôle est de s'assurer du bon déroulement du projet :

- Coordination de l'équipe
- Communication avec les différents membres de son équipe
- Communication avec le manager de l'équipe audit
- Etablissement des deadlines et des jalons

2.1.3 Responsable de pôle

Son rôle est tout d'abord de faire le lien avec le chef de projet :

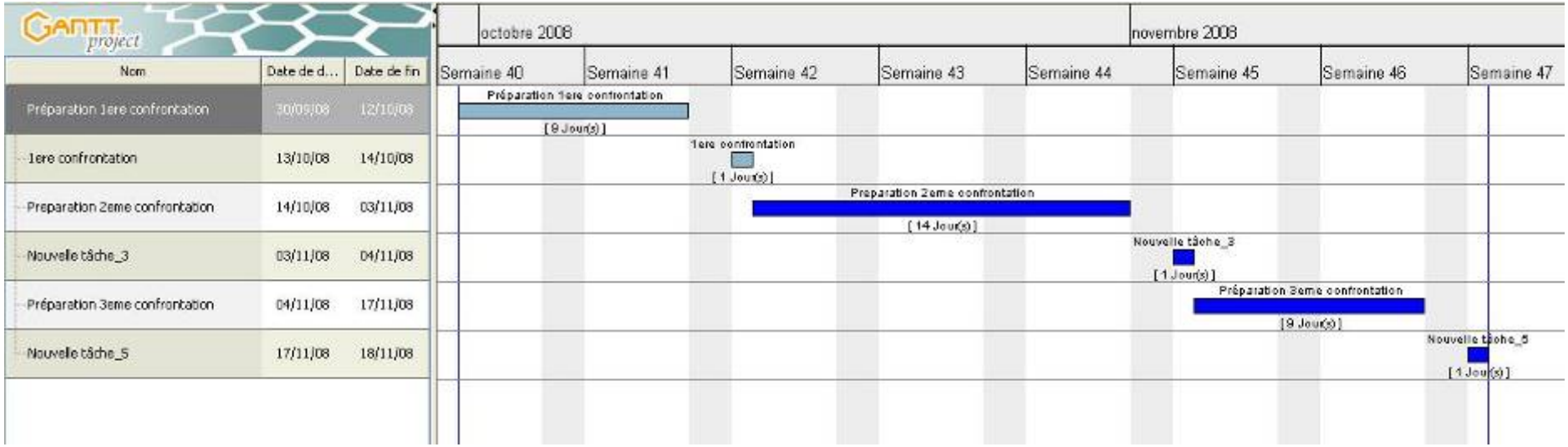
- Orienter les choix techniques en termes de sécurité
- Coordonne les activités des techniciens de son équipe
- Communique l'avancement du projet au chef de projet
- Rédige des comptes rendus périodiques

2.1.4 Technicien

Son rôle est de mettre en place l'architecture du système d'information :

- Mise en place des différents services
- Configuration des postes clients
- Configuration des serveurs

2.2 Déroulement du projet



2.3 Les différentes confrontations

Ce projet se déroule sur une durée de 8 semaines, sur ces 8 semaines 3 confrontations sont prévues. A chacune des confrontations l'architecture réseau évolue, et les moyens techniques mis en place par l'équipe attaque afin de pénétrer dans le système d'information sont de plus en plus importants.

2.3.1 Première confrontation

La première confrontation est représentative d'une situation classique d'attaque d'entreprise : les attaquants se situent à l'extérieur et tentent de compromettre notre architecture et de provoquer des dénis de services.

Nous nous sommes donc concentré sur la paire Routeur / Switch comme la base de notre architecture, sur notre premier service : le serveur WEB SQL et sur les postes clients virtualisés. Un groupe a aussi commencé ses recherches en parallèle sur le thème de la supervision avec comme objectif l'implémentation de Nagios à la deuxième confrontation.

2.3.2 Deuxième confrontation

Pour la deuxième confrontation un système de supervision Nagios est mis en place afin de surveiller certains points de notre architecture. De plus un serveur DNS est mis en place et un système de hot spot wifi sera accessible.

2.3.3 Troisième confrontation

Pour la troisième confrontation un firewall est mis en place, il assura la protection du parc client ainsi que du serveur de supervision. Le serveur mail est mis en place afin que les clients puissent contacter la société Candide-SA.

3. LA PREMIÈRE CONFRONTATION

Cette étape a eu pour but de mettre en place l'organisation en termes de hiérarchie dans le projet mais aussi en termes de planification du projet, et de choix techniques.

3.1 Réunion de lancement du projet

Une première partie du projet a été l'élaboration des groupes de défense, d'attaque et d'audit. Une fois le groupe constitué, il a été nécessaire de définir le périmètre d'action de chacun des membres du groupe.
A la suite de cette répartition des tâches, nous avons pu prendre un premier contact avec l'équipe d'audit afin d'organiser la communication entre nos deux équipes et de leur présenter une esquisse de notre première architecture.
Pour plus d'informations sur cette réunion cf. annexes.

3.2 Le travail collaboratif

Lors de cette première réunion le point du travail collaboratif pour la rédaction du rapport a était abordé. En effet la liste de diffusion mise à disposition ne permet pas la rédaction et le « versionnage » des différents documents postés.
Afin de remédier à cela nous avons décidé d'utiliser l'outil « Google Docs » qui permet de rédiger et de modifier des documents depuis une plateforme Web.
Pour cela il était nécessaire que tous les membres du groupes se crée une adresse électronique de type GMAIL. Une adresse type à donc était définit pour tous les membres du groupe prenom.stridef@gmail.com.
Pour plus d'information sur cet outil cf. annexes.

3.3 Négociation du contrat avec l'équipe analyse

Un premier échange a eu lieu avec les membres de la communication de l'équipe d'audit. Ceci nous a permit d'établir les grandes lignes du contrat afin qu'il réponde au mieux aux attentes que nous avions vis-à-vis de leur équipe.
De plus cette réunion a aussi permis de définir les droit que nous allions laisser aux membres de cette équipe ainsi que les endroits ou nous les autorisions à placer leurs sondes.

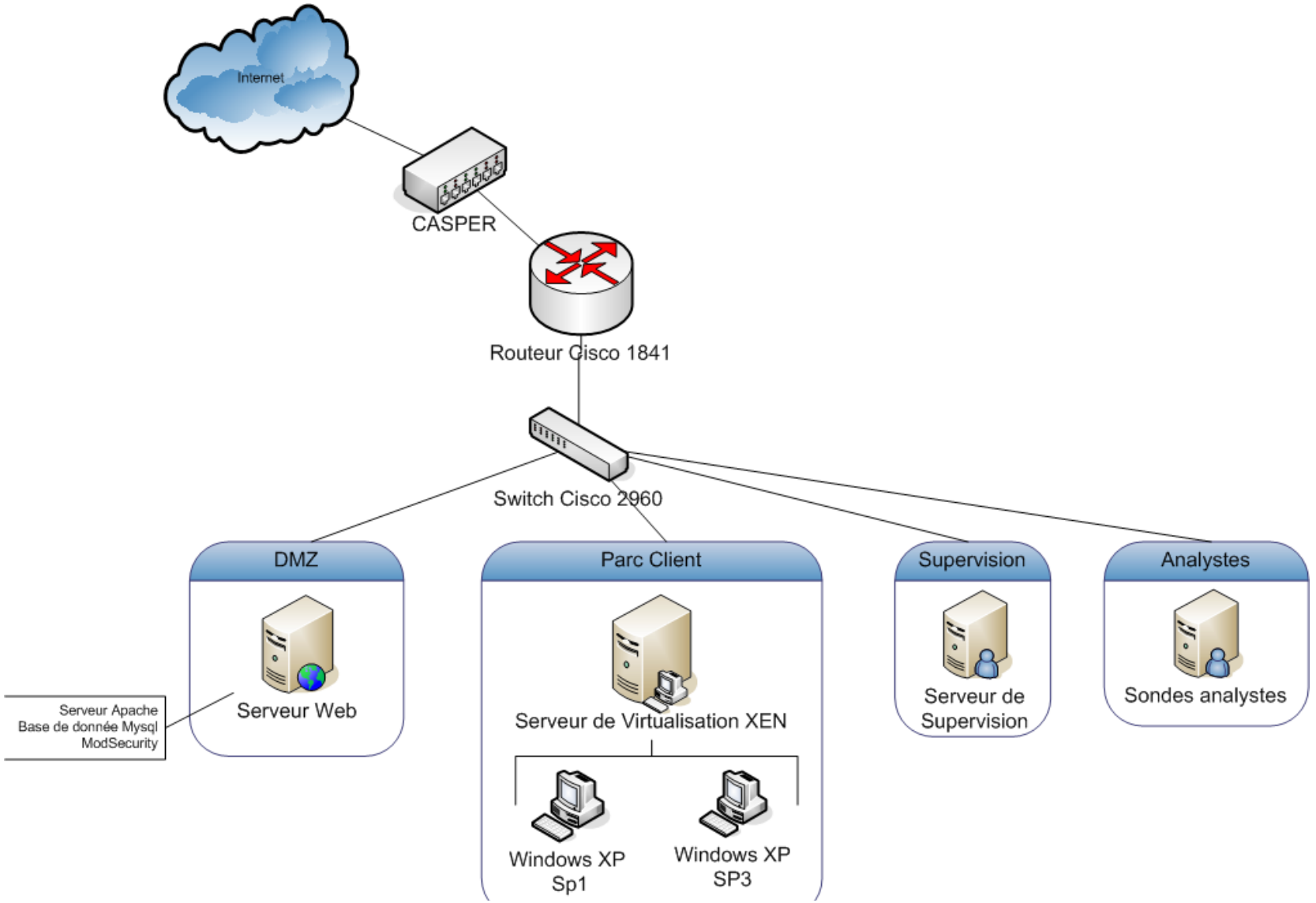
Lors d'une la seconde réunion l'équipe audit nous a fournit le contrat rédigé. De notre coté nous leurs avons fait signer à tous les membres de l'équipe analyse une clause de confidentialité permettant de définir les droits de chaque utilisateurs et de nous protéger en cas de non respect des termes de ce contrat.
Pour plus d'information sur le contrat et la clause de confidentialité cf annexes.

3.4 Architecture mis en place pour la première confrontation

Lors de la première réunion une architecture de base avait était définit, par la suite après les réunions et les négociations avec l'équipe analyse, certaines modifications ont étaient réalisées.

3.4.1 Schéma

Afin de mettre en place une architecture, il nous était mis a disposition un routeur et un Switch CISCO pour les équipements réseaux et des machines afin d'héberger nos différents services.


Internet
CASPER
Routeur Cisco 1841
Switch Cisco 2960
DMZ
Serveur Web
Serveur Apache
Base de donnée Mysql
ModSecurity
Parc Client
Serveur de Virtualisation XEN
Windows XP Sp1
Windows XP SP3
Supervision
Serveur de Supervision
Analystes
Sondes analystes

3.4.2 Présentation

Comme nous l'avons vue précédemment un routeur et un Switch CISCO étaient à notre disposition afin de mettre en place un système d'information complet. Pour la première confrontation il nous était demandé de mettre en place une architecture minimale comportant un Switch un routeur avec un service web accessible depuis l'extérieur et un parc de machines XP.
Sur ce parc de machine XP l'une de ces machines devait être mise à jour (SP3+antivirus), et l'autre devait simuler une machine à la dérive (SP0 sans antivirus). Etant donné la limitation en nombre de machine, nous avons choisi d'utiliser un système de virtualisation afin de d'héberger les deux machines clientes.
Afin de délimiter des périmètres de sécurité, et de diviser notre architecture réseau en fonction des domaines d'applications, nous avons décidé de mettre en place des VLANs sur le Switch. Nous expliquerons en détails tous ces choix dans la suite de ce rapport.

3.5 Politique de sécurité

Explication
Implémentation
Connexion avec live CD
Création d'un compte expliquée en 3.2
Signature des membres de l'équipe défense

3.6 Le Routeur

Lors de cette première confrontation nous nous somme limités à gérer la connectivité des hôtes du réseau et à sécuriser l'accès au routeur.

3.6.1 Liaison trunk :

La liaison « trunk » entre le routeur et le commutateur est rendu possible par la déclaration de sous-interfaces qui correspondent chacune à un Vlan de l'entreprise Candide. Typiquement :

```
interface FastEthernet0/1.6
encapsulation dot1Q 6
```

La déclaration de l'encapsulation dot1q (norme IEEE 802.1q) suffit pour que le routeur soit en mesure faire du routage inter-Vlan.

3.6.2 Gestion des accès au routeur :

Il est indispensable de limiter l'accès au routeur, pour ne pas se faire voler, corrompre ou détruire la configuration du routeur. La NSA suggère les commandes suivantes :

```
service password-encryption
```

Ainsi que :

```
transport input ssh
transport output ssh
```

3.6.3 NAT :

Dans un premier temps, nous avons choisi ne traduction d'adresse statique pour diriger les requêtes HTTP externe vers l'adresse interne du serveur web. La traduction d'adresse statique correspond à l'association d'une adresse externe à une adresse interne. Par la suite, la traduction d'adresse dynamique a été mise en place pour autoriser l'accès à Internet des postes du réseau local. Le NAT dynamique est la traduction d'un ensemble d'adresses internes dans un petit ensemble d'adresses externes. Ici on autorise les machines de la liste 10 à être NAT sur l'interface externe :

```
ip nat inside source list 10 interface FastEthernet0/0 overload
```

Pour autoriser une machine dans la liste 10 :

```
access-list 10 permit 172.10.200.6
```

Et pour autoriser un réseau :

```
access-list 10 permit 172.10.160.0 0.0.0.7
```

Enfin, il faut que chaque sous-interface interne soit configurée pour faire du NAT :

```
ip nat inside
```

Et sur l'interface extérieure :

```
ip nat outside
```

Pour accéder, depuis l'extérieur, aux services Web de l'entreprise il faut aussi ajouter des translations statiques. Dans le cas présent on devait autoriser, entre autre, les flux HTTP & HTTPS :

```
ip nat inside source static tcp 172.10.140.2 80 172.18.4.2 80 extendable
ip nat inside source static tcp 172.10.140.2 443 172.18.4.2 443 extendable
```

3.6.4 ACL :

Nous avons choisi de limiter l'accès à notre réseau en le restreignant aux requêtes HTTP, HTTPS, SSH en entrée du réseau. Mais suite à quelques problèmes, il nous a été demandé de se contenter seulement du NAT pour cette première confrontation.

3.7 Le Switch

3.7.1 Choix du niveau de VLAN

Nous avons choisi de faire nos vlan par ports car cela présentais le double avantage sécurité/simplicité : En effet la configuration faite pouvais demeurer jusqu'à la fin du TP alors qu'avec un de niveau 2, il aurait fallu intégrer toute les nouvelles adresses mac en cas de changement de machine ou de carte réseau. Egalement écarté, les Vlan de niveau 3 était trop risqué dans le cas des usurpations d'IPs : alors qu'avec les Vlan par ports, un attaquant doit ce recâbler physiquement pour communiquer avec les autres Vlans.

```
--Commandes pour créer un VLAN :
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name LAN
Switch(config-vlan)# end
```

3.7.2 Administration du Switch

L'administration du Switch à commencé par le port console par lequel nous avons pu faire la configuration et sécurité de base et l'accès SSH. Une fois cet accès implémenté le port console à été désactivé pour plus de sécurité.

3.7.3 Accès à distance SSH

Cet accès nécessite de déclarer une interface sur le Switch, de l'assigner à un Vlan et de lui déclarer une adresse IP.

```
-- Déclarer une interface d'administration à distance
Switch# configure terminal
Switch(config)# interface vlan 5
Switch(config-if)# ip address 172.10.170.2 255.255.255.248
Switch(config-if)# end
```

Le protocole SSH version ayant été reconnu pour avoir des failles. Nous avons choisi d'implémenter le protocole SSH_V2.

3.7.4 Mode des ports : « ACCES / TRUNK ».

- Le mode « Trunk » permet de transmettre des informations VLAN entre commutateurs. Dans notre cas le routeur est connecté au switch par un port Gigabit en mode trunk, Ce qui permet au routeur de recevoir les communications de tout les VLANs. Il peut ainsi effectuer les opérations de filtrage et routage.

- Le mode « Accès » permet de limiter la vision des communications au seul Vlan auquel le port appartient.

- Le mode « Span » a été implémenté pour les analystes et permet de « mirrorer » ce qui se passe sur un port vers le port en mode SPAN. Cet option a permis d'envoyer au groupe analyse les flux traversant notre architecture vers leur sonde, leur permettant de faire de l'analyse du trafic.

3.7.5 Politiques de sécurité.

La politique de sécurité défini au début de notre étude nous oblige à implémenter :

- Mot de passe fort (avec caractères, chiffes, caractères spéciaux)
- Des Mot de passe crypté (`password encryption aes`)
- Des mots de passe différents pour les connexions en SSH et pour la prise en main du switch.
- Désactivation des accès non sécurisé :
  - `Switch(config)# no ip http server`
  - `Switch(config)# no ip http secure-server`
  - **L'accès au switch via telnet est aussi désactivé**.

3.8 Le parc informatique

3.8.1 Choix de la virtualisation

La virtualisation nous a apporté un certain nombre d'avantages sur ce projet :

- Nombre de machines utilisées limité
- Remise en service rapide après un incident (évite perte de temps)
- Simuler un parc de machine visualisé (en développement dans les entreprises).
- Optimiser la sécurité en centralisant sur une machine hôte

Nous avons choisi d'étudier les trois principales solutions de virtualisation pour PC clients qui sont VMware, VirtualPC et XEN.
Notre choix c'est porté sur la solution XEN pour diverses raisons que nous allons vous présentés par la suite. (Pour plus d'information sur les autres technologies CF annexes)

3.8.2 La solution XEN

XEN est un « paravirtualiseur » ou « hyperviseur » de machines virtuelles, c'est à dire que les systèmes invités ont « conscience » de sa présence. Les systèmes d'exploitation invités doivent être modifiées (« portées »).
Dans le cadre de l'émulation de postes clients Windows, la présence de processeurs Intel intégrant la technologie VT (Virtualization Technology) nous permet d'installer des OS Windows « normaux ».
La distribution supportant Xen sont les suivantes : Red Hat, projet Fedora, SuSE, Mandriva, Ubuntu Linux, Debian, Gentoo et Arch Linux.

- Avantages
  - performance (pas de pile protocole sur une autre pile protocole), l'une des solutions de virtualisation les plus efficaces en termes de temps de réponse.
  - Exploitation des possibilités des processeurs VT des machines de TP.
  - License GPL (pas de limitations en termes de taille de disque simulé, de RAM simulée,…comme sur les versions gratuites de VMware ou VirtualPC).
  - Contrôle d'accès sHype/Xen pour autoriser ou refuser la communication et l'accès aux ressources.
- Inconvénients
  - Difficulté d'installation et de configuration de XEN

3.8.3 Installation et configuration de XEN

L'installation de Xen se fait en 3 étapes :

- Installation du système Hôte
- Installation du Noyau Xen
- Installation des outils de contrôle de Xen
- Installation des machines clientes

Pour plus d'informations sur l'installation et la configuration de XEN cf annexes

3.8.4 Configurations des machines clientes

	Poste 1	**Poste 2**
OS	Windows XP SP0	Windows XP SP3
ANTIVIRUS	Aucun	AVG Antivirus
FIREWALL	Aucun	Firewall XP
IP	172.10.150.2	172.10.150.3
MASQUE	255.255.255.248	255.255.255.248
PASSERELLE	172.10.150.1	172.10.150.1
DNS	172.16.4.1	172.16.4.1

Sur chaque machine nous avons :

- créé un utilisateur simple ayant les droits utilisateurs (user1 et user2)
- créé un compte administrateur (client)
- mis un mot de passe pour le bios
- configuré IE en niveau élevé
- mot de passe doit respecter des exigences de sécurité
- compte verrouillé après 5 tentatives d'ouverture de session non valide

En ce qui concerne la reprise sur incidents, si un problème persiste lors d'une confrontation nous avons décidé de cloner le disque dur afin que le temps d'interruption soit le plus petit possible. Nous avons en plus de cloner le disque dur fait une sauvegarde de tous les fichiers de configurations afin que les services puissent redémarrer le plus vite possible.

3.8.5 Bilan 1ere confrontation

Lors de la première confrontation, le groupe attaque nous a demandé d'accéder à une adresse web (http://stri-attaque.ifrance.com), sur cette adresse web se trouvait leurs consignes. Il nous avait demandé d'accéder à différents liens en respectant un intervalle de trois minutes. En suite il nous demandé de télécharger et d'exécuter un fichier bat. Ce fichier ne faisait qu'afficher des fenêtres à l'infini.

Après avoir accédé aux différents liens sur les deux machines, il ne sait rien passé ni sur le pc protégé ni sur le pc non protégé. De plus le fichier bat a été stoppé en tuant le processus. Nous avons donc pu constater que les PCs clients n'ont pas été dégradé.

3.9 Le Serveur WEB

3.9.1 Choix du Système d'exploitation et des logiciels

Le but du Projet est de proposer une architecture ressemblant à celle d'une entreprise standard. Nous avons choisi d'implémenter un serveur «LAMP» : Linux, Apache, MySQL, PHP pour mettre en place le serveur WEB et le sécuriser.

Nous nous sommes logiquement tournés vers le monde du libre. Plus précisément vers les distributions DEBIAN car elles bénéficient d'une très bonne stabilité, fiabilité, et c'est la distribution sur laquelle nous avions le plus grand retour d'expérience.

3.9.2 Paramétrage & Sécurisation

Nous avions prévu de mettre en place plusieurs serveurs sous linux : WEB et SQL, DNS, MAIL, pour cela nous avons fait un « master ». Ce dernier, contenait le système sans les premiers éléments de sécurités indépendant des services. Ce qui nous a permis de gagner du temps.

Pour mettre en place le serveur WEB nous avons installé les logiciels suivants pour la première confrontation :

- Apache 2.2
- PHP 5
- MySQL 5.0
- phpMyAdmin

Afin de sécuriser ce serveur nous avons choisi de procéder par étapes.

Première étape : sécurité du matériel

Pour la première confrontation, nous avons supprimé à partir du BIOS la possibilité de booter avec un CD, clé USB… De plus, le mot de passe pour accéder au BIOS a été ajouté.

Afin de respecter la politique de sécurité, le mot de passe du compte « root » a été modifié et ceux tout au long du projet.

Enfin, comme nous avons récupéré un ghost d'une machine Linux, il a été nécessaire de supprimer les services et les paquets inutiles pour notre projet :

- Atftpd
- Portmap
- Lisa
- Lpd

- Dns-clean
- Pppd-dns
- Gpm
- Isdnutil
- Fem control

Ceci en vu de restreindre les possibilités d'intrusions.

Deuxième étape : sécurité des logiciels

Après avoir installé MySQL nous avons démunis le compte « root » de ses droits et créé un nouvel utilisateur « admincandide » avec les droits nécessaires pour l'administration.

Pour se protéger au maximum des attaques par injection SQL, vulnérabilité du code du site WEB…, les sources de « ModSecuity » ont été installées. Lors du déploiement des sources nous avons été confrontés à quelques problèmes notamment dus aux dépendances avec d'autres paquets. Enfin, nous avons recherché des librairies pour configurer « ModSecurity » afin de se protéger des attaques.

3.9.3 Mise en place du site Internet

Lors de la première confrontation, par manque de temps une ébauche de site internet a été mise en place.

Il s'agit d'une plateforme d'e-learning, reprise du projet de L3, et adapté pour le projet.

Modifications du site :
La partie graphique du site a été entièrement refaite, à l'aide de CSS.

La fonction d'envoie de mails via le site a été enlevé faute de serveur SMPT. Nous avons aussi enlevé le forum (phpbb) car il aurait été lourd à gérer et n'aurait pas apporté un réel intérêt.

Pour cela, il a fallu créer un Virtual host dans le fichier de configuration d'Apache qui permet de préciser où les pages du site internet se trouvent. Dans notre cas les sources étaient situées dans le répertoire « /var/www/candide ».

LA DEUXIEME CONFRONTATION

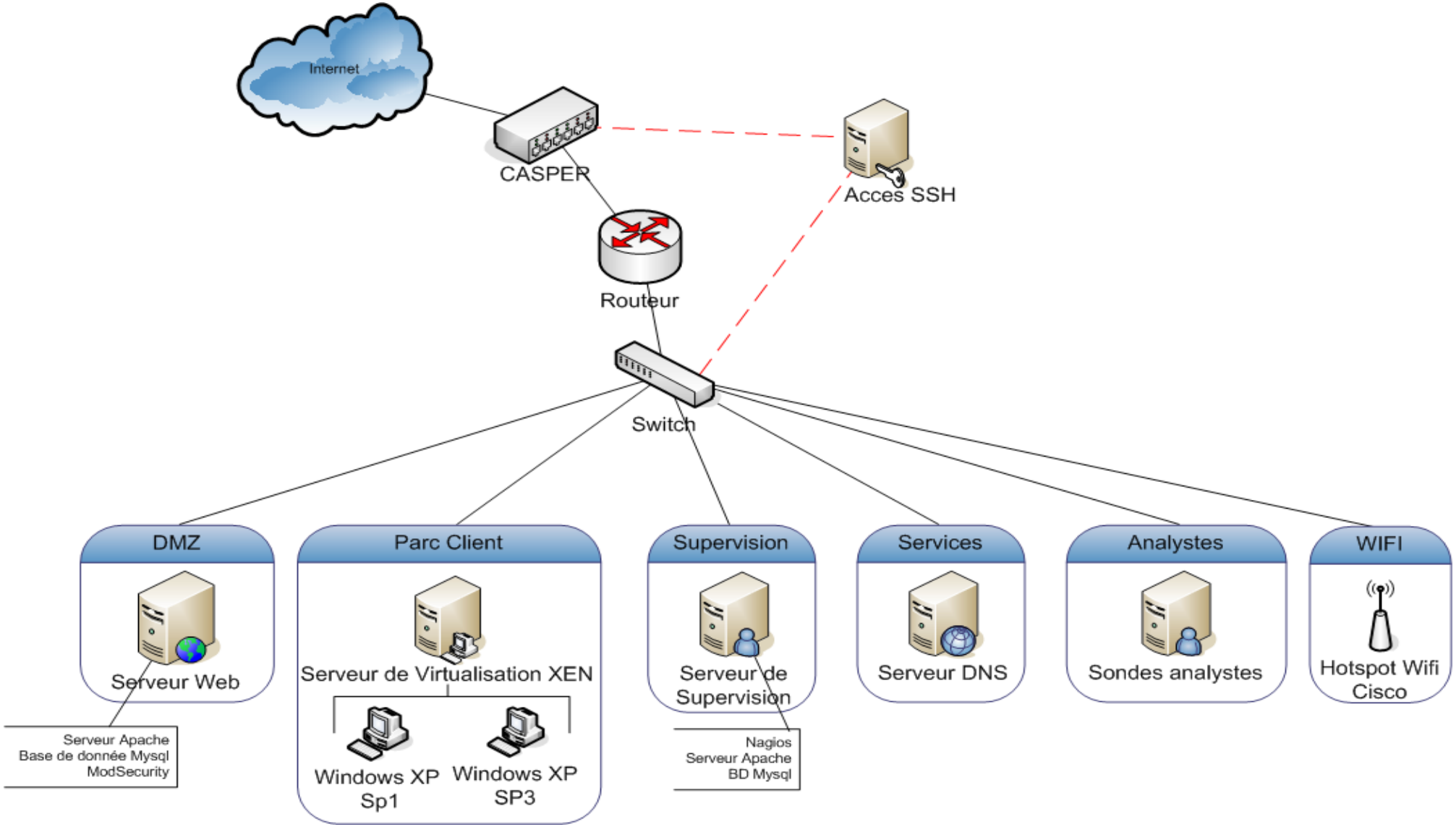
Cette étape avait pour objectif de compléter l'architecture que nous avions mise en place lors de la première confrontation.
Pour cela nous avons mis en place une architecture plus complète.

3.10 Architecture mis en place pour la première confrontation

Lors d'une réunion la nouvelle architecture a était définit afin de compléter l'architecture existante.

3.10.1 Schéma

De nouveau service comme le wifi ou le DNS ont été rajoutés à l'ancienne architecture.


Internet
CASPER
Acces SSH
Routeur
Switch
DMZ
Serveur Web
Serveur Apache
Base de donnée Mysql
ModSecurity
Parc Client
Serveur de Virtualisation XEN
Windows XP Sp1
Windows XP SP3
Supervision
Serveur de Supervision
Nagios
Serveur Apache
BD Mysql
Services
Serveur DNS
Analystes
Sondes analystes
WIFI
Hotspot Wifi Cisco

3.10.1 Présentation

Comme nous l'avons dis précédemment l'architecture de la première confrontation à été modifiée, un serveur DNS ainsi qu'un hot spot wifi ont été mis en place. Un vlan wifi est donc mis en place afin d'accueillir le hot spot, et un vlan service est aussi mis en place afin d'accueillir le serveur DNS.

3.11 Le routeur

3.11.1 Sécurité générale

La configuration du routeur en préparation de la deuxième confrontation à été axé sur la sécurité de celui-ci et l'envoi de données à l'équipe Analyse. La NSA propose un guide de sécurité dédié aux routeurs Cisco à l'adresse suivante : http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1

Certains services ne sont pas indispensables au bon fonctionnement du routeur et peuvent donc être désactivés afin d'améliorer la sécurité de celui-ci :

```
no ip source-route
no ip http server
! Désactive l'accès au serveur de configuration du routeur en HTTP.
no ip https server
! Désactive l'accès au serveur de configuration du routeur en HTTPS.
no snmp-server
! Désactive le serveur SNMP.
no cdp run
! Désactive les communications entre le matériel Cisco, protocole propriétaire.
```

Sur chaque interface on a appliqué les commandes suivantes :

```
no ip directed-broadcast
no ip mask-reply
no ip proxy-arp
```

On verra par la suite que l'ajout du VPN nous a contraint à reconfigurer l'interface (ip proxy-arp) sur laquelle il était connecté, afin de router correctement l'information vers l'ensemble des VLAN.

3.11.2 Limitation du nombre d'entrées NAT

Lors de la première confrontation, une machine de l'équipe attaque à effectuer un NAT FLOODING en vue de générer un DoS et/ou un bruit de fond. Nous avons donc mis en place la règle ci-dessous. On notera que qu'elle est facilement contournable si l'attaquant change d'adresse IP régulièrement.

```
ip nat translation max-entries 300
```

Puis, si on veut auditer les translations NAT pour le Syslog :

```
ip nat log translations syslog
```

3.11.3 Création des ACL sur l'interface externe

On ajoute la commande suivante sur l'interface de sorte f0/0.

```
ip access-group 112 in
```

Puis on ajoute les règles suivantes dans la configuration générale :

```
! Permet de vérifier l'état des machines qui hébergent les services web de l'entreprise depuis
l'extérieur
!
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 unreachable
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 packet-too-big
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 echo-reply
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 time-exceeded
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 traceroute
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 administratively-prohibited
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 echo
!
! Autorise les machines externes à accéder aux services internes.
!
access-list 112 permit tcp any host 172.18.4.2 eq www
access-list 112 permit tcp any host 172.18.4.2 eq 443
access-list 112 permit tcp any host 172.18.4.2 eq 55555
access-list 112 permit tcp any host 172.18.4.2 eq 55556
access-list 112 permit tcp any host 172.18.4.2 eq 143
access-list 112 permit tcp any host 172.18.4.2 eq smtp
access-list 112 permit udp any host 172.18.4.2 eq 25
!
! Bloque le reste et envoie les échecs dans un fichier de log
!
access-list 112 deny   ip any any log
```

3.11.4 Envoi des données Syslog.

Pour envoyer le contenu du fichier de log généré par les ACL :

```
logging facility local1
logging host 172.10.200.2 transport tcp port 46001 audit
```

3.11.5 Envoi des données Net Flow.

Sur l'interface externe :

```
ip flow ingress
ip flow egress
ip route-cache flow
```

Puis sur la configuration générale :

```
!
ip flow-export source FastEthernet0/1.7
ip flow-export version 5
ip flow-export destination 172.10.200.2 2055
!
```

Si on veut obtenir des informations exploitables il faut que le routeur soit à la bonne heure. Sinon il n'y aura pas de correspondance entre ce qui est audité et les attaques réelles. Ici notre NTP local.

```
ntp server 172.10.180.3
```

3.12 Le Switch

3.12.1 2nd et 3eme Confrontation

3.12.1.1 Sécurité : éviter le saut de Vlan Hopping

La négociation du trunk est gérée par le DTP (Dynamic Trunking Protocol). Ce protocole peut être utilisé pour des attaques de saut de vlan en transmettant des trames DTP mal formées.

Cette attaque est plus que probable pour la troisième confrontation car le groupe attaque sera cette fois ci à l'intérieur. Nous avons donc décidé d'interdire la génération de trames DTP et donc la négociation du trunk par la commande suivante :

```
--Commandes pour interdire les trames DTP:
Switch# configure terminal
Switch(config)# interface fastethernet0/XX
Switch(config-if)# switchport nonegotiate
Switch(config-if)# end
```

3.12.1.2 Sécurité : éviter les attaques par dénie de service

L'Attaque par dénie of service envoie des messages pour faire recalculer la topologie incessamment. Le but étant de simuler un Switch et se faire élire comme « root » pour récupérer alors tout le trafic.

Parade :

Sous CISCO activer BPDU guard et ROOT guard.

Désactiver le STP sur les ports ou ne sont pas connectés des Switchs.

Enabling BPDU Guard

```
--Commandes pour activer le BPDU Guard:
Switch# configure terminal
Switch(config)# spanning-tree portfast bpduguard default
Switch(config)# interface interface-id
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

Enabling BPDU Filtering

```
--Commandes pour activer le BPDU filtering:
Switch# configure terminal
Switch# spanning-tree portfast bpdufilter default
Switch# interface interface-id
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

Enabling Root Guard

```
--Commandes pour activer le Root Guard:
Switch# configure terminal
Switch# interface interface-id
Switch(config-if)# spanning-tree guard root
Switch(config-if)# end
```

3.12.1.3 Intégration des sondes des analystes

Le Switch fessait déjà du miroring vers une sonde des analystes du port G1 vers le port G2 pour qu'ils puissent analyser tout les flux géré par le routeur.

Pour plus de précision, une nouvelle sonde à été intégré dans la DMZ pour analyser les communications interne à cette zone critique. Pour ce faire il à fallut cette fois rediriger les communications d'un VLAN vers l'interface d'écoute de la sonde.

```
--Commandes de redirection des port vers les sonde des analystes:
Switch# conf t
Switch(config)# monitor session 1 source interface Gi0/1
Switch(config)# monitor session 1 destination interface Gi0/2
Switch(config)# monitor session 2 source vlan 1
Switch(config)# monitor session 2 destination interface Fa0/3
```

3.13 Le serveur web

3.13.1 Paramétrage & Sécurisation

Première étape : sécurité du matériel

En ce qui concerne la deuxième confrontation, nous avons choisi de partitionner le système à l'aide d'un live CD Knoppix et du logiciel Gparted et qtparted. Cette partition a été construite comme indiquée ci-dessous :

- Swap : 512 Ko
- Boot : 512 Ko
- Système : 15Go
- Données : 58 Go

La partition du système avait pour but de séparer les données et les logiciels de sorte que si les données avaient été altérées, la machine ne fut pas saturée et continuer encore à tourner.

Le système de fichier qui a été utilisé est « reiserfs » car il est journalisé, optimisé pour les fichiers de petites tailles. De plus le codage pour le journal est fait sur plus de bits que les autres systèmes de fichier ainsi en cas de problème il y a plus d'informations disponibles pour reconstituer le journal.

Deuxième étape : sécurité des logiciels

En vue de renforcer la sécurité, pour la deuxième confrontation, le mode SSL avec redirection automatique du http sur le https a été mis en place (Mise en place du Virtual host pour le mode SSL). De plus, l'outil MySQLTuner a été installé pour nous aider à améliorer la configuration de MySQL en fonction de l'analyse des connections à la base de données. Cette analyse nous a permis de mettre en place une restriction sur les demandes de connexion d'Apache et de MySQL à 300 connexions.

Pour se protéger au maximum des attaques par le code, les règles suivantes ont été déployées avec « ModSecurity » :

- Rejet des requêtes ayant le status 500
- Ne donner aucune précision sur le serveur web
- Scanner le flux de sortie
- Masquer le serveur
- Règles dédiées au spam
- Règles de filtrage des hotes, proxy, etc...
- Règles interdisant certains clients, robots, etc...
- Protection contre les rootkits
- Règles empêchant l'utilisation du serveur comme proxy
- Règles contre l'injection SQL
- Règles contre l'injection de code php
- Règles contre les attaques par chemin transversal

Lors de la deuxième confrontation, le groupe Attaque a atteint le seuil maximum de demandes de connexions par heures. C'est pourquoi nous avons immédiatement basculé ce seuil en illimité afin de rétablir l'utilisation du site.

3.13.2 Mise en place du site Internet

Pour la deuxième confrontation, suite à la demande du groupe d'analyse, la redirection des logs d'apache vers le routeur a été configurée. De plus, un nouveau site web a été mis à disposition ouvrant des vulnérabilités pour le groupe Attaque.

Afin de protéger les sources du site internet un changement du propriétaire « **www-data.www-data** » du répertoire « /var/www/candide » a été établi avec comme droits sur les répertoires « **2755** » et sur les fichiers « **644** ».

De plus il y a eu une refonte du site avec une meilleure charte graphique, création d'une partie privée accessible par authentification.

Trois comptes avec des droits différents ont été crées :

- Un compte étudiant qui ne peut que naviguer sur le site, télécharger les ressources en lignes et modifier ses informations personnelles.
- Un compte professeur qui peut en plus, ajouter/supprimer des questions/réponses dans le foire aux questions, ajouter/supprimer des ressources et des news.
- Un compte administrateur qui peut ajouter et supprimer des utilisateurs, modifier des droits et inscrire des personnes dans des Unités d'Enseignements.

Lors de la seconde confrontation, nous avons donné le compte étudiant aux attaquants.

Connexion à la base de données :
Nous avons crée un compte n'ayant des droits que sur la base de données « candide », du site. Nous avions décidé lors de la première confrontation de limiter le nombre de connexions par heure à 500. Lors de la seconde confrontation, après avoir rapidement atteint la limite de connexions, nous avons augmenté la limite à 10000 connexions par heure.

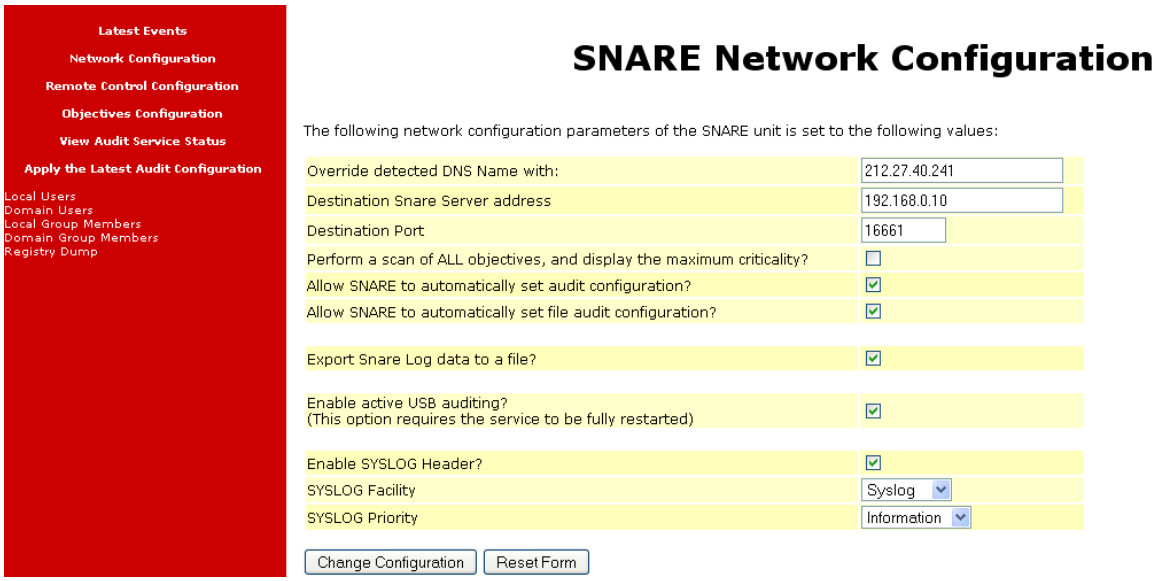
3.14 Le parc client

Pour la deuxième confrontation une gestion des logs à été mise en place pour le parc client. Pour cela nous nous sommes mis en relation avec la personne chargée du serveur syslog auprès de l'équipe analyse. Nous nous sommes mis d'accord pour le logiciel SNARE.

La gestion des logs des clients XP se fait donc grâce au logiciel SNARE (System iNtrusion Analysis and Reporting Environment). Ce logiciel permet le transfert à distance et en temps réel des informations contenues dans les Eventlog Windows.
Ce logiciel convertit ces informations au format texte et les délivre à un serveur syslog distant appartenant au groupe analyse grâce au protocole UDP.

Pour cela il a fallu installer et configurer sur les clients un agent SNARE. Cela permet de lancer un service « SnareCore.exe ».
Ensuite il a fallu configurer ce petit logiciel pour qu'il puisse envoyer les logs au serveur syslog.

3.14.1 Configuration de Snare

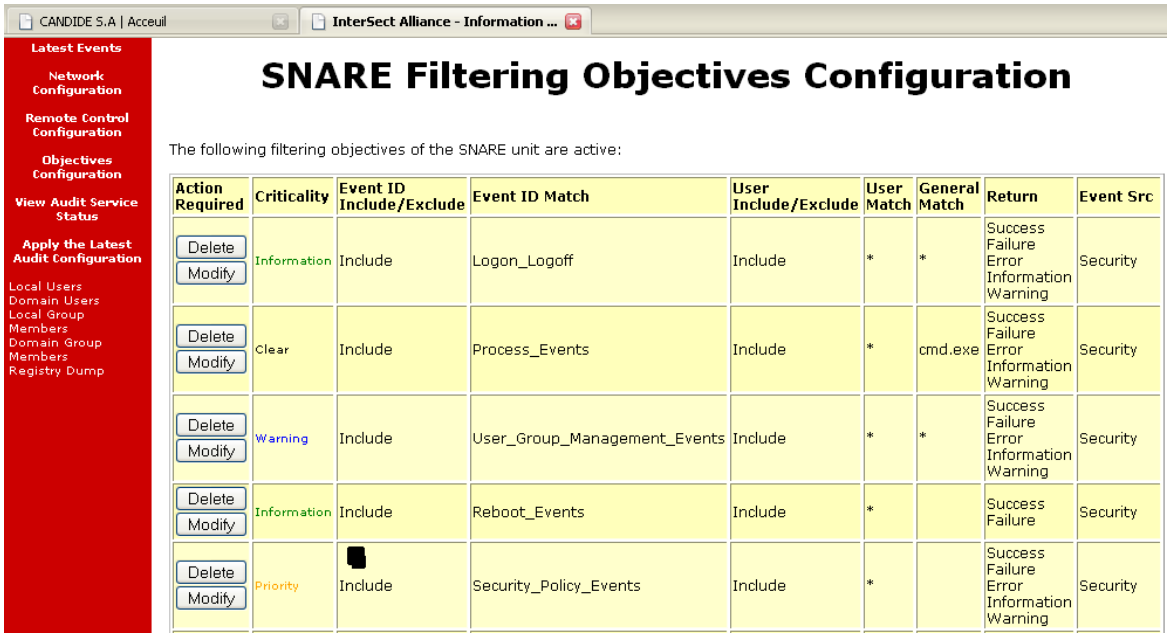


Comme le montre l'imprimé d'écran ci-dessus il faut spécifier :

- Le serveur DNS
- L'adresse du serveur syslog
- Le port de destination
- Cocher selon les préférences
- Choisir Syslog et Information pour que le serveur Syslog reçoive les informations.

Ensuite il faut spécifier l'adresse de la machine qui peut contrôler le service syslog du client ainsi que le mot de passe pour y accéder et le port sur lequel se trouve le service. Par exemple si nous mettons 16661 il faudra taper http://@ip:16661 dans le navigateur.

Ensuite il suffit de régler ce que l'on veut surveiller.



3.14.2 Le frameworks

Pour la deuxième confrontation le groupe attaque nous a également demandé de mettre sur l'ordinateur non protégé le système d'exploitation Windows XP SP1. Il nous a également demandé d'installer le logiciel Framework sur les deux PCs. Nous avons donc installé ce logiciel, sur le SP1 la version Framework 1.1 car c'était la seul compatible et sur le SP3 la version Framework 3.5.

3.14.3 Bilan 2eme confrontation

A la suite de cette première confrontation nous avons remis à neuf nos PCs clients et changé les mots de passe administrateur et utilisateurs.
Pour la deuxième confrontation le groupe attaque nous a demandé de mettre sur l'ordinateur non protégé le système d'exploitation Windows XP SP1. Il nous a également demandé d'installer le logiciel Framework sur les deux PCs. Nous avons donc installé ce logiciel, sur le SP1 la version Framework 1.1 car c'était la seul compatible et sur le SP3 la version Framework 3.5.
De plus il fallait gérer pour la deuxième confrontation la gestion centralisée des logs. Pour cela nous nous sommes mis en relation avec la personne chargée du serveur syslog auprès de l'équipe analyse. Nous nous sommes mis d'accord pour le logiciel SNARE.

Récapitulatif des PCs pour la deuxième confrontation :

PC CLIENT SP1 :
- Installation de Windows XP service pack1
- Installation du Framework 1.1
- Changement des mots de passes administrateurs et utilisateurs
- Installation du logiciel SNARE pour la supervision des logs

PC CLIENT SP3 :
- Installation du Framework 3.5
- Changement des mots de passes administrateurs et utilisateurs
- Mise à jour de l'antivirus
- Analyse antivirus
- Installation du logiciel SNARE pour la supervision des logs

Le déroulement de la deuxième confrontation était identique à la première confrontation. En effet il a fallu ce rendre sur la même adresse web (http://stri-attaque.ifrance.com) où se trouvait la consigne. Lorsque l'on essayer d'accéder à cette adresse avec le PC SP1 cela ne fonctionnait pas, en effet IE renvoyé une erreur et se fermer. Nous n'avons donc pas pu faire de test avec le PC SP1 car le site ne fonctionnait pas.

Nous avons donc accéder à ce site avec le PC SP3. La consigne était quasiment identique à la première confrontation. Il fallait accéder à une multitude de liens en attendant trois minutes entre chaque. Nous avons exécuté ces différents liens.
Ensuite il fallait lancer un fichier bat qui ne faisait qu'ouvrir une fenêtre à l'infini. Cette attaque consistait à saturer la machine. Pour la stoppée il suffisait pour un utilisateur non informaticien de redémarrer la machine et pour un informaticien de tuer le processus.

Nous avons pu remarquer que les deux machines clientes étaient aussi stables qu'avant la confrontation.

Leurs différentes attaques s'étaient donc abouties par des échecs. C'est pourquoi par la suite, la personne chargée de la communication du groupe attaque qui était présente lors des manipulations est revenu et nous a demandé de recommencer les manipulations sur les deux PCs car ils avaient effectués des modifications. Nous avons donc joué le jeu et avons recommencé les manipulations. Sur le PC SP3 le constat était identique, aucune dégradation n'a été constatée. Par contre sur le PC SP1, lorsque l'on a accéder au site (http://stri-attaque.ifrance.com) nous avons constaté que l'équipe attaque a exploité une faille de sécurité du Service Pack 1 de Windows XP. En effet quand on a accédé à ce site, quelques secondes après l'équipe attaque avait le contrôle de la machine. Pour les empêcher de découvrir des informations sensibles, nous avons fermé la session. Cette faille de sécurité a été corrigée avec le Service Pack 2 de Windows XP.

3.15 Le DNS

3.15.1 Le système d'exploitation

Le système d'exploitation hébergeant le DNS est Linux Debian 4.0, ce système libre à été choisi pour sa simplicité d'implémentation, sa légèreté et sa réactivité.
Bind9 a été choisi pour l'implémentation du DNS, ceci nous permettant de mettre rapidement en oeuvre cette fonctionnalité à partir d'un modèle déjà exploité en TP les années précédentes.

3.15.2 Paramétrages

Le DNS a été paramétré pour permettre les résolutions DNS aux éléments du parc informatique et serveur déployés. Ainsi il a donc été déployé dans la DMZ, dans ce but.

Les zones ont été définies pour que les requêtes DNS et RDNS des sous-réseaux locaux soient desservies et non celles del'extérieur.
Ces requêtes sont résolues à partir des serveurs racines DNS directement et ont en seconde source les Serveur DNS de M LATU.

3.15.3 Résolutions DNS spécifiques

Les résolutions DNS se font à partir des « Root DNS », néanmoins n'étant pas déclarés vis à vis du monde internet certaines résolutions doivent être faite localement du point de vue du DNS mis en place ainsi :

- www.candide-sa.com pointe sur le Serveur Web
- webmail.candide-sa.com pointe sur le « Serveur Webmail »

- imap.candide-sa.com point sur le serveur « Postfix Courier »
- le NS sur l'adresse privée du DNS
- et bien sur le domaine candide-sa.com sur le domaine local.

3.15.4 Sécurisation

Les règles appliquée au serveur DNS afin d'assurer la sécurité sont les suivantes :

Implémentation Locale	Implémentation distantes
Réponse aux requêtes DNS des sous réseaux locaux uniquement	
Interprétation locale du domaine « .candide-sa.com. »	Seules les requêtes DNS et HTTP sortantes sont autorisées

Les restrictions d'accès se font à partir du « Routeur Firewall » pour la plupart. Ainsi les requêtes à destination du DNS ne sont autorisées que s'il s'agit de requêtes de résolution DNS, seul les réponses à ces requêtes peuvent être renvoyées à des éléments des sous réseaux privés de l'entreprise candide-sa.com.

Le DNS quant à lui à accès aux protocoles permettant sa mise à jour via internet (essentiellement HTTP), et aux requêtes DNS à destination des root DNS.

3.16 Le wifi

3.16.1 Introduction

Dans le cadre du projet de sécurité de M2 STRI il est demandé à l'équipe « défense » de mettre en place une infrastructure réseau informatique. Cette infrastructure doit être représentative du fonctionnement des infrastructures réelles des entreprises. De nos jours, les gestionnaires et architectes de réseaux doivent faire face aux nouveaux besoins de mobilités des systèmes informatiques. En effet il y a déjà quelques années que les ordinateurs portables ont fait leurs entrée dans l'univers de l'entreprise mais désormais de nouvelles entité viennent se greffer : les ordinateurs de poches (PDA ou autres Smartphones). Ces systèmes, utilisés par le personnel mobile (commerciaux..), ont besoin de ce connecté au réseau internet et aux réseaux de l'entreprise.
L'équipe de défense a donc voulu recréer les problématiques posées aux entreprises par la mise en place de réseaux sans fil.

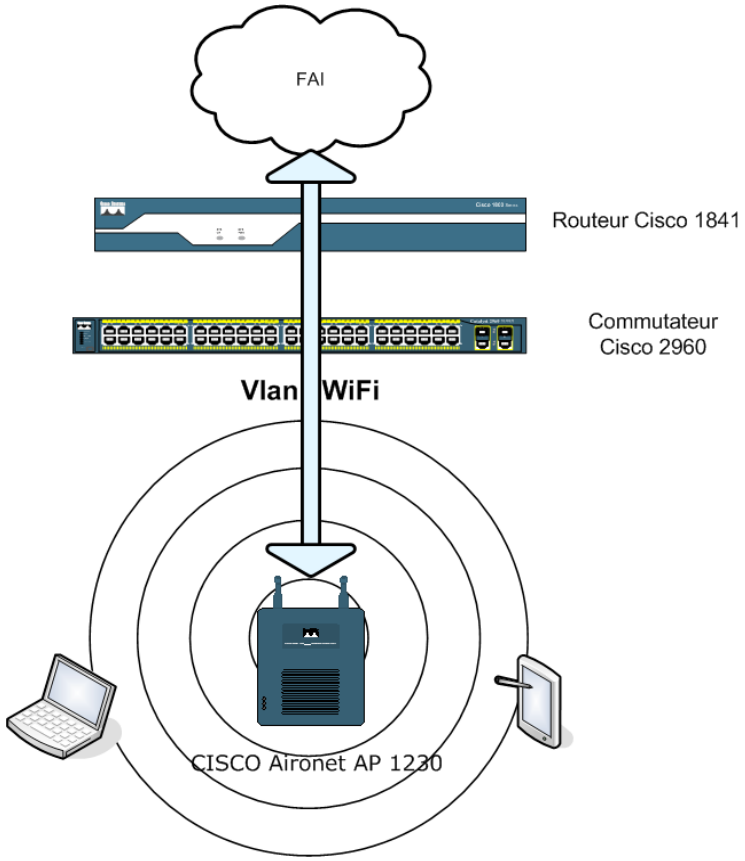
3.16.2 Problématiques

On peut distinguer deux catégories d'utilisateur du réseau sans fil :
L'employés de l'entreprise : qui souhaite se connecter de n'importe quel endroit aux réseaux de l'entreprise pour consulter des mails, échanger des fichiers... Les invités de l'entreprise (client, fournisseur, ou autres visiteur) qui souhaitent eux pouvoir récupérer les mails ou partager des informations simplement lors de réunions. Le principal souci rencontré lors de la mise en place d'un réseau sans fil est la sécurité. Tout d'abord, comme le sous entend l'expression « réseau mobile » on ne sait pas ou ce trouve l'utilisateur le contrôle d'accès au réseau ne peut donc ce faire physiquement. Ensuite le sans fil introduit les problèmes de confidentialité car toute personne écoutant le réseau est susceptible de récupéré des informations d'un autre utilisateur, ce qui pourrait porter préjudice à l'entreprise.

3.16.3 Solution proposée

Le Wifi (norme iso 802.11) est le type de réseau utilisé pas ces systèmes. Pour ce projet nous disposons d'un pont d'accès CISCO Aironet AP 1230 et de cartes réseaux permettant de simuler une configuration d'entreprise. Avec ce matériel nous souhaitons mettre en place un réseau wifi qui permettrait aux personnes étrangères à l'entreprise d'avoir accès web et de pouvoir échanger des données. De plus pour le personnel de l'entreprise nous souhaitons leur permettre de se connecter au réseau de l'entreprise.
Pour simplifier notre étude nous considérerons que le réseau wifi à été préalablement dimensionné et qu'une étude de couverture à déjà été faite. Le réseau est donc bien capté de l'intérieur de l'entreprise et déborde pas trop à l'extérieur. Pour permettre à tous les invitées de l'entreprise de se connecter nous avons décidé de déployer le réseau sans fils sous forme de hot Spot. C'est-à-dire

qu'il sera ouvert et sans identification préalable. Ce mode de fonctionnement permet d'accroitre grandement l'ergonomie du système. Pour éviter une utilisation abusive de ce réseau et pour qu'il reste un réseau secondaire dans l'entreprise, les services offerts seront limité au web.
Architecture



3.16.4 Principe

Nous avons donc mis en place, pour la seconde confrontation un réseau wifi sous forme d'un hot Spot. C'est-à-dire qu'il est ouvert à toutes personnes se trouvant dans le périmètre de couverture wifi de l'entreprise. Pour cela l'utilisateur ce connecte au réseau puis on lui attribuera une adresse IP grâce au serveur DHCP installé sur le point d'accès.

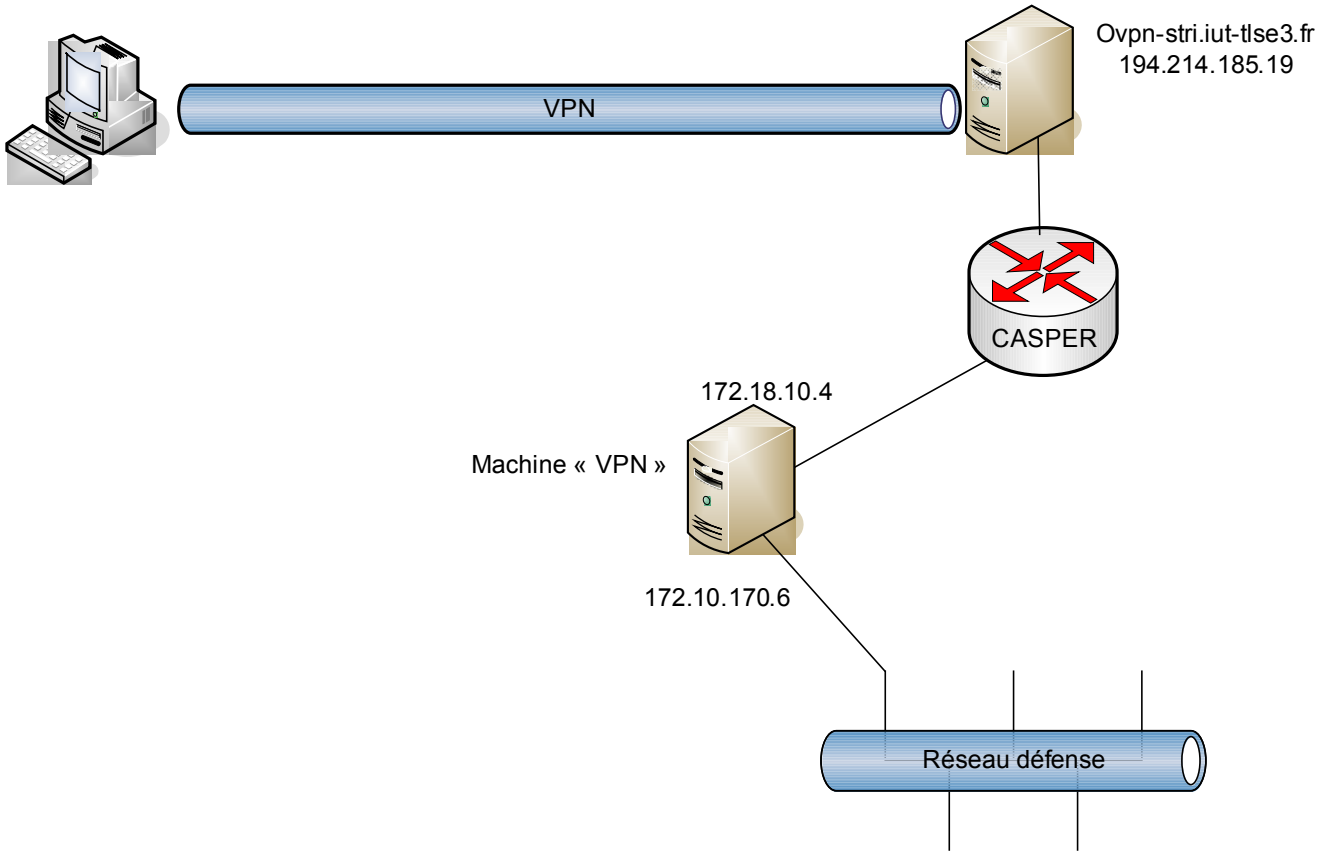
```
ip dhcp pool ipwifi
network 172.10.190.0 255.255.248.0
default-router 172.10.190.1
```

Le service offert par ce réseau est tout de même limité: accédé web uniquement. Pour cela les seuls ports disponibles sont : http, https, dns.
Pour cloisonner ce réseau ouvert au public et garantir la sécurité du réseau interne de l'entreprise, nous avons réservé un vlan spécifique totalement dédié au wifi. L'ensemble du trafic de ce vlan est redirigé vers l'extérieur du réseau ainsi il n'est pas possible de pénétré le réseau de l'entreprise via cet accès.

Cf - 4.2 Config vlan wifi routeur.

Pour ce qui est de la confidentialité des données qui transite sur le réseau elle n'est pas garantie car ce réseau est construit dans le but premier donnée un accès web de consultation aux invitées (car ils n'ont pas accès un réseau de l'entreprise) et non d'être utilisé pour des applications métier. Ce dernier permet tout de même de consulté ces mails grâce a des web mail. Pour ces consultations il sera recommandé d'utilisé du cryptage de haut niveau (https) pour garantir un minimum sécurité.

3.17 L'acces SSH



Pour travailler de chez nous sur les machines présentent sur le réseau défense de l'IUP, nous utilisons un VPN qui est mis à notre disposition par M. Latu.
Tout d'abord, pour les clients Windows, il faut installer openvpn GUI.
Nous utilisons les certificats que M. Latu nous a confiés. Nous avons donc trois fichiers à placer dans C:\Program Files\OpenVPN\config:

- ca.crt (certificat signé par l'autorité de certification)
- m2-stri.defense.crt (certificat du client)
- m2-stri.defense.key (clé du client)

Ensuite, pour configurer le client nous éditons le fichier client.ovpn.
Voici les lignes auxquelles il faut prêter attention :

```
# Nous utilisons le protocole TCP :
proto tcp

# Le serveur VPN à joindre (ovpn-stri.iut-tlse3.fr) sur le port 443
remote ovpn-stri.iut-tlse3.fr 443

#Le nom des trois fichiers de certification
ca ca.crt
cert m2-stri.defense.crt
key m2-stri.defense.key
```

Nous lançons openvpn gui pour accéder à Casper en VPN.

Pour aller sur les machines du LAN, nous nous connectons en ssh sur notre machine « VPN » (172.18.4.10) à l'aide de putty. Le port SSH classique (22) est redirigé sur le port 65023. Nous rentrons le login et le mot de passe de la machine. Une fois connecté, nous utilisons une connexion SSH pour aller sur le LAN interne et sur la machine de notre choix. Afin de réduire le risque d'intrusion depuis notre machine VPN nous avons créé un utilisateur spécifique ayant des droits très restreints.

3.18 La supervision Nagios

L'objectif de l'équipe est de fournir une solution de supervision et de gestion des logs pour la protection de l'architecture choisie. Cette supervision nous permettra d'avoir une vision globale sur le comportement des équipements constituant notre parc informatique. En effet il permet par exemple de remonter une alerte à chaque fois que des anomalies apparaissent sur un équipement. Ainsi cela permet une maitrise de l'ensemble des éléments du réseau et une meilleure reprise de service en cas de défaillance d'un équipement sur le réseau.
Pour mettre en place cette solution nous allons par faire une comparaison des solutions de supervision existante, ensuite nous continuerons par identifier les différents éléments du réseau à superviser suivi de la présentation de la solution que nous avons mis en place. En fin nous terminerons par les bilans sur les différentes confrontations.

3.18.1 Les différentes solutions existantes

Avant de choisir une solution nous avons fait une étude des différents logiciels existants :

De nombreuses plateformes de supervision existent aujourd'hui. Certaines se contentent de connaître à tout instant l'état des nœuds du réseau, d'autres permettent également de connaître l'état des services sur ces nœuds, les derniers offrent la possibilité de ressortir de nombreuses statistiques du réseau permettant une analyse assez fine. Le tableau suivant donne une vue globale sur les produits les plus répandus

Plateforme	**Logiciels**	
Windows	- JFFNMS	(http://www.jffnms.org)
	- openNMS	(http://www.opennms.org)
	- NetXMS	(http://www.netxms.org)
	- Nino	(http://nino.sourceforge.net/)
	- LookAtLan	(http://www.lookatlan.com/)
	- Big Brother	(www.bb4.org)
	- Big Sister	(http://www.bigsister.ch/)
	- OpManager	(http://manageengine.adventnet.com/products/opmanager/index.html) (version freeware limités à 10 équipements)
Linux	- Nagios	(http://www.nagios.org)
	- Zabbix	(http://www.zabbix.com/index.php)
	- Cacti	(http://www.cacti.net/index.php)
	- Pandora	(http://pandora.sourceforge.net/en/index.php)

	- Nino	(http://nino.sourceforge.net/)
	- JFFNMS	(http://www.jffnms.org)
	- openNMS	(http://www.opennms.org)
	- Centreon	(http://www.centreon.com)
	- NeDi	(http://www.nedi.ch/doku.php)
	- NetXMS	(http://www.netxms.org)
	- Zenoss	(http://www.zenoss.org)

Voir tableau comparatif en annexe

Comme on peut constater le nombre des outils est assez élevé et donc le choix d'un outil se fera selon le besoin de chacun. En ce qui nous concerne nous avons décidé d'utiliser une plateforme linux et des solutions sous License GPL. Donc ce choix va permettre déjà de restreindre les possibilités. Notre choix s'est donc porté sur Nagios.

3.18.2 Le choix d'une solution Nagios

Nagios est stable, dispose d'une grande communauté de développeurs derrière elle et est utilisée par un grand nombre de fournisseurs d'accès ou de grands noms comme Air France, le CNRS4 (taille de l'organisation : 26000 machines), l'IFSIC5 (2500 machines) ou encore le modeste Ministère de l'Education National (130 000 machines).

L'ensemble des spécifications est disponible en ligne sur http://www.Nagios.org/about/ Nagios va permettre, entre autre, de superviser des services réseaux (SMTP, POP3, HTTP, DNS6, etc.), de superviser les ressources systèmes (charge du processeur, processus en cours, etc.), de faire de la notification, classer les contacts à avertir par groupe de contacts, les machines par groupe de machines, de représenter par coloration les états des services et de leurs hôtes, de cartographier le réseau, de faire du « reporting », d'intégrer de nouveaux plugins, etc…

Pour plus d'information sur Nagios cf annexe

3.18.3 Les équipements à superviser

Conformément à notre architecture réseaux les équipements suivants sont à surveiller :

- routeur (passerelle)
- deux postes sous Windows XP
- postes sur Linux distribution debian (serveur web et serveur de messagerie)

Pour cette confrontation nous nous sommes fixés comme objectif la supervision du serveur web installé sur un système linux et ainsi les machines du parc qui sont sous Windows xp. La surveillance du routeur sera testée pendant la troisième confrontation.

3.18.4 Mise en place de Nagios

Pour mettre en place le serveur nagios nous nous avons choisi un système d'exploitation debian sur une machine dédié sur laquelle va tourner nagios. La démarche que nous avons mise en place a pour but de toujours avoir un système opérationnel sur cette machine.
Nous avons eu quelques difficultés dans cette phase car nous avions décidé de mettre en place la dernière version de nagios (nagios 3) mais il existe peu de documentation sur cette version ce qui nous a emmenés à installer une version antérieure (nagios2).

3.18.5 Bilan 1ere et 2eme confrontation

Lors de la première confrontation nous avions réussi à mettre en place le service « ping » sur le serveur Web, les deux postes du parc ainsi que les différents routeurs. Ce service nous permet juste de voir l'état de l'équipement s'il est connecté sur le réseau ou pas. Il était également possible d'observer sous forme graphique le taux de disponibilité d'un équipement dans le temps.

A la deuxième confrontation nous pouvions observer différents services tels que la charge mémoire, le taux d'utilisation du processeur, l'occupation de l'espace disques…

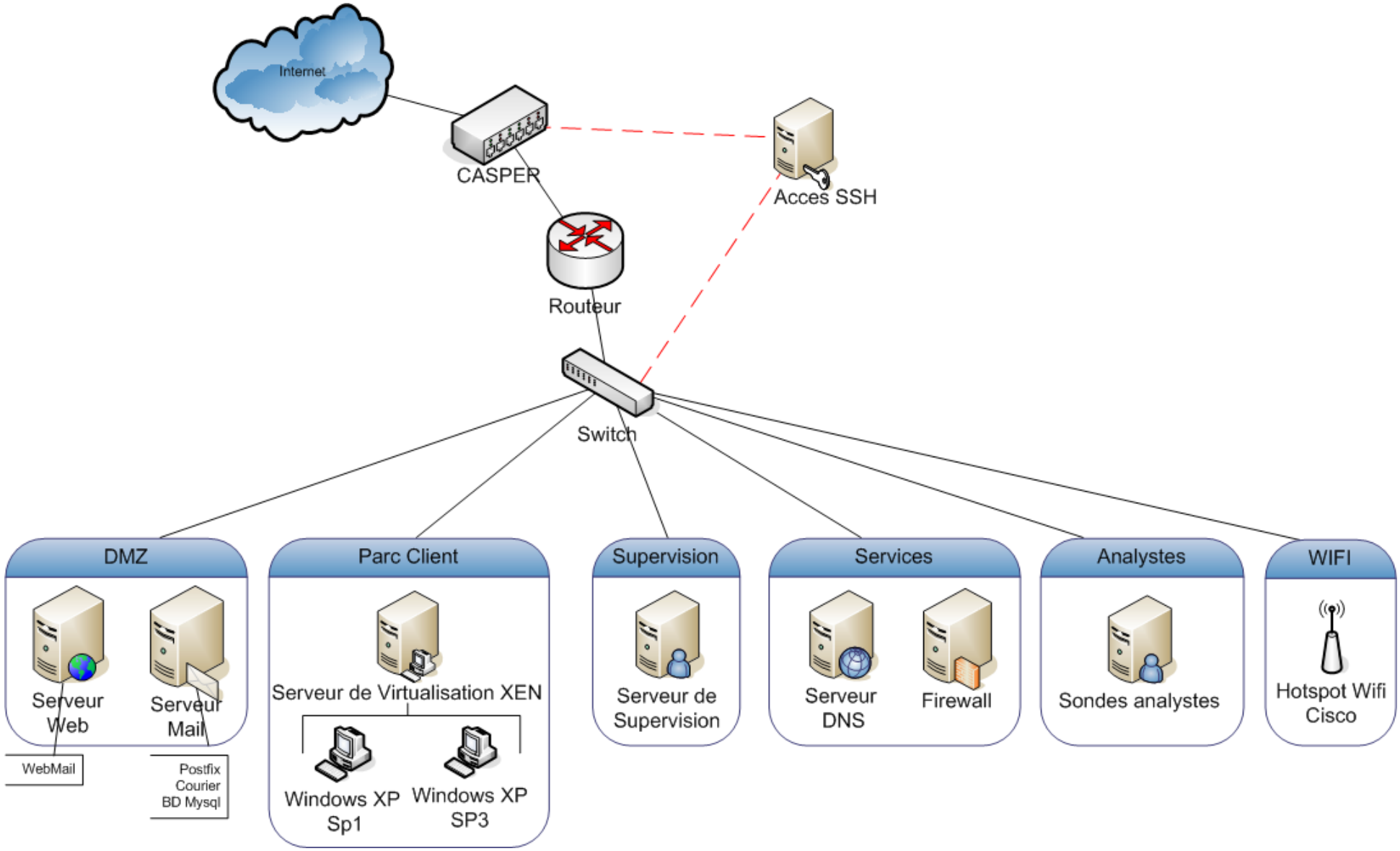
Ces services ont été ajoutés sur le serveur web (installé sur un système debian) et les deux postes du parc sous Windows xp. Sur le serveur nagios nous pouvons observer les variations de ces valeurs sauf pour le poste sous windows XP sans service pack qui posait des problèmes que nous n'avons pas réussi à résoudre à ce jour.

Nous avions également prévu d'afficher sous forme graphique la variation de valeurs observées mais ceci est en travaux et n'a pas pu fonctionner jusqu'à présent. Ces tâches sont reportées à la prochaine confrontation prévue pour le 17 novembre

4. TROISIÈME CONFRONTATION

4.1 Architecture mis en place pour la troisième confrontation

4.1.1 Schéma


Internet
CASPER
Acces SSH
Routeur
Switch
DMZ
Serveur Web
Serveur Mail
WebMail
Postfix
Courier
BD Mysql
Parc Client
Serveur de Virtualisation XEN
Windows XP Sp1
Windows XP SP3
Supervision
Serveur de Supervision
Services
Serveur DNS
Firewall
Analystes
Sondes analystes
WIFI
Hotspot Wifi Cisco

4.1.2 Présentation

Pour la troisième confrontation nous avons apporté différentes mise à jour sur les services mis en place aux précédentes confrontations. Pour cette troisième confrontation, nous avons décidé d'améliorer la protection du réseau en rajoutant un Firewall qui protégera le Parc client et le serveur de supervision. De plus afin d'améliorer la communication de l'entreprise un serveur Mail a été mis en place, afin de pouvoir envoyer et recevoir des emails.

4.2 Le routeur

4.2.1 Association ARP statique

Lors de la seconde confrontation nous avions eu la surprise de voir notre trafic DNS redirigé vers une machine de l'équipe attaque. Nous avons donc ajouté des associations statiques entre adresse MAC et adresse IP. Pour le serveur DNS via Cooper :

```
arp 172.18.4.1 0004.23b8.4e2c ARPA
```

Et pour la sonde audit à l'extérieur du réseau local :

```
arp 172.18.4.200 0010.5ad8.8960 ARPA
```

4.2.2 Ajout d'un serveur SNMP pour l'équipe NAGIOS

On doit faire attention à limiter l'accès en écriture au serveur SNMP.

```
snmp-server community public RO
snmp-server community private RW
```

4.2.3 Configuration d'IPinspect

Nous avions précédemment mis en place des ACL. Ici nous allons voir comment ajouter un contrôle de niveau applicatif via la commande ip inspect. On définit la liste protocoles à analyser via la commande ip inspect name.

```
ip inspect name ethernetout http audit-trail on timeout 3600
ip inspect name ethernetout https audit-trail on timeout 3600
ip inspect name ethernetout smtp audit-trail on timeout 3600
ip inspect name ethernetout imap audit-trail on timeout 3600
ip inspect name ethernetout ssh audit-trail on timeout 3600
```

La commande audit-trail on permet de récupérer des informations de filtrage. On choisit ensuite l'interface sur laquelle on va appliquer ce contrôle. Les transactions qui ne respecteront donc pas les protocoles analysés seront systémétiquement jetées par le routeur.

```
interface FastEthernet0/0
ip inspect ethernetout in
```

Prenons maintenant l'exemple de la DMZ. Voici ci-dessous la liste des autorisations en sortie du VLAN vers les autres réseaux.

```
access-list 140 deny   ip any any log
```

Avec

```
interface FastEthernet0/1.1
ip access-group 140 in
```

On veut inspecter les protocoles suivants :

```
ip inspect name dmz http audit-trail on timeout 3600
ip inspect name dmz https audit-trail on timeout 3600
ip inspect name dmz imap audit-trail on timeout 3600
ip inspect name dmz smtp audit-trail on timeout 3600
ip inspect name dmz icmp audit-trail on timeout 3600
```

On ajoute cette liste de protocoles à inspecter sur l'interface choisie.

```
interface FastEthernet0/1.1
ip inspect dmz out
```

Lorsqu'une requête est effectuée depuis l'extérieur, une ACL dynamique autorisant la réponse de la DMZ vers l'extérieur est ajoutée dans la liste 140 vu précédement.

4.3 Le Switch

Conservation des paramètres de ma seconde confrontation

4.4 Le serveur web

4.4.1 Paramétrage & Sécurisation

Première étape : sécurité du matériel

Pour une sécurité maximum du serveur web nous avions prévu pour la troisième confrontation de répartir sur une machine Apache en mode proxy (avec squid) et ModSecurity, et sur une autre machine Apache normal, MySQL, php et le code du site web. Compte tenu des problèmes rencontrés pour mettre en place « squid » il n'a pas été possible de réaliser cette migration.

Deuxième étape : sécurité des logiciels

Pour se protéger au maximum des attaques par le code, les règles suivantes ont été déployées avec « ModSecurity » et complétées pour la troisième confrontation :

- Règles contre l'injection de JavaScripts
- Règles contre les attaques XSS
- Cacher la version d'apache pour éviter des attaques en rajoutant dans le fichier http.conf les lignes suivantes :
  - ServerTokens ProductOnly
  - ServerSignature Off
- Cacher la version de php pour cela, modifier le fichier php.ini en rajoutant la ligne de code suivante :
  - expose_php Off
- Modifier le fichier de ModSecurity afin d'interdire les redirections à l'aide de $...
- Ajout de la ligne de code : « **SecFilterSelective THE_REQUEST "! ^[\x0a\x0d\x20-\x7f]+$"** »

4.4.2 Bilan sur le serveur Web

Le paquet ModSecurity nous a permis après une longue période de documentation de nous protéger efficacement des attaques sur notre serveur web. Le seul problème qui a été résolu s'est trouvé être le dépassement du nombre de connexions par heure sur la base de données. Cependant dés lors de l'apparition de ce dénis de service nous avons tout mis en œuvre dans les minutes qui ont suivis

pour le rétablir. A aucun moment nous avons du faire appel à une sauvegarder pour réinstaller le service.

4.5 Le reverse PROXY

4.5.1 Choix d'une solution de relais inverse (reverse proxy)

La mise en place d'un reverse proxy (ou accelerator) a été envisagé sur l'infrastructure de candide sa.
En effet, l'importance d'un reverse proxy réside sur le fait qu'il permet un traitement plus rapide des requêtes à destination du serveur web mais surtout d'établir des règles de filtrage afin de préserver le serveur web contre des attaques provenant de l'extérieur.
Afin de réaliser cet objectif, on a envisagé deux solutions qui sont: un serveur apache auquel on intègre des modules pour la gestion du mode proxy et le serveur squid en relais inverse. Le serveur squid est une solution répandue et reconnue tandis que le ModProxy est censé être plus simple d'installation mais moins performant.

4.5.2 Implémentation des solutions envisagées

Dans un premier temps, nous avons décidé de partir sur la deuxième solution : un serveur squid.
Etant donné que les pages web de candide-sa.com ne sont accessibles qu'avec le protocole HTTPS, l'installation de squid devient plus complexe. En effet, il a fallu télécharger les sources du logiciel squid (la version 3.10 dans notre cas) depuis internet et ensuite les compiler afin d'activer les options nécessaires à l'intégration de la gestion du SSL (--enable-ssl et --with-openssl). Nous avons rencontré un problème lors de la compilation de squid: nous n'avons pas su trouver toutes les dépendances nécessaires.

Dans un deuxième temps, nous nous sommes rabattu sur le ModProxy du serveur apache qui permettait également de définir des règles de filtrages. Le module a été lancé correctement. Toutefois nous ne voyons rien apparaître dans les fichiers de log qui pouvait confirmer le bon fonctionnement du module. Après plusieurs tests infructueux de plusieurs fichiers de configuration, nous ne pouvions laisser un module inutile fonctionner sur le serveur et c'est pour cela que le ModProxy n'a pas été activé pour les confrontations.

4.5.3 Bilan sur le reverse proxy

Nous n'avons pas pu implémenter Squid de par le manque d'information concernant les dépendances nécessaires à la compilation des sources.
La mise en place du ModProxy n'a pas pu se faire malgré les nombreux essais de fichier de configuration.

4.6 Le serveur Mail

4.6.1 Serveur Mail

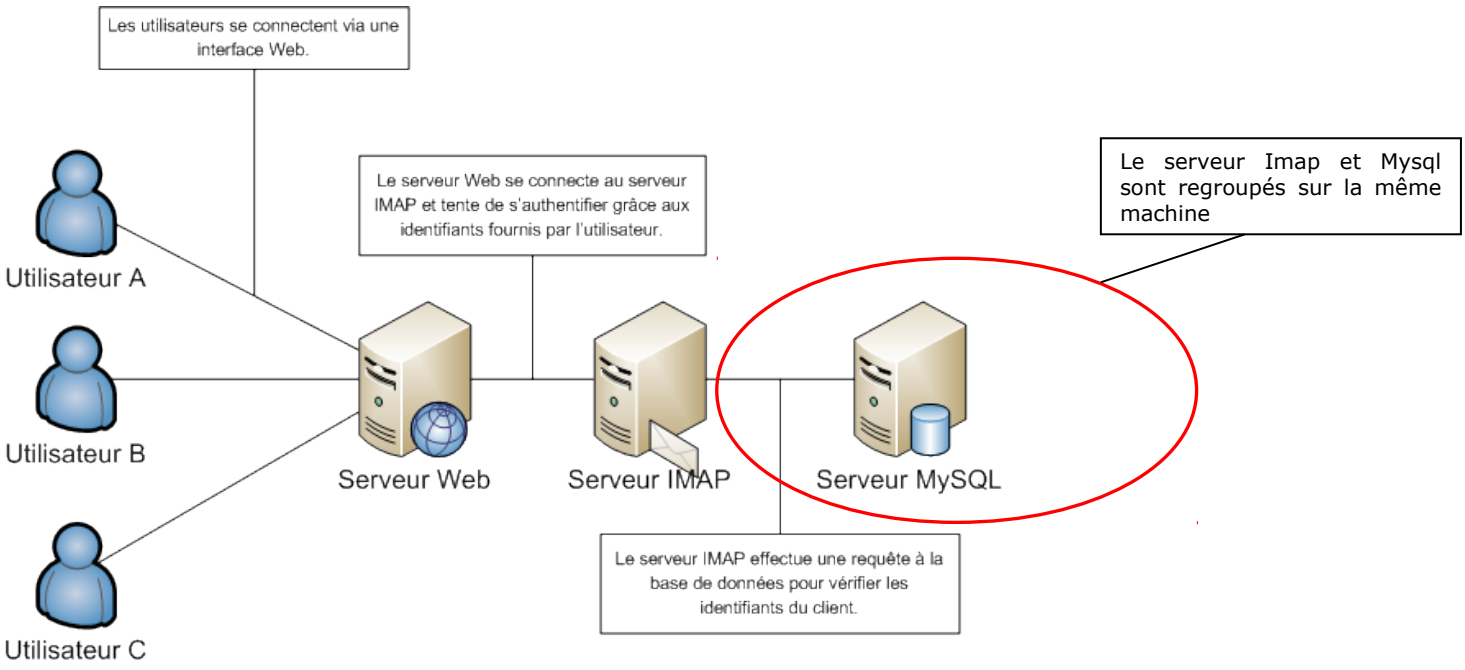
L'entreprise Candide SA doit avoir un serveur de messagerie afin de pouvoir communiquer avec ses clients. Le serveur de mail choisi est Postfix avec une interface webmail RoundCube.

4.6.2 Choix de l'architecture & du gestionnaire de mail

Postfix est un serveur de messagerie électronique, il se charge de la livraison de messages électroniques. Le serveur Postfix utilise le protocole IMAP (Internet Message Access Protocol), qui permet de laisser les e-mails sur le serveur dans le but de pouvoir les consulter de différents clients e-mails ou webmail. Le fait que les messages soient archivés sur le serveur fait que l'utilisateur peut accéder à tous ses messages depuis n'importe où sur le réseau et que l'administrateur peut facilement faire des copies de sauvegarde.
Le webmail utilisé pour vérifier les emails est RoundCube, il utilise le couple PHP/MySQL afin d'afficher/créer des emails mais aussi la technologie AJAX. Il permet de gérer les e-mails de sa boite mail grâce au protocole IMAP.
Le serveur Mail a été installé sur une machine Debian Etch. Je vais vous présenter la démarche suivi pour mettre en place le serveur de messagerie.

4.6.3 Infrastructure du serveur

Le serveur va se composer de quatre services: l'agent de livraison (Postfix), le serveur de mails IMAP (Courier), la base de données (MySQL) et le serveur web (Apache + PHP).
Pour accéder aux mails j'ai décidé d'utiliser RoundCube et PostfixAdmin pour administrer les utilisateurs, les alias et les domaines.



4.6.4 Création du compte virtuel

On va d'abord créer un utilisateur sur le serveur qui stockera les mails des utilisateurs :

```
addgroup --gid 20001 virtualcandide
adduser --uid 20001 --gid 20001 virtualcandide
```

4.6.5 Installation des services

On commence par l'installation de MySQL qui va permettre de stocker les utilisateurs du serveur mail. On va tout simplement les récupérer dans les dépots :

```
1   apt-get install mysql-server-5.0
```

4.6.5.1 Base de données

A fin de gérer plus facilement les comptes mails du domaine j'ai choisi d'utiliser PostfixAdmin. Il faut créer la base de données que vont utiliser les autres services pour identifier les utilisateurs.
Grace au script suivant PostfixMySQL.sql récupéré sur: http://sourceforge.net/projects/postfixadmin/

```
# Postfix Admin
# by Mischa Peters <mischa at high5 dot net>
# Copyright (c) 2002 - 2005 High5!
# License Info: http://www.postfixadmin.com/?file=LICENSE.TXT
#

# This is the complete MySQL database structure for Postfix Admin.
# If you are installing from scratch you can use this file otherwise you
```

```
# need to use the TABLE_CHANGES.TXT or TABLE_BACKUP_MX.TXT that comes with Postfix Admin.
#
# There are 2 entries for a database user in the file.
# One you can use for Postfix and one for Postfix Admin.
#
# If you run this file twice (2x) you will get an error on the user creation in MySQL.
# To go around this you can either comment the lines below "USE MySQL" until "USE postfix".
# Or you can remove the users from the database and run it again.
#
# You can create the database from the shell with:
#
# mysql -u root [-p] < PostfixMySQL.sql

USE postfix;

#
# Table structure for table admin
#
CREATE TABLE admin (
  username varchar(255) NOT NULL default '',
  password varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  modified datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (username),
  KEY username (username)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Admins';

#
# Table structure for table alias
#
CREATE TABLE alias (
  address varchar(255) NOT NULL default '',
  goto text NOT NULL,
  domain varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  modified datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (address),
  KEY address (address)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Aliases';

#
# Table structure for table domain
#
CREATE TABLE domain (
  domain varchar(255) NOT NULL default '',
  description varchar(255) NOT NULL default '',
  aliases int(10) NOT NULL default '0',
  mailboxes int(10) NOT NULL default '0',
  maxquota int(10) NOT NULL default '0',
  transport varchar(255) default NULL,
  backupmx tinyint(1) NOT NULL default '0',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  modified datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (domain),
  KEY domain (domain)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Domains';

#
# Table structure for table domain_admins
#
CREATE TABLE domain_admins (
  username varchar(255) NOT NULL default '',
  domain varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(1) NOT NULL default '1',
  KEY username (username)
) TYPE=MyISAM COMMENT='Postfix Admin - Domain Admins';
```

```
#
# Table structure for table log
#
CREATE TABLE log (
  timestamp datetime NOT NULL default '0000-00-00 00:00:00',
  username varchar(255) NOT NULL default '',
  domain varchar(255) NOT NULL default '',
  action varchar(255) NOT NULL default '',
  data varchar(255) NOT NULL default '',
  KEY timestamp (timestamp)
) TYPE=MyISAM COMMENT='Postfix Admin - Log';

#
# Table structure for table mailbox
#
CREATE TABLE mailbox (
  username varchar(255) NOT NULL default '',
  password varchar(255) NOT NULL default '',
  name varchar(255) NOT NULL default '',
  maildir varchar(255) NOT NULL default '',
  quota int(10) NOT NULL default '0',
  domain varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  modified datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (username),
  KEY username (username)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Mailboxes';

#
# Table structure for table vacation
#
CREATE TABLE vacation (
  email varchar(255) NOT NULL default '',
  subject varchar(255) NOT NULL default '',
  body text NOT NULL,
  cache text NOT NULL,
  domain varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(1) NOT NULL default '1',
  PRIMARY KEY  (email),
  KEY email (email)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Vacation';
```

Ensuite on se connecte a la base Mysql afin de créer la base de données pour PostfixAdmin et lancé le script de création de la BDD.

```
mysql
...
mysql>CREATE DATABASE postfix;
mysql>GRANT ALL PRIVILEGES ON postfix.* TO 'adminpostfix'@'%' IDENTIFIED BY
'P@ssP0stfix';
mysql>\. PostfixMySQL.sql
```

On ajoute l'administrateur de PostfixAdmin directement dans la base de données :

```
mysql>INSERT INTO domain (domain, description)
      VALUES ('candide-sa.com', 'Domaine de la societé Candide SA');
Query OK, 1 row affected (0.00 sec)

mysql>INSERT INTO admin (username, password, active)
      VALUES ('admin_candide@candide-sa.com', '$1$CeeAzXb...J8njWAw1', '1');
Query OK, 1 row affected (0.00 sec)

```

```
9   mysql>INSERT INTO domain_admins (username, domain, active)
10        VALUES ('admin_candide@candide-sa.com', 'ALL', '1');
11  Query OK, 1 row affected (0.00 sec)
12
13  mysql>INSERT INTO mailbox (username, password, name, maildir, domain, active)
14        VALUES (' admin_candide@candide-sa.com ', '$1$ExhxBRG6$...qhF/unIwe0Kk1',
15                'Candide SA', '/home/virtualcandide', 'candide-sa.com', '1');
16  Query OK, 1 row affected (0.00 sec)
```

Le mot de passe est hashé en MD5.
On vérifie que l'utilisateur que l'on vient de créer a bien accès à la base de données :

```
1   mysql postfix -u adminpostfix -p
2   Enter password: P@ssP0stfix
3   ...
4   mysql>
```

Voilà la base de données est prête à être utilisée par les différents services.

4.6.5.2 Postfix

On commence par installer Postfix et le module de connexion à la base de données.
Nb : L'installation de Postfix supprime le paquet Exim4.

```
apt-get install postfix postfix-mysql
```

Note : pendant l'installation sélectionner *Site Internet* afin de considérer que le serveur de messagerie sera disponible sur internet.
Configurer Postfix revient à modifier essentiellement deux fichiers dans /etc/postfix :

```
/etc/postfix/main.cf
/etc/postfix/master.cf
```

Classiquement il n'y a pas grand chose à modifier au niveau du master.cf
Il faut modifier le fichier suivant: **/etc/postfix/main.cf**.
En ce qui concerne le main.cf on peut s'intéresser a un certain nombre de variables, plus précisément ayant choisi d'utiliser MySQL, il faut renseigner ces variables :

virtual_alias_maps,
virtual_gid_maps,
virtual_mailbox_base,
virtual_mailbox_domains,
virtual_mailbox_maps,
virtual_minimum_uid,
virtual_uid_maps.

On doit configurer ce fichier afin de faire fonctionner le serveur Postfix, on rajoute donc certaines propriétés afin de spécifier que l'on va des utilisateurs virtuels:

```
1 virtual_transport = maildrop
2 virtual_mailbox_base = /home/virtualcandide
3 virtual_alias_maps = proxy:mysql:/etc/postfix/mysql_virtual_alias_maps.cf
4 virtual_mailbox_domains = proxy:mysql:/etc/postfix/mysql_virtual_domains_maps.cf
5 virtual_mailbox_maps = proxy:mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf
6 virtual_minimum_uid = 20001
7 virtual_uid_maps = static:20001
8 virtual_gid_maps = static:20001
```

On crée alors les fichiers de mapping avec la base de données. En créant ainsi les fichiers de configuration on peut avoir un postfix capable d'interroger une base MySQL.

```
1 Fichier : /etc/postfix/mysql_virtual_alias_maps.cf
2 user = adminpostfix
3 password = P@ssP0stfix
4 hosts = 172.10.140.3
5 dbname = postfix
6 query = SELECT goto FROM alias WHERE address = '%s' and active ='1'

1 Fichier : /etc/postfix/mysql_virtual_domains_maps.cf
2 user = adminpostfix
3 password = P@ssP0stfix
4 hosts = 172.10.140.3
5 dbname = postfix
6 query = SELECT domain FROM domain WHERE domain = '%s' and active ='1'
```

```
1 Fichier : /etc/postfix/mysql_virtual_mailbox_maps.cf
2 user = adminpostfix
3 password = P@ssP0stfix
4 hosts = 172.10.140.3
5 dbname = postfix
6 query = SELECT goto FROM alias WHERE address = '%s' and active ='1'
```

On modifier le fichier /etc/postfix/master.cf afin de modifier la livraison par maildrop :

```
Remplacer la ligne :
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}

par :
maildrop  unix  -       n       n       -       -       pipe
   flags=DRhu user=virtual argv=/usr/bin/maildrop -w 90 -d ${user}@${nexthop}
   ${extension} ${recipient} ${user} ${nexthop} ${sender}
```

On redémarre alors le service :

```
 /etc/init.d/postfix restart
```

4.6.5.3 Maildrop

On va alors installer le livreur de mails : maildrop.

```
apt-get install maildrop
```

On créer le fichier /home/virtualcandide/.mailfilter de livraison.

```
Fichier : /home/virtualcandide/.mailfilter
logfile "/home/virtualcandide/.maildrop.log"
`[ -d $DEFAULT ] || (maildirmake $DEFAULT && maildirmake -f Spam $DEFAULT &&
maildirmake -f sent-mail $DEFAULT && maildirmake -f SpamToLearn $DEFAULT &&
maildirmake -f SpamFalse $DEFAULT)`

`test -r $HOME/$DEFAULT.mailfilter`
if( $RETURNCODE == 0 )
{
    log "(==)  Including $HOME/$DEFAULT.mailfilter"
    exception {
        include $HOME/$DEFAULT.mailfilter
    }
}
```

Une fois ce fichier créé il faut modifier les droits à ce fichier :

```
chmod 600 .mailfilter
```

4.6.5.4 Courier

Bon ce n'est pas tout cela mais il faudrait quand même pouvoir consulter ses mails …
C'est là qu'intervient courier-imap. Il peut fonctionner tant en imap qu'en pop, il suffit d'installer ce que l'on désire. On installe alors Courier Imap et le module de connexion à la base de données :

```
apt-get install courier-imap courier-authlib-mysql
```

Note : pendant l'installation choisissez *NON* lorsqu'il vous propose de créer les répertoires Web.

On modifie les paramètres dans les fichiers suivants :

```
Fichier : /etc/courier/authdaemonrc
authmodulelist="authmysql"

Fichier : /etc/courier/authmysqlrc
MYSQL_SERVER            172.10.140.3
MYSQL_USERNAME          adminpostfix
MYSQL_PASSWORD          P@ssP0stfix
MYSQL_SOCKET    /var/run/mysqld/mysqld.sock
MYSQL_PORT      3306
MYSQL_OPT       0
```

```
12   MYSQL_DATABASE postfix
13   MYSQL_USER_TABLE       mailbox
14   MYSQL_CRYPT_FIELD      password
15   MYSQL_LOGIN_FIELD      username
16   MYSQL_HOME_FIELD       '/home/virtualcandide'
17   MYSQL_UID_FIELD        '20001'
18   MYSQL_GID_FIELD        '20001'
19   MYSQL_NAME_FIELD       name
20   MYSQL_MAILDIR_FIELD    maildir
21   MYSQL_WHERE_CLAUSE     active='1'
```

Note : vérifier qu'il n'y a que des tabulations entre le nom et la valeur d'une propriété.

Il faut donner les accès à l'utilisateur virtualcandide :

```
1  chown virtualcandide /usr/lib/courier/authdaemon
2  chmod 750 /usr/lib/courier/authdaemon
```

On redémarre alors les services IMAP et AuthDaemon de Courier :

```
1   /etc/init.d/courier-imap restart
2   /etc/init.d/courier-authdaemon restart
```

Pour vérifier que le serveur IMAP arrive bien à se connecter à la base de données on exécute un test d'authentification :

```
1  authtest admin_candide@candide-sa.com
2  Authentication succeeded.
3
4       Authenticated: admin_candide@candide-sa.com  (uid 20001, gid 20001)
5      Home Directory: /home/virtualcandide
6             Maildir: admin_candide@candide-sa.com
7               Quota: 0S
8  Encrypted Password: $1$CeeAzXb...J8njWAw1
9  Cleartext Password: (none)
10            Options: (none)
```

Maintenant tous les services sont configurés et communiquent entre eux, on peut configurer les accès Web.

4.6.5.5 PostfixAdmin et Roundcube

L'affichage des pages web se fait sur un serveur différent que celui du serveur mail. On installera donc les archives de Roundcube et Postfixadmin sur le serveur Web qui fera l'affichage des pages, le traitement des mails se fera sur le serveur mail.
Tout d'abord on récupère les archives (récupérer les dernières versions depuis RoundCube et PostfixAdmin) :

```
1 wget http://garr.dl.sourceforge.net/sourceforge/roundcubemail/roundcubemail.tar.gz
2 apt-get install postfixadmin
```

On extrait alors les sources.

4.6.5.6 Configuration de PostfixAdmin

Pour configurer PostfixAdmin il faut modifier les paramètres suivants du fichier **config.inc.php** et supprimer le fichier **setup.php** :

```
$CONF['configured'] = true;
$CONF['postfix_admin_url'] = 'http://www.candide-sa.com/postfixadmin';
$CONF['create_default_folders'] = true;
$CONF['database_type'] = 'mysqli';
$CONF['database_host'] = '172.10.1403';
$CONF['database_user'] = 'adminpostfix';
$CONF['database_password'] = 'P@ssP0stfix';
$CONF['database_name'] = 'postfix';
```

On peut donc maintenant se connecter via le serveur web et enregistrer des utilisateurs

Pour le projet j'ai créé une adresse mail contact@candide-sa.com, Il s'agit de l'adresse qui apparaissait sur le site web Candide-sa.

4.6.5.7 Configuration de RoundCube

On va tout d'abord créer la base de données que va utiliser RoundCube :

```
mysql
...
mysql>CREATE DATABASE roundcube;
Query OK, 1 row affected (0.00 sec)

mysql>GRANT ALL PRIVILEGES ON roundcubemail.* TO 'roundcube'@'172.10.140.2'
IDENTIFIED BY 'RCube963';
Query OK, 1 row affected (0.00 sec)
```

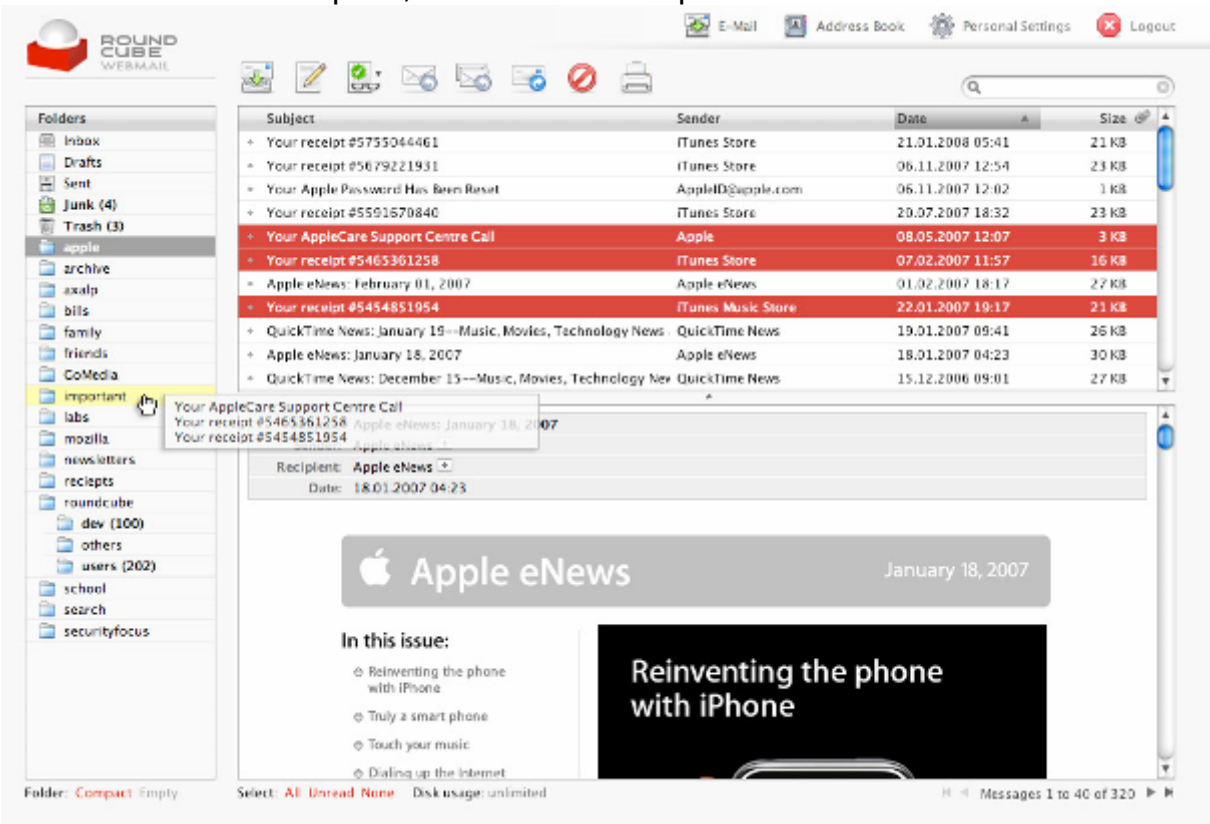
Pour configurer RoundCube il faut déplacer les fichiers :

```
mv ./config/db.inc.php.dist ./config/db.inc.php
mv ./config/main.inc.php.dist ./config/main.inc.php
```

Et modifier les paramètres :

```
 Fichier : config/db.inc.php
1 $rcmail_config['db_dsnw']             =           $rcmail_config['db_dsnw']           =
2 'mysql://roundcube:Rcube963@172.10.140.3/roundcubemail';
3
4 Fichier : config/main.inc.php
5 $rcmail_config['default_host']  =  ''172.10.140.3';  $rcmail_config['smtp_server']  =
  '172.10.140.3';
```

On peut maintenant accéder à ses mails en utilisant le Webmail Roundcube. Il offre la possibilité de voir les mails que l'on a reçus mais aussi d'envoyer des emails et d'afficher les mails spam, si on a un anti spam installé sur le serveur mail.



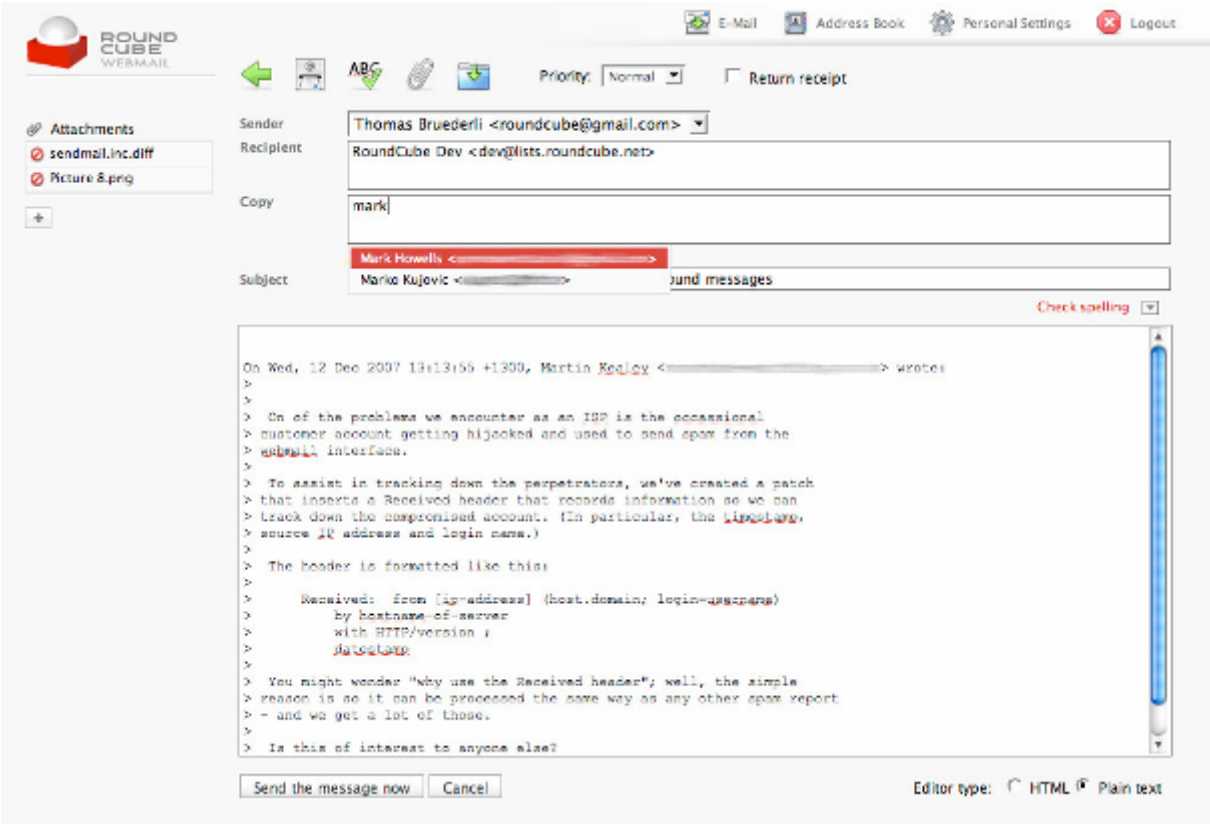


Figure 1 : Exemple - Création d'un mail avec Roundcube

4.6.6 Sécurisation du serveur Mail

La sécurité mise en place sur le serveur mail a été minimale, un audit a été fait par l'équipe analyse sur les fichiers Postfix et courier. Ils nous on fournit quelque éléments afin de réduire les attaques.
Dans le fichier main.cd ils ont proposé de rajouté ces éléments :

```
##### Ajout conseil Anlayse ####
#rejet permanent des utilisateurs non connu
unknown_local_recipient_reject_code = 450

#doit s'annoncer en faisant un helo
smtpd_helo_required = yes
#limit d'attente du hello
smtp_helo_timeout = 60s
#nombre d'erreurs maximum autorisé avant retour point précédent
smtpd_soft_error_limit = 3
#nombre d'erreurs maximum avant fermeture de la connexion
smtpd_hard_error_limit = 12

#smtpd_client_connection_count_limit = 35
#smtpd_client_recipient_rate_limit = 35
#smtpd_client_connection_rate_limit = 10

# réseau autorisé à faire un helo
#smtpd_helo_restrictions = permit_mynetworks, warn_if_reject reject_non_fqdn_hostname, reject_invalid_hostname, reject

# réseau autorisé à faire un 'mail from:'
```

```
#smtpd_sender_restrictions = permit_mynetworks, warn_if_reject reject_non_fqdn_sender, reject_unknown_sender_domain, reject_unauth_pipelining, reject

# accèpte la partie 'rcpt to:'
#smtpd_recipient_restrictions = reject_unauth_pipelining, permit_mynetworks, reject_non_fqdn_recipient, reject_unknown_recipient_domain, reject_unauth_destination, permit smtpd_data_restrictions = reject_unauth_pipelining


#incrémenter à chaque tantative infructueuse le temps d'attente
smtpd_delay_reject = yes

#désactive le scannage des adresses mails du serveur
disable_vrfy_command = yes
```

Il y a certaines règles qui ont été commentée, car en faite si elle avait été mise en place, les attaquants n'auraient jamais pu envoyer de mail.
Certaines des ces règles gèrent quel type de réseau sont autorisés à faire un « helo » ou un « mail from » ou mettre des limite d'ouverture de connexion par client qui souhaite envoyé un mail.

4.6.7 2eme Confrontation : Problèmes rencontrés

Le serveur de messagerie aurait du être disponible à la deuxième confrontation, sauf qu'il n'a été finalisé que pour la 3eme confrontation.

Pour la deuxième, le serveur Postfix était prêt à fonctionner, le problème qui a fait que l'on ne l'a pas mis en place c'est qu'il était impossible d'accéder en webmail à la base de données qui stockait les utilisateurs du serveur mail.

Le problème se situé au niveau des accès à la base de donnée du serveur mail, il fallait autoriser les ip à communiquer avec la BD dans MySQL. Quand la BDD a été créée la première fois elle a été déclarée comme suit :

```
mysql>GRANT ALL PRIVILEGES ON postfix.* TO 'adminpostfix'@'172.10.140.3' IDENTIFIED BY 'P@ssP0stfix';
```

Seules les connexions de la machine 172.10.140.3 fonctionnaient. Pour éviter ce problème, et aller au plus vite j'ai recrée la BDD en utilisant le paramètre % qui permet à n'importe quelle machine d'accéder a la BD.

```
mysql>GRANT ALL PRIVILEGES ON postfix.* TO 'adminpostfix'@'%' IDENTIFIED BY 'P@ssP0stfix';
```

Ce n'est pas sécurisé mais c'était rapide à faire. Pour plus de sécurité il aurait fallut faire 2 Grant All privilèges, un avec l'adresse du serveur Web et l'autre avec l'adresse du serveur Mail. La communication n'aurait été possible qu'entre les deux machines.

Le problème de la connexion à la BD réglé, je me suis rendu compte que le serveur Postfix ne fonctionnait pas correctement, les mails pouvait être envoyés en local, c'est-à-dire en utilisant la commande mail de la console. Les mails été stockés

correctement et affichés sous RoundCube. Par contre il était impossible d'envoyer un email depuis RoundCube.

Ce problème venait du fait que RoundCube utilise la fonction mail() de php afin d'envoyer ses emails. Le serveur apache utilisé Mod Security afin d'être plus sécurisé, ModSecurity bloqué la fonction Mail() de Php, j'ai donc du spécifier a RoundCube le serveur SMTP a utiliser pour envoyer des emails.
$rcmail_config['smtp_server'] = '172.10.140.3';

4.6.8 3eme Confrontation

Lors de la 3eme confrontation les attaquants ont lancés des attaques contre le serveur de messagerie. Il on lancé un script qui envoyé un mail a l'adresse contact@candide-sa.com.
Ils n'ont pas particulièrement fait de dégâts, leur méthode d'attaque (apparente) a été d'envoyer le même message autant de fois que possible.

Je n'ai pas la capture Roundcube, mais je peux montrer le du message qu'ils ont envoyé.

L'entête

```
Return-Path: <root@tuxi.lan-211.stri>
Delivered-To: contact@candide-sa.com
Received: from tuxi.lan-211.stri (unknown [172.18.4.102])
        by mx.candide-sa.com (Postfix) with SMTP id 01C14793
        for <contact@candide-sa.com>; Mon, 17 Nov 2008 10:59:54 +0100 (CET)
Received: by tuxi.lan-211.stri (Postfix, from userid 0)
        id E49A2306DBE; Mon, 17 Nov 2008 10:50:05 +0100 (CET)
To: contact@candide-sa.com
Subject: test
Message-Id: <20081117095005.E49A2306DBE@tuxi.lan-211.stri>
Date: Mon, 17 Nov 2008 10:50:05 +0100 (CET)
From: root@tuxi.lan-211.stri (root)
```

Le corps du message : Il été vide a l'ouverture.

Leur attaque a eu comme effet de remplir le disque dur du serveur Mail. La capacité de la partition ou été stocké les mails été de 10Go, la quantité de message reçu s'est élevée a 6, 7Go sur les 2 heures de l'attaque. Ils auraient normalement du faire tomber le service si ils avaient eu plus de temps.
Par manque de temps je n'ai pas pu mettre en place des fonctionnalités essentielles d'un serveur mail, tel que des Quota par utilisateur, un antispam ou un antivirus. Avec de tels outils, l'envoi de massif de mail aurait été inutile car il aurait été détecté comme spam ou alors arrêté grâce à la gestion des quotas mis en place.

4.7 Le parc client

A la suite de la deuxième confrontation nous avons remis à neuf nos PCs clients et changé les mots de passe administrateur et utilisateurs. Sur le PC protégé nous avons mis à jour notre anti-virus pour pouvoir être protégé des derniers virus.

De plus nous avons changé la passerelle des PC clients en mettant celle du pare-feu et nous avons également changé l'adresse DNS en mettant celle de notre serveur DNS interne à l'entreprise.
Lors de la confrontation, le processus était le même que les deux autres confrontations. Nous nous sommes donc rendus sur leur site internet afin de suivre la démarche à exécuter. Sur le SP1, lorsque nous avons accédé à leur site, un processus s'est installé (nous l'avons laissé pour jouer le jeu) et quelques minutes après le pc a redémarré. Une fois redémarré, un message d'erreur est apparu sur le bureau de l'utilisateur. Le message d'erreur signifiait en fait que le trojan s'est bien installé.
L'équipe attaque avait donc pris le contrôle de la machine SP1 grâce à une faille de sécurité qui a été corrigé avec le SP2.
L'équipe attaque avait fait des recommandations auprès de notre responsable communication, en effet il fallait installer « Excel ». Nous avons donc installé le viewer d'Excel. Une consigne était de téléchargé un dossier rar contenant des fichiers Excel et de les ouvrir. Malheureusement, les fichiers contenaient des macros et le viewer ne peut pas les exécuter. En effet sur la recommandation, il ne nous précisait pas de ne pas installer le viewer. Ces fichiers Excel n'ont donc rien donnée.
Il souhaitait également que l'on se connecte via telnet ou putty en SSH sur une machine mais notre politique dé sécurité bloquait les requêtes SSH du client.
Sur le SP3, aucune attaque n'a été observée. Il nous encore fait lancer un fichier nommé « boucle.exe » qui ne faisait qu'afficher des fenêtres à l'infini. Une simple fermeture de session ou « terminer le processus » permettait de supprimer ces fenêtres.
Nous avons donc pu apercevoir lors de ces différentes confrontations que plusieurs failles de sécurité ont été corrigées à partir du Service Pack 2 de Windows XP. En effet notre pc client SP3 n'a subit aucune dégradation.

4.8 Le wifi

4.8.1 Amélioration du système

Pour la troisième confrontation nous avons corrigé un certain nombre de faille et de problème détecté lors de la confrontation précédente.

4.8.1.1 L'attribution d'adresse.

En effet lors de la première confrontation dés que plusieurs d'adresse IP avait été distribué par le serveur DHCP, celui-ci s'arrêter. Ce problème été du au nombre d'adresses disponibles qui été limitées par le masque sous réseau par défaut. Nous l'avons donc changé dans la configuration du pool d'adresse IP du serveur DHCP ainsi que sur le routeur.
Cf. Annexe configuration point accès.

4.8.1.2 Interdiction du saut de vlan

L'équipe d'analyse nous a fait ensuite par d'une remarque concernant la possibilité d'attaque par saut de vlan. En effet le wifi étant ouvert au public il aurait été possible, en modifiant l'entête des trame Ethernets la balise de vlan (802.1q), de s'introduire sur un vlan interne. Cette faille a donc été corrige en paramétrant correctement le Switch et en interdisant le saut de Vlan.
Cf. 3.7 Le Switch

4.8.1.3 Accès wifi du personnel

Enfin nous avons mis en place un nouveau service pour les employés de l'entreprise qui on un besoin de mobilité important, et qui souhaitent avoir accès à l'ensemble du réseau de l'entreprise. Ce service permet de se connecté par le Wifi, de manière sécurisé, au réseau interne de l'entreprise. Pour cela ces usagers sont considérés comme des télétravailleurs (travail a distance). Nous avons simulé dans le cadre de ce projet cette connexion en utilisant la connexion VPN. La sécurité est ainsi garantie par un cryptage des données haut niveau. Pour mettre en place ce service il suffit d'ouvrir le port 65022 sur le routeur pour le vlan wifi. Ensuite nous avons suivis la procédure de connexion au VPN.

Cf. 4.8-5.8 VPN

4.9 Le VPN

Intérêt de la mise en place de notre VPN :

Avoir son autorité de certification pour pouvoir créer autant de certificats que l'on souhaite avec la plus grande confiance (puisque c'est nous même qui les créons).
Nous pourrons donner à chaque client VPN un certificat qu'il lui est propre et ainsi l'adresse IP de notre choix (selon son affectation). Exemple : 1 groupe du vlan métier n'aura pas le même certificat qu'un groupe du vlan Supervision.

Installation des paquets sur le serveur :

- openvpn
- openssh-server
- openssl

Le principe :

La première étape dans la construction d'une configuration OpenVPN est d'établir une PKI. On a donc besoin :

- Une clé publique pour le serveur et une clé privée pour chacun des clients
- Un certificat de l'Autorité de Certification maître et des clés qui sont utilisées pour identifier (signer, identifier…) chaque certificat serveur et client.

OpenVPN supporte une authentification bidirectionnelle basée sur les certificats, ce qui signifie que le client doit authentifier le certificat du serveur et le serveur doit authentifier le certificat du client avant qu'une confiance mutuelle puisse être établie.

Générer le certificat et la clé de l'Autorité de Certification maître

Nous avons générer un certificat/une clé de l'Autorité de Certification maître, un certificat/une clé pour le serveur et des certificats/des clés pour 3 clients différents. Pour la gestion de la PKI, nous utiliserons un jeu de scripts livrés avec OpenVPN. Il faut tout d'abord ouvrir un terminal et effectuer une copie dans son dossier /home des scripts de génération de clés :

```
cp /usr/share/doc/openvpn/examples/easy-rsa ~/openvpn/ -R
cd ~/openvpn/2.0/
```

Maintenant nous éditons le fichier vars et nous initialisons les variables KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, and KEY_EMAIL comme ci dessous.
Nous générons une clé de 2048 bits.

```
export KEY_SIZE=2048
export KEY_COUNTRY=fr
export KEY_PROVINCE=midipyrenees
export KEY_CITY=toulouse
export KEY_ORG=candide-sa.com
export KEY_EMAIL=admin@candide-sa.com
```

On initialise les variables :

```
./vars
```

On nettoie toutes les clés et certificats existants :

```
./clean-all
```

Puis, nous créons le certificat de l'Autorité de Certification :

```
./build-ca
```

Le certificat de l'Autorité de Certification est à présent créé.

Générer un certificat et une clé pour le serveur

Nous générons ensuite un certificat et une clé privée pour le serveur :

```
./build-key-server vpn
```

Dans notre cas, le nom de notre serveur est : `vpn`
Quand le Common Name est demandé, il faut entrer « vpn » comme le dernier paramètre entré dans la commande précédente. Puis nous mettons un mot de passe. Le certificat du serveur est à présent créé.

Générer les certificats et les clés pour 1 client

Générer des certificats et des clés pour 1 client est une étape similaire à l'étape précédente. Exemple avec un client nommé test :

```
./build-key test
```

Quand le Common Name est demandé, il faudra donc entrer « client1 »

```
./build-key test
```

Il faut toujours se rappeler que pour chaque client, le champ Common Name doit être renseigné et unique. Nous pouvons donc créer autant de client que nous le souhaitons.

Générer des paramètres Diffie-Hellman

Les paramètres Diffie Hellman doivent être générés pour le serveur OpenVPN :

```
./build-dh
```

Voici tous les fichiers générés :

Nom de fichier	Utile à	Utilité	Secret
ca.crt	serveur et tous les clients	certificat racine CA	non
ca.key	clé signant la machine seulement	clé racine CA	oui
dh2048.pem	serveur seulement	paramètres Diffie Hellman	non
server.crt	serveur seulement	certificat serveur	non
server.key	serveur seulement	clé serveur	oui
test.crt	client test seulement	certificat test	non
test.key	client test seulement	clé test	oui

Configuration du Serveur

Nous éditons le fichier /etc/openvpn/server.conf
Nous modifions :

```
#Les 4 fichiers que l'on vient de créer et que l'on place dans le bon
répertoire
ca ../keys/ca.crt
cert  ../keys/ vpn.crt
key ../keys/ vpn.key
dh ../keys/dh2048.pem

# ifconfig 10.18.0.1 10.18.0.2 configure l'interface tun du serveur
ifconfig 10.18.0.1 10.18.0.2

#La directive route 10.18.0.0 255.255.255.252 ajoute une route statique au
```

```
serveur VPN pour joindre #les clients du VPN.
route 192.168.0.0 255.255.255.252
#La directive push "route 10.18.0.0 255.255.255.252" force les routes au client lors de sa connexion.
push "route 192.168.0.0 255.255.255.252"
push "route 172.10.170.0 255.255.255.248"

# client-config-dir ccd  permet de forcer les clients à utiliser les paramètres contenu dans le fichier #ccd/[CommonName Client] du répertoire :
client-config-dir ccd
```

Nous éditons le fichier etc/openvpn/cdd/test (qui correspond à la liste des paramètres de notre client test) :

```
#On force son IP à 10.18.0.5 avec une passerelle vers le VPN de 10.0.8.0.6
ifconfig-push 10.18.0.5 10.0.8.6
```

Attention ! Le client en mode routé obtient une IP, un réseau, un broadcast et un gateway. Pour que cela fonctionne dans tous les cas, sous Windows, le driver de carte réseau TAP-WIN32 a besoin de travailler avec un sous réseau de 252.

Ainsi nous ne pouvons pas adresser n'importe comment nos clients, et toutes les IP ne sont pas disponibles. Les couples d'IP (IP du client, IP du serveur pour le client) sont donc limités aux possibilités suivantes (openvpn -show-valid-subnets pour les retrouver) :

[1, 2] [5, 6] [9, 10] [13, 14] [17, 18] [21, 22] [25, 26] [29, 30] [33, 34] [37, 38] [41, 42] [45, 46] [49, 50] [53, 54] [57, 58] [61, 62] [65, 66] [69, 70] [73, 74] [77, 78] [81, 82] [85, 86] [89, 90] [93, 94] [97, 98] [101,102] [105,106] [109,110] [113,114] [117,118] [121,122] [125,126] [129,130] [133,134] [137,138] [141,142] [145,146] [149,150] [153,154] [157,158] [161,162] [165,166] [169,170] [173,174] [177,178] [181,182] [185,186] [189,190] [193,194] [197,198] [201,202] [205,206] [209,210] [213,214] [217,218] [221,222] [225,226] [229,230] [233,234] [237,238] [241,242] [245,246] [249,250] [253,254]

Configuration du client sous windows comme avec l'ancien VPN

Nous éditons le fichier C:\Program Files\OpenVPN\ovpn

Nous modifions :

```
#Nous utiliserons le protocole TCP
proto tcp
```

```
#Les 3 fichiers que l'on vient de créer et que l'on place dans le répertoire
config
ca ca.crt
cert  test.crt
key test.key

#l'adresse du serveur qui sur le port 65022 fait un forward vers notre
serveur
remote ovpn-stri.iut-tlse3.fr 65022
```

Iptables

Nous configurons l'iptables afin que chaque client vpn (avec son adresse IP spécifique) ne puisse pas accéder à des informations qui ne le concernent pas.

4.10 La supervision Nagios

Lors de la troisième confrontation nous avions réussis à mettre en place la supervision du routeur via le protocole SNMP (Simple Network Management Protocol). Grâce à ce protocole nous pouvions remonter les informations sur la charge CPU, charge mémoire du routeur. Mais nous n'avons pas réussi à mettre en place les résultats sous forme graphique.

4.11 La supervision Nagios

Lors de la troisième confrontation nous avions réussis à mettre en place la supervision du routeur via le protocole SNMP (Simple Network Management Protocol). Grâce à ce protocole nous pouvions remonter les informations sur la charge CPU, charge mémoire du routeur. Mais nous n'avons pas réussi à mettre en place les résultats sous forme graphique.

4.12 Le Firewall

Pour optimiser le filtrage du trafic à l'intérieur de notre réseau nous avons choisi de mettre en place un Firewall. Ce Firewall nous permettra de filtrer plus finement le trafic entrant et sortant du réseau.

4.12.1 Configuration utilisée

Pour mettre en place notre firewall, nous avons choisi d'utiliser un poste physique dédié totalement au filtrage. Ce choix vient du fait que nous ne voulions pas rencontrer des problèmes de charge CPU sur cette partie du réseau. En effet la fonction de filtrage est une fonction importante pour le fonctionnement du réseau.
Au niveau logiciel, nous avons choisi de mettre en place une solution DEBIAN etch, ce qui nous permet d'utiliser les fonctions Iptables et netfilter, qui sont des fonctions très complètes et tout à fait adaptées à la solution de firewall que nous voulons mettre en place.

4.12.2 Préparation du firewall

Une fois l'OS du firewall installé, nous avons configuré le Switch de telle façon que le trafic entrant sur le réseau passe par le firewall (configuration d'un TRUNK). De cette façon, nous pourrions filtrer le trafic désiré. De plus, nous avons créé 7 interfaces logiques, permettant d'avoir une patte réseau vers le routeur, parc client, serveur métier, DMZ, Vlan supervision, etc.…

4.12.3 Configuration du firewall

4.12.3.1 Script pour désactiver le firewall

Ce script que nous avons nommé et placer dans « **/etc/firewall-stop** » permettra de désactiver le firewall :

```
#!/bin/sh

# Nous vidons les chaînes :
iptables -F
# Nous supprimons d'éventuelles chaînes personnelles :
iptables -X

# Nous les faisons pointer par défaut sur ACCEPT
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

# Cette ligne permet de supprimer toutes les redirections de ports
iptables -t nat -F
```

4.12.3.2 Script pour démarrer le firewall

Ce script que nous avons nommé et placer dans « /etc/firewall-stop » permettra de désactiver le firewall :

```
#!/bin/sh

# REMISE à ZERO des règles de filtrage
iptables -F
iptables -t nat -F

# Mise en place des régles par défaut
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# On enlève le firewall sur le loopback et le reseau local
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT

iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Ouverture de ports
# Exemple pour un port TCP (ici 80)
# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
# Exemple pour un port UDP (ici 110)
# iptables -A INPUT -p udp --dport 110 -j ACCEPT
# Exemple d'un ensemble de ports (de 2072 a 2080 inclus)
# iptables -A INPUT -p tcp --dport 2072:2080 -j ACCEPT

# J'accepte le protocole ICMP (i.e. le "ping")
iptables -A INPUT -p icmp -j ACCEPT

# J'accepte le protocole IGMP (pour le multicast)
iptables -A INPUT -p igmp -j ACCEPT

# J'accepte les packets entrants relatifs à des connexions déjà établies
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Décommentez les deux lignes suivantes pour que le serveur FTP
éventuel
# soit joignable de l'extérieur
#iptables -A INPUT -p tcp --dport 20 -j ACCEPT
#iptables -A INPUT -p tcp --dport 21 -j ACCEPT

# Décommentez la ligne suivante pour que le serveur SSH éventuel
# soit joignable de l'extérieur
#iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
# A placer en FIN DU FICHIER
iptables -A INPUT -j DROP
```

4.12.3.3 Arrêt et démarrage manuel du firewall

Avant de lancer les scripts, il faut les rendre exécutables :

```
# chmod +x /etc/firewall-start
# chmod +x /etc/firewall-stop
```

Ensuite, il est possible de lancer manuellement le firewall et de vérifier le résultat :

```
# /etc/firewall-start
# iptables -L -v
```

Il est possible également de l'arrêter manuellement et de vérifier le résultat :

```
# /etc/firewall-stop
# iptables -L -v
```

4.12.3.4 Lancement automatique du firewall au démarrage

Pour activer le firewall automatiquement au démarrage de l'ordinateur, il faut créer le script « **/etc/init.d/firewall** » contenant les lignes suivantes :

```
#!/bin/sh
stop() {
/etc/firewall-stop
}

case $1 in
"start")
/etc/firewall-start
;;
"stop")
stop
;;
"restart")
stop
/etc/firewall-start
;;
esac
```

Rendre ce script exécutable avec la commande :

```
chmod +x /etc/init.d/firewall
```

Créer les liens permettant de démarrer automatiquement le script au démarrage de l'ordinateur :

```
# update-rc.d firewall defaults
```

La commande suivante permet d'arrêter le firewall :

```
# /etc/init.d/firewall stop
```

La commande suivante permet de démarrer le firewall :

```
# /etc/init.d/firewall start
```

4.12.4 Configuration coté serveur et client métier

Une fois le firewall mis en place, il nous a fallu configurer les postes clients et les serveurs pour qu'il puisse passer par le Firewall et non plus directement par le routeur. Pour cela, il a juste fallu modifier la route par défaut, qui est devenu celle du Firewall (172.18. ***.2).

4.12.5 Conclusion

La mise en place du Firewall nous a posée pas mal de problèmes, tout d'abord au niveau de la configuration du TRUNK et des interfaces logiques. Nous avons perdu beaucoup de temps pour cette partie de la configuration, dû à un manque d'informations disponibles sur le sujet. Ensuite, nous avons rencontré quelques problèmes au niveau de la configuration du Firewall en lui-même, plus particulièrement les iptables. Notre liste de règles était longue, et la configuration nous à pris pas mal de temps.
Cependant le firewall nous a permit de filtrer plus de trafic que le routeur n'en filtré. En regardant les paquets REJET / ACCEPT, nous avons remarqué que beaucoup de règles que nous avons mis en place étaient indispensable au bon fonctionnement du réseau, et plus particulièrement des règles évitant des attaques réseaux.

5. ANNEXES

Annexe 1 : compte rendu de la première réunion

Compte rendu de la première réunion

Lors de cette réunion plusieurs points ont étaient abordés :

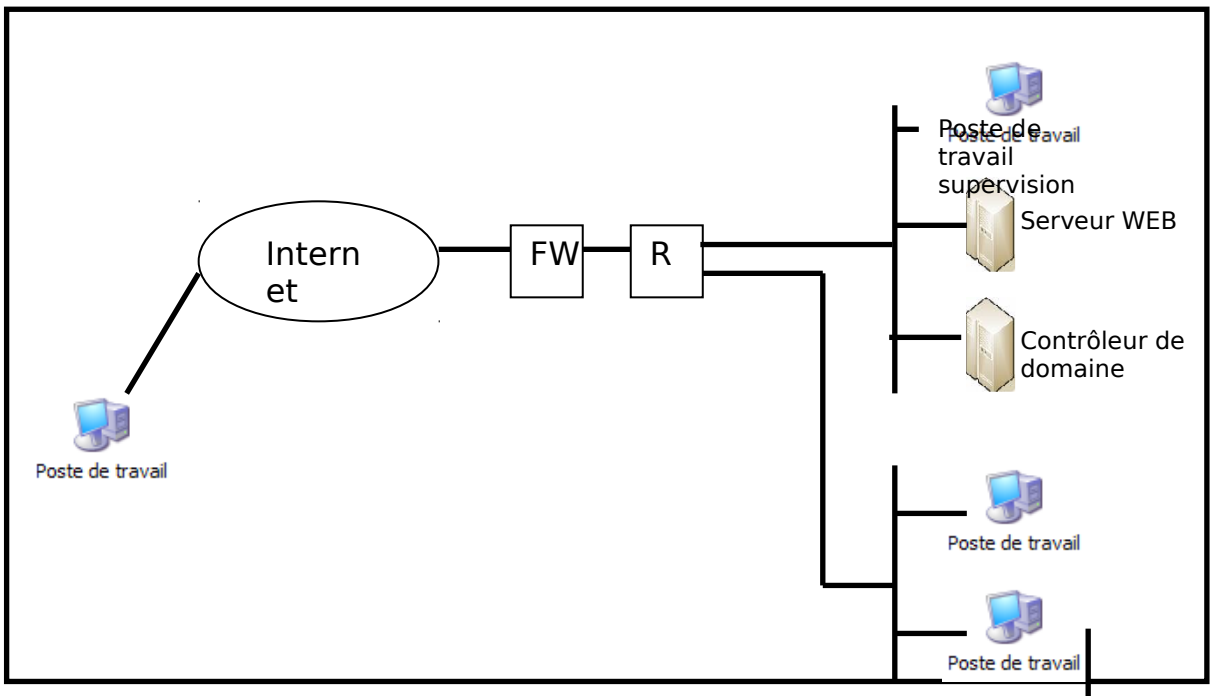
- Dates des différentes confrontations
- Choix de l'architecture de travail
- Liste des différents points à mettre en place afin de garantir la sécurité de cette infrastructure
- Mise en place d'un outil de travail collaboratif
- Création des différents pôles de compétences
- Organisation du travail et date de la prochaine réunion

Dates des différentes confrontations

1ere Confrontation : 13/10/2009
2eme Confrontation : 3/11/2009
3eme Confrontation : 17/11/2009

Choix de l'architecture de travail

Ceci est une schématisation de l'architecture de base à mettre en place pour la première confrontation



Différents points de sécurité

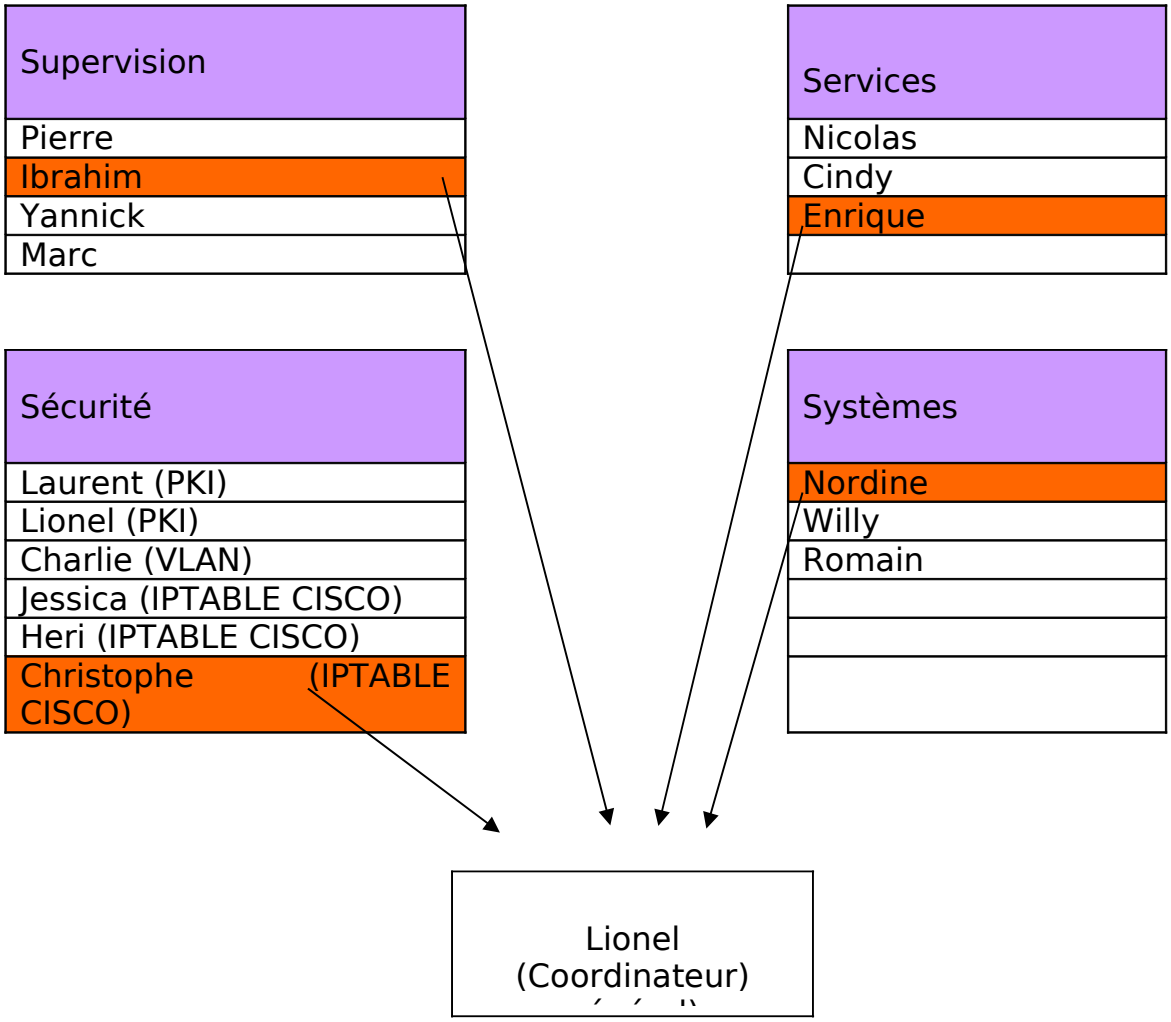
- Virtualisation
- Ghost (reprise d'activité)
- FireWall (IPTABLE)
- Supervision (Nagios …)
- VPN (PKI et certificats)
- Wifi
- Politique de sécurité
- Antivirus
- Gestions des logs
- Plan de reprise
- Code PHP pour site web
- Gestion des utilisateurs (contrôleur de domaine)

Outil de travail collaboratif

Pour le moment la liste de diffusion mise à disposition par Monsieur Latu sera utilisée afin de communiquer enter nous.
Par la suite l'outil « GoogleDocs » sera mis en service afin de travailler en commun sur les même documents.

Différents pôles de compétences

Sur le schéma ci-dessous les différents groupes avec en orange les coordinateurs de chaque groupe.



Organisation du travail

Chaque groupe doit commencer à se documenter sur la partie à laquelle il est assigné et rédiger un compte rendu de la solution qu'il souhaite mettre en place.
Ce compte rendu devra être envoyé mardi soir au coordinateur général.
Une réunion de générale est fixée Mercredi 1 Octobre à 10h dans le bâtiment U2.
Lors de cette réunion chaque coordinateur de groupe devra décrire et expliquer la solution qu'ils souhaitent mettre en place.

Annexe 2 : contrat de l'équipe audit

CONTRAT D'AUDIT

lundi 13 octobre 2008	Salle U2
Objet	Contrat avec l'équipe d'audit
Participants	Responsables groupes *analyse/défense*

Sommaire

Suite à la demande du client ***Candide S.A*** d'établir un **audit réseau** de son infrastructure, nous établissons le **contrat** ayant pour but de définir une **collaboration entre les équipes *défense* (Candide SA) et *analyse*.**

Cette collaboration doit **assurer le bon fonctionnement de la mission d'audit de sécurité** par la validation des moyens de protection mis en œuvre sur les plans organisationnels, procéduraux et techniques, au regard de la politique de sécurité rédigé par les soins de la *défense*.

Nous avons donc convenu après négociation avec la *défense*, les **clauses** suivantes :

Article1 - Informations sur le Réseau :

L'audité, ayant confié à l'équipe d'*analyse* le soin d'assurer un audit complet des systèmes d'information de *Candide S.A*, s'engage à fournir le recensement détaillé de l'ensemble des éléments qui constituent ce système. **L'auditeur aura accès aux informations suivantes:**

- **Réglementation interne, procédures, organigramme du personnel, charte d'utilisation des ressources.**
- **Sécurité physique :** Normes de sécurité, protection des accès (équipements, infrastructure câblée, etc.).
- **Exploitation et administration :** journalisation des logs, informations SNMP.
- **Réseaux et télécoms :** architecture réseau (topologie, plan d'adressage), matériels (routeurs, commutateurs, pare-feux), contrôle des accès logiques.
- **Systèmes :** poste de travail (gestion des droits), serveurs et les services qu'ils délivrent, applications, solutions antivirales, ainsi que le détail des versions utilisées.

PK

Article2 - Périmètre d'actions de l'audit :
Ayant connaissance des éléments composant le système d'information, l'**auditeur** pourra **définir le périmètre de l'audit** et **planifier ses interventions et ses entretiens** avec les personnes à interviewer au sein de la *défense*. L'équipe d'***analyse*** sera **responsable de l'organisation des réunions avec l'équipe auditée** et devra, à l'issue de celles-ci, proposer des recommandations pour la mise en place de mesures organisationnelles et techniques.

Article3 - Mise en place des outils de supervision :
L'audité conviendra avec l'auditeur d'un **droit d'accès physique au système** pour la **mise en place d'outils d'analyse et de détection** (analyse des logs, scans, sondes, récupération de trafic). Sur autorisation explicite de la *défense*, l'auditeur pourra effectuer des **tests d'intrusions** selon des scénarios potentiels d'attaque, afin de déterminer les vulnérabilités et les failles de sécurité.

Article4 - Compte-rendu :
Chaque phase d'analyse et d'évaluation réalisée par les soins de l'équipe d'***analyse*** devra faire l'œuvre d'un **rapport complet** présentant de manière explicite les **vulnérabilités détectées sur le système audité**, et **proposant des améliorations techniques et organisationnelles** pouvant entraîner une revue de la politique de sécurité.
A son tour la ***défense*** devra informer l'auditeur de **toute modification ou évolution de son système de sécurité.**

Article5 - Confidentialité :
L'organisme d'audit, à savoir l'ensemble des personnes qui interviendra pour la mission d'audit de sécurité, s'engage, sous sa responsabilité exclusive, à considérer confidentielles toutes informations transmises par la *défense*, de façon orale ou écrite, et par conséquent à ne pas les divulguer à un tiers. Une **clause de confidentialité** sera établie **à l'initiative de la *défense*** et devra faire l'objet d'une **signature par l'ensemble des membres composant l'équipe d'*analyse*.**
L'organisme d'audit est entièrement responsable de la sécurisation de la sonde et de l'accès au réseau de la *défense* par celle-ci.
De la même manière, les différents droits octroyés à l'organisme d'audit sont sous leur entière responsabilité.
En cas de violation volontaire ou négligente de cette clause, la ou les personnes responsables devront répondre de sanctions négociées au préalable avec la *défense*.

Article6 - Cadre juridique :
L'organisme audité doit être conscient de la législation concernant les systèmes d'informations. Les responsables de sécurité ont une obligation de moyens pour que leur système de sécurité rentre en conformité juridique. Ils doivent être vigilants au respect de la protection des données privées des employés. L'organisme responsable doit également sensibiliser ses employés sur le cadre d'utilisation d'internet. Un usage abusif sortant du cadre professionnel pouvant induire des problèmes de sécurité et mettre en cause la responsabilité civile ou pénale de l'entreprise et de l'employé.
A cet effet une **charte d'utilisation de l'informatique et des** télécommunications devra être établie à l'initiative de la *défense*.

Article7 - Financier :
Par ce contrat **la *défense* s'engage à prendre en charge la totalité des frais matériels** indispensables à la mise en place d'une supervision efficace. Une fois l'installation effectuée, une rémunération mensuelle sera versée à l'organisme d'audit pour le travail

P.K

fourni. Une déduction sur cette rémunération pourra être effectuée en cas de responsabilité de l'organisme d'audit dans un quelconque déni de service portant atteinte aux activités de l'entreprise *Candide S.A.*
Au terme des actions entreprises par l'équipe d'attaque durant le temps imparti aux trois séances de TP, et après établissement du rapport d'analyse, un bilan organisationnel et technique de la mission accomplie par les deux équipes en collaboration permettra d'évaluer la part de responsabilité de la *défense* et de *l'audit*.

Article8 - Modification de Contrat :
Pour des éventuelles **modifications** de contrat des avenants seront produits et devront être **obligatoirement signés par les deux partis** que ce soit pour une modification mineure ou majeure afin que tout malentendu soit évité.

Article9 - Intégrité physique :
L'audit se dégage de toute responsabilité dans l'éventualité d'une attaque de niveau physique, le matériel étant hébergé dans les locaux clients ; **La *défense* prendra** donc **en charge l'intégrité physique du matériel de supervision.**

Article 10 – Accès à distance :
L'équipe *défense* s'engage à fournir un **accès sécurisé depuis l'extérieur de l'entreprise.** Cet accès permettra à l'équipe *analyse* d'accéder à ses équipements, donc à l'ensemble des machines qu'elle aura pu installer au sein de l'entreprise *Candide S.A.*

Signatures des deux parties *(précédées de la date et de la mention « lu et approuvé »)* :

Pour le groupe ***Défense***,
M. Rouault
Le 13/10/08
Lu et Approuvé
"Lu et Approuvé"

Pour le groupe ***Analyse***,
M. Pooga KHADEMI
Le 13/10/08
Lu et Approuvé
"lu et Approuvé"

Annexe 3 : Clause de confidentialité

Clause de confidentialité

La présente charte à pour objet de formaliser les règles de déontologie et de sécurité que les membres du groupe "analyse" s'engagent à respecter en contrepartie de la mise à disposition de l'infrastructure réseau mise en place par l'équipe "défense".

- Domaine d'application

Les règles et obligations énoncées ci dessous s'appliquent à tous les utilisateurs système, matériel et réseau informatique du bâtiment "U2". Est déclaré utilisateur toutes les personnes membre du groupe "analyse".
L'utilisateur est en tout lieu responsable de l'usage qu'il fait des ressources informatiques.

Le non respect des règles énoncées dans le présent document engage la responsabilité personnelle de l'utilisateur.

- Règles d'utilisations du matériel informatique des Bâtiments U2 et U3

- Ne pas utiliser les boites mail personnelles sauf dans le cas d'utilisation de LiveCd (qui pourront vous être fourni par l'équipe défense)
- Effacer toutes les traces de navigation après le passage sur l'une des machines
- Fermeture des sessions après utilisation d'un poste
- Remise à zéro des machines linux après leurs utilisations
- changement des mots de passes des comptes mail réguliers
- De verrouiller son poste de travail en cas d'absence et/ou d'utiliser les économiseurs d'écran avec mot de passe afin de préserver l'accès à son poste de travail

- Droits et devoir de l'utilisateur

- Être en accord avec les politiques de sécurité de l'équipe "défense"
- Interdiction de divulguer quelconques informations à l'équipe "attaque"
- Le droit d'accès est temporaire et il sera retiré si la qualité de l'utilisateur ne le justifie plus ou le comportement n'est plus en accord avec les règles énoncées dans la présente charte
- De garder confidentiel ses mots de passes et de ne pas les divulguer à un quelconque tiers

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouvait dans l'obligation de communiquer son mot de passe, il devra procéder, dès qu'il en a la possibilité, au changement de mot de passe ou en demander la modification à l'administrateur.

- D'avertir les administrateurs de tout dysfonctionnement constaté
- D'avoir une obligation de confidentialité et de discrétion à l'égard des informations et documents électroniques à caractère confidentiel disponibles dans le système d'information
- De respecter l'architecture réseau de l'équipe "défense" et de ne pas modifier sa configuration (connexion d'équipement réseau sur les prises murales)
- ne prendre aucune copie des documents et supports d'informations confiés, à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales

- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques
- prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations
- et en fin de contrat à :
  - procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies ;

  ou à :
  - restituer intégralement les supports d'informations selon les modalités prévues au présent contrat.

- Droits de l'équipe défense

- L'équipe "analyse"

se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par l'équipe "analyse".

- Il est rappelé que, en cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-17 et 226-5 du code pénal.
- L'équipe "défense" pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

Fait le 10/10/2008 à TOULOUSE signature

Nicolas LEYMARIE

Cyrille HOUANSOU

Walter GIN

Jean Thierry ENOH

Karen Alexandre

Cécile ZANNEAETONNE

Sylvain LACOUE

Sami KACHA

ISSAH Thomas

GALONNIER Arnaud

MADELAINE Nicolas

LEBRETON Julien

KHADEMI Pooya

MACHETO Jérémy

JAMOIS Frédéric

LEGALLAIS Dimitri

Anh Dung Hoang

Libasse Hanne

Annexe 3 : choix de virtualisation

Depuis quelques années, la virtualisation est au cœur des préoccupations des entreprises du secteur informatique. Pour une entreprise, les technologies de virtualisation permettent de séparer des applications et des systèmes de manière logique. En effet elle permet de faire fonctionner sur une seule machine physique plusieurs systèmes d'exploitation ou plusieurs applications.

La virtualisation permet de réduire le nombre de machines physiques à acheter, administrer et maintenir. Il y a donc une économie financière à la clef, qui peut être substantielle si l'entreprise a besoin de beaucoup de serveurs pour son activité. En plus du simple gain en nombre de machines, les économies réalisées en consommation d'électricité, location d'espace dans un Datacenter et location de bande passante sont aussi à prendre en compte.

Intérêt de la virtualisation pour le projet :

- Remise en service rapide après un incident :(évite perte de temps)
- Simuler un parc de machine visualisé (en développement dans les entreprises).
- Optimiser la sécurité en centralisant sur une machine hôte (à vérifier)

Un des principaux avantages de la virtualisation est de pouvoir supporter des systèmes d'exploitation invités hétérogènes.
Les technologies de virtualisation sont donc très intéressantes car elles permettent de réduire le temps passé à administrer les machines et les systèmes en automatisant et centralisant la plupart des activités traditionnelles. Il existe de nombreuses solutions permettant de faire de la virtualisation. Les solutions sont relativement équivalentes en ce qui concerne le réseau. Elles permettent toutes de mettre en place de la redondance, même si cette tâche est un plus fastidieuse en environnement XenServer qui requiert l'usage de l'outil en ligne de commande. Tous les produits supportent le standard 802.1q qui permet de créer des réseaux virtuels.
Ces solutions se distinguent selon différents critères.

Notre besoin est d'installer des clients sous Windows XP. Pour le moment nous avons deux clients mais notre parc pourrait évoluer dans l'avenir.
Nous avons donc choisi de vous présenter les trois principales solutions de virtualisation pour PC clients.

- **Virtual PC**

Virtual PC est la solution Microsoft de virtualisation adaptée aux stations. C'est une machine virtuelle, c'est-à-dire un logiciel gratuit qui tourne sur l'OS hôte. Ce logiciel permet de lancer un ou plusieurs OS invités. La machine virtualise le matériel pour les OS invités, ces derniers croient dialoguer directement avec le matériel.
L'unité centrale de calcul (le microprocesseur), la mémoire de travail (ram) ainsi que la mémoire de stockage (via un fichier) sont directement accessible aux machines virtuelles.
Pour virtualiser un parc de client sous Windows xp, ce logiciel n'est pas recommandé. Virtual PC est le meilleur choix pour virtualiser un OS antérieur à Windows 98 avec des applications ayant besoin d'une carte son.
La version de Virtual PC 2007 propose la prise en charge des technologies matérielles Intel VT (Virtualization Technology) et AMD V. Windows Vista est bien sûr supporté officiellement, qu'il soit système hôte ou système invité. Virtual PC 2007 supporte également les systèmes hôtes 64 bits (mais pas les systèmes invités 64 bits).
Virtual PC peut s'installer uniquement sur les systèmes Windows mais peut avoir comme systèmes invités des systèmes tels que DOS, Windows, OS/2 (OS d'IBM), Linux (Suse, Xubuntu), OpenSolaris(Belenix).
Microsoft Virtual PC est aussi disponible en version serveur nommée Microsoft Virtual Server. C'est une évolution de VirtualPC. Il permet de faire tourner des machines virtuelles disposant de 3,6 Go de mémoire maximum. Il est moins performant que VMware ou Xen car il émule les accès aux périphériques à travers Windows alors que ses concurrents font un accès direct aux ressources.
C'est pourquoi nous allons donc maintenant faire un bilan sur les solutions VMware et Xen.

- **XEN**

XEN est un « paravirtualiseur » ou « hyperviseur » de machines virtuelles, c'est à dire que les systèmes invités ont « conscience » de sa présence. Les systèmes d'exploitation invités doivent être modifiées (« portées »).
Dans le cadre de l'émulation de postes clients Windows, la présence de processeurs Intel intégrant la technologie VT (Virtualization Technology) nous permet d'installer des OS Windows « normaux ».
Distribution supportant Xen : Red Hat, projet Fedora, SuSE, Mandriva, Ubuntu Linux, Debian, Gentoo et Arch Linux. Enrique conseil d'utiliser une Gentoo.
Avantage :
performance (pas de pile protocole sur une autre pile protocole), l'une des solutions de virtualisation les plus efficaces en terme de temps de réponse, on exploite les possibilités des processeurs VT, license GPL (pas de limitations en termes de taille de disque simulé, de RAM simulée,…comme sur les versions gratuites de VMware ou VirtualPC), contrôle d'accès sHype/Xen pour autoriser ou refuser la communication et l'accès aux ressources.
Inconvénient :
Installation de Xen complexe,

- **VMware**

VMware utilise son propre format de disques virtuels, le format VMDK. Citrix utilise le format VHD de Microsoft. Les spécifications de ces deux formats de disques virtuels sont ouvertes au public. Il est possible d'utiliser des disques virtuels mais aussi des disques physiques en accès direct (Raw Device Mapping, Passthrough Disk, etc.). En fonction des choix effectués, toutes ou partie des fonctionnalités apportées à la virtualisation ne seront plus disponibles (redimensionnement, snapshot, disque de démarrage de la VM, etc.).
Il est possible de stocker des machines virtuelles sur des baies SAN mais aussi sur des NAS et utiliser l'espace au travers de systèmes de fichiers réseau de type CIFS (Microsoft) ou NFS (Citrix et VMware).
VMware est sans conteste le produit le plus abouti sur le marché, le plus cher aussi, environ 1000 Euros pour VMware Infrastructure 3 Foundation et gratuit chez Citrix avec XenServer Express (pas de support).

Les prix sont tirés vers le haut lorsqu'on souhaite utiliser des fonctionnalités de type VMotion ou XenMotion, jusqu'à 6000 Euros par serveur biprocesseur.
De manière plus générale, on peut aussi comparer le degré de maturité de chacune de ces trois solutions. Autant dire qu'il n'y a aujourd'hui aucun recul sur les produits Microsoft. VMware est sans conteste la solution la plus aboutie, talonnée par Citrix.

Argument pour ou contre

VMware :
Gratuit mais pas libre
Emulation complète, les machines hébergées n'ont pas conscience de qemu.
C'est le plus populaire, donc propose tout pour le néophyte de base => interface graphique de gestion basé sur le mode client/serveur. C'est à dire que l'on peut avoir tes VM sur une machine dédiée, et le client graphique sur un poste client. Permet de gérer à distance (instancier de nouvelle machine, en arrêter, en supprimer, faire des snapshot, etc...)
Facile d'installation.

Xen :
Libre
Encore jeune, mais ça commence à bien marcher.
Peut être couplé avec une interface d'admin web
Intégré par défaut dans les derniers systèmes GNU/Linux (Red Hat 5 par exemple, Debian 4 (bientôt !), Fedora, Suse, Ubuntu, etc...)
Xen est encore jeune, mais il fait plus que bien marcher ! En terme de performance, il n'a rien à envier à VmWare. Pour rappel, Xen est développé par RedHat et IBM.
Depuis les dernières versions de Xen, TOUT OS EST VIRTUALISABLE.
Pas de support technique
Les versions 64 bits de Windows XP et Vista ne sont pas supportées par XenServer.
Par rapport à ces différents critères, nous avons choisi de faire de la virtualisation grâce à XEN. Le chapitre suivant va expliquer l'installation et la configuration de ce système.
Mise en place sur une machine neuve d'une distribution Gentoo car c'est la distribution qui supporte XEN pour la virtualisation. Une fois cette distribution

installée nous avons installé XEN. Cette solution de virtualisation a été choisie car elle permet une transparence ainsi qu'une performance et il n'y a aucune absence de limitation de réseau. De plus elle s'installe sur un système d'exploitation libre donc il n'y a pas besoin de licence.

Annexe 4 : installation de xen

L'installation de Xen se fait en 3 étapes :

- Installation du système Hôte
- Installation du Noyau Xen
- Installation des outils de contrôle de Xen

Installation du système Hôte

L'installation de xen peut se faire à partir des différentes distributions Unix/ Linux, en raison des difficultés rencontrées avec certaines distributions Debian Based et dans l'optique de fournir un service basé sur un système libre OpenSource et Gratuit tout en privillégiant les performances et optimisations du système hôte la distribution Gentoo dans sa déclinaison « Hardened » a été retenue. Cette distribution bénéficie des optimisations apportées dans le but d'une utilisation d'un équipement de type serveur.
L'installation de cette distribution SourceBased a donc été entreprise avec les optimisations correspondantes à notre matériel et à l'utilisation prévue de notre « Serveur de Virtualisation ».

Installation du Noyau XEN

L'installation et la reconfiguration des sources relatives au noyau Xen sous la distribution gentoo se fait Grace à la commande :

```
# emerge xen-sources
```

Vient ensuite la phase de configuration du noyau par rapport à nos besoins et à notre matériel et l'activation des fonctionnalités relatives à la Virtualisation.

```
Bus options (PCI etc.)  --->
  [*] PCI support
  [ ]     Xen PCI Frontend Debugging

Networking  --->
  Networking options  --->
    <*> 802.1d Ethernet Bridging
    Uniquement requis pour les ponts réseaux.

XEN  --->
  [*] Privileged Guest (domain 0)
  <*> Backend driver support
  <*>   Block-device backend driver
  <*>   Network-device backend driver
  <*>   PCI-device backend driver
        PCI Backend Mode (Virtual PCI) --->
  [*] Scrub memory before freeing it to Xen
  [*] Disable serial port drivers
      Xen version compatibility (3.0.4 and later)
```

Compilation du noyau

Installation des outils de Monitoring et d'Administration des VM

Les outils d'administration sont installés grâce à la commande suivante :

```
# emerge xen xen-tools
```

Le paramétrage de l'hyperviseur (domain 0) est également nécessaire : c'est le premier qui a le droit de voir les machines virtuelles.
Nous avons choisi de lancer au démarrage de la machine les services suivants :

- Démarrage du démon XEN : /etc/init.d/xend start
- Démarrage du démon xdm (l'installation de VM Windows demande l'accès au serveur X)

Une fois tous les paquets installés et le redémarrage de la machine il faut créer les disques durs des machines virtuelles.

Création des disques virtuels pour les deux clients sous Windows XP
Création des disques durs virtuels
Attention pour faire tourner Windows, il faut avoir un processeur supportant la virtualisation matérielle. Voici les lignes de commande permettant de créer les disques durs virtuelles :

```
dd if=/dev/zero of=/xen/disks/winXPSP0.img bs=1M seek=2048 count=1
dd if=/dev/zero of=/xen/disks/winXPSP3.img bs=1M seek=2048 count=1
```

Nous avons choisit de créer des disques virtuelles de 2 Go.
Il faut maintenant créer les fichiers de configuration du Domaine U SP0.hvm et SP3.hvm
SP3.hvm :

```
kernel = '/usr/lib/xen/boot/hvmloader'
# The domain build function. HVM domain uses 'hvm'.
builder='hvm'
# Initial memory allocation (in megabytes) for the new domain.
memory = 512
# A name for your domain. All domains must have different names.
name = 'WINXPSP3'
vif = [ 'bridge=xenbr1']
# Define the disk devices you want the domain to have access to, and
# what you want them accessible as.
disk = [ 'file:/xen/disks/winXPSP3.qcow,hda,w']
# New stuff
```

```
device_model = '/usr/lib/xen/bin/qemu-dm'
# Disk image for
cdrom='/dev/cdrom'
# boot on floppy (a), hard disk (c) or CD-ROM (d)
boot='c'
sdl=1
vnc=0
nographic=0
ne2000=0
```

Afin de pouvoir installer les clients XP, il a été nécessaire d'installer un environnement graphique. Nous avons choisi d'installer KDE. De plus il a fallut configurer Grub pour XEN.

Installation des machines virtuelles

Une fois que l'on n'a ouvert une session sur KDE avec un utilisateur il suffit d'ouvrir un terminal et de lancer cette commande en route :

- xm create /xen/confs/SP0.hvm et xm create /xen/confs/SP3.hvm

Maintenant il suffit de faire l'installation de Windows XP.

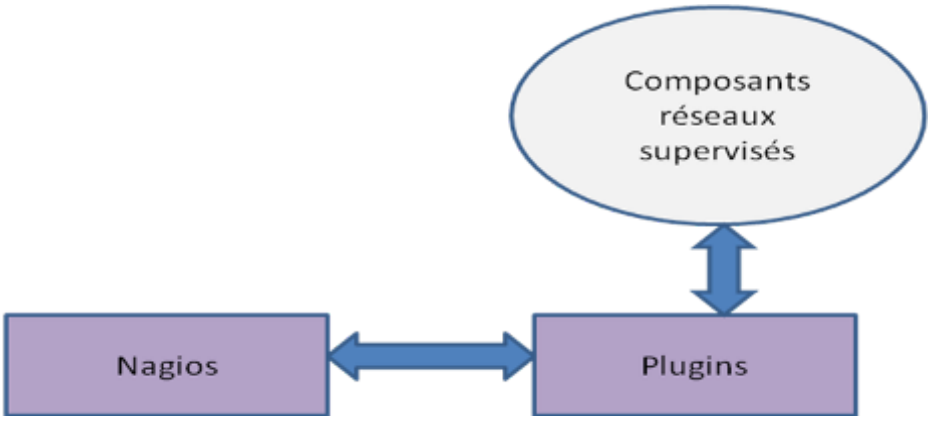
Annexe 5 : tableau comparatif des solutions de supervision

Name	Nagios Centreon	Nino	Pandora	NetXMS	JFFNMS	BigBrother	Zabbix	Cacti	Zenoss	OpManager	OpenNMS	NeDi
Network Map	Yes (Plugin)	Yes	Yes	Yes	No (To verify)	Yes	Yes	Yes (plugins)	Yes	?	Yes	Yes
Charts	No	Yes	Yes	?	Yes	?	Yes	Yes	Yes	Yes	Yes	Yes
Network Auto discovery	No (plugin)	Yes	Yes	Yes	No	?	Yes	Yes (plugin)	Yes	Yes	Yes	Yes
Agent	Yes	No	Yes	Yes	?	?	Yes	No	No	No	Yes, using NRPE	SNMP & CDP
SNMP (v1,v2,v3)	Yes (plugin)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Import MIB	Yes	Yes	Yes	?	No	?	Yes	No	Yes	?	?	?
Ping	Yes	Yes	Yes	Yes	Yes	?	Yes	?	?	?	?	?
External scripts	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	?
Plugins	Yes	No	?	?	Yes	?	Yes	Yes	Yes	Yes	Yes	?
Trigger/ Alerts	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WebApp	Viewing only	Full control	Full control	Full control	Full control	Full control	Full control	Full control	Full control	Full control	Full control	Full control
Data storage method	SQL	SQL	SQL	SQL	SQL	?	SQL	RRDtool & MySQL	RRDtool & MySQL	MySQL	RRDtool & PostgreSQL	SQL
License	GPL	GPL	GPL	GPL	GPL	?	GPL	GPL	GPL	?	GPL	GPL
OS	Linux	Linux & windows	Linux	Linux & windows	Linux & windows	Linux & windows	Linux	Linux & windows	Linux	Windows	Linux & windows	Linux

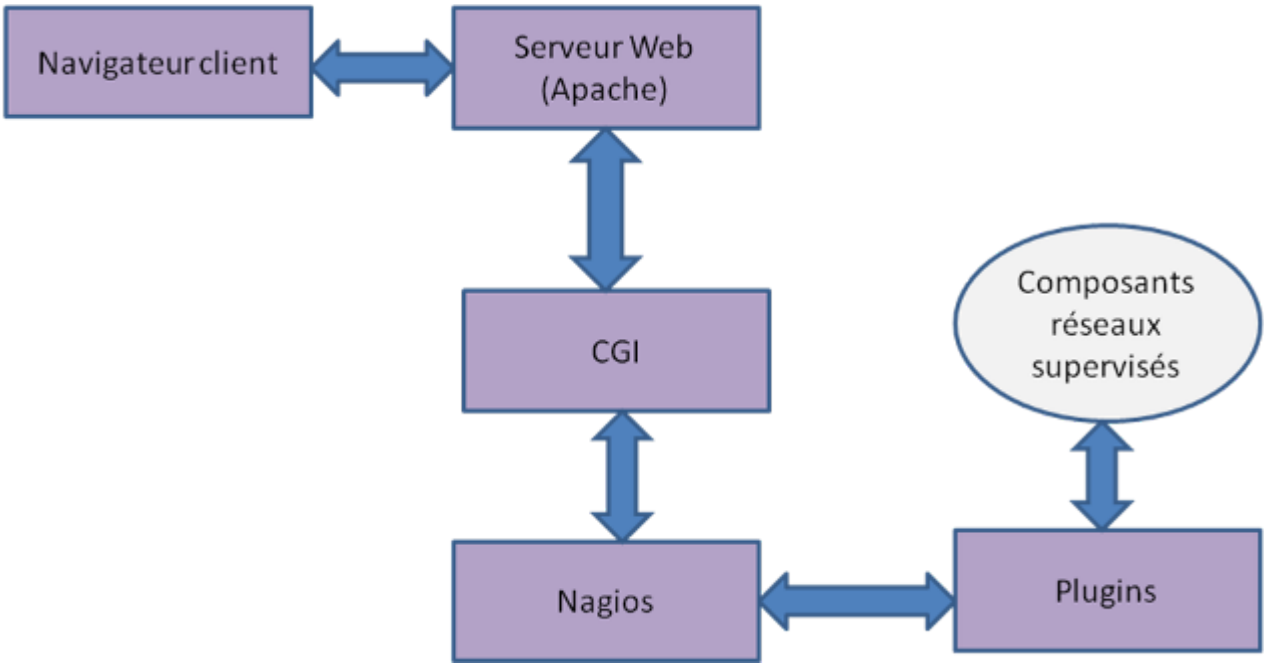
Annexe 6 : Présentation Nagios

Le concept

Nagios est un système de supervision de service développé pour des plateformes linux. Le concept consiste au lancement de contrôle des services et/ou stations définis à l'aide de « plugins » externes. Ces contrôles se font selon un intervalle défini durant la phase de configuration.
Les services de surveillance fournissent à l'application les résultats issus de l'analyse. Si ces résultats font remonter un problème, une notification est faite. Elle peut être effectuée par sms, messagerie instantanée ou mail. Dans le cadre du CERMA, nous nous contentons d'envoyer un mail à l'administrateur.
L'architecture
Nagios peut être considéré comme un noyau qui gère l'ordonnancement des vérifications (effectuées à l'aide de plugins) et les actions à prendre en fonction des incidents (alertes, actions correctives, etc.)



Afin de rendre plus exploitable les résultats, une interface web (nous utiliserons apache) basée sur les CGI(Common Gateway Interface) fournis par l'installation par défaut de Nagios a été rajoutée.
Nous obtenons alors l'architecture suivante :



A cette architecture nous ajouterons le module centreon (anciennement oreon) qui est une interface permettant de configurer Nagios à partir d'un navigateur web.

Annexe 7 : Serveur Mail

Fichier de configuration de Postfix :

Master.cf

```
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master").
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
#smtp      inet  n       -       -       -       -           smtpd
smtp      inet  n       -       -       -       20      smtpd
#submission inet n       -       -       -       -       smtpd
#  -o smtpd_enforce_tls=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#smtps     inet  n       -       -       -       -       smtpd
#  -o smtpd_tls_wrappermode=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#628       inet  n       -       -       -       -       qmqpd
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       -       300     1       oqmgr
tlsmgr    unix  -       -       -       1000?   1       tlsmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
smtp      unix  -       -       -       -       -       smtp
# When relaying mail as backup MX, disable fallback_relay to avoid MX loops
relay     unix  -       -       -       -       -       smtp
          -o fallback_relay=
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       -       -       -       showq
error     unix  -       -       -       -       -       error
discard   unix  -       -       -       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       -       -       -       lmtp
anvil     unix  -       -       -       -       1       anvil
scache    unix  -       -       -       -       1       scache
#
# ==========================================================================
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent.  See the pipe(8) man page for information about ${recipient}
# and other message envelope options.
# ==========================================================================
#
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
### OLD ############################
#maildrop  unix  -       n       n       -       -       pipe
#  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
```

```
### NEW ##############################
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=virtualcandide argv=/usr/bin/maildrop -w 90 -d ${user}@${nexthop} ${extension} ${recipient} ${user}
${nexthop} ${sender}
#
# See the Postfix UUCP_README file for configuration details.
#
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
#
# Other external delivery methods.
#
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
scalemail-backend unix  -       n       n       -       2       pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user} ${extension}
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
```

Main.cf

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# Debian specific:  Specifying a file name will cause the first
# line of that file to be used as the name.  The Debian default
# is /etc/mailname.
myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

# TLS parameters
#smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
#smtpd_use_tls=yes
#smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
#smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

myhostname = mx.candide-sa.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
#mydestination = tartarin, localhost.localdomain, localhost
mydestination = $myhostname
relayhost =
mynetworks = 172.10.140.0/29, 127.0.0.0/8
#mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
message_size_limit = 5120000

#User Virtuel
virtual_transport = maildrop
virtual_mailbox_base = /home/virtualcandide
virtual_alias_maps = proxy:mysql:/etc/postfix/mysql_virtual_alias_maps.cf
virtual_mailbox_domains = proxy:mysql:/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_maps = proxy:mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_minimum_uid = 20001
virtual_uid_maps = static:20001
virtual_gid_maps = static:20001
```

```
##### Ajout conseil Anlayse ####
#rejet permanent des utilisateurs non connu
unknown_local_recipient_reject_code = 450

#doit s'annoncer en faisant un helo
smtpd_helo_required = yes
#limit d'attente du hello
smtp_helo_timeout = 60s
#nombre d'erreurs maximum autorisé avant retour point précédent
smtpd_soft_error_limit = 3
#nombre d'erreurs maximum avant fermeture de la connexion
smtpd_hard_error_limit = 12

#smtpd_client_connection_count_limit = 35
#smtpd_client_recipient_rate_limit = 35
#smtpd_client_connection_rate_limit = 10

# réseau autorisé à faire un helo
#smtpd_helo_restrictions = permit_mynetworks, warn_if_reject reject_non_fqdn_hostname, reject_invalid_hostname, reject

# réseau autorisé à faire un 'mail from:'
#smtpd_sender_restrictions = permit_mynetworks, warn_if_reject reject_non_fqdn_sender, reject_unknown_sender_domain, reject_unauth_pipelining, reject

# accèpte la partie 'rcpt to:'
#smtpd_recipient_restrictions = reject_unauth_pipelining, permit_mynetworks, reject_non_fqdn_recipient, reject_unknown_recipient_domain, reject_unauth_destination, permit smtpd_data_restrictions = reject_unauth_pipelining


#incrémenter à chaque tantative infructueuse le temps d'attente
smtpd_delay_reject = yes

#désactive le scannage des adresses mails du serveur
disable_vrfy_command = yes
```

mysql_virtual_mailbox_maps.cf

```
user = adminpostfix
password = P@ssP0stfix
hosts = 172.10.140.3
dbname = postfix
query = SELECT maildir FROM mailbox WHERE username = '%s' and active ='1'
```

mysql_virtual_domains_maps.cf

```
user = adminpostfix
password = P@ssP0stfix
hosts = 172.10.140.3
dbname = postfix
query = SELECT domain FROM domain WHERE domain = '%s' and active ='1'
```

mysql_virtual_alias_maps.cf

```
user = adminpostfix
password = P@ssP0stfix
hosts = 172.10.140.3
dbname = postfix
query = SELECT goto FROM alias WHERE address = '%s' and active ='1'
```

Annexe 8 : configuration point accès WIFI

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```
hostname barrere
!
enable secret 5 $1$dN5Q$9vIyXQC5DsojUOcD9Nhjp/
!
ip subnet-zero
ip domain name candide.com
ip dhcp excluded-address 172.10.190.1 172.10.190.2
!
ip dhcp pool ipwifi
   network 172.10.190.0 255.255.248.0
   default-router 172.10.190.1
!
no aaa new-model
!
dot11 ssid Candide_SA
   authentication open
   guest-mode
!
crypto pki trustpoint TP-self-signed-2205098824
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2205098824
 revocation-check none
 rsakeypair TP-self-signed-2205098824
!
crypto ca certificate chain TP-self-signed-2205098824
 certificate self-signed 01 nvram:IOS-Self-Sig#3401.cer
username yoplait password 7 083645480058574742534D0A283D273024
!
bridge irb
!
interface Dot11Radio0
 bandwidth 1000000
 no ip address
 no ip route-cache
 !
 ssid Candide_SA
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 no power client local
 power client 5
 power local 5
 station-role root access-point
 beacon period 1000
 beacon dtim-period 1
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
```

```
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 hold-queue 160 in
!
interface BVI1
 ip address 172.10.190.2 255.255.248.0
 no ip route-cache
!
ip default-gateway 172.10.190.1
no ip http server
ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
access-list 111 permit tcp any any neq telnet
!
control-plane
!
bridge 1 route ip
!
line con 0
 access-class 111 in
line vty 0 4
 access-class 111 in
 login local
!
End
```

Annexe 9 : Configuration finale du routeur Cisco

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname michel
!
boot-start-marker
boot-end-marker
!
logging buffered 65536 debugging
no logging rate-limit
enable secret 5 $1$KfpZ$Z3dB2MmOaKnlGQ/fOrjw7/
enable password 7 151713051038
!
no aaa new-model
no ip source-route
ip cef
!
ip inspect max-incomplete high 20000000
ip inspect max-incomplete low 20000000
ip inspect one-minute high 100000000
ip inspect one-minute low 100000000
ip inspect udp idle-time 15
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 1
ip inspect tcp synwait-time 1
ip inspect tcp max-incomplete host 100000 block-time 0
ip inspect name ethernetin cuseeme audit-trail on timeout 3600
ip inspect name ethernetin ftp audit-trail on timeout 3600
ip inspect name ethernetin http audit-trail on timeout 3600
ip inspect name ethernetin rcmd audit-trail on timeout 3600
ip inspect name ethernetin realaudio audit-trail on timeout 3600
ip inspect name ethernetin smtp audit-trail on timeout 3600
ip inspect name ethernetin sqlnet audit-trail on timeout 3600
ip inspect name ethernetin streamworks audit-trail on timeout 3600
ip inspect name ethernetin tcp audit-trail on timeout 3600
ip inspect name ethernetin tftp audit-trail on timeout 30
ip inspect name ethernetin udp audit-trail on timeout 15
ip inspect name ethernetin vdolive audit-trail on timeout 3600
ip inspect name ethernetin https audit-trail on timeout 3600
ip inspect name ethernetin dns audit-trail on timeout 3600
ip inspect name ethernetout http audit-trail on timeout 3600
ip inspect name ethernetout https audit-trail on timeout 3600
ip inspect name ethernetout smtp audit-trail on timeout 3600
ip inspect name ethernetout imap audit-trail on timeout 3600
ip inspect name ethernetout ssh audit-trail on timeout 3600
ip inspect name wifi dns audit-trail on timeout 3600
ip inspect name wifi http audit-trail on timeout 3600
ip inspect name wifi https audit-trail on timeout 3600
ip inspect name Vldsn dns audit-trail on timeout 3600
```

```
ip inspect name dmz http audit-trail on timeout 3600
ip inspect name dmz https audit-trail on timeout 3600
ip inspect name dmz imap audit-trail on timeout 3600
ip inspect name dmz smtp audit-trail on timeout 3600
ip inspect name dmz icmp audit-trail on timeout 3600
ip inspect name dns dns audit-trail on timeout 3600
ip inspect name dns ssh audit-trail on timeout 3600
ip inspect name vclient ftp audit-trail on timeout 3600
ip inspect name vclient http audit-trail on timeout 3600
ip inspect name vclient smtp audit-trail on timeout 3600
ip inspect name vclient https audit-trail on timeout 3600
ip inspect name vclient dns audit-trail on timeout 3600
!
crypto pki trustpoint TP-self-signed-1593281617
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1593281617
 revocation-check none
 rsakeypair TP-self-signed-1593281617
!
!
crypto pki certificate chain TP-self-signed-1593281617
 certificate self-signed 01
  30820246 [ ... ici la clé ... ] 9C56
  quit
username willy privilege 15 password 7 02071E575E520925141B0E
archive
 path flash:archive
!
ip ssh version 2
!
!interface FastEthernet0/0
 ip address 172.18.4.2 255.255.240.0
 ip access-group 112 in
 no ip proxy-arp
 ip flow ingress
 ip flow egress
 ip nat outside
 ip inspect ethernetout in
 ip virtual-reassembly
 ip route-cache flow
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 172.10.140.1 255.255.255.248
 ip access-group 140 in
 no ip proxy-arp
 ip nat inside
 ip inspect dmz out
 ip virtual-reassembly
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 172.10.150.1 255.255.255.248
 ip access-group 150 in
 no ip proxy-arp
```

```
 ip nat inside
 ip inspect vclient in
 ip virtual-reassembly
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 172.10.160.1 255.255.255.248
 no ip proxy-arp
 ip nat inside
 ip inspect ethernetin in
 ip virtual-reassembly
!
interface FastEthernet0/1.4
 encapsulation dot1Q 5
 ip address 172.10.170.1 255.255.255.248
 ip nat inside
 ip inspect ethernetin in
 ip virtual-reassembly
!
interface FastEthernet0/1.5
 encapsulation dot1Q 4
 ip address 172.10.180.1 255.255.255.248
 no ip proxy-arp
 ip nat inside
 ip inspect ethernetin in
 ip virtual-reassembly
!
interface FastEthernet0/1.6
 encapsulation dot1Q 6
 ip address 172.10.190.1 255.255.255.0
 ip access-group 190 in
 no ip proxy-arp
 ip nat inside
 ip inspect wifi in
 ip virtual-reassembly
!
interface FastEthernet0/1.7
 encapsulation dot1Q 7
 ip address 172.10.200.1 255.255.255.248
 no ip proxy-arp
 ip nat inside
 ip virtual-reassembly

interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.18.4.1 permanent
!
```

```
ip flow-export source FastEthernet0/1.7
ip flow-export version 5
ip flow-export destination 172.10.200.2 2055
!
no ip http server
no ip http secure-server
ip nat log translations syslog
ip nat translation max-entries 300
ip nat inside source list 10 interface FastEthernet0/0 overload
ip nat inside source static tcp 172.10.140.3 25 172.18.4.2 25 extendable
ip nat inside source static udp 172.10.140.3 25 172.18.4.2 25 extendable
ip nat inside source static tcp 172.10.140.2 80 172.18.4.2 80 extendable
ip nat inside source static tcp 172.10.140.3 143 172.18.4.2 143 extendable
ip nat inside source static tcp 172.10.140.2 443 172.18.4.2 443 extendable
ip nat inside source static tcp 172.10.200.3 22 172.18.4.2 55555 extendable
ip nat inside source static tcp 172.10.200.2 22 172.18.4.2 55556 extendable
!
logging facility local1
logging host 172.10.200.2 transport tcp port 46001 audit
access-list 10 permit 172.10.160.6
access-list 10 permit 172.10.170.4
access-list 10 permit 172.10.170.5
access-list 10 permit 172.10.170.6
access-list 10 permit 172.10.180.3
access-list 10 permit 172.10.180.6
access-list 10 permit 172.10.140.2
access-list 10 permit 172.10.150.2
access-list 10 permit 172.10.150.3
access-list 10 permit 172.10.200.6
access-list 10 permit 172.10.200.2
access-list 10 permit 172.10.15.2
access-list 10 permit 172.10.160.0 0.0.0.7
access-list 10 permit 172.10.190.0 0.0.0.255
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 unreachable
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 packet-too-big
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 echo-reply
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 time-exceeded
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 traceroute
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 administratively-prohibited
access-list 112 permit icmp any 172.18.140.0 0.0.0.7 echo
access-list 112 permit tcp any host 172.18.4.2 eq www
access-list 112 permit tcp any host 172.18.4.2 eq 443
access-list 112 permit tcp any host 172.18.4.2 eq 55555
access-list 112 permit tcp any host 172.18.4.2 eq 55556
access-list 112 permit tcp any host 172.18.4.2 eq 143
access-list 112 permit tcp any host 172.18.4.2 eq smtp
access-list 112 permit udp any host 172.18.4.2 eq 25
access-list 112 deny   ip any any log
access-list 140 deny   ip any any log
access-list 150 permit udp host 172.10.150.2 host 172.10.200.2
access-list 150 permit udp host 172.10.150.3 host 172.10.200.2
access-list 150 permit tcp host 172.10.150.2 eq 1248 host 172.10.160.2
access-list 150 permit tcp host 172.10.150.3 eq 1248 host 172.10.160.2
access-list 150 permit udp host 172.10.150.2 eq 1248 host 172.10.160.2
access-list 150 permit udp host 172.10.150.3 eq 1248 host 172.10.160.2
access-list 150 deny   ip any any log
access-list 190 permit tcp 172.10.190.0 0.0.0.255 any eq www
```

```
access-list 190 permit tcp 172.10.190.0 0.0.0.255 any eq 443
access-list 190 permit udp 172.10.190.0 0.0.0.255 host 172.10.180.3 eq domain
access-list 190 deny   ip any any
dialer-list 1 protocol ip permit
snmp-server community public RO
snmp-server community private RW
arp 172.18.4.200 0010.5ad8.8960 ARPA
arp 172.18.4.1 0004.23b8.4e2c ARPA
!
control-plane
!
line con 0
 password 7 151104021725272138322631001304 0A50040A
 login
line aux 0
line vty 0 4
 exec-timeout 15 0
 privilege level 15
 login local
 transport input ssh
 transport output ssh
!
scheduler allocate 20000 1000
ntp server 172.10.180.3
end
```