Sécurisation d'un système d'information

Groupe défense

Candide S.A

SOMMAIRE

I. PRESENTATION DU SUJET 3

II. L'EQUIPE DEFENSE 4

A. LES DIFFERENTS MEMBRES 4
1. Chef de projet 4
2. Chargé de la politique de sécurité 5
3. Coordinateur technique 5
4. Rédacteur, Communication 5
5. Techniciens 5
B. PLANIFICATION DU PROJET 6
C. DESCRIPTION DES DIFFERENTES ETAPES DU PROJET 7
1. Etape 1 7
2. Etape 2 9
3. Etape 3 16
4. Etape 4 24

III. CONCLUSION 24

IV. ANNEXE 24

A. ANNEXE 1 : POLITIQUE DE SECURITE 25
B. ANNEXE 2 : CONTRAT D'AUDIT 27
C. ANNEXE 3 : PROCEDURE D'INSTALLATION DES CLIENTS 30
D. ANNEXE 4 : RAPPORT DE L'EQUIPE CONFRONTATION N°1 31
E. ANNEXE 5 : RAPPORT DE L'EQUIPE CONFRONTATION N°2 31
F. ANNEXE 6 : QUESTIONNAIRE AUDIT 31
G. ANNEXE 7 : ..... **ERREUR ! SIGNET NON DEFINI.**

I. Présentation du sujet

L'objet du projet de sécurisation d'un réseau d'information d'une entreprise est de diviser la promotion en différent groupe ayant chacun un rôle bien définit.

Groupe Défense : Etablir un réseau d'entreprise sécurisé offrant différents services à ses employés

Groupe Audit : Collecter un certain nombre d'information permettant d'identifier les attaques extérieures et proposer des solutions à l'équipe défense pour améliorer la sécurité de son réseau.

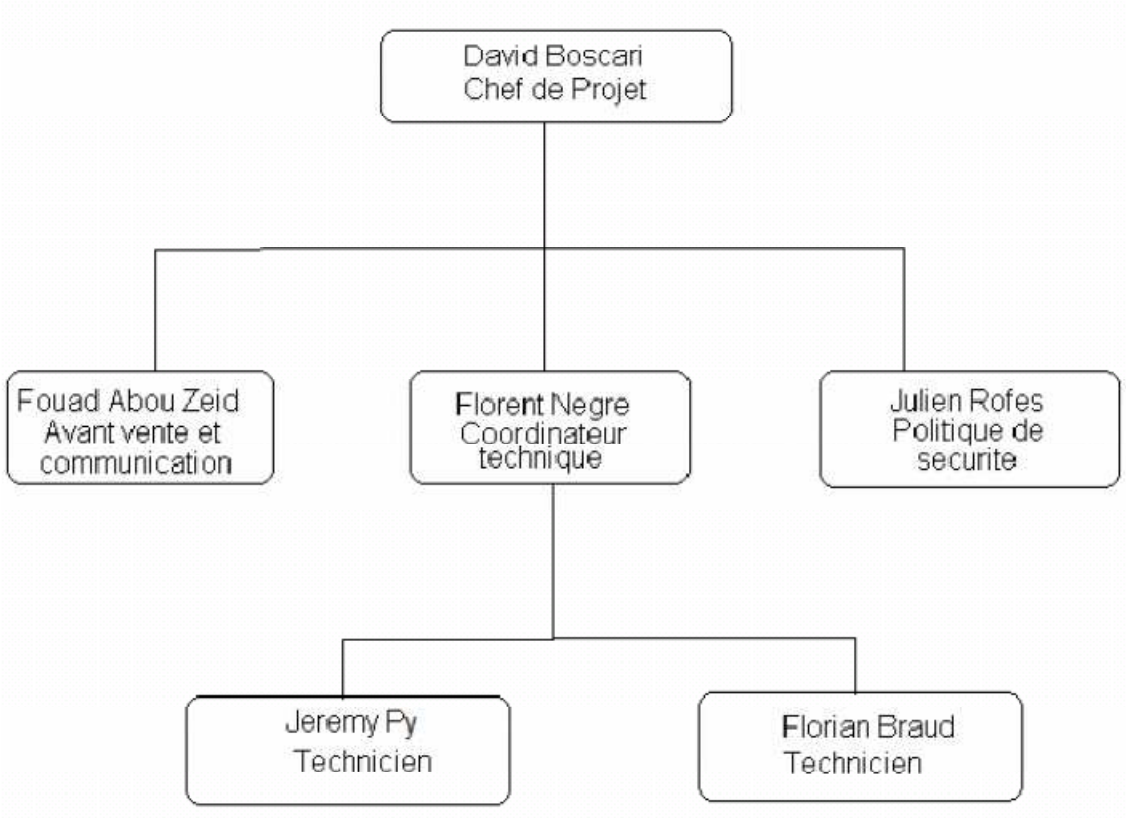
Groupe Attaque : Mettre en œuvre différents moyens afin de compromettre le réseau mis en place par l'équipe défense.

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.

II. L'équipe défense

Comme énoncé ci-dessus l'équipe défense s'est vue attribuer le rôle de mise en place et sécurisation d'un réseau d'entreprise. Afin de mener à bien la tâche qu'on nous avait confiée, nous avons découpé le projet en différentes phases dont nous prendrons soin de détailler par la suite.

A. Les différents membres



1. 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. Chargé de la politique de sécurité

Son rôle est de s'occuper de la politique de sécurité de l'entreprise :

- Définir les aspects juridiques de celle ci
- S'assurer du bon usage du système d'information

3. Coordinateur technique

Son rôle est d'orienter les choix techniques en termes de sécurité :

- Coordonne les activités des techniciens
- S'assure de la veille technologique du SI
- Communique l'avancement du projet au chef de projet

4. Rédacteur, Communication

Son rôle est de rédiger les différents rapports et contrats :

- Compte rendu de réunion
- Contrat avec l'équipe audit

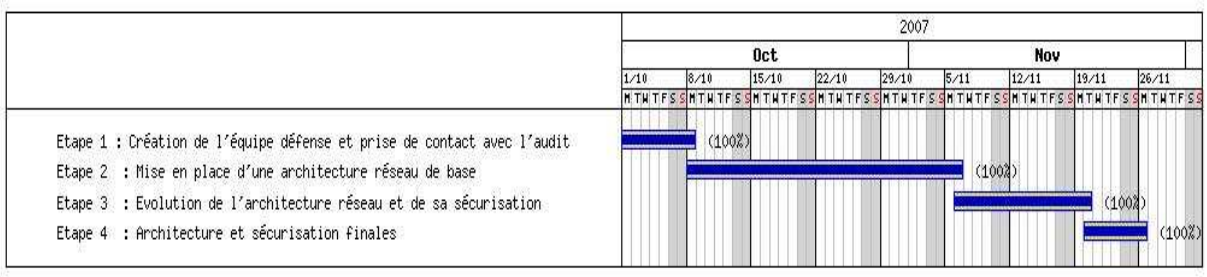
5. Techniciens

Leur 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

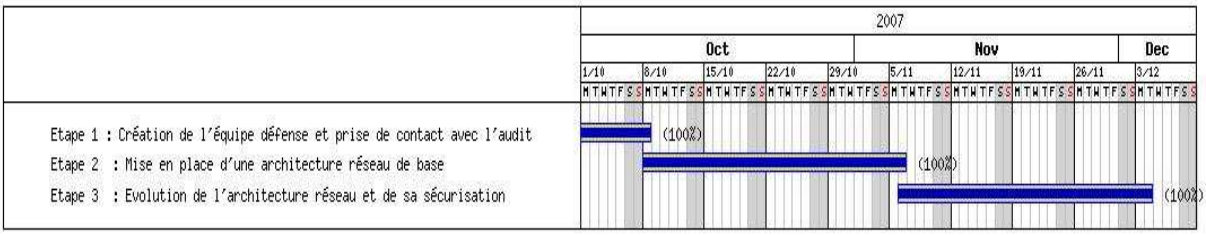
B. Planification du projet

Diagramme de GANTT du planning prévisionnel



Le planning prévisionnel établit en vue de mener à bien le projet n'a malheureusement pas pu être tenu du fait du blocage du bâtiment U2. Ce blocage a eu de nombreux impacts sur l'avancée du projet, nous avons malgré tout pu mettre en place la plupart des services proposés aux employés et sécuriser au mieux le système d'information.

Diagramme de GANTT du planning réel



C. Description des différentes étapes du projet

Nous allons exposer dans ce chapitre les différentes étapes du projet ainsi que les problèmes rencontrés, ce que nous avons pu faire pour les résoudre et les choix que nous avons été obligés d'adopter pour palier le manque de temps et de moyens.

1. Etape 1

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.

Une première partie du projet a été l'élaboration des groupes de défense, d'attaque et d'audit. Une fois notre groupe constitué, nous avons le hiérarchiser et délimiter le périmètre d'action de chacun de ses membres.

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.

a) Etablissement de la planification du projet

Les rôles étant définis, la planification du projet a pu être mise en place. Comme vu précédemment cette élaboration n'était que prévisionnelle ; elle ne prenait pas en compte les différents aléas du projet (manque de matériels, blocage du bâtiment U2 etc.).

Afin de programmer les dates des différentes confrontations nous avions prévu une réunion, à la fin de la première séance, avec les différents chefs de projet en l'occurrence pour l'équipe Attaque M. Frédéric Stremler, pour l'équipe Audit M. David Gerbaulet et pour l'équipe Défense M. David Boscari. La prompte disparition de M. Stremler en fin de séance, a contraint M.Gerbaulet et M.Boscari de décider des dates des confrontations, afin de ne pas prendre de retard sur l'organisation du projet. Par la suite nous avons soumis à M. Stremler, ces dernières. Il n'a vu aucun inconvénient quant aux choix que nous avions fait.

b) Rédaction de la politique de sécurité

Une politique de sécurité est un ensemble de règles d'utilisation des systèmes, réseaux et applications. Son but est d'imposer aux différents utilisateurs un mode de fonctionnement qui permette d'assurer la protection de Candide SA, de ses employés et de ses associés face à des disfonctionnement survenus sciemment ou inconsciemment.

La sécurité est un effort d'équipe impliquant la participation et l'appui de chacun des employés et sous-traitants. C'est la responsabilité de chaque utilisateur de connaître ces directives et agir en conséquence.

Ce document a été approuvé par le chef de projet et signé par les différents membres de l'équipe. Vous pourrez trouver ce document en annexe (Annexe 1).

c) Négociation du contrat avec l'équipe Audit

Un premier échange a eu lieu avec M. Blanc de l'équipe Audit ; il 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.

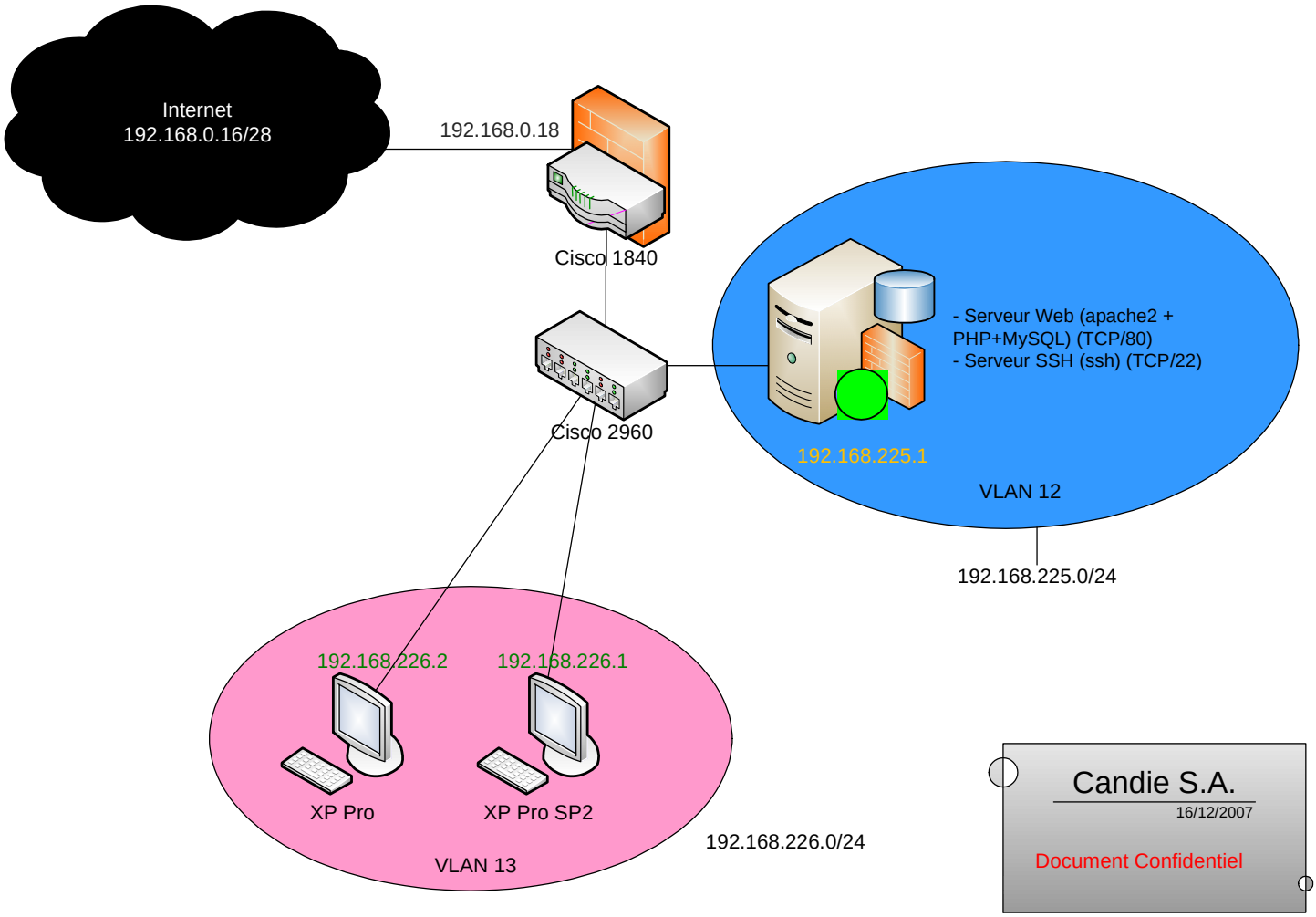
Lors de la seconde réunion M. Blanc nous a fournit le contrat rédigé par l'équipe Audit. A la suite de quoi, nous avons émis des réserves en ce qui concerne la mise en place de leur sonde et des responsabilités qu'entraînait celle-ci. Nous avons donc rédigé un avenant à ce contrat afin d'inclure ces aspects.

Le contrat établit par la suite correspondait aux attentes de chacun des groupes, le manager de l'équipe Audit et le chef de projet ont donc pu le valider conjointement (Annexe 2).

La deuxième étape consistait à mettre en place la première architecture. Nous avons volontairement mis en place une sécurisation de bas niveau afin de prendre la mesure des attaques envisagées par l'équipe des vilains et pour permettre une avancée progressive des différents aspects d'architecture et de sécurisation de notre société Candide S.A.

2. Etape 2

a) Architecture du Réseau



b) Configuration du Routeur

Tables de configuration du routeur CISCO 1840

```
Building configuration...

Current configuration : 2522 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname defense2-rtr
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$FX/q$pz836ey3CJAO/E0UDe1xT.
!
aaa new-model
!
!
!
aaa session-id common
ip cef
!
!
!
!
no ip domain lookup
ip domain name defense2
!
!
!
username bob privilege 15 password 7 00050507175A06514E
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 12
 ip address 192.168.225.254 255.255.255.0
 ip access-group 101 out
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip virtual-reassembly
!
```

```
interface FastEthernet0/0.2
 encapsulation dot1Q 13
 ip address 192.168.226.254 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip virtual-reassembly
!
interface FastEthernet0/1
 ip address 192.168.0.18 255.255.255.240
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
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
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.0.17
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
ip nat inside source static tcp 192.168.225.1 22 192.168.0.18 22 extendable
ip nat inside source static tcp 192.168.225.1 80 192.168.0.18 80 extendable
ip nat inside source static tcp 192.168.225.20 22 192.168.0.18 2222
extendable
ip nat inside source static tcp 192.168.225.20 3000 192.168.0.18 3000
extendable
ip nat inside source static tcp 192.168.225.20 80 192.168.0.18 8080
extendable
!
access-list 1 permit 192.168.225.0 0.0.0.255
access-list 1 permit 192.168.226.0 0.0.0.255
access-list 101 permit tcp any host 192.168.225.1 eq www
access-list 101 permit tcp any host 192.168.225.1 eq 22
access-list 101 permit tcp any host 192.168.225.20 eq 3000
access-list 101 permit tcp any host 192.168.225.20 eq 2222
access-list 101 permit tcp any host 192.168.225.20 eq 8080
access-list 101 deny   ip any any log
access-list 102 remark depuis_serv_web
access-list 102 permit tcp host 192.168.225.1 eq www any
access-list 102 permit tcp host 192.168.225.1 eq 22 any
access-list 102 deny   ip any any log
access-list 103 permit tcp host 192.168.225.1 0.0.0.0 192.168.225.254 eq 22
!
!
!
!
```

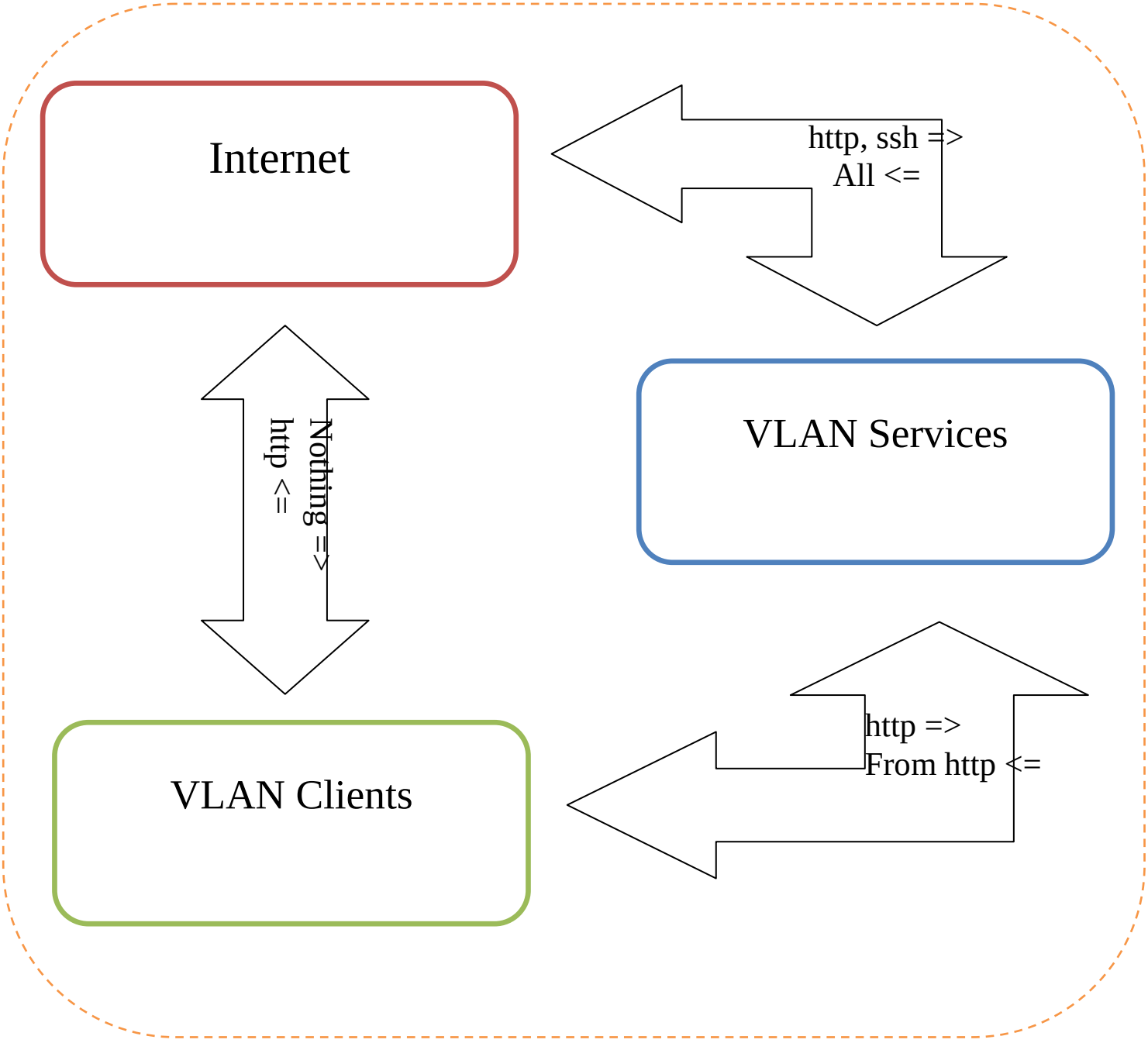
```
control-plane
!
!
!
line con 0
line aux 0
line vty 0 5
 password 7 0207125A180702760D
 transport input ssh
!
scheduler allocate 20000 1000
endip nat inside source list 1 interface FastEthernet0/1 overload

//Regles NAT
ip nat inside source static tcp 192.168.225.1 22 192.168.0.18 22 extendable
ip nat inside source static tcp 192.168.225.1 80 192.168.0.18 80 extendable
ip nat inside source static tcp 192.168.225.20 22 192.168.0.18 2222
extendable
ip nat inside source static tcp 192.168.225.20 3000 192.168.0.18 3000
extendable
ip nat inside source static tcp 192.168.225.20 80 192.168.0.18 8080
extendable
!
access-list 1 permit 192.168.225.0 0.0.0.255
access-list 1 permit 192.168.226.0 0.0.0.255
access-list 101 permit tcp any host 192.168.225.1 eq www
access-list 101 permit tcp any host 192.168.225.1 eq 22
access-list 101 permit tcp any host 192.168.225.20 eq 3000
access-list 101 permit tcp any host 192.168.225.20 eq 2222
access-list 101 permit tcp any host 192.168.225.20 eq 8080
access-list 101 deny   ip any any log
access-list 102 remark depuis_serv_web
access-list 102 permit tcp host 192.168.225.1 eq www any
access-list 102 permit tcp host 192.168.225.1 eq 22 any
access-list 102 deny   ip any any log
access-list 103 permit tcp host 192.168.225.1 0.0.0.0 192.168.225.254 eq 22
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 5
 password 7 0207125A180702760D
 transport input ssh
!
scheduler allocate 20000 1000
end
```

c) Configuration du firewall

```
#!/bin/sh
```

```
# Firewall Iptables

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

# On drop tout par defaut, on libere au fur et a mesure
# dit : "politiques par defaut"
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Regles de filtrage
# On enleve le firewall sur le loopback
iptables -A INPUT -i lo -j ACCEPT

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

# Ouverture de ports
# Port Http
iptables -A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
# Port SSH
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
# ICMP
iptables -A INPUT -p icmp -m state --state NEW -j ACCEPT

iptables -A INPUT -j DROP


iptables -A OUTPUT -m state --state NEW -j ACCEPT
```

d) Ports ouverts sur le serveur



e) Configuration des postes clients

La configuration des postes clients répond à une procédure que vous trouverez en annexe (Annexe 3.A).

Le projet nécessitait deux clients, l'un très peu protégé (aucune protection logicielle, seul un firewall matériel était présent), l'autre protégé comme indiqué sur la politique de sécurité (Annexe 3.A).

Poste 1 :

OS : Windows XP SP0
Antivirus : aucun
Firewall : aucun
@IP : 192.168.226.1
Masque : 255.255.255.0
Passerelle : 192.168.226.254
DNS : 192.168.225.1

Poste 2 :

OS : Windows XP SP2
Antivirus : aucun
Firewall : firewall XP
@IP : 192.168.226.1
Masque : 255.255.255.0
Passerelle :192.168.226.254
DNS : 192.168.225.1

Cela correspond à la configuration réseau des postes, il fallait rajouter à ça la configuration de l'OS (Annexe 3.C):

- création d'un compte admin et d'un compte utilisateur (limité en droit d'installation et d'accès fichiers)) n'ayant pas pu avoir une machine supplémentaire pour serveur 2003 ou active Directory nous n'avons pas pu approfondir ces droits.
- Définir des mots de passe « correct » et les changer avant chaque rencontre
- Configurer IE : bloquer les intrusions : niveau « élevé »

3. Etape 3

a) Propositions de l'audit

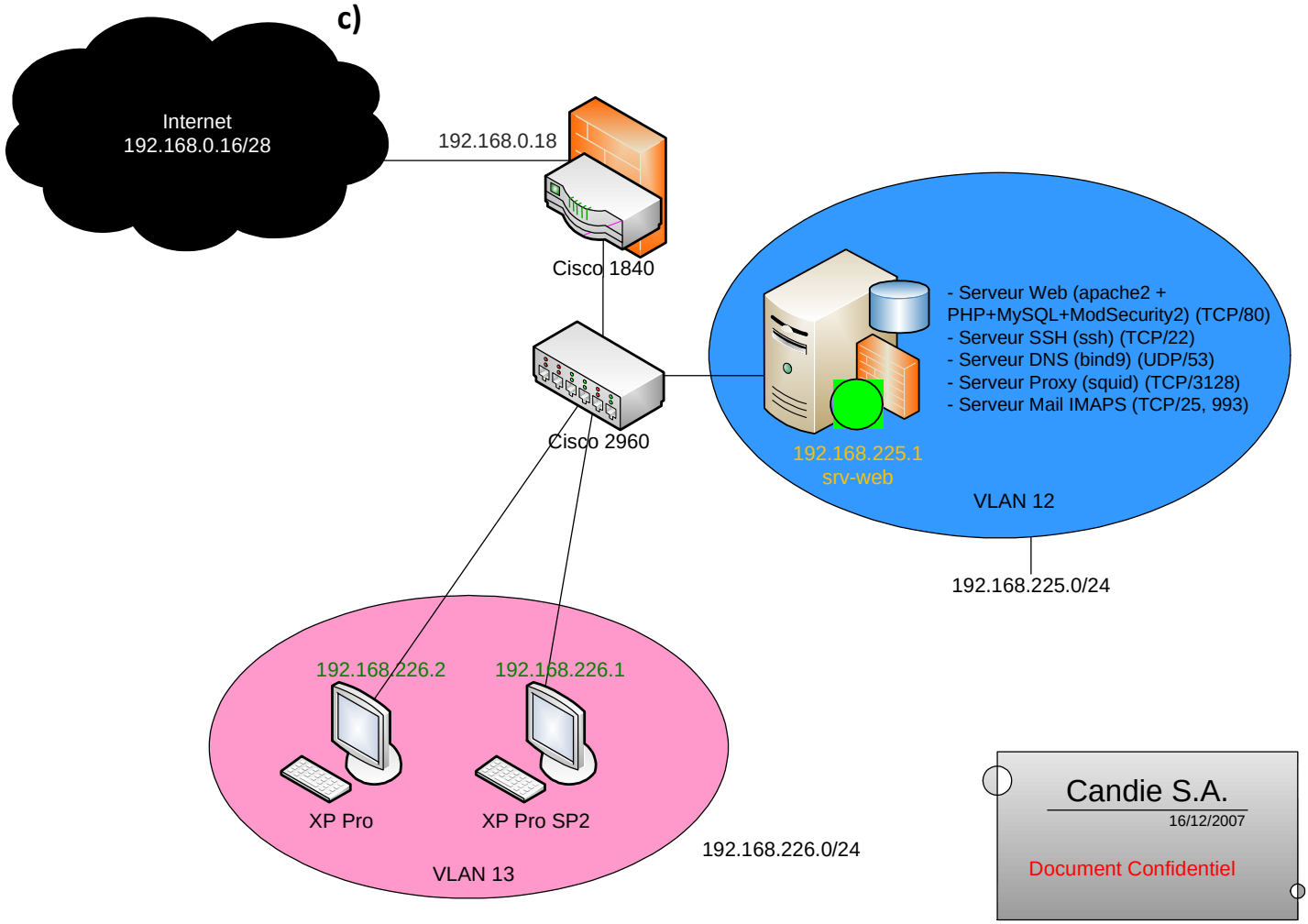
Suite à la première confrontation l'équipe audit nous a fait parvenir un rapport stipulant « *Pour conclure, l'équipe a bien défendu son réseau. Les différents assauts soviétiques n'ont pas anéanti les serveurs facilement. Et même si l'équipe attaque semble avoir réussi à se connecter aux serveurs SSH dans la nuit, les dangers seront écartés grâce à une reconfiguration des serveurs.*

Finalement, la brèche de sécurité permise en cours de confrontation n'a explicitement provoqué qu'un affichage de pages web dans le périmètre clients, mais a bien été exploitée côté serveurs : accès fichiers serveur défense et échange de clés SSH de la sonde !!! »

Suite à la lecture de ce rapport, nous n'avons donc pas renforcé la sécurité des services mis en place lors de la première confrontation.

b) Architecture réseau de la deuxième confrontation

c)



C) Configuration du routeur

```
Building configuration...

Current configuration : 3215 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname defense2-rtr
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$FX/q$pz836ey3CJAO/E0UDe1xT.
!
aaa new-model
!
!
!
aaa session-id common
ip cef
!
!
!
!
no ip domain lookup
ip domain name defense2

//les lignes suivantes permettent de faire du suivi de connexion et laisser
passer si la connexion est déjà établie
ip inspect name ifpubl ntp timeout 30
ip inspect name ifpubl dns timeout 30
ip inspect name ifpubl http timeout 30
ip inspect name ifpubl ssh timeout 30
ip inspect name ifpubl https timeout 30
ip inspect name ifservout dns timeout 30
ip inspect name ifservout ssh timeout 30
ip inspect name ifservout http timeout 30
ip inspect name ifservout https timeout 30
ip inspect name ifservout ntp timeout 30
!
!
!
username bob privilege 15 password 7 00050507175A06514E
!
!
```

```
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
```

```
 encapsulation dot1Q 12
 ip address 192.168.225.254 255.255.255.0
 ip access-group services out
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip inspect ifservout in
 ip virtual-reassembly
!
interface FastEthernet0/0.2
 encapsulation dot1Q 13
 ip address 192.168.226.254 255.255.255.0
 ip access-group clientin in
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip virtual-reassembly
!
interface FastEthernet0/1
 ip address 192.168.0.18 255.255.255.240
 ip access-group publicin in
 ip nat outside
 ip inspect ifpubl in
 ip virtual-reassembly
 duplex auto
 speed auto
!
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
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.0.17
!
!
no ip http server
no ip http secure-server

//Regles de NAT
ip nat inside source list 1 interface FastEthernet0/1 overload
ip nat inside source static tcp 192.168.225.1 22 192.168.0.18 22 extendable
ip nat inside source static tcp 192.168.225.1 80 192.168.0.18 80 extendable
ip nat inside source static tcp 192.168.225.20 22 192.168.0.18 2222
extendable
ip nat inside source static tcp 192.168.225.20 3000 192.168.0.18 3000
extendable
ip nat inside source static tcp 192.168.225.20 80 192.168.0.18 8080
extendable
!
//access-lists nommées pour une manipulation aisée
ip access-list extended clientin
```

```
//on laisse passer les requetes DNS et les connexions vers le proxy des
clients vers les serveurs
 permit udp 192.168.226.0 0.0.0.255 host 192.168.225.1 eq domain
 permit tcp 192.168.226.0 0.0.0.255 host 192.168.225.1 eq 3128

ip access-list extended publicin
//on laisse passer le http et SSH, DNS et smtp depuis l'extérieur
permit tcp any host 192.168.0.18 eq 22
 permit tcp any host 192.168.0.18 eq www
 permit tcp any host 192.168.0.18 eq 2222
 permit tcp any host 192.168.0.18 eq 3000
 permit tcp any host 192.168.0.18 eq 8080
permit tcp any host 192.168.0.18 eq 25
permit udp any host 192.168.0.18 eq 53
permit tcp any host 192.168.0.18 eq 53

ip access-list extended services
//on laisse passer le http et SSH, DNS, smtp vers le serveur d'agence
 permit tcp any host 192.168.225.1 eq www
 permit tcp any host 192.168.225.1 eq 22
permit tcp any host 192.168.225.1 eq 53
permit udp any host 192.168.225.1 eq 53
permit tcp any host 192.168.225.1 eq 25

//partie audit
 permit tcp any host 192.168.225.20 eq 3000
 permit tcp any host 192.168.225.20 eq 22
 permit tcp any host 192.168.225.20 eq www

//on laisse passer le  uniquement DNS, proxy,smtp, et IMAPS venant des
clients
 permit udp 192.168.226.0 0.0.0.255 host 192.168.225.1 eq domain
 permit tcp 192.168.226.0 0.0.0.255 host 192.168.225.1 eq 3128
permit tcp any host 192.168.225.1 eq 25
permit tcp any host 192.168.225.1 eq 993 //imaps

!
access-list 1 permit 192.168.225.0 0.0.0.255
access-list 1 permit 192.168.226.0 0.0.0.255
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 5
 password 7 0207125A180702760D
 transport input ssh
!
scheduler allocate 20000 1000
end
```

d) Configuration du firewall

```
#!/bin/sh
# Firewall Iptables

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

# On drop tout par defaut, on libere au fur et a mesure
# dit : "politiques par defaut"
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Regles de filtrage
# On enleve le firewall sur le loopback
iptables -A INPUT -i lo -j ACCEPT

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

# Ouverture de ports
# Port Http
iptables -A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
# Port SSH
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
# Port DNS UDP
iptables -A INPUT -p udp --dport 53 -m state --state NEW -j ACCEPT
# Port DNS TCP
iptables -A INPUT -p tcp --dport 53 -m state --state NEW -j ACCEPT
# Port SQUID
iptables -A INPUT -p tcp --dport 3128 -m state --state NEW -j ACCEPT
# Port SMTP
iptables -A INPUT -p tcp --dport 25 -m state --state NEW -j ACCEPT
# ICMP
iptables -A INPUT -p icmp -m state --state NEW -j ACCEPT

iptables -A INPUT -j DROP


iptables -A OUTPUT -m state --state NEW -j ACCEPT
```

Même configuration que lors de la précédente confrontation, avec l'ajout des règles permettant l'utilisation de nouveaux services, à savoir : Proxy, DNS et Mail

e) Configuration du DNS

Nous avons crée 2 zones
La première étant utilisée en interne dénommée intra.defense2.stri nous sert à nommer nos serveurs en interne
La seconde étant une délégation effectuée par le serveur de la salle : defense2.stri. Elle nous sert pour le nommage de notre site web (www.defense2.stri), ainsi que notre serveur mail (smtp.defense2.stri)

f) Configuration du proxy

Nous avons décidé d'utiliser un proxy afin d'éviter toute communication directe entre le périmètre client et l'extérieur. Ce proxy est basé sur Squid. Il autorise nos clients à se connecter uniquement aux sites web http et https.

g) Configuration du serveur Mail

Installé en urgence par nos techniciens, pour répondre à une demande de l'équipe attaque, la configuration de celui-ci n'était certainement pas la meilleure.
En effet, lors de la seconde confrontation, il a tout de suite été utilisé pour relayer du courrier que l'on pourrait apparenter à du spam.

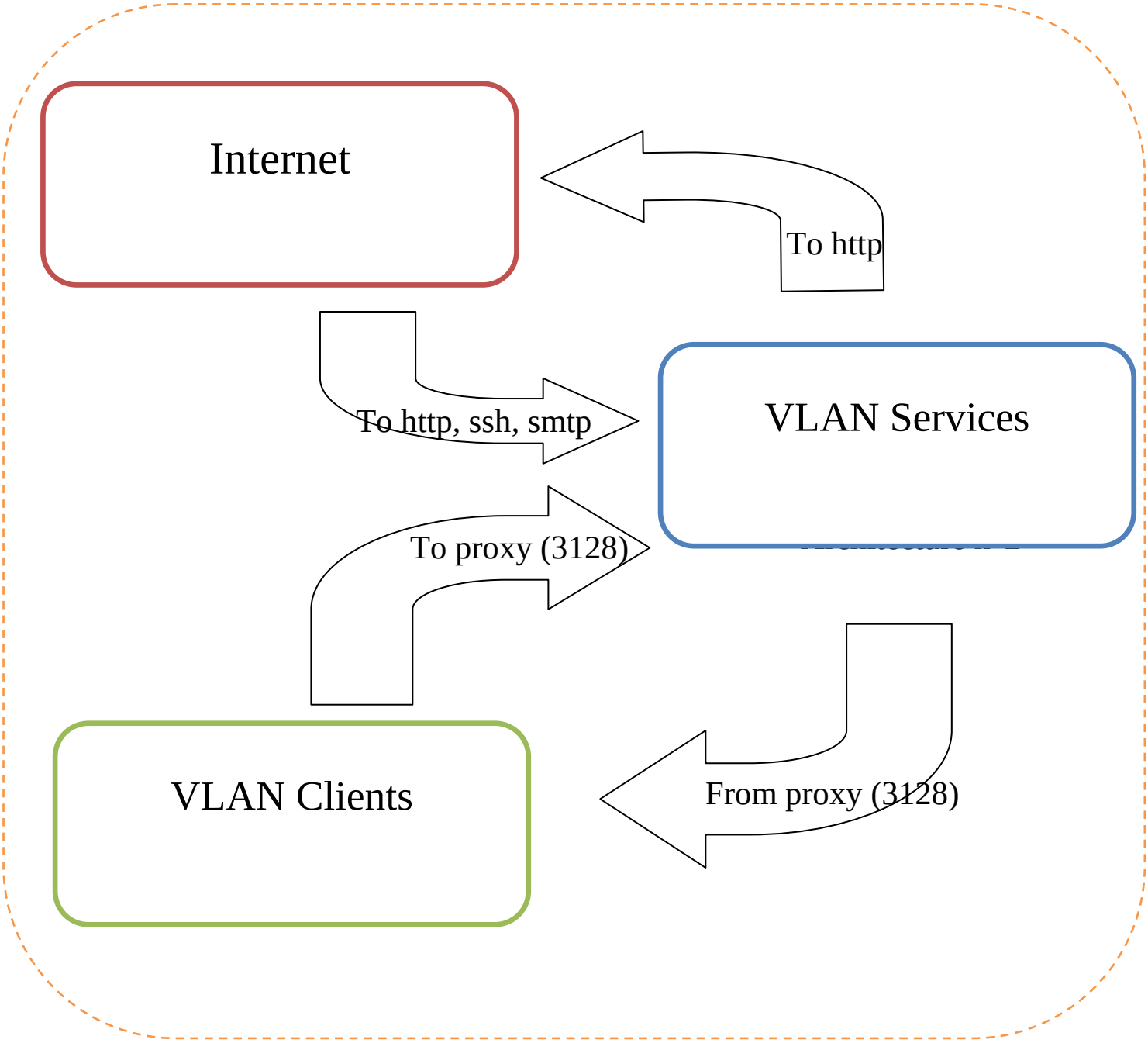
h) Configuration d'AMP

Apache était en version 2.2 avec mod_security.
Notre base de données a été attaquée. En effet, la table reliée directement au formulaire PHP à très vite saturée, ainsi que la partition /var contenant cette table…

i) Configuration SSH

Afin d'éviter les attaques en force brute sur notre service SSH, nous avons installé un paquet debian nommé fail2ban. Celui-ci nous a permis de limiter le nombre de tentatives infructueuses d'authentification. Pour réaliser ceci, il se base sur IPTables, en ajoutant des règles permettant de bannir les IP (mot clé Iptables : recent).

j) Ports ouverts sur le serveur



k) Configuration des postes clients

Pour permettre une reprise d'activité rapide entre les deux confrontations nous avons ghosté les postes, une fois la réinstallation des postes effectuée nous avons installé Firefox (browser Internet), un antivirus (« Antivir ») ainsi qu'un Pare-feu («sunbelt ») : configuré afin de limiter l'accès à certains sites, laisser que les ports « normaux » ouvert pour les protocoles http, FTP ; etc...(Annexe 3.C) Il était également nécessaire d'y intégrer l'adresse Proxy lors de la confrontation finale : 192.168.225.1 port 3128.

Les mots de passe ont été à nouveau changés avant la confrontation.

4. Etape 4

Une dernière étape de notre projet a été de constater les dégâts infligés lors de la deuxième confrontation suite à la lecture du rapport d'analyse de l'équipe audit.

Les recommandations telles quelles nous ont été transmises : « *Pour conclure, l'équipe défense a défendu son réseau tant bien que mal. Le serveur web a bien tenu le choc grâce à une bonne configuration système (Des volontaires pour compter le nombre d'occurrences de ''Permission Denied'' sur les logs ? :)*
La présence du keylogger a su faire pencher la balance du côté obscur de la force, ouvrant ainsi la porte du réseau interne au bon vouloir des hackers en herbe !!!
De nombreuses traces suspectes sur les deux serveurs ont été découvertes...
Et même si l'équipe attaque semble avoir réussi à se connecter à la sonde, les dangers ont été très vite écartés en modifiant tous les mdp et en redéployant le firewall interne. »

III. Conclusion

Au vu de ces quelques mois de travail, candide SA est assez fière de la sécurité de son réseau. En effet bien épaulée par l'équipe Audit, l'équipe défense à su montrer que son réseau résistait à la plupart des attaques (le seul dénis de service résultant du code étudiant de l'application PHP que nous n'avons volontairement pas modifié), et qu'il tenait le coup même contre des « cadors ».

Au-delà de l'aspect technique, l'aspect humain a été primordial pour mener à bien ce projet, et pour pouvoir coordonner les 3 groupes. Tout le monde s'est senti impliqué, et a apporté sa contribution au projet, prouvant la motivation, et l'envie de bien faire de chacun.

Nous avons trouvé l'expérience très enrichissante, surtout à quelques jours de notre départ en entreprise, et espérons que l'équipe attaque ne nous tiendra pas rigueur du cuisant échec que nous lui avons infligé.

IV. Annexe

A. Annexe 1 : Politique de sécurité

I) Généralités

Une politique de sécurité est un ensemble de règles d'utilisation des systèmes, réseaux et applications. Son but est d'imposer aux différents utilisateurs un mode de fonctionnement qui permette d'assurer la protection de Candide SA, de ses employés et de ses associés face à des disfonctionnement survenus sciemment ou inconsciemment. La sécurité est un effort d'équipe impliquant la participation et l'appui de chacun des employés et sous-traitants. C'est la responsabilité de chaque utilisateur de connaitre ces directives et agir en conséquence.

II) Sessions sur machines utilisateurs

Seuls les techniciens ont le droit de se loguer avec une session administrateurs.
Un technicien doit être logué en session utilisateur, sauf dans un cas de configuration du système (installation de programmes).
Un utilisateur n'a pas le droit de :

_accéder au panneau d'administration
_installer un programme
_configurer un programme
_écrire sur le disque dur ailleurs que dans un répertoire bien défini

III) Mot de passe

Tous les mots de passe de niveau d'utilisateur doivent être changés au moins tous les mois. L'intervalle de changement recommandé est toutes les 2 semaines.

Tous les mots de passe de niveau administrateur doivent être changés AVANT chaque confrontation.

Un mot de passe ne dois JAMAIS être communiqué via l'électronique (mail/msn/etc…)

a. Ce qu'il faut absolument éviter :

_Le mot de passe contient moins de quinze caractères
_Le mot de passe est un mot trouvé dans un dictionnaire (français ou étranger)
_Le mot de passe est un mot d'utilisation commun comme :
Les Noms de famille, animaux de compagnie, amis, collaborateurs, etc.
Le nom de l'ordinateur, de sites, de sociétés, de matériel, de logiciel.
Anniversaires et d'autre information personnelle comme adresses et numéros de téléphone.
Les numéros 123321, etc.

b. Ce qu'il faut faire:

Le mot de passe contient des Majuscules et minuscules en alternance
Ont des chiffres et des caractères de ponctuation aussi bien que des lettres par exemple, 0-9! *$ % ^* * () _ + | ~-= \ ` {} [] : "; ' < > ?./)
Ont au moins quinze caractères alphanumériques et est si possible une passphrase (LeGr0u£eA !!a0uePuL$CaCa).

IV) La reprise d'activité

Il est demandé, dans la mesure du possible de ne pas connecter un système sur le réseau public tant qu'une sauvegarde (fichiers de config et commandes coté serveur, « image » de l'install coté client) « propre » n'a pas été faite.
Les sauvegardes doivent être faites sur support amovibles, et en aucun laissées sur les machines interne a l'entreprise.

Si un disfonctionnement apparait sur un des systèmes, la démarche à suivre est la suivante :

_Identification du problème (faille/intrusion/etc)
_Résolution du problème
_Retour du/des systèmes à la dernière bonne configuration connue
_Déploiement de la solution
_Sauvegarde
_Changement des mots de passes des systèmes touchés
_Connexion sur le réseau public

V) Configuration des routeurs

Chaque routeur doit suivre les standards de configuration suivants :

1. Aucun compte d'utilisateur local n'est configuré sur le routeur.
2. Le mot de passe « admin » du routeur doit être crypté.
3. Rendre impossible :
    1. Émissions adressées IP (IP broadcast)
    2. Paquets entrants dans le routeur avec des adresses sources invalides
    3. TCP vieux services
    4. UDP vieux services
    5. Toutes les sources de routage
    6. Tous les services web en fonctionnement sur le routeur
4. Utiliser des chaines SNMP standardisées.
5. Les règles d'accès doivent être ajoutées au fur et a mesure de l'apparition des besoins
6. Le routeur doit être inclus dans le système de gestion de parc avec un point d'entrée désigné.

VI) Remarques sur les confrontations

Dans l'ensemble, la politique de sécurité à été bien appliquée par les employés de candide SA. Apparemment aucune intrusion n'est venue suite à une erreur d'un des employés. La reprise d'activité a été gérée après chaque confrontation. Cependant nous aurions peut être pu vérifier les postes client de la salle 213, qui contenaient, lors de notre 2eme confrontation, des keylogger bien que l'attaque ne semble pas s'en être servi).

B. Annexe 2 : Contrat d'audit

La collaboration entre les équipes « défense » et « analyse » doit faire l'œuvre d'un contrat permettant de fixer les limites d'actions auprès de Candide S.A. Ce contrat aura pour but d'assurer le bon déroulement de la mission d'audit de sécurité, à savoir la validation des moyens de protections 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, des 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 pourra réaliser l'état des lieux et des objectifs de sécurité, à savoir :

- Réglementation interne, procédures, organigramme du personnel, charte d'utilisation des ressources.
- Sécurité physique : Normes de sécurité, protection des accès (équipements, infrastructure câblée, etc.), redondance physique, plan de maintenance.
- Exploitation et administration : sauvegarde et archivage des données, continuité de service, journalisation.
- Réseaux et télécoms : architecture réseau (topologie, plan d'adressage), matériels (modems, 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.

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 accès physique au système pour la mise en place d'outils d'analyse et de détection (analyse des logs, scans, sondes). 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 ou par éventuelle adresse IP donnée pour cette même sonde.
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 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 Défense.
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.
L'équipe ayant le plus failli à sa mission aura l'honneur d'inviter l'autre équipe au restaurant de son choix.

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 compromis 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 - Facilité de supervision :
Lors d'une connexion à distance par le VPN mis à disposition à l'équipe défense, une signalisation de cet accès doit être effectuée à M David NEMBROT par mail, afin que la lecture des logs en soit facilitée.

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

Pour le groupe Défense,
M. David BOSCARI
Le 13/11/07
Lu et Approuvé

Pour le groupe Analyse,
M. **David GERBAULET**
Le 12/11/07
Lu et Approuvé

C. Annexe 3 : Procédure d'installation des clients

Procédure d'installation

Poste Windows XP Pro SP2

- Formatage du disque dur :
  - 5 Go pour la partition système
  - Le reste pour les données
- Configuration du BIOS
  - Mise en place d'un mot de passe administrateur
  - Blocage des ports USB
- Installation de Microsoft Windows XP Pro SP2
- Le mot de passe utilisateur doit expirer tout les mois
- Le mot de passe administrateur doit être d'au moins 15 caractères et contenir des Majuscules ET des Minuscules ET des Chiffres ET des caractères spéciaux (# !:)
- Configurer le système afin que l'utilisateur ne puisse pas:
  - accéder au panneau d'administration
  - installer un programme
  - configurer un programme
  - écrire sur le disque dur ailleurs que dans un répertoire bien défini
- Mise en place de l'anti-virus **ANTIVIR**
- Mise en place du **Firewall Windows XP Pro SP2**
- Installation des applications métiers

Poste Windows XP Pro

- Formatage du disque dur :
  - 5 Go pour la partition système
  - Le reste pour les données
- Configuration du BIOS
  - Mise en place d'un mot de passe administrateur
  - Blocage des ports USB
- Installation de Microsoft Windows XP Pro
- Le mot de passe utilisateur doit expirer tout les mois
- Le mot de passe administrateur doit être d'au moins 15 caractères et contenir des Majuscules ET des Minuscules ET des Chiffres ET des caractères spéciaux (# !:)
- Configurer le système afin que l'utilisateur ne puisse pas:
  - accéder au panneau d'administration
  - installer un programme
  - configurer un programme
  - écrire sur le disque dur ailleurs que dans un répertoire bien défini
- Pas d'anti-virus
- Pas de Firewall
- Installation des applications métiers

Reprise d'activité

Avant d'être mis sur le réseau, la partition système doit être sauvegardée sur un support amovible à l'aide de **Symantec GHOST.**

D. Annexe 4 : Rapport de l'équipe Audit confrontation n°1

Voir rapport analyse 1

E. Annexe 5 : Rapport de l'équipe Audit confrontation n°2

Voir rapport analyse 2

F. Annexe 6 : Questionnaire Audit

Voir questionnaire audit