Projet 2019 Groupe 6 : Plate-forme sécurisée

Dossier technique du projet - partie commune

Table des matières

1 - Introduction

Mettre en place un Firewall dans une infrastructure réseau académique afin de protéger l'environnement académique des menaces extérieurs : logiciels espions, malwares, virus. Il assure les fonctions de pare-feu telles que le filtrage d'URL et le routage interzones.

1.1 - Situation du projet dans son contexte industriel

1.1.1 - Synoptique général du système

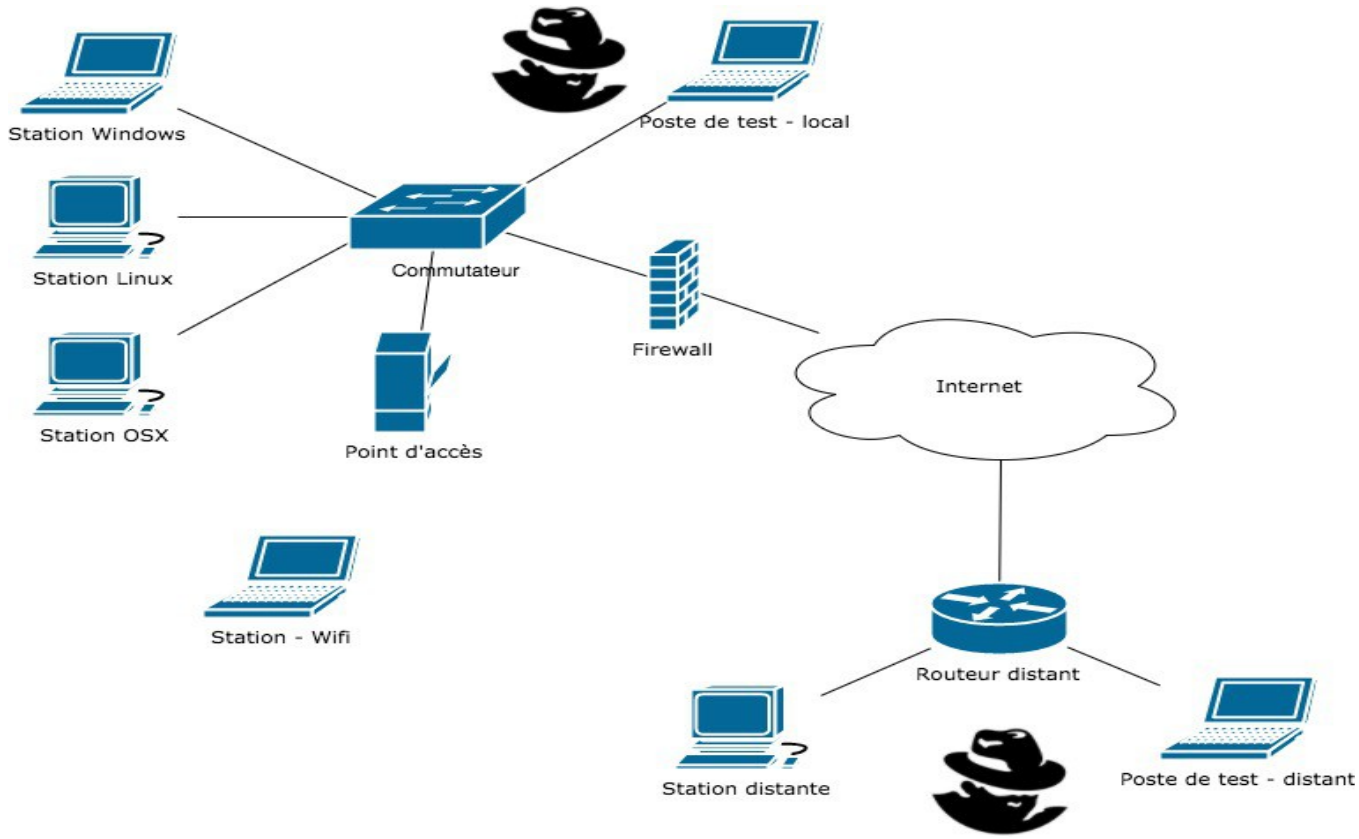

Fig. 1 : Système Customers Flow Tracking

Le réseau d'un établissement est un réseau global mutualisant les moyens d'accès administratifs et pédagogiques et utilisant le protocole IP pour le dialogue entre les équipements.

Le réseau global se décline en quatre zones au minimum, séparées par une passerelle de sécurité. Ces zones peuvent elles-mêmes être segmentées en plusieurs sous-zones en fonction de leur mise en œuvre technique. Il est organisé autour d'un équipement fédérateur, relié à des commutateurs d'extrémité selon une topologie de type « étoile » à deux niveaux de hiérarchie. Il doit être capable de segmenter et d'isoler les populations selon plusieurs zones dites « de confiance ». Le commutateur fédérateur peut assurer les fonctions de routage et de filtrage entre les sous-zones au sein de la partie pédagogique.

L'accès Internet de l'établissement est centralisé sur un seul point de connexion protégé par la passerelle de sécurité. Celle-ci doit assurer les fonctions de pare-feu, filtrage d'URL et routage interzones. La passerelle peut se décomposer en briques indépendantes et cohérentes qui assureront ces fonctions.

Cet ensemble est régi par une politique de sécurité locale respectant la politique académique et nationale, sous la responsabilité de la Personne Juridiquement Responsable (PJR) représentée par le Chef d'Établissement.

1.1.2 - Missions du système

L'objectif du projet est d'évaluer une solution pour assurer aux installations dans les établissements un niveau acceptable de sécurité.

Les principales missions du système :

- réduire les failles de sécurité liées au matériel installé dans l'infrastructure ;
- faciliter la maintenance des installations ;
- réduire les coûts d'installation et de maintenance

1.1.3 - Diagramme de déploiement d'exploitation

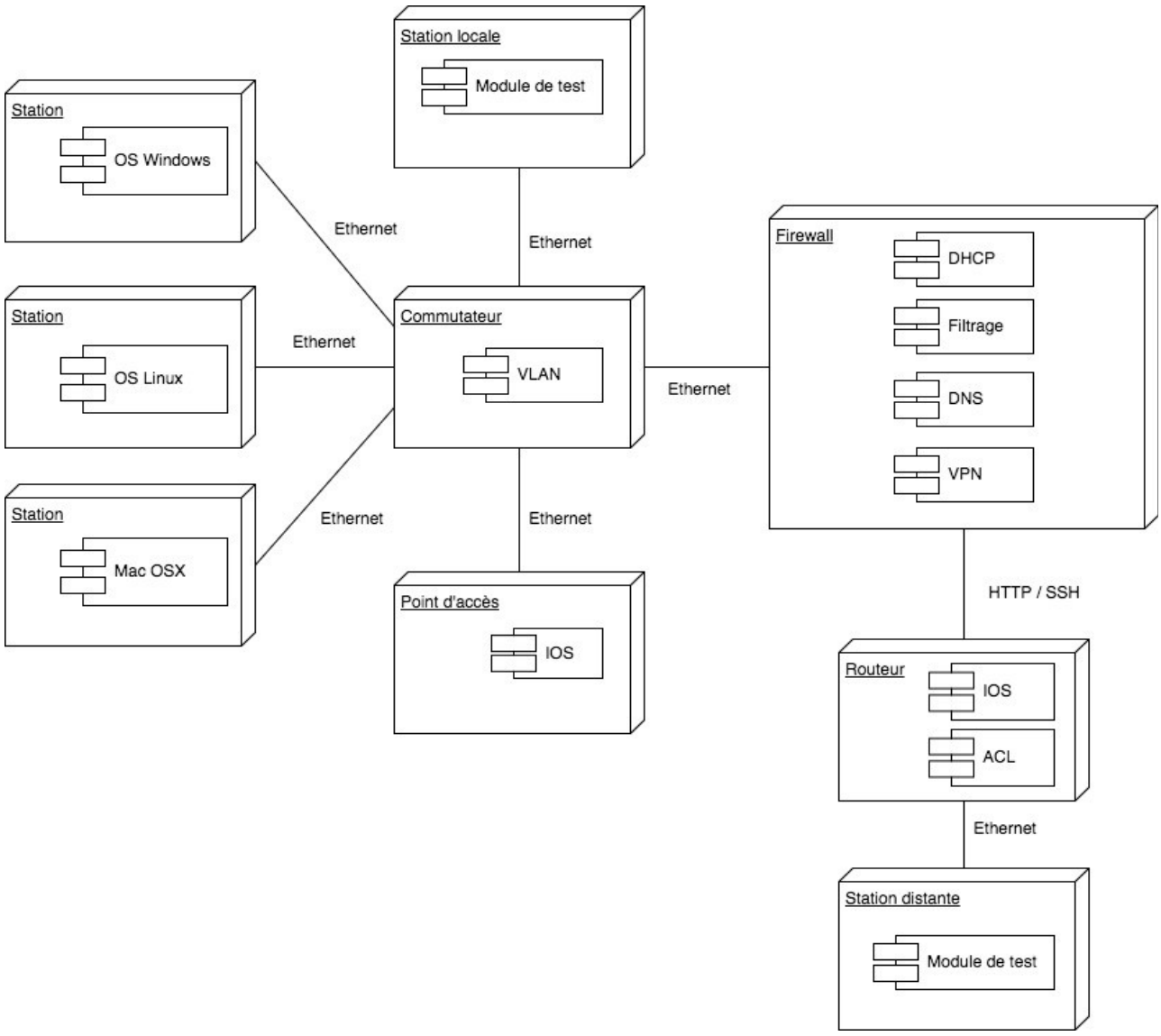

Fig. 2 : Diagramme de déploiement

1.2 - Contraintes diverses exprimées par le demandeur

Exigences fonctionnelles	***Observation***
Le couplage	Les communications entre l'applications n'entraînent pas d'erreur
L'efficacité	Les applications réalisent les fonctions principales priorisées par le Maître d'Ouvrage.
La robustesse	L'utilisation de framework et de patrons de développements standards (design pattern) est un gage de robustesse des applications. Toutes les valeurs de retour des fonctions devront être testées pour gérer les erreurs. Toutes les méthodes sont testées unitairement.
La maintenabilité	Le code est documenté et respecte les styles de codage définis par le Maître d'Ouvrage.
La sécurité	L'application doit être programmée de manière à être insensible aux attaques possibles (Internet, Wi-Fi, etc.).
L'adaptabilité	La programmation orientée objet permettra une adaptation facile de l'application vers de nouveaux besoins.
La portabilité	L'application fonctionnera sur PC
L'ergonomie	La lisibilité et la facilité d'utilisation de l'Interface-utilisateur font parties des exigences principales du demandeur. L'interface utilisateur devra respecter les standards définis par le Maître d'Ouvrage.

Exigences Technologiques	***Observation***
PC client	Fonctionne sur différents systèmes d'exploitations : Linux, Window, MAC OSX
PC Firewall	Disposer de fonctions de routage lui permettant de connecter plusieurs réseaux informatiques D'outils et services utilisés habituellement sur des routeurs professionnels propriétaires Convenir pour la sécurisation d'un réseau domestique ou de petite entreprise.

Exigences Economiques	***Observation***
Firewall	Opensource
Point d'accès	500 €

2 - Spécifications fonctionnelles

2.1 - Catalogue des acteurs

Acteur	***Rôle***
Administrateur	*Personne chargée de la gestion du réseau informatique. Il a les droits de modifications de l'équipement*
Client	*Personne qui utilise un système informatisé mais qui n'est pas nécessairement informaticien*

2.2 - Diagramme des cas d'utilisation

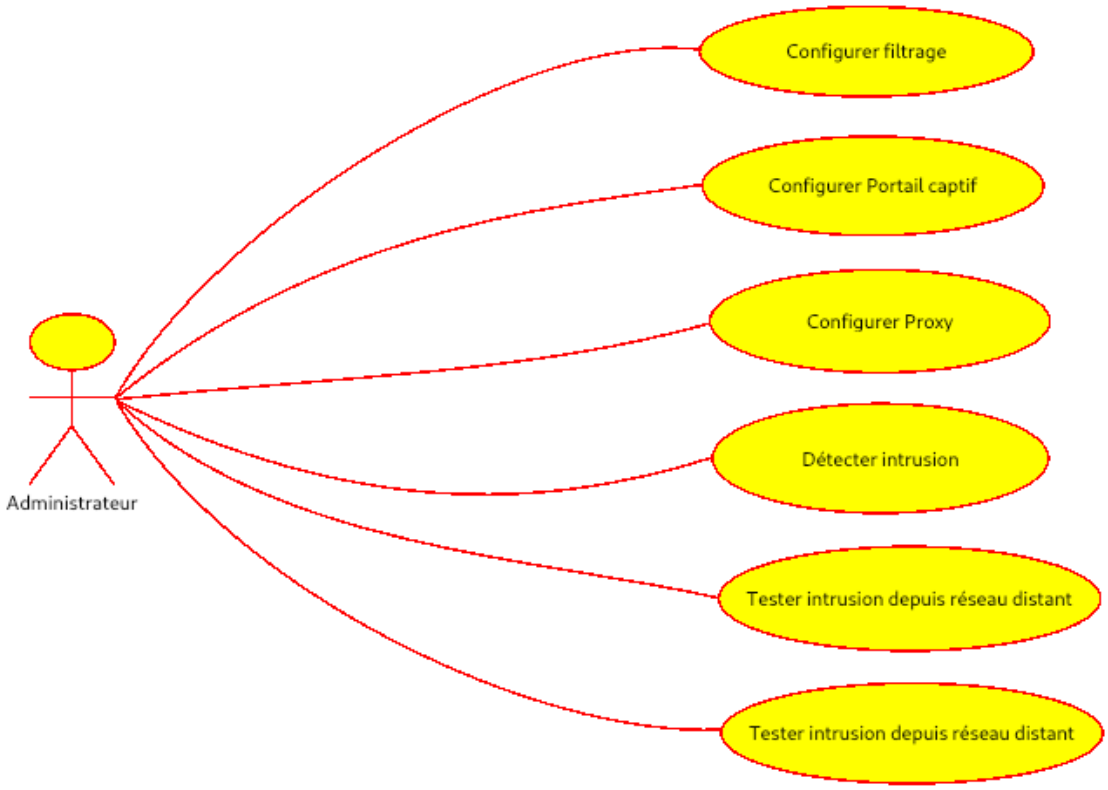

Fig. 3 : Diagramme des cas d'utilisation

2.3 - Cas d'utilisation «Configuration du Portail captif»

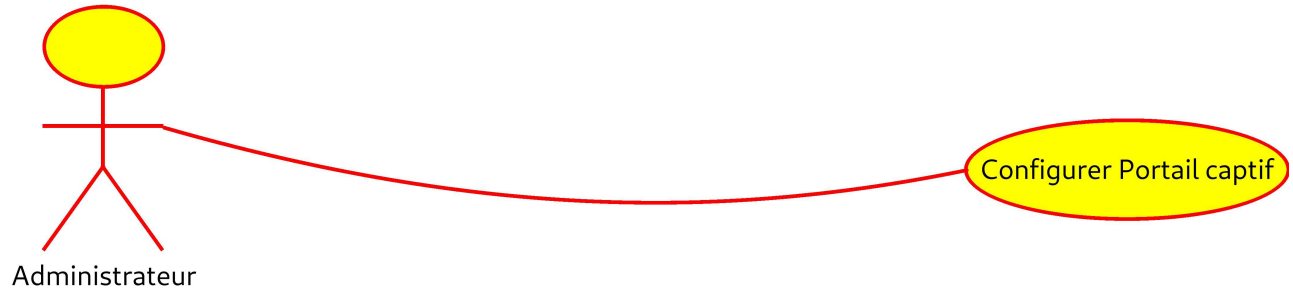

Fig. 4 : Diagramme cas d'utilisation Portail Captif

2.3.1 - Description du cas d'utilisation

Nom CU: Portail captif	***Référence : Fs2***	***MONNIER SIMON***
Pré-condition(s) *(Liste l'(es) état(s) dans le(s)quel(s) le système peut être avant que ce cas d'utilisation débute)*	*1.Firewall OPNSense en état de fonctionnement.* *2.Borne Wi-Fi configurée.*	
Scénario nominal *(Décrit le déroulement "normal", sans accroc, du processus)*	*1.Un client se connecte au SSID de la borne Wi-Fi.* *2.Le client est redirigé vers le portail captif.* *3.Le client se connecte à l'aide de son identifiant et son mot de passe.*	
Scénario alternatif A *(Décrit un cas variant du déroulement du processus)*	*Condition:* *A1.Le client n'a pas d'identifiant et ne peut se connecter.* *Il est invité à prendre contact avec l'administrateur.*	
Post-condition(s) *(Listez l'(es) état(s) dans le(s)quel(s) le système peut être quand le cas d'utilisation se termine)*	*1.Le client a accès à internet via la borne Wi-Fi après s'être connecté.*	

2.4 - Cas d'utilisation « Test d'intrusion depuis le réseau local »

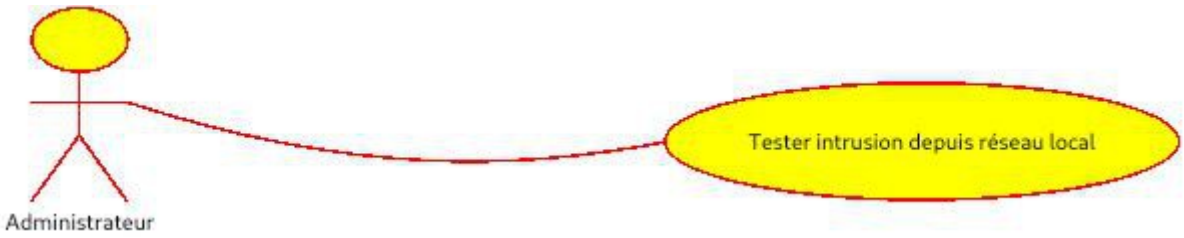

Fig. 5 : Diagramme cas d'utilisation Test d'intrusion

2.4.1 - Description du cas d'utilisation

Nom CU: Test d'intrusion depuis le réseau local	***Référence : Fs7***	***MONNIER SIMON***
Pré-condition(s) *(Liste l'(es) état(s) dans le(s)quel(s) le système peut être avant que ce cas d'utilisation débute)*	*1.Station sur le réseau local LAN ou WLAN ayant la distribution Kali Linux installée.* *2.Firewall OPNSense en état de fonctionnement.*	
Scénario nominal *(Décrit le déroulement "normal", sans accroc, du processus)*	*1.L'administrateur effectue un scan du réseau LAN ou WLAN avec l'utilitaire Zenmap, pour visualiser la topologie du réseau et détecter les stations actives ainsi que leur distribution OS et éventuellement leurs ports ouverts.* *2.L'administrateur effectue un scan des différentes stations du réseau LAN ou WLAN avec l'utilitaire Openvas security, pour détecter de potentielles failles de securité.* *3.L'administrateur exploite les failles découvertes à l'aide du framework Metasploit et/ou les ports ouverts à l'aide Medusa en brute force.*	
Scénario alternatif A *(Décrit un cas variant du déroulement du processus)*	*Condition:* *A1.L'administrateur n'a détecté aucune failles exploitable et/ou ports ouverts.* *A2.L'administrateur lance une attaque d'ingénierie social à l'aide du framework Social-Engineer Toolkit.*	
Scénario alternatif B *(Décrit un cas variant du déroulement du processus)*	*Condition:* *B1.L'administrateur n'a détecté aucune faille exploitable et/ou port ouvert.* *B2.L'administrateur simule une attaque par le biais d'une clé USB infectée.*	
Post-condition(s) *(Listez l'(es) état(s) dans le(s)quel(s) le système peut être quand le cas d'utilisation se termine)*	*1.L'attaque a réussi, le réseau est compromis et un maintien d'accès est en place via une backdoor.*	

2.5 - Cas d'utilisation « Configuration du proxy »

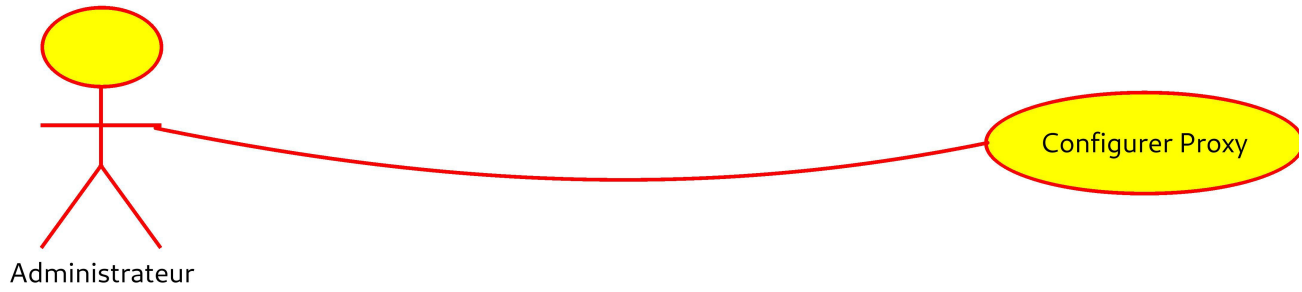

Fig. 6 : Diagramme cas d'utilisation Configuration du Proxy

2.5.1 - Description du cas d'utilisation

Nom CU: Configuration Proxy	***Référence : Fs5***	***DESNOËL David***
Pré-condition(s) *(Liste l'(es) état(s) dans le(s)quel(s) le système peut être avant que ce cas d'utilisation débute)*	*1.Firewall OPNsense en état de fonctionnement.* *2.Proxy configuré.*	
Scénario nominal *(Décrit le déroulement "normal", sans accroc, du processus)*	*1.Un client cherche à se connecter depuis le réseau local vers internet.* *2.Le client demande la page au serveur proxy.* *3.Le serveur proxy va chercher la page demandée sur internet.* *4.Le serveur proxy renvoie la page demandée au client.*	
Post-condition(s) *(Listez l'(es) état(s) dans le(s)quel(s) le système peut être quand le cas d'utilisation se termine)*	*1.Le proxy a enregistré les pages web demandées en cache.* *2.Les périphériques finaux du réseau local adoptent les adresses IP du proxy.*	

2.6 - Cas d'utilisation « Test d'intrusion depuis un réseau distant »

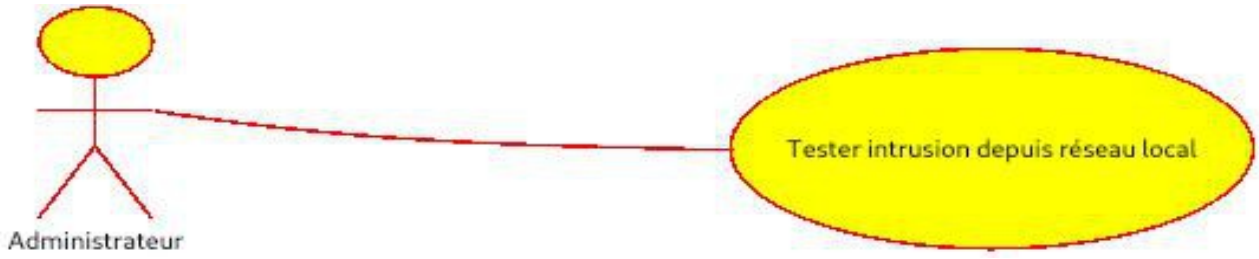

Fig. 7 : Diagramme cas d'utilisation Intrusion depuis un réseau distant

2.6.1 - Description du cas d'utilisation

Nom CU: Test intrusion depuis un réseau externe	***Référence : Fs7***	***DESNOËL David***
Pré-condition(s) *(Liste l'(es) état(s) dans le(s)quel(s) le système peut être avant que ce cas d'utilisation débute)*	*1.Firewall OPNsense en état de fonctionnement.* *2.Station depuis un réseau WAN ayant la distribution Kali-Linux installée.* *3.Obtention de l'adresse IP du Firewall.* *4.Adresse mail d'utilisateur du Réseau Local.*	
Scénario nominal *(Décrit le déroulement "normal", sans accroc, du processus)*	*1.L'administrateur effectue un scan avec ZenMap sur l'adresse IP du Firewall afin de voir quelle distribution est utilisée et quels ports sont ouverts.* *2.L'administrateur utilise Openvas security afin de détecter les failles du Firewall.* *3.L'administrateur exploite une faille avec Metasploit et /ou un port ouvert avec Medusa BrutForce.*	
Scénario alternatif A *(Décrit un cas variant du déroulement du processus)*	*A1.Aucune faille et aucun port ouvert.* *A2.Envoi d'un fichier infecté avec Metasploit ou Playload via un mail.*	
Scénario alternatif B *(Décrit un cas variant du déroulement du processus)*	*B1. Aucune faille, aucun port ouvert et pas d'adresse mail connue.* *B2. Clé USB infectée.*	
Post-condition(s) *(Listez l'(es) état(s) dans le(s)quel(s) le système peut être quand le cas d'utilisation se termine)*	*1.Réseau Local compromis.* *2.Accès au Firewall.* *3.Maintient des différents accès.*	

2.7 - Cas d'utilisation « Configuration du filtrage »

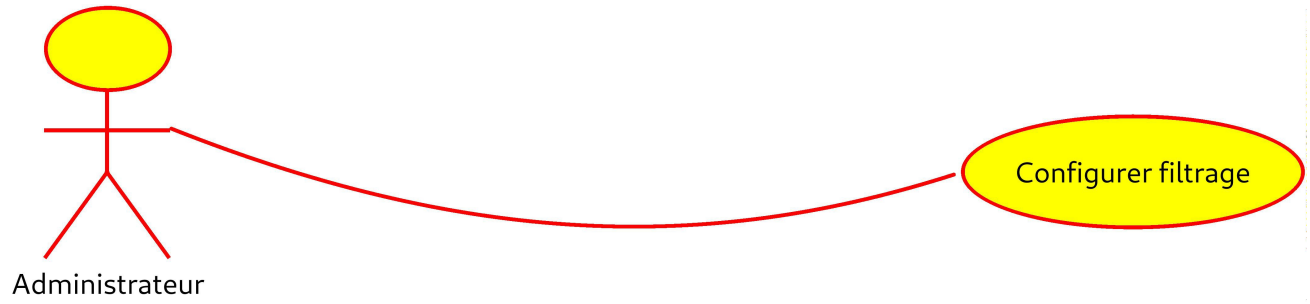

Fig. 8 : Diagramme cas d'utilisation Configuration du filtrage

2.7.1 - Description du cas d'utilisation

Nom CU: Filtrage URL	***Référence : Fs3***	***ROUHIER Quentin***
Pré-condition(s) *(Liste l'(es) état(s) dans le(s)quel(s) le système peut être avant que ce cas d'utilisation débute)*	*1.Firewall OPNSense est actif.* *2.Filtrage URL activé sur le réseau utilisé.* *3.Liste noire téléchargée et sélectionnée dans le Firewall.*	
Scénario nominal *(Décrit le déroulement "normal", sans accroc, du processus)*	*1.Un client lance un navigateur Web.* *2.Le client tente de d'accéder un site internet autorisé par l'académie.* *3.Le filtrage URL ne filtre pas ce site.* *4.Le client peut accéder au site Internet.*	
Scénario alternatif A *(Décrit un cas variant du déroulement du processus)*	*1.Un client lance un navigateur Web.* *2.Le client tente de d'accéder à un site internet interdit par l'académie.* *3.Le filtrage URL trouve ce site dans la liste noire.* *4.Une page d'erreur (ou d'avertissement) s'affiche, le site est inaccessible.*	
Nom CU: Filtrage URL	Référence : Fs3	
Pré-condition(s) *(Liste l'(es) état(s) dans le(s)quel(s) le système peut être avant que ce cas d'utilisation débute)*	*1.Firewall OPNSense est actif.* *2.Filtrage URL est activé sur le réseau utilisé.* *3.Liste noire est téléchargée et sélectionnée dans le Firewall.*	

2.8 - Cas d'utilisation « Détecter les intrusions »

Les entreprises mettent tout en œuvre pour protéger leurs ressources informatiques stratégiques, mais elles ne testent pas toujours systématiquement leurs défenses. Les tests d'intrusion aident à renforcer la sécurité de ces ressources en identifiant les vulnérabilités et les erreurs de configuration dans le Firewall.

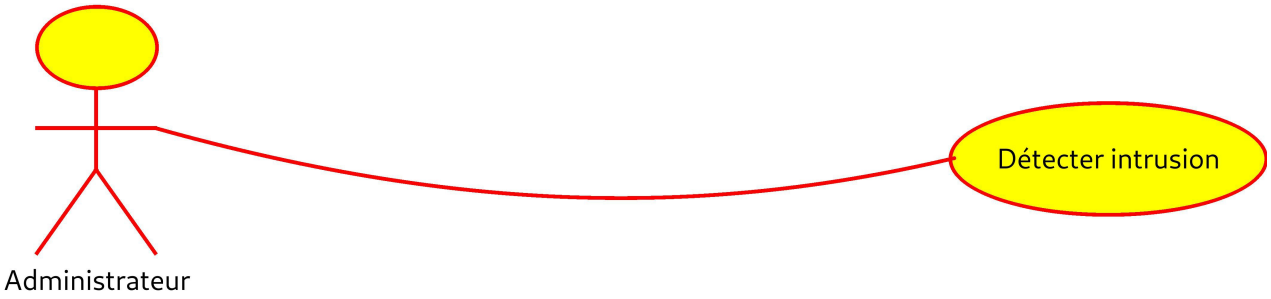

Fig. 9 : Diagramme cas d'utilisation Détection des intrusions

2.8.1 - Description du cas d'utilisation

Nom CU: Détecter les intrusions	***Référence : Fs6***	***ROUHIER QUENTIN***
Pré-condition(s) *(Liste l'(es) état(s) dans le(s)quel(s) le système peut être avant que ce cas d'utilisation débute)*	*1. Firewall OPNSense est actif sur l'ensemble des réseaux LAN, WLAN et VLAN.* *2. Le système de détection du Firewall est actif.* *3. Les modes suivants sont activés :* *- normal (génération d'alertes)* *- IPS (blocage du trafic réseau)* *- Promiscuous mode (sur les VLAN)*	
Scénario nominal *(Décrit le déroulement "normal", sans accroc, du processus)*	*1. Un client autorisé se connecte sur le réseau LAN ou WLAN.* *2. L'administrateur ne constate pas d'alerte sur son interface.* *3. Le trafic réseau reste le même.*	
Scénario alternatif A *(Décrit un cas variant du déroulement du processus)*	*1. Un client non autorisé se connecte sur le réseau LAN ou WLAN.* *2. L'administrateur constate des alertes sur son interface.* *3. Si le mode IPS est activé, il bloque le trafic réseau.*	
Scénario alternatif B *(Décrit un cas variant du déroulement du processus)*	*1. Un client non autorisé se connecte sur le réseau VLAN.* *2. L'administrateur constate des alertes sur son interface.* *3. Si le Promiscuous mode est activé, il capture des données sur l'interface réseau physique.*	
Post-condition(s) *(Listez l'(es) état(s) dans le(s)quel(s) le système peut être quand le cas d'utilisation se termine)*	*Le trafic réseau est suspendu.* *Les réseaux et les services Internet légitimes fonctionnent correctement.*	

3 - Étude préliminaire

3.0.1 - Choix du Firewall

Un pare-feu est un programme important de la sécurité informatique de nos jours, et la plupart des routeurs modernes en ont un intégré. Bien qu'utile, il peut être difficile à configurer. Heureusement, il existe également des distributions du système d'exploitation libre Linux spécialement conçues pour fonctionner en tant que pare-feu. Celles-ci ont généralement des fonctionnalités beaucoup plus avancées que celles d'un routeur et permettent d'avoir un contrôle bien plus important sur la sécurité d'un réseau personnel ou professionnel.

La plupart des distributions peuvent être téléchargées sous forme de fichier ISO. Il existe six distributions de pare-feu gratuites populaires. Voici un tableau comparatif de ces pare-feux :

Nom du pare-feu	Caractéristiques	Version
ClearOS	Design élégant, installation rapide, simple d'utilisation	ClearOS Community 7.2.0
IPCop	Code couleur des réseaux, léger, interface web maladroite	IPCop 2.1.9
OPNsense	Interface graphique riche, inspection des paquets, prise en charge d'OpenVPN	OPNsense 18.1 (Groovy Gecko)
IPFire	Code couleur des réseaux, Interface web, détection d'intrusion avec Snort, conçu pour les débutants, léger, portail captif	IPFire 2.19
pfSense	Démarrage avec clé USB ou CD, portail captif intégré, tombe en panne lors de l'ajout de fonctionnalités	pfSense 2.4.3
Smoothwall Express	Populaire, paramétrage en quelques clic, problème de bails DHCP, nécessite la création d'un profil my.smoothwall	Smoothwall Express 3.1 (Standard)
Eole – Amon	Gagne en popularité, Utilisé par le rectorat, Problèmes d'adressage et de masques ,Interface graphique non intuitive	EOLE 2.7.0

Fig. 10 : Tableau comparatif des pare-feu open-source sur Debian

Après une première expérience avec IPFire, l'utilisation de Pakfire s'est avérée difficile. Par manque de documentation sur ce Firewall libre, nous n'avons pas pu résoudre les problèmes liés à l'installation de package importants comme Squid. De plus, la mise en place du portail captif ne correspondait pas à nos attentes ; nous avions le choix entre un système de ticket et un simple portail où il faut cocher une case pour se connecter.

Nous nous sommes tournés vers OPNsense, fortement recommandé par la communauté Linux car les documentations sont sensiblement les mêmes que pfSense. Avec la documentation facilement accessible sur le Web, nous avons installé OPNsense pour remplacer l'IPFire sur la maquette réseau.

3.0.2 - Schéma du réseau

Les réseaux LAN et WLAN représentent l'établissement protégé par le Firewall. Nous avons simulé un espace Internet avec un accès réel vers Internet et un WAN pour représenter les postes pouvant commettre des intrusions.

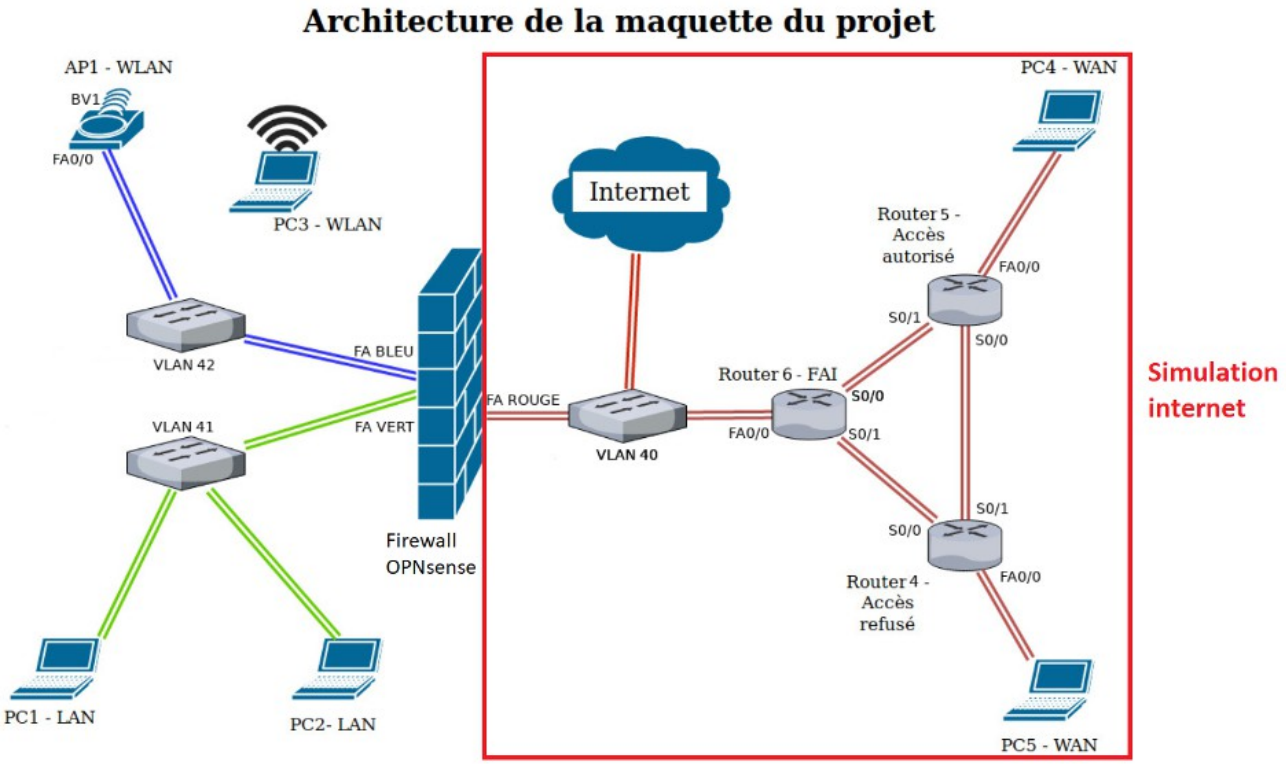

Fig. 11 : Maquette du réseau

3.0.3 - Plan d'adressage

Le plan d'adressage ci-dessous correspond au schéma de la maquette du réseau ci-dessus. Chaque équipement est adressé en Ipv4 :

- *le réseau LAN en 192.168.0.1/24*
- *le réseau WLAN en 192.168.1.1/24*
- *la passerelle du Firewall OPNsense en 10.3.2.1/23*
- *deux réseaux WAN distants en 17.16.0.0/26 et en 17.32.0.0/26*

Périphérique	Interface	Adresse IP	Masque de sous réseaux	Passerelle par défaut
Router1 – FAI (RT6)	FastEthernet	10.3.2.2	255.255.254.0	10.3.2.1
Router1 – FAI (RT6)	Serial 0/0	12.0.0.1	255.255.255.252	
Router1 – FAI (RT6)	Serial 0/1	14.0.0.2	255.255.255.252	
Router2 – accès autorisé	FastEthernet	172.16.0.1	255.255.255.0	
Router2 – accès autorisé	Serial 0/0	13.0.0.1	255.255.255.252	
Router2 – accès autorisé	Serial 0/1	12.0.0.2	255.255.255.252	
Router3 – accès refusé	FastEthernet	172.31.0.1	255.255.255.0	
Router3 – accès refusé	Serial 0/0	14.0.0.1	255.255.255.252	
Router3 – accès refusé	Serial 0/1	13.0.0.2	255.255.255.252	
FireWall – WAN	FastEthernet	10.3.2.3	255.255.254.0	10.3.2.1
FireWall – WLAN	FastEthernet	192.168.1.1	255.255.255.0	
FireWall – LAN	FastEthernet	192.168.0.1	255.255.255.0	
PC1 – LAN	Carte Réseau	DHCP 2-254	255.255.255.0	192.168.0.1
PC2 – LAN	Carte Réseau	DHCP 2-254	255.255.255.0	192.168.0.1
PC3 – WLAN	Carte Réseau	DHCP 4-254	255.255.255.0	192.168.1.1
PC4 – WAN	Carte Réseau	DHCP 2-254	255.255.255.192	172.16.0.1
PC5 – WAN	Carte Réseau	DHCP 2-254	255.255.255.192	172.31.0.1
AP1 -WLAN « Ethernet »	FastEthernet	192.168.1.2	255.255.255.0	192.168.1.1
AP1 -WLAN « Pont »	BV1	192.168.1.3	255.255.255.0	192.168.1.1

Fig. 12 : Plan d'adressage des équipements du réseau

3.0.4 - Outils utilisés

Trello

- Gestionnaire de projet en ligne
- Adapté et poursuit la méthode agile (SCRUM)

Gitlab

- Gestionnaire de projet en ligne

OPNsense (V19.1)

OPNSense est une distribution spécialisée dans la sécurité.

OPNSense cumule dans un même environnement organisé de manière cohérente :

- un Firewall avancé (filtrage sur la couche 7, priorisation, stateful inspection, ...)
- un proxy (transparent, filtrant ou authentifié)
- des fonctions VPN (OpenVPN, mais aussi IPSec, L2TP, PPTP et PPPoE)
- un portail captif pour le réseau Wi-Fi, l'authentification à double-facteur (pour le portail captif, le proxy, le VPN, ...)
- un outil de détection d'intrusion (ou IPS basé sur la solution Suricata)
- la haute disponibilité

Ipfire (V2.21)

IPfire est un Firewall OpenSource, il intègre les fonctions suivantes nativement :

- Firewall
- Intrusion Detection System (Snort) de prévention des intrusions
- Serveur proxy avec filtrage de contenu et les fonctions de mise en cache des mises à jour (par exemple mises à jour Microsoft Windows, antivirus, et bien d'autres)
- Serveur de temps NTP
- VPN pour IPSec et serveur OpenVPN
- Serveur DHCP
- Dynamic DNS (DynDNS, No-IP)
- Analyse fonctions de surveillance du système et analyse des logs
- Qualité de service (QoS)

EOLE – Amon(V2.3)

Le module Amon permet de partager en toute sécurité un accès Internet entre les sous-réseaux d'un réseau local.
Installé sur un serveur dédié, équipé de deux, trois, quatre ou cinq interfaces réseau, il permet d'organiser au mieux l'architecture réseau d'un établissement.

Kali-Linux(V 2019.1)

Kali Linux est une distribution GNU/Linux, basée sur Debian.
L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion.

Openvas(V9)

OpenVAS est un scanner de vulnérabilités complet. Ses capacités incluent des tests non authentifiés, des tests authentifiés, divers protocoles Internet et industriels de haut niveau et de bas niveau, le réglage des performances pour les analyses à grande échelle et un puissant langage de programmation interne permettant de mettre en œuvre tout type de test de vulnérabilité.

Metasploit (5.0)

Metsploit est un outil pour le développement et l'exécution d'exploits contre une machine distante, il permet de réaliser des audits en sécurité, de tester et développer ses propres exploits.

Set -social engineer toolkit- (V 8.0)

Set est conçu pour effectuer des tests de pénétration du côté humain.

Medusa(V2.0)

Medusa est un logiciel disponible sous Linux permettant de tester la robustesse de différents services au moyen d'une attaque de type brute force.

4 - Recette

Voici une figure qui représente le positionnement du FireWall dans le réseau de l'académie :

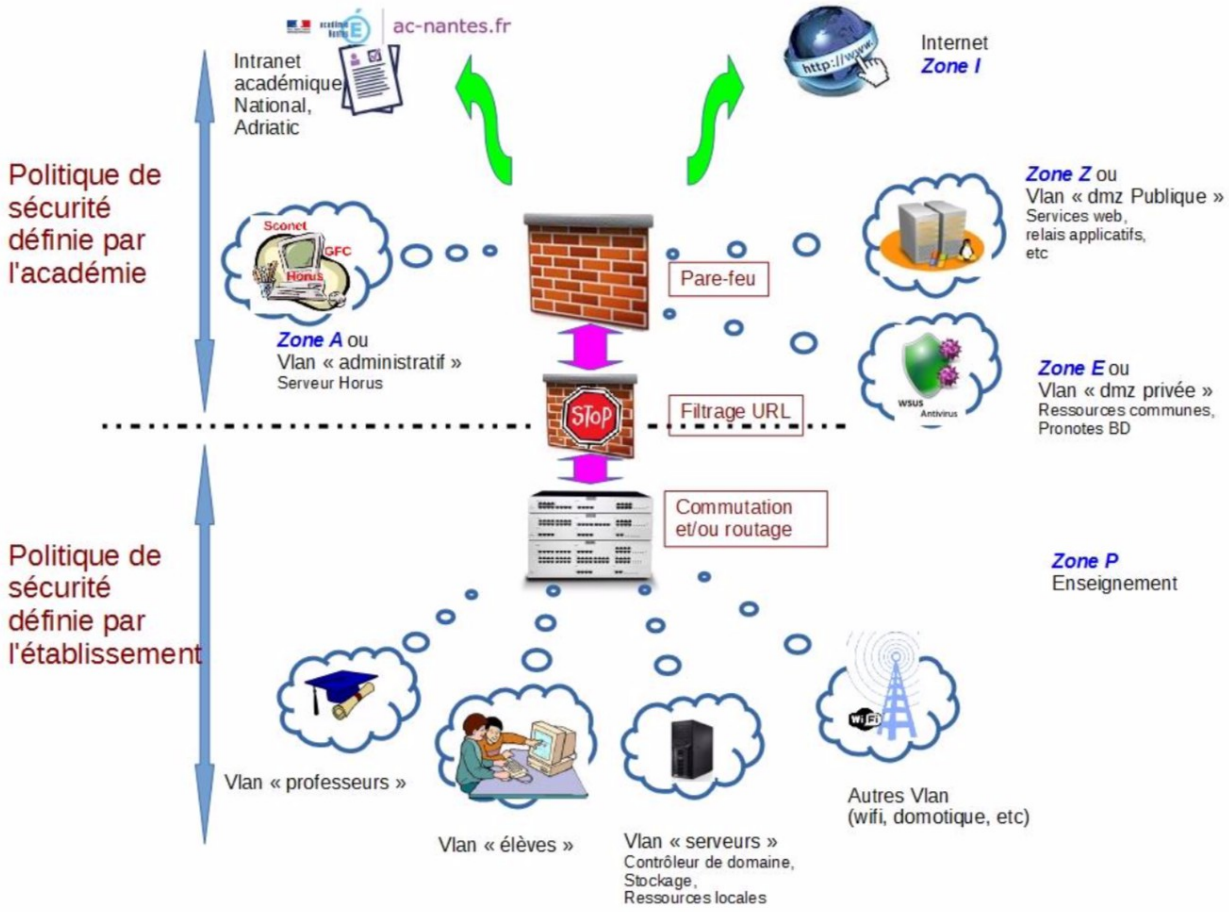

Fig. 13 : Situation du pare-feu dans le réseau académique

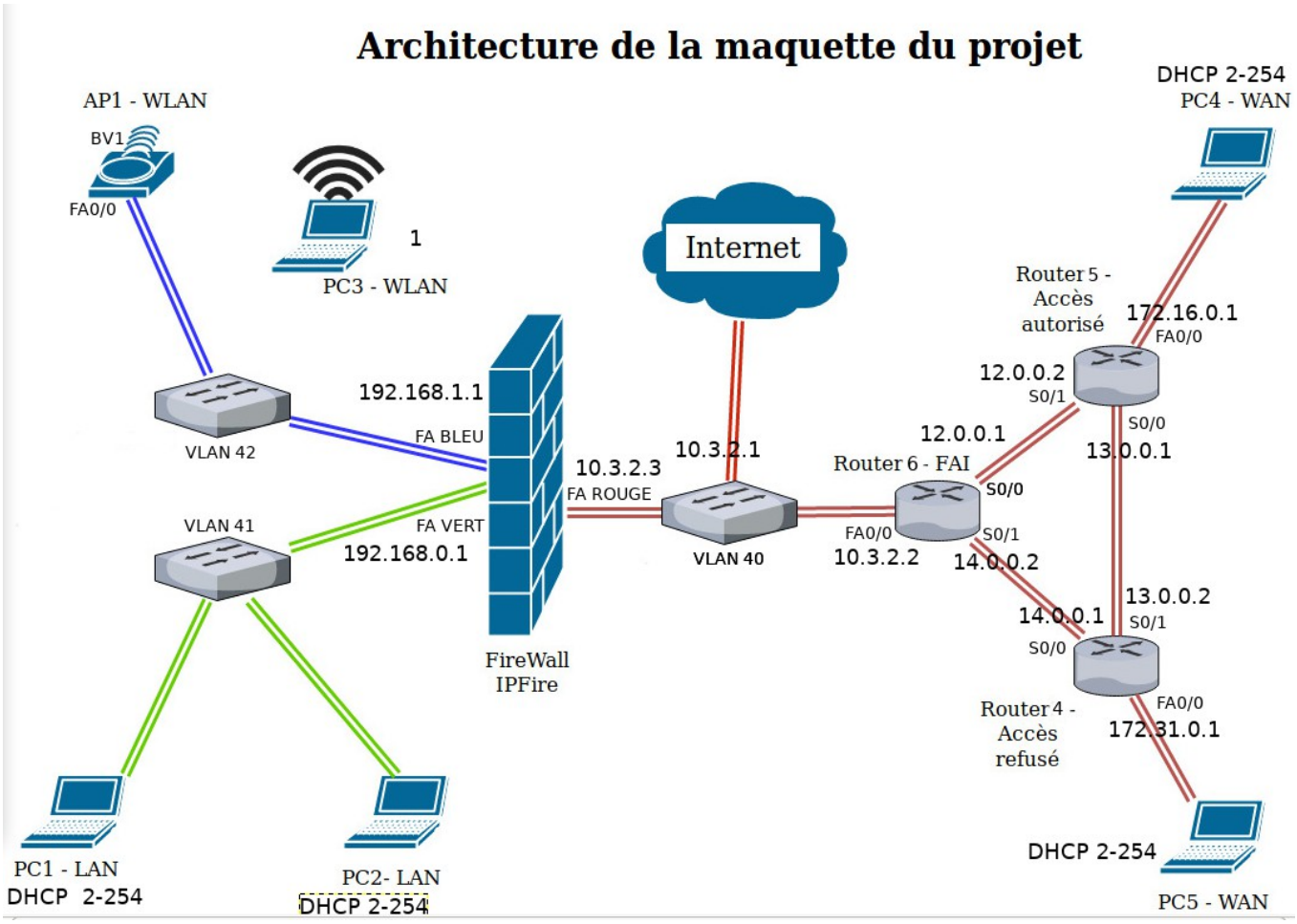

Fig. 14 : Maquette du réseau avec adressage

5 - Bilan

5.1 - Conclusion

Points positifs

- *Découverte de nouvelles distributions et leurs outils logiciels : Kali-Linux, OPNSense, Ipfire, Eole-Amon*
- *Travail d'équipe enrichissant*

Point négatif

- *Changement de Firewall car manque de documentation technique sur Ipfire*