

P2019 : G6 : Plate-Forme Sécurisée
ROUHIER Quentin

Dossier technique du projet - partie individuelle

Table des matières

1 - SITUATION DANS LE PROJET.....	2
1.1 - RAPPEL DES TÂCHES PROFESSIONNELLES À RÉALISER.....	2
1.2 - SYNOPTIQUE DE LA MAQUETTE DU RÉSEAU.....	5
2 - RÉALISATION DU RÉSEAU LAN AVEC ADRESSAGE DYNAMIQUE DES POSTES.....	7
2.1 - CONCEPTION DÉTAILLÉE DU RÉSEAU LAN.....	7
2.2 - PROCÉDURE DE TEST DE L'ADRESSAGE DYNAMIQUE DU RÉSEAU LAN.....	9
2.3 - RAPPORT D'EXÉCUTION DE L'ATTRIBUTION D'UNE ADRESSE DYNAMIQUE.....	10
3 - MISE EN PLACE DU PROXY WEB TRANSPARENT.....	11
3.1 - PARAMÉTRAGE DÉTAILLÉ DU PROXY TRANSPARENT.....	11
3.2 - PROCÉDURE DE TEST DE LA NÉCESSITÉ DU PROXY SUR LE RÉSEAU LAN.....	13
3.3 - RAPPORT D'EXÉCUTION.....	14
4 - TEST DU FILTRAGE URL.....	16
4.1 - PARAMÉTRAGE DÉTAILLÉ DU FILTRAGE URL.....	16
4.2 - PROCÉDURE DE TEST DU FILTRAGE URL SUR LE LAN.....	18
4.3 - RAPPORT D'EXÉCUTION.....	19
5 - TEST DE LA DÉTECTION D'INTRUSION.....	20
5.1 - PARAMÉTRAGE DÉTAILLÉ DE LA DÉTECTION D'INTRUSION SURICATA.....	20
5.2 - PROCÉDURE DE TEST DE LA DÉTECTION D'INTRUSION SURICATA (À VALIDER).....	25
5.3 - RAPPORT D'EXÉCUTION.....	26
6 - BILAN DE LA RÉALISATION PERSONNELLE.....	27
6.1 - STATUT DES FONCTIONS À CHARGE.....	27
6.2 - CONCLUSION.....	27

1 - Situation dans le projet

1.1 - Rappel des tâches professionnelles à réaliser

- Créer une maquette simulant l'architecture réseau du Rectorat de Nantes
- Ajouter une passerelle sécurisée pour les élèves ayant des droits intermédiaires
- Mettre en place une architecture réseau LAN (encadré en vert) sur notre maquette. Elle répond aux critères du schéma de topologie ci-dessous
- Configuration du Proxy pour l'utilisation du filtrage URL
- Filtrage URL avec la blacklist UT1
- Détection d'intrusion avec Suricata

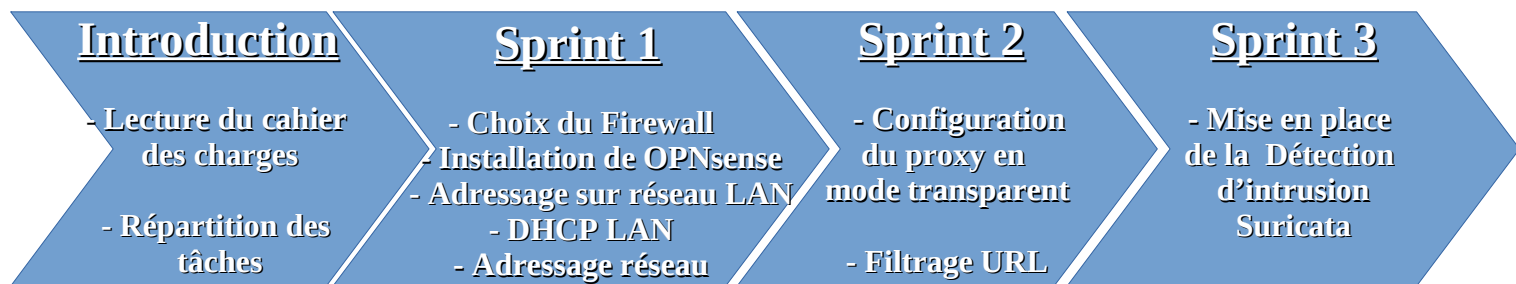


Fig. 1 : Diagramme des sprints synthétisant l'organisation sur Trello

Les objectifs du projet ont été extraits du cahier des charges.

Objectifs :

- 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
- Mes tâches personnelles ont été affectées selon la méthode Agile. Nous avons réparti les tâches avec Trello selon les fonctions à développer et à configurer. Chaque étape a été vérifiée et validée (dans l'onglet « To Validate ») par un autre membre du groupe de projet.

Dans l'exemple ci-dessous, les étapes « Done » ont été traitées avec succès, il reste à traiter les tickets dans « In Progress » et « To Do ».



Fig. 2 : Avancée du projet sur Trello

Phases du projet :

- Lecture du cahier des charges
- Création du plan d'adressage et de la topologie réseau de la maquette sur Draw.io (1)(2)
- Maquette réseau : câblage, paramétrage des routeurs sur le réseau LAN (3)
- Choix du FireWall et de la machine qui l'héberge : IPFire au début, puis OPNSense en définitive (4)(5)(6)
- Mise en place du DHCP sur le réseau LAN (5)(6)(7)
- Mise en place du filtrage URL et modification du proxy en conséquences (8)
- Paramétrage de la détection d'intrusion Suricata (9)

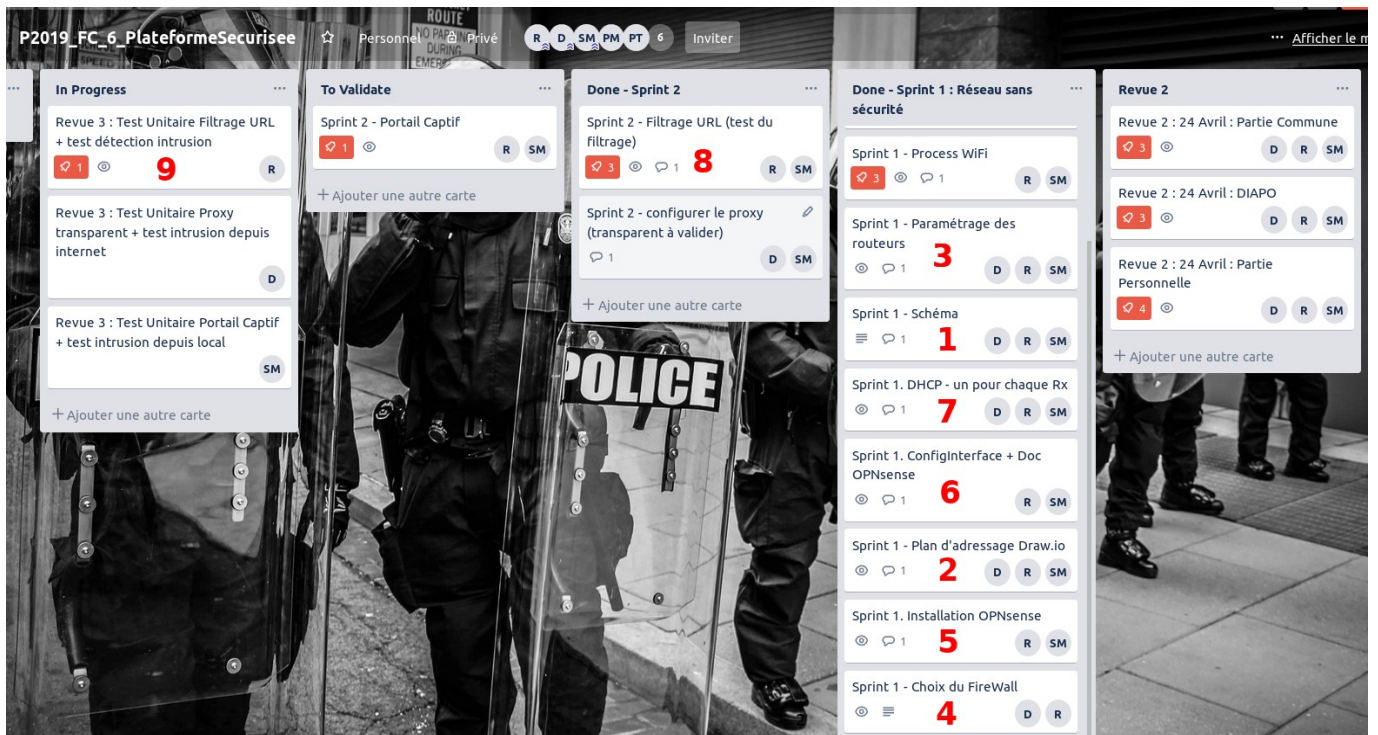


Fig. 3 : Partie personnelle avec étapes numérotées sur Trello

1.2 - Synoptique de la maquette du réseau

- Installation de la machine hébergeant le FireWall avec ajout de 2 cartes réseau (une filaire pour le WAN et une sans fil pour le WLAN).



Fig. 4 : Vue arrière de la machine

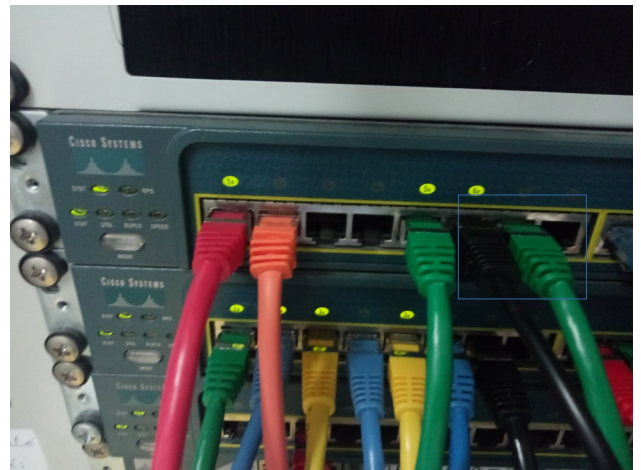


Fig. 5 : Vue LAN de la baie

Le câble vert côté machine est l'interface LAN du FireWall. La passerelle du réseau LAN est branchée au premier port du VLAN comprenant 4 ports. Les câbles encadrés côté baie représentent l'ensemble des postes connectés au LAN.

- Installation du FireWall IPFire sur la machine avec une clé bootable dans un premier temps, puis remplacement de celui-ci par OPNsense.



Fig. 6 : Créateur de disque Unbuntu



Fig. 8 : écran d'installation OPNsense



Fig. 7 : écran installation IPFire

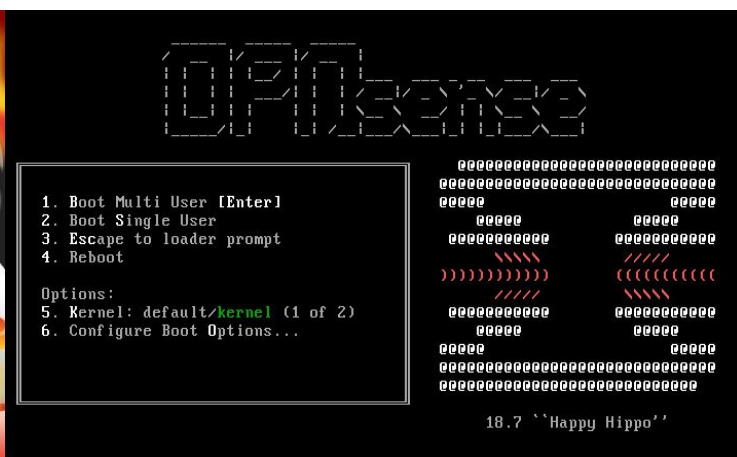


Fig. 8 : écran installation OPNsense

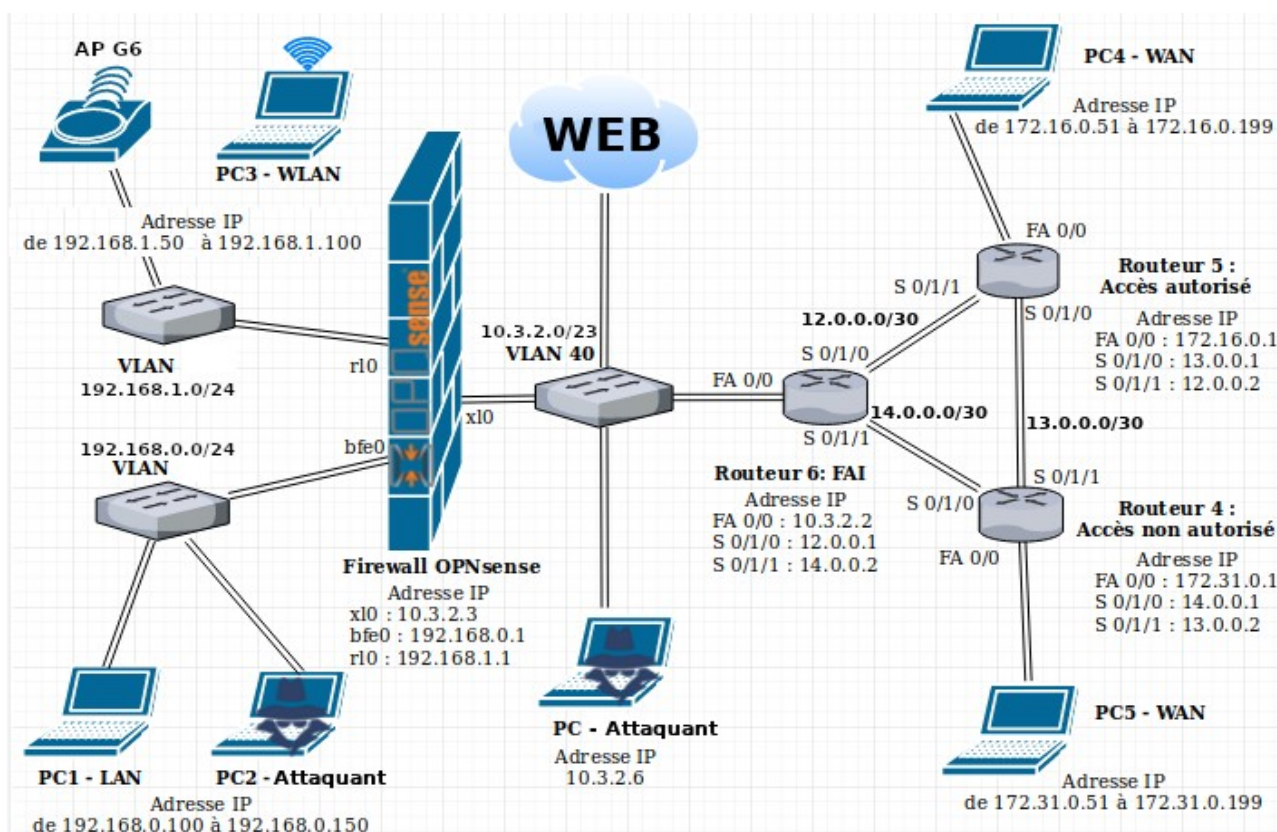


Fig. 9 : Topologie de la maquette simulant l'architecture réseau du Rectorat de Nantes

2 - Réalisation du réseau LAN avec adressage dynamique des postes

2.1 – Conception détaillée du réseau LAN

Je suis intervenu sur la configuration du réseau LAN, en 192.168.0.0, illustré par l'extrait issu de notre schéma topologique.

Cette partie du réseau simule les utilisateurs du réseau LAN du lycée concernée. En réalité, pour prouver le bon fonctionnement du DHCP, on attribue une plage d'adresse plus restreinte (100-150).

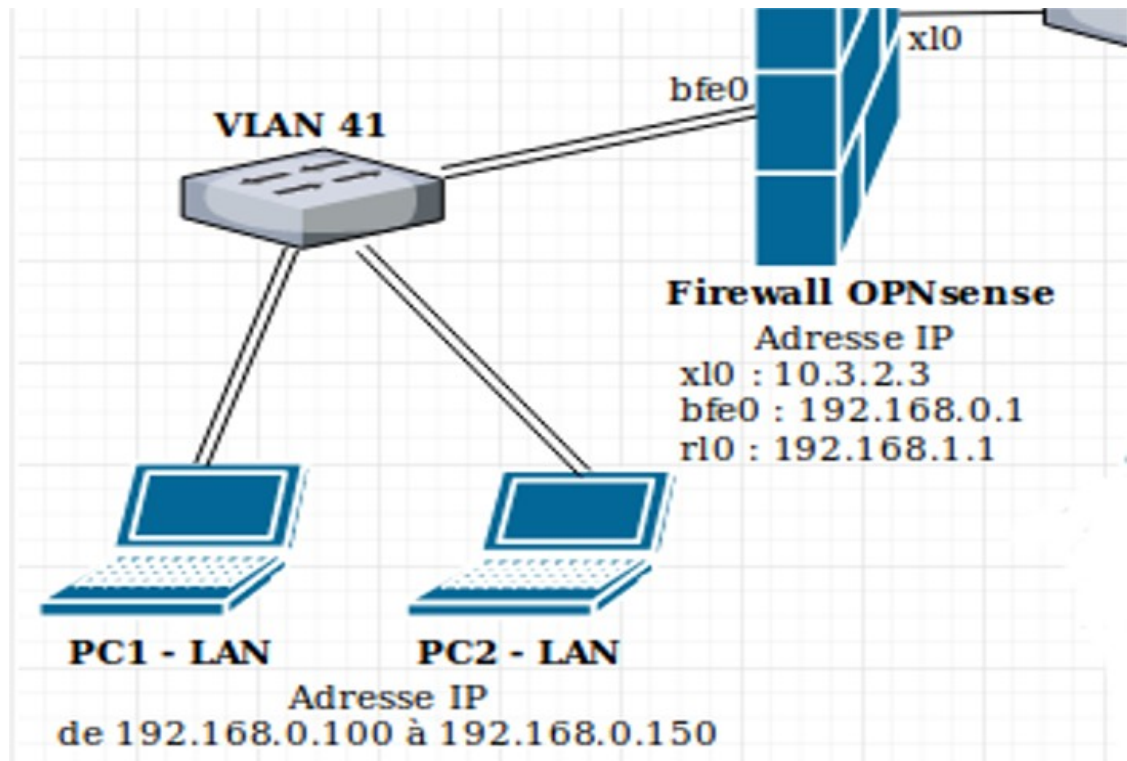


Fig. 10 : Zoom sur la partie LAN de la maquette

On utilise le PC1 (administrateur) sur un système d'exploitation Linux. On se sert du PC2 comme PC client sur lequel on lance un Terminal :

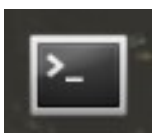


Fig. 11 : Icône du Terminal

Ensuite, on active le DHCP sur le poste admin utilisé PC1.

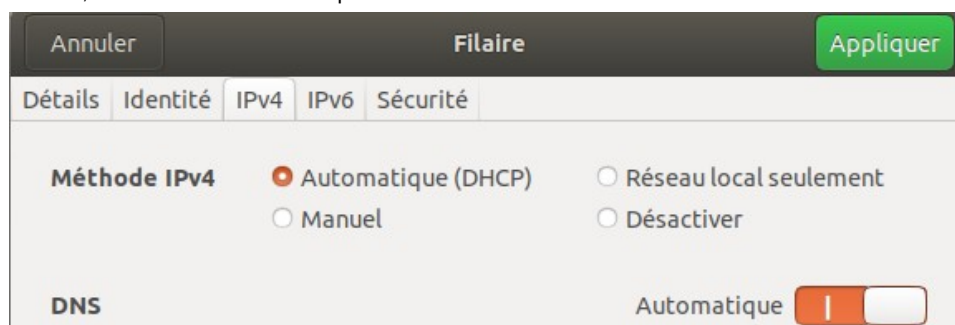


Fig. 12 : Activation DHCP en mode graphique

Le poste administrateur peut être utilisé pour modifier la plage d'adressage DHCP à l'aide de l'interface de OPNsense dans le navigateur. On utilise le PC2 (client) pour vérifier le fonctionnement du DHCP. Ce PC2 a les paquets « net-tools » installés.

Sur le réseau LAN, le serveur DHCP de notre FireWall OPNsense est paramétré comme indiqué ci-dessous :

☒ Activer le serveur DHCP sur l'interface LAN

☐ Refuser les clients inconnus
Si cette option est cochée, seuls les clients définis ci-dessous obtiendront des baux DHCP à partir de ce serveur.

Sous-réseau : 192.168.0.0

Masque de sous-réseau : 255.255.255.0

Plage disponible : 192.168.0.1 - 192.168.0.254

Plage : de 192.168.0.100 à 192.168.0.150

Fig. 13 : Paramétrage DHCP sur interface graphique

La plage d'adressage sur le LAN s'étend de 192.168.0.100 à 192.168.0.150.

Serveurs DNS

Serveur DNS	Utiliser la passerelle
195.83.167.1	GW_WAN - wan - 10.3.2.1
195.83.167.2	GW_WAN - wan - 10.3.2.1

Fig. 14 : Paramétrage DNS sur interface graphique

La passerelle du FireWall a le DNS 8.8.8.8, celui de www.google.com. On remplace par celui du Rectorat de Nantes :

2.2 - Procédure de test de l'adressage dynamique du réseau LAN

Id.	Architecture réseau testée Description Sommaire	Procédure de test														
		Résultats attendus														
U1.0	Le PC2 est hors tension.	Aucune manipulation														
		Rien ne se passe														
U1.1	<p>Le PC2 est mis sous tension et se connecte au réseau LAN. On vérifie que l'adressage automatique DHCP est activé.</p> <p>Il demande une adresse au serveur DHCP de OPNsense.</p> <p>Le PC2 reçoit une adresse IP de la plage définie sur OPNsense : de 192.168.0.100 à 192.168.0.150, ainsi que le DNS de la passerelle du FireWall.</p> <p>Par défaut celui-ci sera 8.8.8.8, celui de www.google.com. Par la suite, on ajoute celui du Rectorat de Nantes</p>	<div>ifconfig</div> <div>ip route</div> <div>inet 192.168.0.107 netmask 255.255.255.0 broadcast 192.168.0.255</div> <div>default via 192.168.0.1 dev eth0 proto dhcp metric 100</div>														
		<div>Traceroute 8.8.8.8</div> <div>route -n</div> <div>1 OPNsense.localdomain (192.168.0.1) 0.413 ms 0.370 ms 0.347 ms</div> <div>2 10.3.2.1 (10.3.2.1) 0.848 ms 1.452 ms 1.437 ms</div> <div>3 172.31.3.252 (172.31.3.252) 0.441 ms 0.430 ms 0.716 ms</div> <div>4 * * *</div> <div>13 google-public-dns-a.google.com (8.8.8.8) 10.129 ms 9.682 ms 10.093 ms</div> <div>Table de routage IP du noyau</div> <table><tr><th>Destination</th><th>Passerelle</th><th>Genmask</th><th>Indic</th><th>Metric</th><th>Ref</th><th>Use</th><th>Iface</th></tr><tr><td>0.0.0.0</td><td>192.168.0.1</td><td>0.0.0.0</td><td>UG</td><td>100</td><td>0</td><td>0</td><td>eth0</td></tr></table>	Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface	0.0.0.0	192.168.0.1	0.0.0.0	UG	100	0
Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface									
0.0.0.0	192.168.0.1	0.0.0.0	UG	100	0	0	eth0									
U1.2	<p>Test de la connectivité à internet : on vérifie que le chemin vers le serveur DNS correspond bien au schéma de topologie.</p> <p>Si oui, on peut visualiser le bon fonctionnement de la passerelle pour que le PC2 ait bien accès à Internet.</p>															

2.3 - Rapport d'exécution de l'attribution d'une adresse dynamique

Id.	OK	!OK	Observations																
U1.1	*		<div><div>Adresse IPv4 192.168.0.107</div><div>Adresse IPv6 fe80::7750:218a:cbe9:c3ba</div><div>Adresse matérielle D4:C9:EF:F0:0D:72</div><div>Route par défaut 192.168.0.1</div><div>DNS 192.168.0.1</div></div>																
U1.2	*		<div>OPNsense.localdomain (192.168.0.1) 0.466 ms 0.444 ms 0.430 ms</div> <div>2 10.3.2.1 (10.3.2.1) 2.908 ms 3.138 ms 3.382 ms</div> <div>3 172.31.3.252 (172.31.3.252) 0.698 ms 0.704 ms 0.692 ms</div> <div>4 ***</div> <div>google-public-dns-a.google.com (8.8.8.8) 10.003 ms 9.694 ms 9.664 ms</div> <div>Table de routage IP du noyau</div> <div><table><tr><th>Destination</th><th>Passerelle</th><th>Genmask</th><th>Indic</th><th>Metric</th><th>Ref</th><th>Use</th><th>Iface</th></tr><tr><td>0.0.0.0</td><td>192.168.0.1</td><td>0.0.0.0</td><td>UG</td><td>100</td><td>0</td><td>0</td><td>eth0</td></tr></table></div>	Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface	0.0.0.0	192.168.0.1	0.0.0.0	UG	100	0	0	eth0
Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface												
0.0.0.0	192.168.0.1	0.0.0.0	UG	100	0	0	eth0												

3 - Mise en place du Proxy Web transparent

3.1 - Paramétrage détaillé du Proxy transparent

Démarrer le PC1 (administrateur), le brancher au réseau LAN puis ouvrir un navigateur Web, comme Firefox.



Fig. 15: Logo FireFox

OPNsense dispose d'un Proxy Web appelé Squid, installé manuellement au préalable, comme tous les services du FireWall.



Fig. 16 : Logo Squid

Le proxy est activé sur l'interface du FireWall OPNsense.

La configuration de base du proxy est la suivante, l'ordre de mise en place des paramètres est important :

- portail captif activé
- proxy Web transparent (l'utilisateur n'a pas le visuel sur la configuration du proxy)
- SSL automatique
- activation du proxy

Réglages Proxy généraux ▾
Forward Proxy ▾
Proxy Auto-Config ▾
Listes de Contrôle d'Accès distantes

● mode avancé

i Activer le proxy

☑

Système: Diagnostics: Services

Service	Description	Statut
captiveportal	Portail Captif	▶ ↺ ■
configd	System Configuration Daemon	▶ ↺ ■
dhcpcd	DHCPv4 Server	▶ ↺ ■
login	Utilisateurs et Groupes	▶ ↺
ntpd	Serveur de temps réseau	▶ ↺ ■
pf	Packet Filter	▶ ↺
squid	Proxy Web	▶ ↺ ■
syslog	Syslog	▶ ↺ ■
unbound	Unbound DNS	▶ ↺ ■

Fig. 17 : Activation du Proxy Web

Configuration du proxy Web en mode transparent :

Interfaces mandataires : LAN, WLAN

Port du proxy : 3128

Activer le proxy HTTP Transparent : ☒

Enable SSL inspection : ☒

Log SNI information only : ☐

SSL Proxy port : 3129

AC à utiliser : opnsense-ssl

SSL no bump sites : .google.com, .google.fr, .googleapis.com, .gstatic.com, .le100.net, .facebook.com, .fr.facebook.com, .staticxx.facebook.com, .scontent-cdt1-1.xx.fbcdn.net, .gitlab.com, .trello.com

Fig. 18 : Configuration du proxy transparent

Le mode transparent est effectif à partir du moment où on modifie les paramètres du NAT sur l'interface de la façon suivante :

↔	LAN	TCP	LAN net	*	*	80 (HTTP)	127.0.0.1	3128	Rediriger le trafic vers le proxy
↔	LAN	TCP	LAN net	*	*	443 (HTTPS)	127.0.0.1	3129	Rediriger le trafic vers le proxy

Fig. 19 : Paramètres du NAT

Ceci génère automatiquement les règles suivantes sur le réseau LAN :

▶	IPv4 TCP	LAN net	*	127.0.0.1	3128	*	NAT Rediriger le trafic vers le proxy	⏪ ⏴
▶	IPv4 TCP	LAN net	*	127.0.0.1	3129	*	NAT Rediriger le trafic vers le proxy	⏪ ⏴

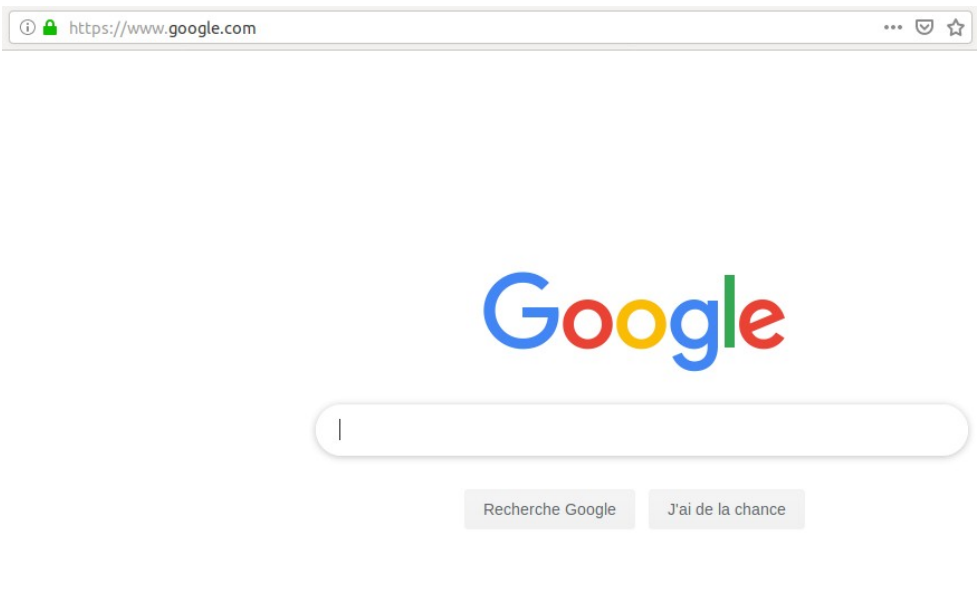
Fig. 20 : Règles auto proxy transparent réseau LAN

3.2 - Procédure de test de la nécessité du proxy sur le réseau LAN

On utilise le PC2 pour tester le fonctionnement du proxy Web :

Id.	Architecture réseau testée Description Sommaire	Procédure de test
		Résultats attendus
U1.0	<p>Le proxy Web est désactivé.</p> 	<p>Peu importe les paramètres du navigateur Web</p> <p>URL entré : www.google.com</p> <p>La connexion au site est impossible.</p>
U1.1	<p>Le proxy Web est activé.</p> <p>Le FireWall OPNsense permet de naviguer sans passer paramétrage du navigateur Web. On désactive les paramètres proxy du navigateur pour essayer de naviguer.</p> 	 <p>URL entré : www.google.com</p> <p>La connexion au site est possible.</p>
U1.2	<p>Le proxy Web est activé.</p> <p>Peu importe les paramètres du navigateur.</p> <p>Tout le trafic est dirigé automatiquement vers le proxy de manière transparente, pour que l'utilisateur ne s'en rende pas compte.</p> <p>Les certificats SSL sont ainsi fournis par le serveur du proxy. Il n'y a pas besoin de les télécharger en local sur les postes.</p>	 <p>La page www.google.com s'affiche</p>

3.3 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.1 U1.2	*		

Sur les journaux d'événement, on constate une connexion sur le réseau LAN en enregistrée par OPNsense :

► lan	→ May 20 14:14:36	192.168.0.107:53002	192.168.0.1:443	tcp	anti-lockout rule
-------	-------------------	---------------------	-----------------	-----	-------------------

Fig. 21 : Journal d'événements du FireWall

Sur le fichier journal du proxy, on a la trace d'une connexion autorisée :

Date	Message
Cache Accès Store	
1558354739.350 13	192.168.0.107 TCP_MISS/200 524 GET http://detectportal.firefox.com/success.txt - ORIGINAL_DST/193.51.224.22 text/plain
1558354739.322 63	192.168.0.107 TAG_NONE/200 0 CONNECT 172.217.18.194:443 - ORIGINAL_DST/172.217.18.194 -
1558354736.971 83	192.168.0.107 TCP_MISS/200 524 GET http://detectportal.firefox.com/success.txt - ORIGINAL_DST/193.51.224.22 text/plain
1558354736.874 62	192.168.0.107 TAG_NONE/200 0 CONNECT 172.217.18.194:443 - ORIGINAL_DST/172.217.18.194 -

Fig. 22 : Fichier journal du proxy

Il est possible de supprimer la mention de l'affichage de la version quand le client se fait bloquer par le proxy. Ceci permet de prévenir d'éventuel contournement propre à la version du FireWall.



Fig. 23 : Mention de la version

4 - Test du filtrage URL

4.1 - Paramétrage détaillé du filtrage URL

Le filtrage URL nécessite une blacklist. Cette liste est un ensemble de dossier représentant chacun une catégorie, avec un fichier « domains » qui regroupe l'ensemble des URL de la catégorie. Cet ensemble est compressé pour créer un fichier tar.gz.

On télécharge la blacklist en indiquant l'URL du lien FTP suivant sur l'interface du PC2 :

ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz

Réglages Proxy généraux Forward Proxy Proxy Auto-Config Listes de Contrôle d'Accès distantes

Liste noire distante

Activé	Nom de fichier	URL
<input checked="" type="checkbox"/>	blacklist	ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz

« < 1 > »

Appliquer Télécharger les ACLs & les Appliquer Télécharger les ACLs Planifier avec Cron

Fig. 24 : Liste de contrôle d'accès distante

La blacklist sera effective quelques minutes après que le bouton « Télécharger les ACLs & les Appliquer » soit utilisé.

Au premier téléchargement, on peut modifier les catégories choisies dans la liste, sachant qu'elles sont toutes cochées par défaut.

Lors de la tentative de connexion à une page Web sécurisée (protocole https), le navigateur du PC2 (client) ne reconnaît pas les certificats utilisés par OPNSense. On a alors la page suivante :

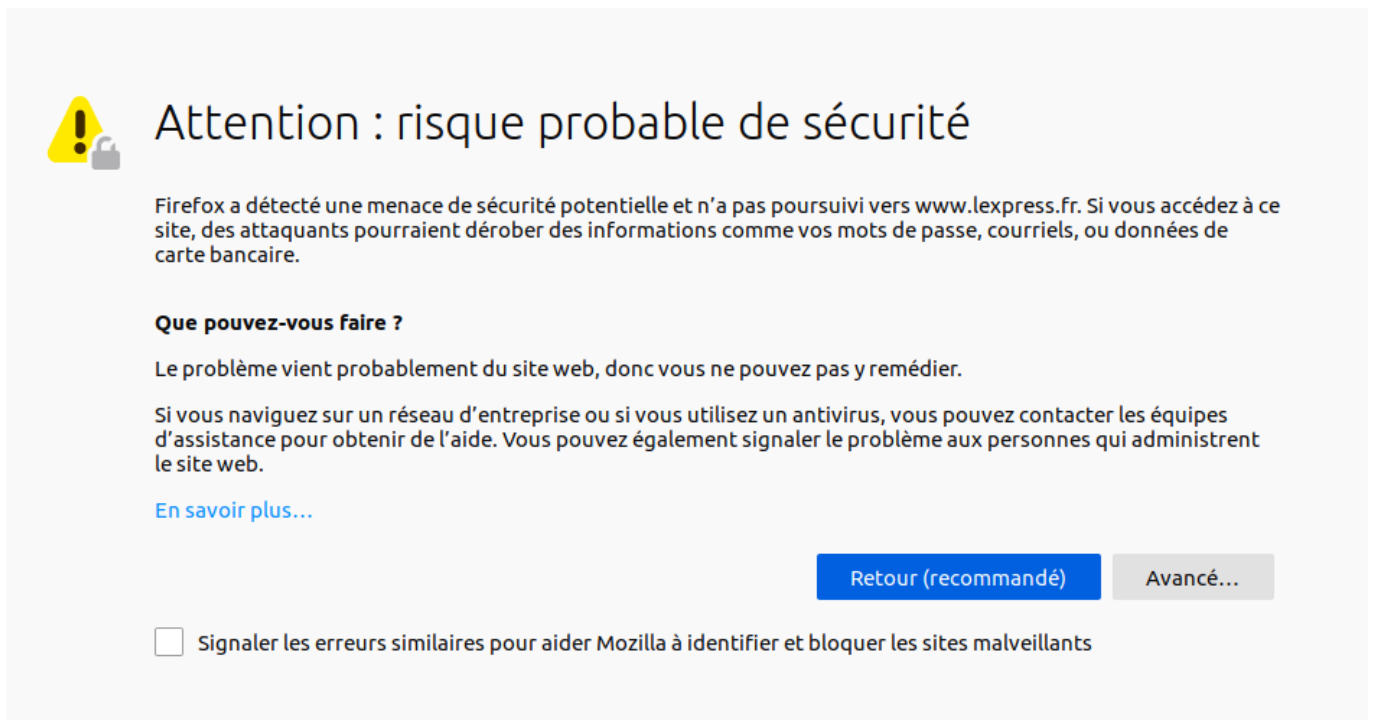
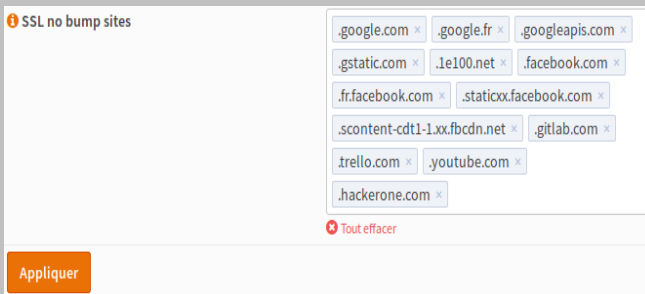




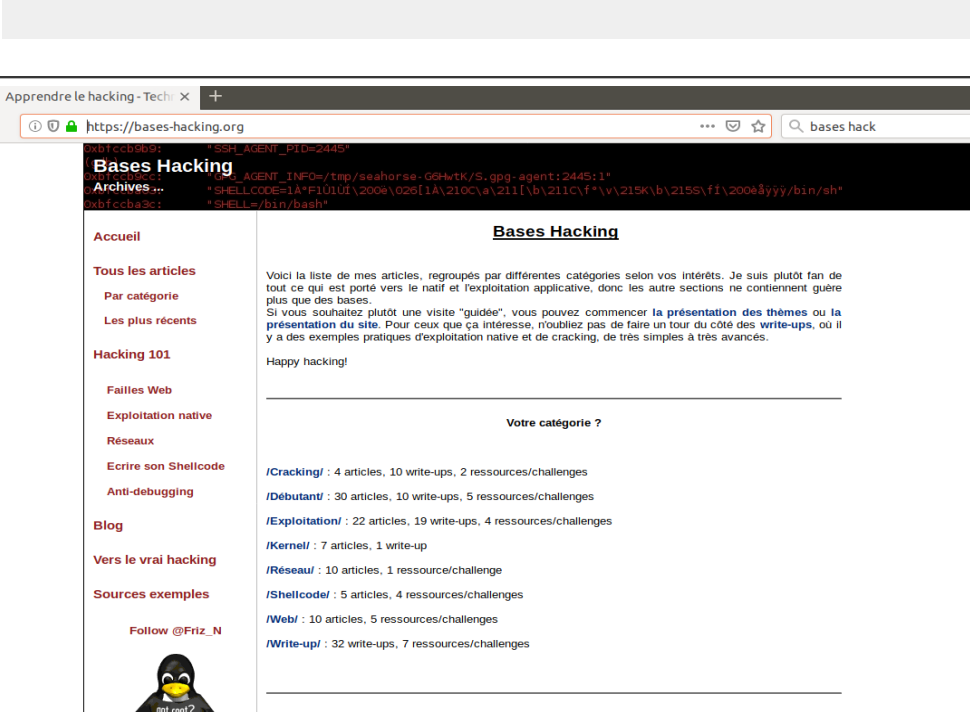
Fig. 25 : Affichage des certificats incompatibles

Il suffit de cliquer sur « Avancé » puis « Poursuivre » pour accéder à la page. Elle sera bien entendu bloquée si elle est filtrée.

4.2 - Procédure de test du filtrage URL sur le LAN

Id.	Architecture réseau testée Description Sommaire	Procédure de test
		Résultats attendus
U1.0	<p>Tentative de connexion à un contenu Web interdit avec le PC2. L'URL est filtré par le proxy qui regarde les correspondance avec la blacklist.</p> <p>Les catégories de site suivantes sont filtrées :</p> <ul style="list-style-type: none"> ✓ sexual_education ✓ mixed_adult ✓ lingerie ✓ adult 	<p>URL entré : www.youporn.com</p> <p>Ce site est forcément bloqué par l'une, voir toutes les catégories de site interdites ci-contre.</p>
		<p>OPNsense :</p> <p>constat sur le fichier journal du Proxy Web</p> <p>192.168.0.107 TCP_DENIED/403 4146 GET https://www.youporn.com/favicon.ico - HIER_NONE/- text/html</p> <p>Le proxy bloque la connexion.</p>
U1.1	<p>Tentative de connexion à un site bloqué par la blacklist si on choisit de cocher toutes les catégories de la blacklist.</p> <p>Ici, les sites de hacking sont bloqués par les catégories suivantes :</p> <ul style="list-style-type: none"> ✓ hacking ✓ bitcoin ✓ cryptojacking ✓ dangerous_material ✓ malware 	<p>URL entré : https://bases-hacking.org/</p> <p>La page est bloquée.</p>
		<p>La page s'affiche.</p>
U1.2	<p>Pour y accéder tout de même, on choisit de l'intégrer à la liste « SSL no bump sites » du FireWall OPNsense.</p> <p>Attention à ce que l'URL soit absent de la liste blanche.</p>	 <p>La page s'affiche.</p>

4.3 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.0	*		 <p>ERREUR</p> <p>L'URL demandée n'a pas pu être trouvé</p> <p>L'erreur suivante s'est produite en essayant d'accéder à l'URL : https://www.youporn.com/</p> <p>Accès interdit.</p> <p>La configuration du contrôle d'accès, empêche votre requête d'être acceptée. Si vous pensez que c'est une erreur, contactez votre fournisseur d'accès.</p> <p>Votre administrateur proxy est admin@localhost.local.</p> <p>Générée le Mon, 20 May 2019 12:32:24 GMT par OPNsense.localdomain (squid/3.5.28)</p>
U1.1	*		 <p>ERREUR</p> <p>L'URL demandée n'a pas pu être trouvé</p> <p>L'erreur suivante s'est produite en essayant d'accéder à l'URL : https://bases-hacking.org/</p> <p>Accès interdit.</p> <p>La configuration du contrôle d'accès, empêche votre requête d'être acceptée. Si vous pensez que c'est une erreur, contactez votre fournisseur d'accès.</p> <p>Votre administrateur proxy est admin@localhost.local.</p> <p>Générée le Mon, 20 May 2019 12:26:00 GMT par OPNsense.localdomain (squid/3.5.28)</p>
U1.2	*		 <p>Apprendre le hacking - Tech X +</p> <p>https://bases-hacking.org</p> <p>... bases hack</p> <p>Bases Hacking</p> <p>Archives...</p> <p>Accueil</p> <p>Tous les articles</p> <p>Par catégorie</p> <p>Les plus récents</p> <p>Hacking 101</p> <p>Faillies Web</p> <p>Exploitation native</p> <p>Réseaux</p> <p>Ecrire son Shellcode</p> <p>Anti-debugging</p> <p>Blog</p> <p>Vers le vrai hacking</p> <p>Sources exemples</p> <p>Follow @Friz_N</p> <p>Bases Hacking</p> <p>Voici la liste de mes articles, regroupés par différentes catégories selon vos intérêts. Je suis plutôt fan de tout ce qui est porté vers le natif et l'exploitation applicative, donc les autres sections ne contiennent guère plus que des bases.</p> <p>Si vous souhaitez plutôt une visite "guidée", vous pouvez commencer la présentation des thèmes ou la présentation du site. Pour ceux que ça intéresse, n'oubliez pas de faire un tour du côté des write-ups, où il y a des exemples pratiques d'exploitation native et de cracking, de très simples à très avancés.</p> <p>Happy hacking!</p> <p>Votre catégorie ?</p> <p>/Cracking/ : 4 articles, 10 write-ups, 2 ressources/challenges</p> <p>/Débutant/ : 30 articles, 10 write-ups, 5 ressources/challenges</p> <p>/Exploitation/ : 22 articles, 19 write-ups, 4 ressources/challenges</p> <p>/Kernel/ : 7 articles, 1 write-up</p> <p>/Réseau/ : 10 articles, 1 ressource/challenge</p> <p>/Shellcode/ : 5 articles, 4 ressources/challenges</p> <p>/Web/ : 10 articles, 5 ressources/challenges</p> <p>/Write-up/ : 32 write-ups, 7 ressources/challenges</p>

5 - Test de la détection d'intrusion

5.1 - Paramétrage détaillé de la détection d'intrusion Suricata

Pour ce test, j'ai d'abord tenté de lancer le module incorporé de détection d'intrusion d'OPNsense : Suricata.

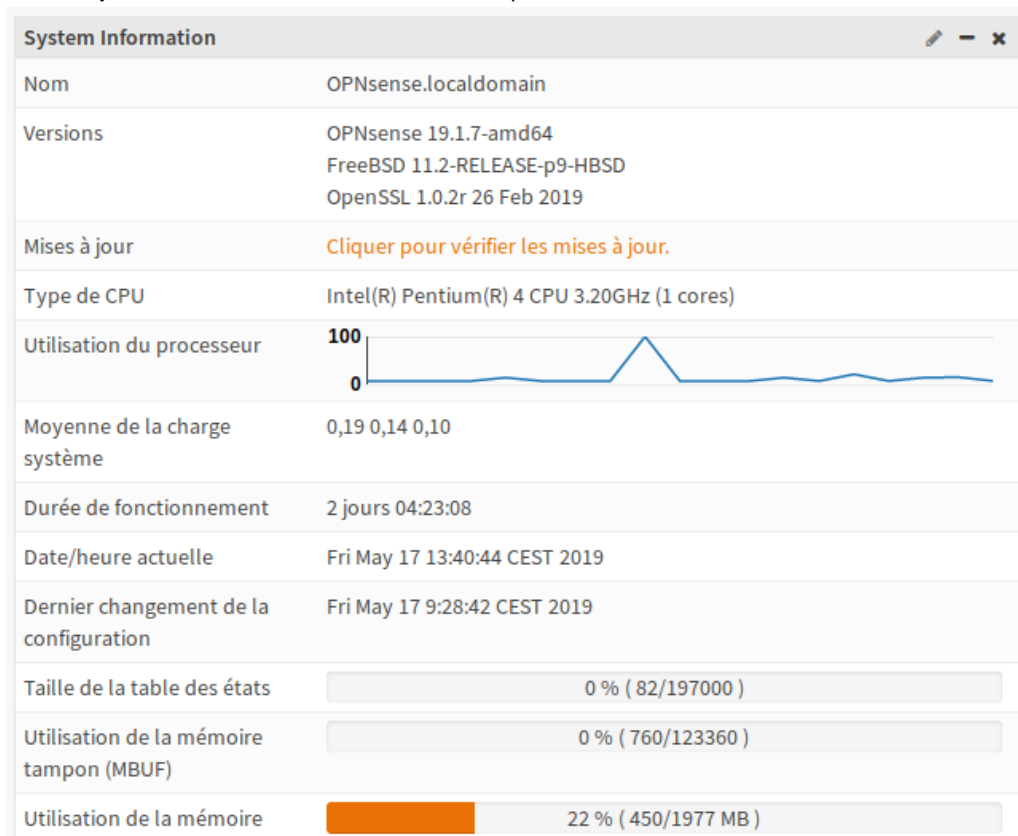


Fig. 26 : Tableau de bord de OPNsense

Sur la machine initiale du projet, il y a 2 GB de mémoire RAM. C'est insuffisant pour supporter Suricata. J'ai donc paramétré une autre machine, qui possède 4 GB de mémoire RAM, avec un réseau LAN et un réseau WAN. Ces interfaces servent de tests pour la détection d'intrusion et les tests d'intrusion.

Ce second réseau permet aussi de réaliser les tests sans impacter les réalisations précédentes de l'ensemble du groupe.

Voici le schéma de topologie pour tester la détection d'intrusion :

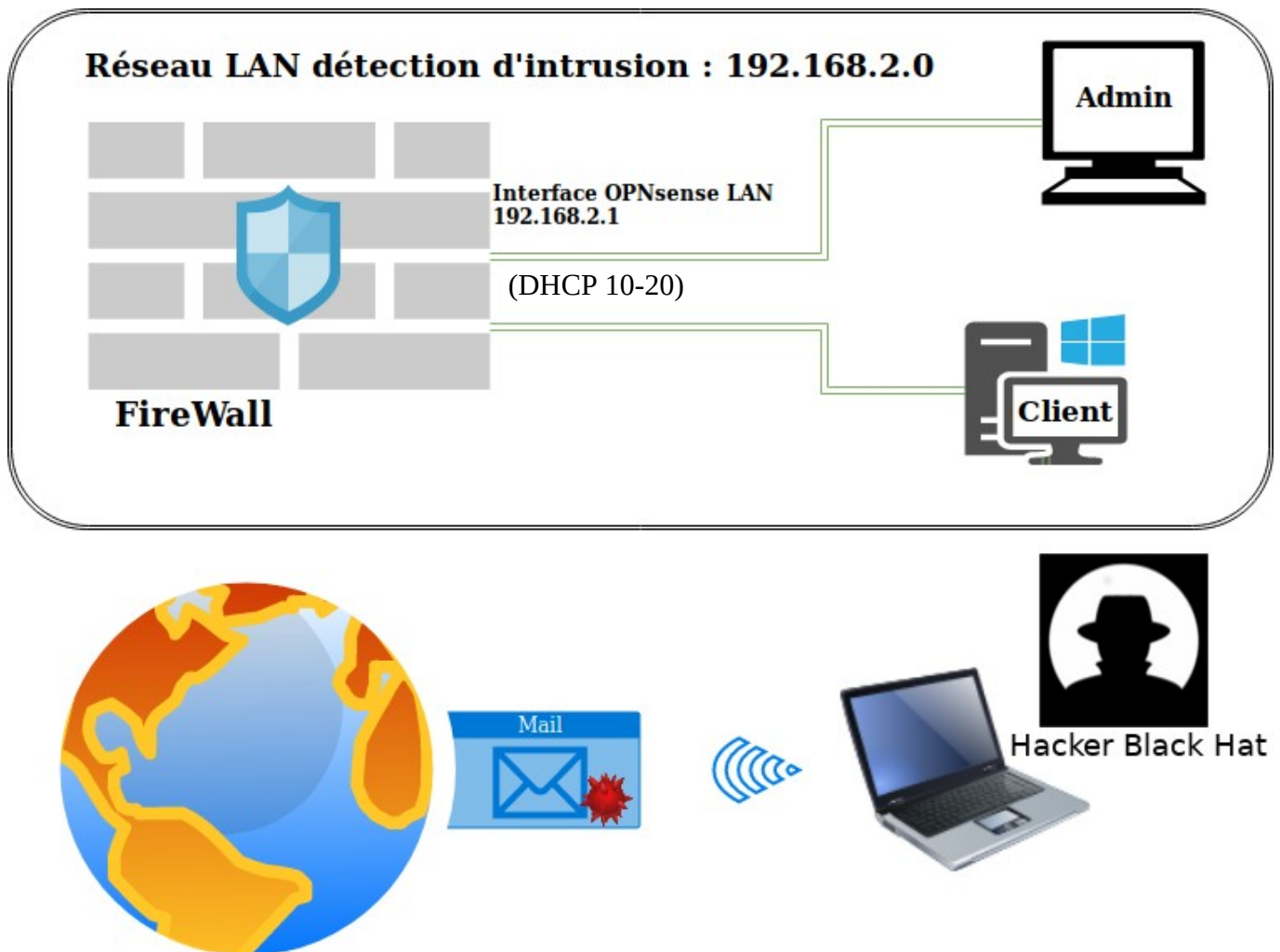


Fig. 27 : Schéma topologique de la maquette pour la détection d'intrusion

Le hacker Black Hat utilise un mail contenant un malware pour infecter le client Windows qui se trouve sur un LAN distant. De son côté, le réseau du client n'est accessible qu'à travers du Firewall OPNsense qui comporte la configuration de détection d'intrusion.

L'administrateur se connecte en LAN à l'interface du FireWall protégée par des identifiants, il est le seul à pouvoir y accéder. Pour mettre le système de détection d'intrusion en place, il faut mettre à jour les « Firmware » du système :

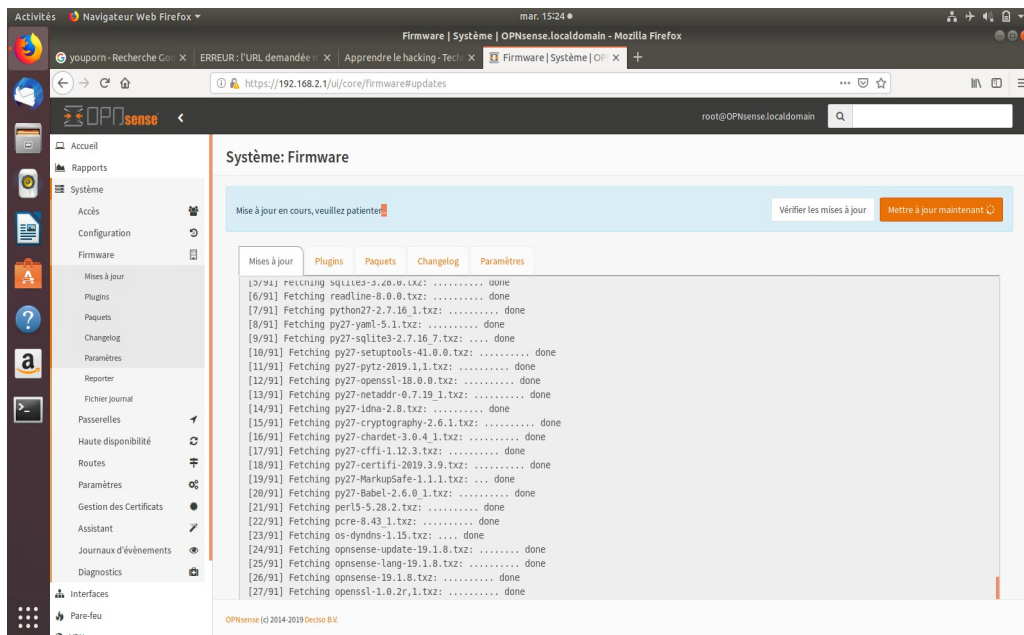


Fig. 28 : Mise à jour des FirmWare

On cherche à mettre à jour Suricata, notre application de détection d'intrusion. Ainsi, toutes les règles correspondantes à des menaces répertoriées par la communauté sont disponibles. Dans chaque cas, le système doit pouvoir générer une alerte dans le fichier log ou de bloquer la menace identifiée.

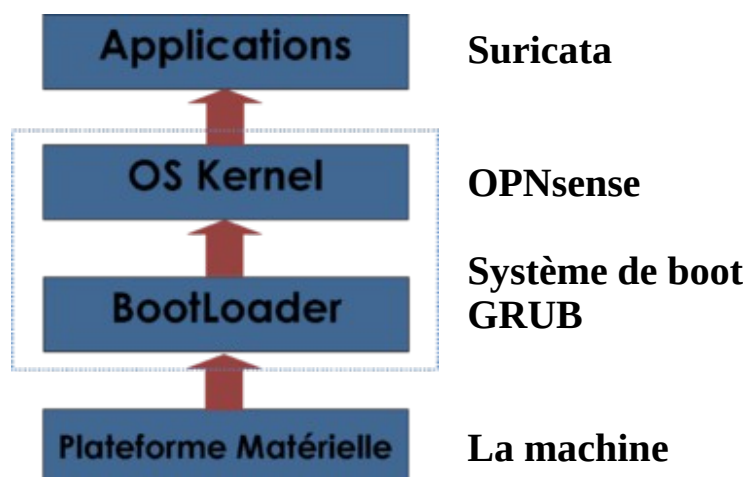


Fig. 28 : Tableau de bord de OPNsense

Le schéma ci-dessous montre qu'OPNsense en tant que Système d'exploitation (OS) lance bien des services ou applications.

La capture ci-dessous montre l'ensemble des services en cours. On peut les activer ou les désactiver. On vient ajouter le service de détection d'intrusion Suricata :























Système: Diagnostics: Services		
Service	Description	Statut
configd	Service Configuration Système	  
dhcpd	DHCPv4 Server	  
login	Utilisateurs et Groupes	 
ntpd	Service de Temps Réseau	  
pf	Filtre de Packet	 
suricata	Détection d'Intrusion	  
syslog	Syslog	  
unbound	Unbound DNS	  

Fig. 29 : Suricata est activé

L'administrateur doit activer le module de détection d'intrusion pour qu'il puisse enregistrer les alarmes correspondantes aux règles activées dans son fichier de logs.

On choisit d'activer le mode IPS pour que les règles puisse aussi bloquer le trafic des ports correspondants aux programmes menaçants.

Activez le mode promiscuous rendre compatible le mode IPS avec des vlans. Cela est nécessaire pour capturer réellement les données sur l'interface physique, notamment avec Wireshark et Suricata.

Services: Détection d'Intrusion: Administration

Paramètres	Téléchargement	Règles	Défini par l'utilisateur	Alertes
<input type="checkbox"/> mode avancé				
Activé	<input checked="" type="checkbox"/>			
Mode IPS	<input checked="" type="checkbox"/>			
Mode promiscuité	<input checked="" type="checkbox"/>			
Enable syslog alerts	<input type="checkbox"/>			
Pattern matcher	<div>Hyperscan</div>			
Interfaces	<div>LAN, WAN</div>			

Fig. 30 : Mode IPS & promiscuous activés sur le LAN et le WAN

Une fois le service activé le système utilise un peu plus de 1Go de RAM pour presque 4 Go de stockage, soit 30 % de la mémoire RAM de la machine :

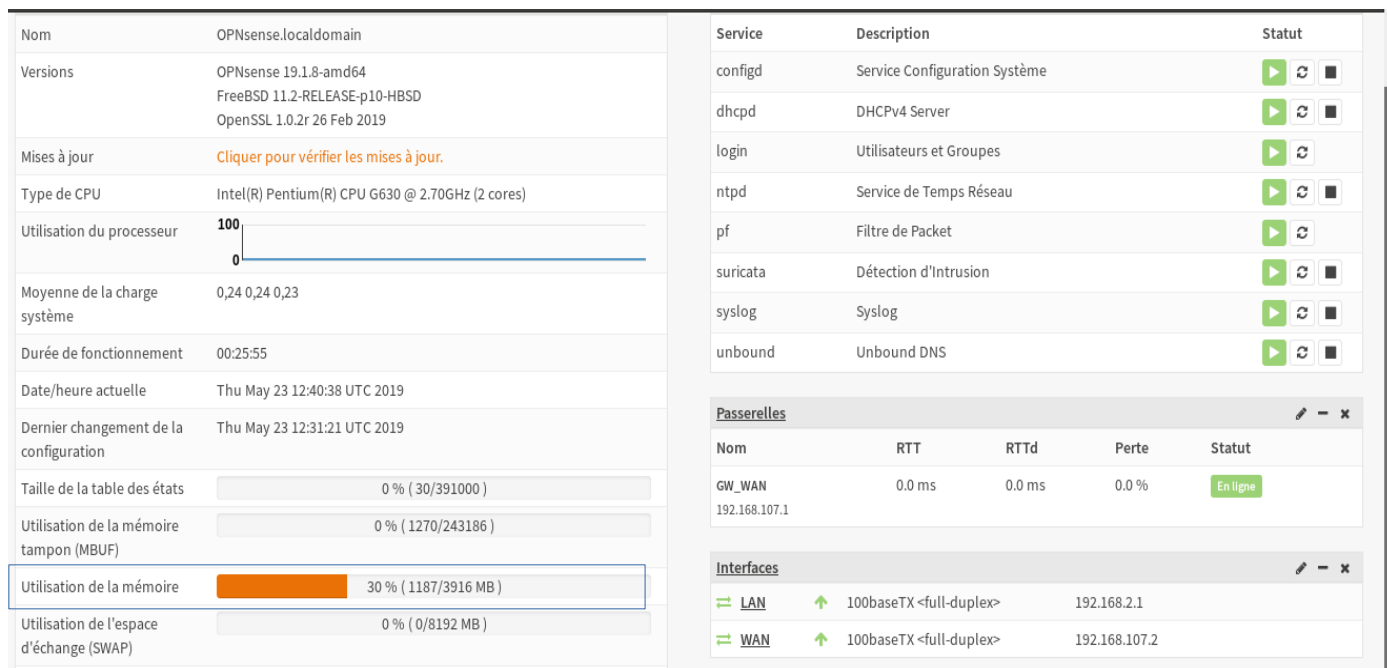


Fig. 30bis : La machine utilise 30 % de ses capacités

Ne pas oublier de paramétrer la bonne heure sur OPNsense en choisissant « Europe/Paris » dans Système: Paramètres: Général.

Fuseau horaire

Europe/Paris

Fig. 31 : Paramétrage du référentiel horaire

Services: Détection d'Intrusion: Administration

Paramètres

Téléchargement

Règles

Défini par l'utilisateur

Alertes

Planifier

2019/05/22 11:13

7

Recherche

Horodatage UNIX	Action	Interface	Source	Port	Destination	Port	Alerte	Info
2019-05-22T11:13:24.520868+0000	allowed	wan	192.168.107.2	43956	172.217.18.197	443	OPN_Mail - Gmail - Related TLS SNI (mail.google.c...	
2019-05-22T11:13:24.520614+0000	allowed	lan	192.168.2.11	36508	172.217.18.197	443	OPN_Mail - Gmail - Related TLS SNI (mail.google.c...	
2019-05-22T10:58:52.385326+0000	allowed	wan	192.168.107.2	62611	172.217.18.197	443	OPN_Mail - Gmail - Related TLS SNI (mail.google.c...	
2019-05-22T10:58:52.385055+0000	allowed	lan	192.168.2.11	36490	172.217.18.197	443	OPN_Mail - Gmail - Related TLS SNI (mail.google.c...	
2019-05-22T10:49:33.506280+0000	blocked	lan	192.168.2.11	59126	192.168.2.1	80	ET SCAN Possible Nmap User-Agent Observed	
2019-05-22T10:49:33.506280+0000	blocked	lan	192.168.2.11	59126	192.168.2.1	80	ET SCAN Possible Nmap User-Agent Observed	
2019-05-22T10:49:25.471035+0000	blocked	lan	192.168.2.11	59118	192.168.2.1	80	ET SCAN Possible Nmap User-Agent Observed	

Fig. 32 : Horodatage

L'onglet d'alertes doit être lisible par l'administrateur. L'horodatage est une preuve montrable aux autorités en cas d'intrusion.

5.2 – Procédure de test de la détection d'intrusion Suricata (à valider)

Le hacker utilise le logiciel Zenmap utilise le script nmap, un logiciel de scan opensource installé sur sa distribution kali linux. Le hacker est situé sur le LAN (192.168.2.0/24) en tant que poste client. La détection de ce genre de scan est importante car les hackers en ont besoin pour détecter les failles éventuelles du système.

Le hacker effectue un scan sur le réseau ciblé. Zenmap utilise une commande du script nmap comme affiché ci-dessous :

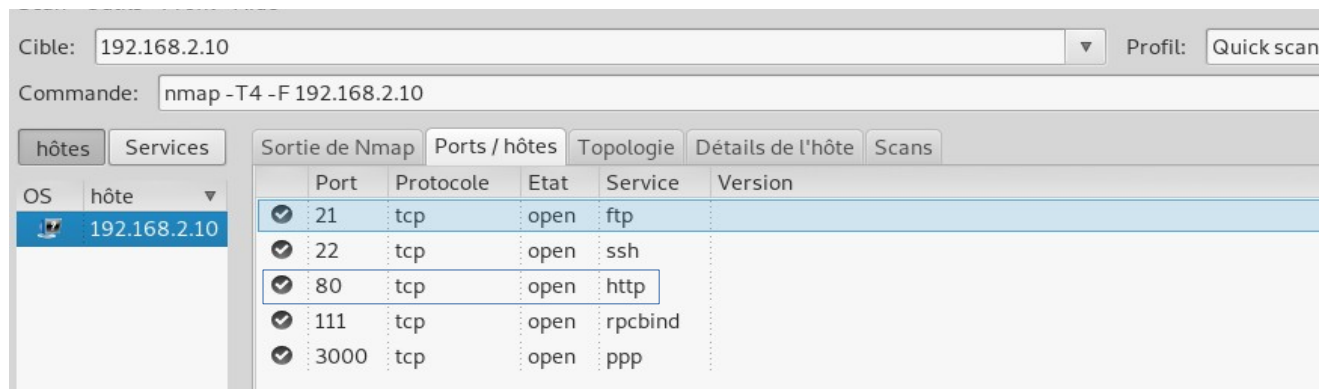
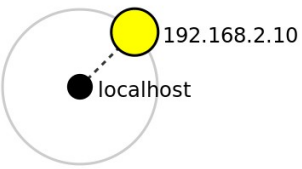
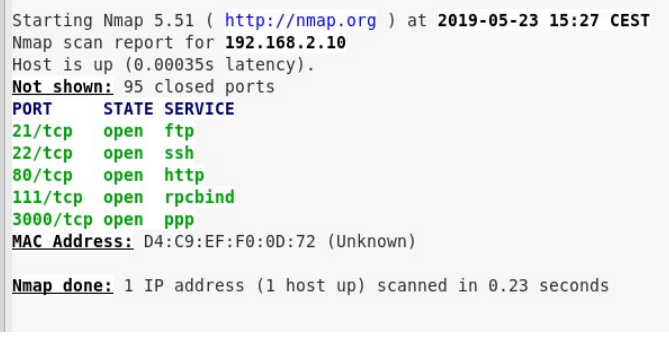


Fig. 33 : commande nmap dans Zenmap

Le système de détection d'intrusion doit afficher les logs correspondants aux ports utilisés par le hacker, comme les ports http et https.

Id.	Architecture réseau testée Description Sommaire	Procédure de test
		Résultats attendus
U1.0	La détection d'intrusion est désactivée sur le FireWall OPNsense. Aucune règle n'est activée. On effectue un scan avec Zenmap 	Nmap concluant .Aucune alarme
		La détection d'intrusion ne fonctionne pas si on applique aucune règle. 
U1.1	Règles nmap et scan activées « rejeter »	Nmap ne fonctionne pas. Fichier log & alarmes Preuve sur WireShark
U1.2	Envoie d'un fichier infecté par mail Gmail règles	Alarme + bloqué ?
		Fichier log & alarmes Preuve sur WireShark
		Alarmes ID de l'IP de l'expéditeur

Le test n'aboutit pas car les contraintes matérielles ont créé un retard du paramétrage de cette fonction. Suricata ne génère pas de règle.

5.3 - Rapport d'exécution

Test TRAMES WIRESHARK (à faire)

Id.	OK	!OK	Observations
U1.0	*		Le scan s'effectue côté hacker
U1.1		*	Les règles ne sont pas disponibles sur l'interface graphique

6 - Bilan de la réalisation personnelle

6.1 – Statut des fonction à charge

- *L'utilisateur doit utiliser le proxy Web pour naviguer sur Internet sans avoir à paramétrer quoi que ce soit*
- *Le réseau permet un trafic convenable tout en appliquant un filtrage URL réglementé et modifiable*

6.2 – Conclusion

Points positifs

- *Application de la méthode Agile*
- *Richesse de la gestion de travail de groupe*

Points négatifs

- *La fonction détection d'intrusion reste à développer.*
- *Contraintes matérielles*

En conclusion, après l'analyse du cahier des charges, on se rend vite compte des contraintes matérielles auxquelles on fait face. Il faut sans cesse s'adapter et trouver des solutions qui rapprochent au maximum de l'objectif final. La mise en place de solutions alternatives est très chronophage mais apporte un vrai plus à la réalisation.