

Rapport de projet

Mise en place d'une solution de gestion des incidents de sécurité avec corrélation d'évènements dans un réseau d'Entreprise

Encadré par

- M. NAJA Najib
- M. BELMEKKI EL MOSTAFA
- M. BELMEKKI ABDELHAMID

Réalisé par

- AUBOUHAN Walid
- CHBAIL Khalid
- IARABEN Ismail
- KADDIRI Marouane
- KOTBI Ilyas

Remerciements

Nous souhaitons exprimer notre profonde gratitude à toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce projet.

En premier lieu, nous tenons à remercier chaleureusement nos encadrants, pour leurs précieuses guidances, leur soutien continu, et leur expertise qui ont grandement contribué à l'aboutissement de ce projet. leurs conseils éclairés et leurs dévouement ont été des éléments clés dans la réussite de notre travail en tant que groupe. Un immense merci va également à nos familles pour leur soutien indéfectible tout au long de cette aventure. Leur encouragement constant a été une source inestimable de motivation pour chacun de nous.

Nous tenons à exprimer notre gratitude envers nos amis qui ont partagé ce voyage avec nous en tant que groupe. Leur soutien moral et leur collaboration ont été des aspects cruciaux de cette expérience collective.

Enfin, nous souhaitons remercier toutes les personnes, collègues et amis, qui ont contribué de quelque manière que ce soit à la réalisation de ce projet en groupe. C'est un honneur d'avoir pu travailler ensemble, et nous sommes reconnaissants envers chacun d'entre vous.

Merci à tous pour votre précieuse contribution et votre soutien tout au long de ce projet.

Table des matières

Introduction	5
Mise en Place et Configuration de l'Infrastructure Réseau en Laboratoire	7
L'architecture reseau	7
Configuration des Routeurs	8
Configuration du Switch Central	11
Conception de l'architecture sur GNS3	14
Déploiement des mesures de sécurité sur l'nfrastructure	15
Pfsense	15
WAF	20
Masquage de la version de DNS	22
Integration de la solution SIEM : ELK STACK	27
Utilité de l'ELK	28
Pourquoi choisir ELK ?	28
Décision et Installation d'ELK	28
Collecte des Logs avec Filebeat, Packetbeat, et Winlogbeat	30
Analyse des Risques de Sécurité	40
Analyse de Sécurité, Identification de Menaces et Évaluation de Vulnérabilités .	40
Attaques et Réponse du WAF	42
Conclusion	48

Table des figures

1	Architecture	7
2	router on a stick	8
3	Les interfaces R1	9
4	ip routes R1	10
5	configuration de NAT sur R2	10
6	les interfaces R2	11
7	ip routes R2	11
8	vlan	12
9	vlan10	12
10	vlan20	13
11	vlan30	13
12	Sur GNS3	14
13	pfsense logo	15
14	Exemple de l'interface de Pfsense	17
15	Exemple de configuration des interfaces	17
16	interface GUI pfsense	18
17	Règles de Pfsense	20
18	Exemple de configuration ACL	24
19	Exemple de configuration crontab	25
20	Exemple de script de sauvegarde (backup.sh)	25
21	ELK STACK	27
22	filebeat.input	31
23	output.elasticsearch	31
24	output.elasticsearch	32
25	collecte des Logs	33

26	packetbeat.protocols (packetbeat)	33
27	output.elasticsearch (packetbeat)	33
28	setup.kibana (packetbeat)	34
29	collecte des logs (packetbeat)	35
30	winlogbeat.yml	35
31	output.Elasticsearch (winlogbeat)	36
32	setup.kibana (winlogbeat)	36
33	collecte des logs (winlogbeat)	37
34	Configuration de l'envoi des logs syslog sur pfSense	38
35	L'envoi de Logs de Pfsense vers Elastitcsearch	39
36	Tableau de bord Kibana montrant les logs de pfSense	39
37	Attaque par Injection SQL sur OWASP Juice Shop	43
38	Réponse du WAF à l'Attaque par Injection SQL	43
39	WAF Bypass de l'Attaque par Injection SQL	44
40	Attaque par Cross-Site Scripting sur OWASP Juice Shop	44
41	Réponse du WAF à l'Attaque XSS	45
42	WAF Bypass de l'Attaque par XSS	45
43	Attaque par Injection de Modèles Côté Serveur sur OWASP Juice Shop	46
44	Réponse du WAF à l'Attaque SSTI	46
45	WAF Bypass de l'Attaque SSII	47

Introduction

Dans un contexte où les cybermenaces sont de plus en plus sophistiquées et fréquentes, la protection des infrastructures informatiques d’une entreprise devient une priorité absolue. Les données sensibles et les services réseau offerts par l’entreprise constituent des cibles de choix pour les attaquants. Afin de répondre à ces défis de sécurité, il est crucial de mettre en place des systèmes robustes de détection et de gestion des incidents. Le projet présenté dans ce rapport vise à implémenter un Système de Gestion des Informations et des Événements de Sécurité (SIEM) pour assurer une surveillance en temps réel et une réponse efficace aux incidents de sécurité.

L’infrastructure de l’entreprise est centralisée au siège social et comprend plusieurs sites distants. Elle fournit divers services réseau à ses employés et à ses clients, et gère des applications manipulant des données critiques. La mise en place d’un SIEM permet de collecter et de corréler les logs provenant des différents actifs de l’infrastructure, afin d’identifier les incidents majeurs et de les présenter dans un tableau de bord clair et exploitable.

Ce projet se décompose en plusieurs phases clés, allant de la mise en place de l’infrastructure réseau et de l’analyse des risques, à la sécurisation de l’architecture, la mise en œuvre du SIEM, et enfin, la réalisation de tests de pénétration pour valider l’efficacité du système. En outre, l’utilisation de la solution ELK (Elasticsearch, Logstash, et Kibana) permet d’assurer une collecte, une analyse et une visualisation performantes des données de sécurité.

Les objectifs principaux de ce projet sont les suivants :

- Appliquer les connaissances techniques acquises dans les différents cours.
- Explorer les métiers d’administrateur d’infrastructure, de sécurité défensive (protection d’une infrastructure), de sécurité offensive (PenTest) et d’analyse SOC.
- Assurer la détection proactive des incidents de sécurité et la mise en place de mesures

de réponse appropriées.

Ce rapport détaille les étapes du projet, les méthodologies employées, les résultats obtenus ainsi que les leçons apprises. Il s'ouvre par la mise en place de l'architecture et l'analyse des risques de sécurité, avant de passer à la sécurisation de l'infrastructure et à la mise en place du SIEM. La phase finale est dédiée aux tests de pénétration et à l'exploitation du tableau de bord du SIEM, permettant de valider l'efficacité de notre solution en conditions réelles.

Mise en Place et Configuration de l'Infrastructure Réseau en Laboratoire

L'architecture réseau :

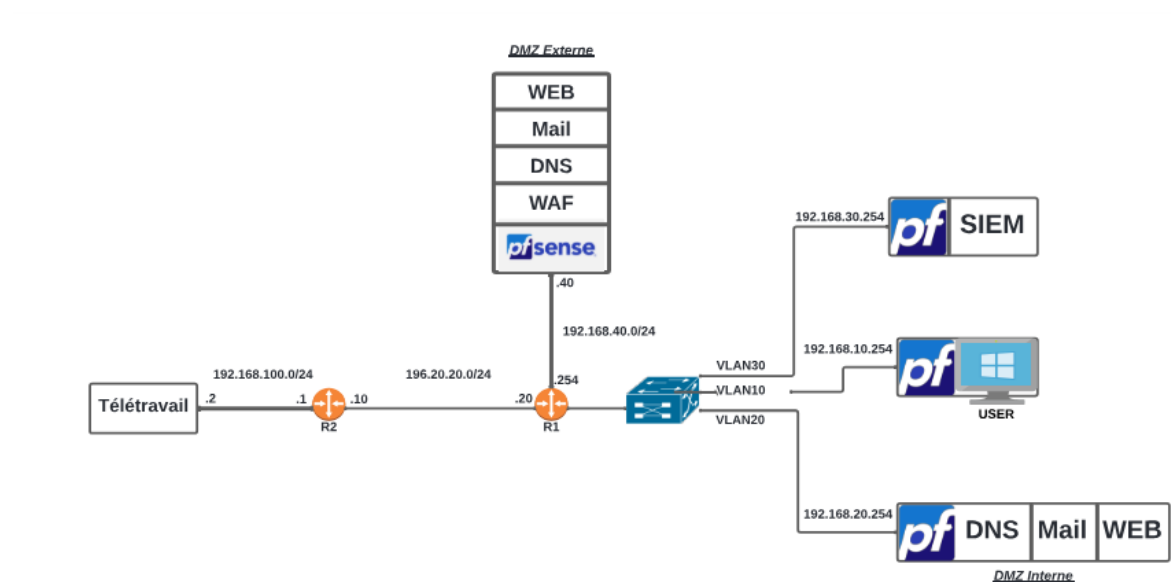


FIGURE 1 – Architecture

Réseaux et Sous-réseaux

L'architecture réseau se compose de plusieurs sous-réseaux et VLANs :

- **192.168.100.0/24** : Sous-réseau pour le télétravail.
- **196.20.20.0/24** : Réseau de transit entre les routeurs R1 et R2.
- **192.168.40.0/24** : DMZ externe, gérée par un pare-feu pfSense.
- **192.168.30.0/24** : VLAN 30, réseau interne pour le SIEM.
- **192.168.10.0/24** : VLAN 10, réseau interne pour les utilisateurs.

- **192.168.20.0/24** : VLAN 20, réseau interne pour les services DNS, Mail, et Web.

Composants Réseau

Les composants principaux du réseau incluent des routeurs, des pare-feu, et des serveurs de services critiques.

- **R1 et R2** : Routeurs assurant l'interconnexion des différents sous-réseaux.
- **pfSense (DMZ Externe)** : Pare-feu gérant l'accès aux services Web, Mail, DNS et WAF.
- **SIEM** : Système de gestion des événements et des informations de sécurité.
- **Serveurs DNS, Mail, Web (DMZ Interne)** : Fournissant des services internes critiques.

Configuration des Routeurs

Routeur R1

```
interface GigabitEthernet0/0.10
  encapsulation dot1Q 10
  ip address 192.168.10.254 255.255.255.0
!
interface GigabitEthernet0/0.20
  encapsulation dot1Q 20
  ip address 192.168.20.254 255.255.255.0
!
interface GigabitEthernet0/0.30
  encapsulation dot1Q 30
  ip address 192.168.30.254 255.255.255.0
!
```

FIGURE 2 – router on a stick

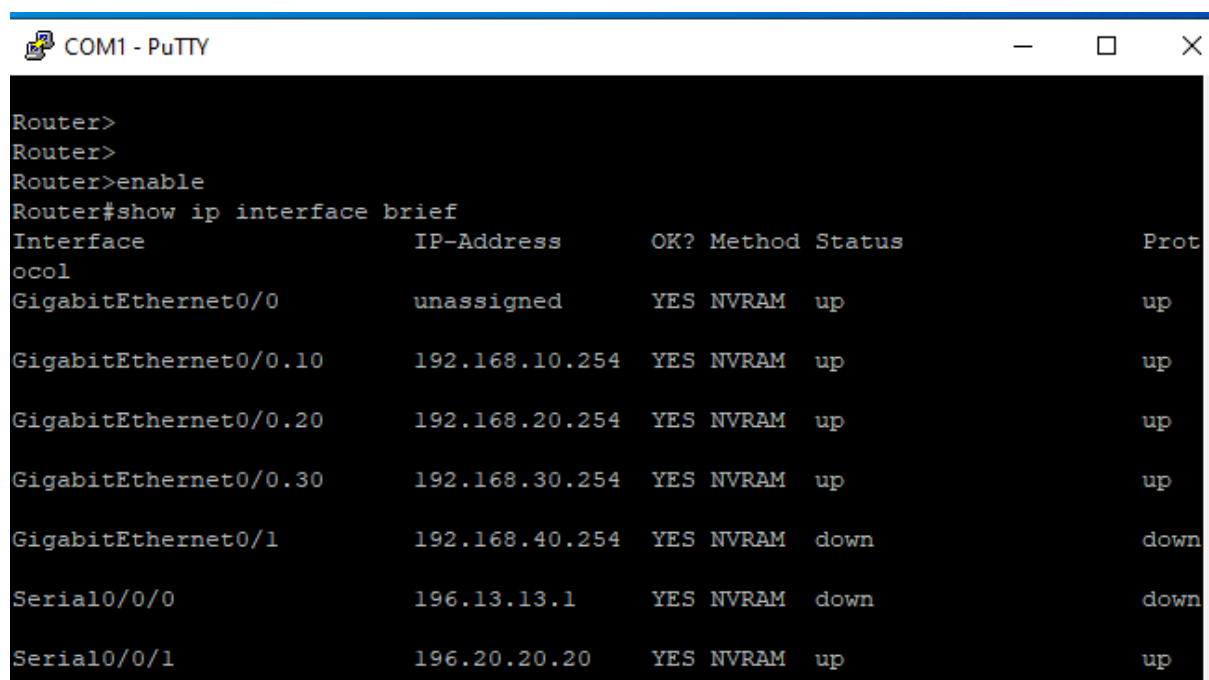
Le concept de "router on a stick" est utilisé pour faciliter la communication entre plusieurs VLANs via un seul port physique du routeur R1. Cette configuration permet

une gestion efficace du trafic inter-VLAN en consolidant les connexions physiques et en maintenant la sécurité et la séparation logique entre les réseaux internes.

Au cœur de cette configuration se trouve le routeur R1, qui agit comme point central de routage entre les VLANs. Une seule interface physique sur ce routeur est subdivisée en plusieurs sous-interfaces logiques, chaque sous-interface correspondant à un VLAN spécifique. Ces sous-interfaces sont configurées avec des adresses IP dans les sous-réseaux correspondants aux VLANs, permettant au routeur de router le trafic entre eux.

Par exemple, si un utilisateur dans le VLAN 10 souhaite accéder à un serveur dans le VLAN 20, le routeur R1 reçoit le paquet sur la sous-interface associée au VLAN 10, le traite et l'envoie vers la sous-interface associée au VLAN 20 pour atteindre sa destination.

Cette approche présente plusieurs avantages pour votre architecture. En utilisant un seul port physique sur le routeur pour gérer plusieurs VLANs, vous économisez des ressources matérielles et simplifiez la gestion des connexions réseau. De plus, cette configuration est flexible et scalable, ce qui facilite l'ajout de nouveaux VLANs sans modification majeure de l'infrastructure. En maintenant une séparation logique et sécurisée entre les réseaux internes, le "router on a stick" garantit une communication efficace tout en préservant la sécurité et l'intégrité des données.



```
Router>
Router>
Router>enable
Router#show ip interface brief
Interface                IP-Address      OK? Method Status    Prot
ocol
GigabitEthernet0/0       unassigned      YES NVRAM   up        up
GigabitEthernet0/0.10    192.168.10.254  YES NVRAM   up        up
GigabitEthernet0/0.20    192.168.20.254  YES NVRAM   up        up
GigabitEthernet0/0.30    192.168.30.254  YES NVRAM   up        up
GigabitEthernet0/1       192.168.40.254  YES NVRAM   down      down
Serial0/0/0              196.13.13.1     YES NVRAM   down      down
Serial0/0/1              196.20.20.20    YES NVRAM   up        up
```

FIGURE 3 – Les interfaces R1

```

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

S    192.168.1.0/24 [1/0] via 192.168.10.10
S    192.168.3.0/24 [1/0] via 192.168.30.30
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L      192.168.10.254/32 is directly connected, GigabitEthernet0/0.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L      192.168.20.254/32 is directly connected, GigabitEthernet0/0.20
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L      192.168.30.254/32 is directly connected, GigabitEthernet0/0.30
S    192.168.100.0/24 [1/0] via 196.20.20.10
S    192.168.106.0/24 [1/0] via 192.168.20.20
--More--

```

FIGURE 4 – ip routes R1

Routeur R2

```

Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 196.20.20.21       192.168.100.2     ---                ---

```

FIGURE 5 – configuration de NAT sur R2

```

Router>
Router>en
Router#show ip interface brief
Interface                IP-Address      OK? Method Status      Prot
ocol
GigabitEthernet0/0       192.168.100.1   YES NVRAM   down        down
GigabitEthernet0/1       unassigned      YES NVRAM   administratively down down
Serial0/0/0              unassigned      YES NVRAM   administratively down down
Serial0/0/1              196.20.20.10    YES NVRAM   up          up
NVIO                     192.168.100.1   YES unset   up          up

```

FIGURE 6 – les interfaces R2

```

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

S    192.168.0.0/16 [1/0] via 196.20.20.20
S    192.168.3.0/24 [1/0] via 196.20.20.20
S    192.168.146.0/24 [1/0] via 196.20.20.20
S    192.168.200.0/24 [1/0] via 196.20.20.20
     196.20.20.0/24 is variably subnetted, 2 subnets, 2 masks
C    196.20.20.0/24 is directly connected, Serial0/0/1
L    196.20.20.10/32 is directly connected, Serial0/0/1

```

FIGURE 7 – ip routes R2

Configuration du Switch Central

Le switch central est configuré avec trois VLANs distincts pour séparer les types de trafic réseau.

- **VLAN 30 (192.168.30.0/24)** : Réseau SIEM.
 - Interface : 192.168.30.254
- **VLAN 10 (192.168.10.0/24)** : Réseau des utilisateurs.
 - Interface : 192.168.10.254

- VLAN 20 (192.168.20.0/24) : Réseau des services DNS, Mail, et Web.
- Interface : 192.168.20.254

```
chbail# show vlans

Status and Counters - VLAN Information

Maximum VLANs to support : 8
Primary VLAN : DEFAULT_VLAN
Management VLAN :

VLAN ID Name | Status Voice Jumbo
-----+-----
1 DEFAULT_VLAN | Port-based No No
10 vlan_10 | Port-based No No
20 VLAN20 | Port-based No No
30 VLAN30 | Port-based No No
```

FIGURE 8 – vlans

```
chbail# show vlan 10

Status and Counters - VLAN Information - Ports - VLAN 10

VLAN ID : 10
Name : vlan_10
Status : Port-based
Voice : No
Jumbo : No

Port Information Mode Unknown VLAN Status
-----
4 Untagged Learn Up
Trkl Tagged Learn Up
```

FIGURE 9 – vlan10

```

chbail# show vlan 20

Status and Counters - VLAN Information - Ports - VLAN 20

VLAN ID : 20
Name : VLAN20
Status : Port-based
Voice : No
Jumbo : No

Port Information Mode      Unknown VLAN Status
-----
5                Untagged Learn      Up
Trkl             Tagged  Learn      Up

```

FIGURE 10 – vlan20

```

chbail# show vlan 30

Status and Counters - VLAN Information - Ports - VLAN 30

VLAN ID : 30
Name : VLAN30
Status : Port-based
Voice : No
Jumbo : No

Port Information Mode      Unknown VLAN Status
-----
6                Untagged Learn      Down
Trkl             Tagged  Learn      Up

```

FIGURE 11 – vlan30

Conception de l'architecture sur GNS3 :

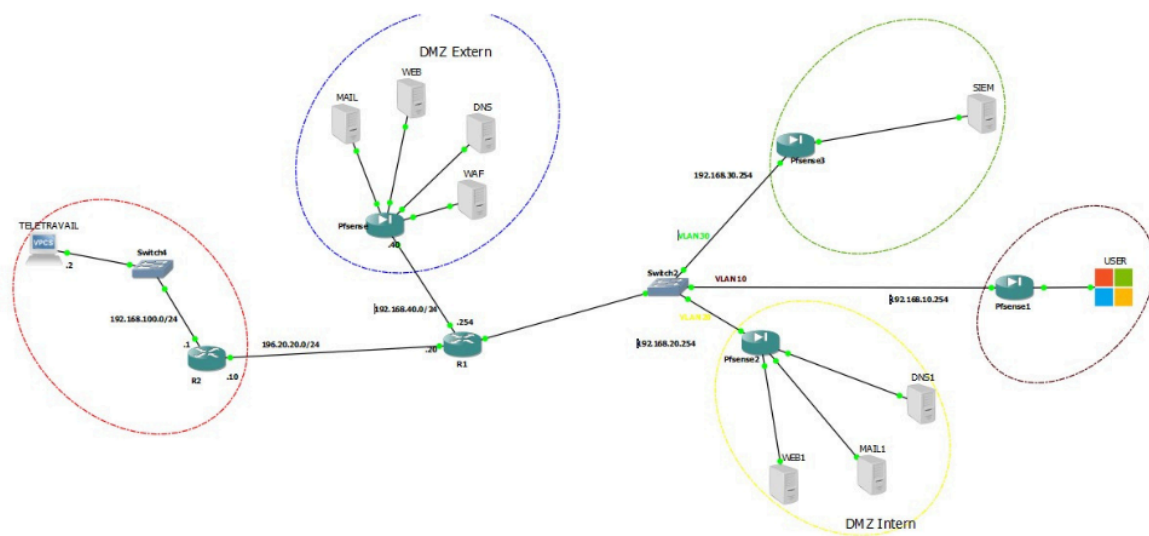


FIGURE 12 – Sur GNS3

Déploiement des mesures de sécurité sur l'nfrastructure

Pfsense :



FIGURE 13 – pfsense logo

Introduction à Pfsense

Les pare-feux servent de mécanisme de défense principal au sein d'un réseau, agissant comme une frontière entre l'internet externe et un réseau interne. Comprendre et configurer les pare-feux sont des aspects fondamentaux de la cybersécurité.

PfSense est une version spéciale de FreeBSD, qui fonctionne comme un videur numérique pour notre réseau. Il se tient à la porte, vérifiant qui est autorisé à entrer et qui ne l'est pas. À l'aide d'une interface web simple, nous pouvons lui indiquer les règles à suivre pour laisser entrer et sortir les données de notre réseau.

Dans notre architecture, nous avons utilisé pfSense comme pont pour les quatre zones (DMZ interne, DMZ externe, SIEM et zone utilisateur). Il va fonctionner comme routeur au sein de ces zones, assurant la gestion et le contrôle du trafic entre elles.

Utilité de pfSense

- **Sécurité** : Fournit un firewall robuste pour protéger les réseaux contre les intrusions et les attaques.
- **VPN** : Permet de configurer facilement des VPN pour des connexions sécurisées entre différents réseaux.
- **Filtrage de Contenu** : Possibilité de mettre en place des règles de filtrage pour contrôler le trafic réseau.
- **Gestion de la Bande Passante** : Offre des outils pour gérer et optimiser l'utilisation de la bande passante.
- **Surveillance et Reporting** : Intègre des outils pour la surveillance du trafic et la génération de rapports.

Configuration Initiale de pfSense

1. Accéder à l'Interface Web :

- Connecter un câble réseau entre le port LAN de la machine pfSense et votre ordinateur.
- Configurer l'ordinateur pour obtenir une adresse IP automatiquement (DHCP).
- Accéder à l'interface web de pfSense en ouvrant un navigateur et en entrant l'adresse `http://192.168.1.1`.
- Se connecter avec les identifiants par défaut (`admin` / `pfsense`).

2. Assistant de Configuration :

- Suivre l'assistant de configuration pour configurer les paramètres de base tels que l'adresse IP WAN, les paramètres DNS, et le mot de passe administrateur.

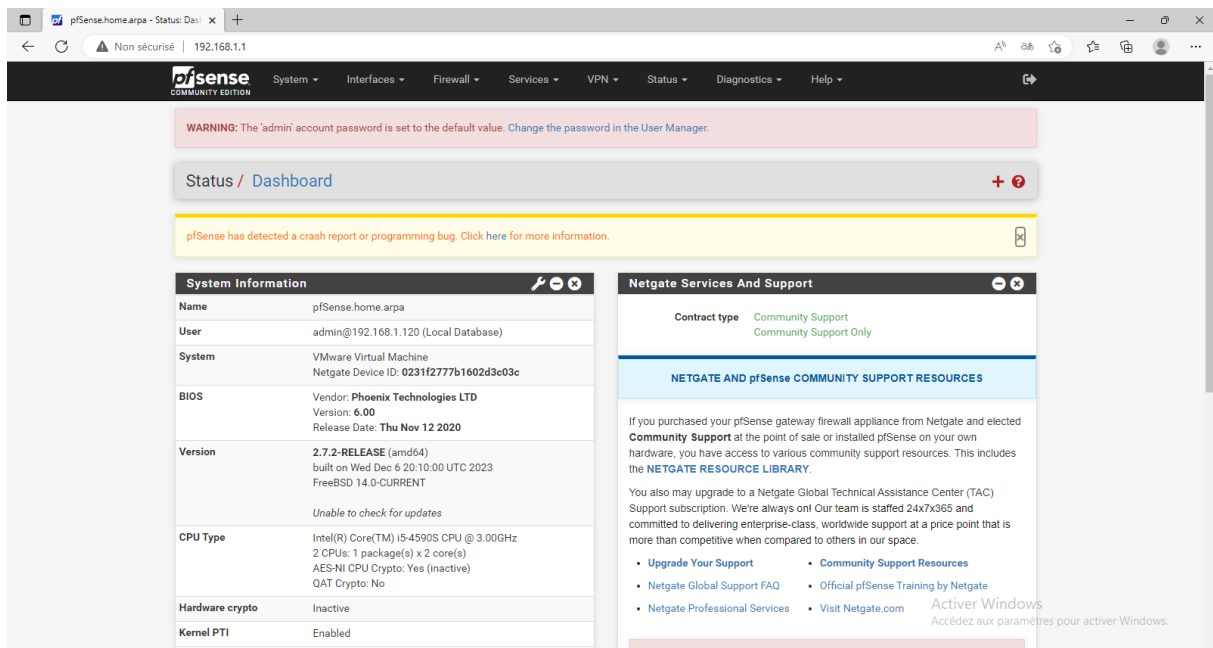


FIGURE 14 – Exemple de l'interface de Pfsense

Après avoir terminé l'installation de pfsense dans nos machines, nous devons configurer les adresses IP des interfaces.

```
Round-trip Min/avg/max/stdev = 2.616/3.394/4.152/0.627 ms

Press ENTER to continue.
^CUMware Virtual Machine - Netgate Device ID: 0231f2777b1602d3c03c

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.10.10/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Jun 5 09:57:56 ...
php-fpm[3871]: /index.php: Successful login for user 'admin' from: 192.168.1.120
(Local Database)
```

FIGURE 15 – Exemple de configuration des interfaces

Nous accèderons à l'interface web de pfSense en entrant l'adresse ip des l'interface wan de pfsense dans le navigateur de notre ordinateur hôte.

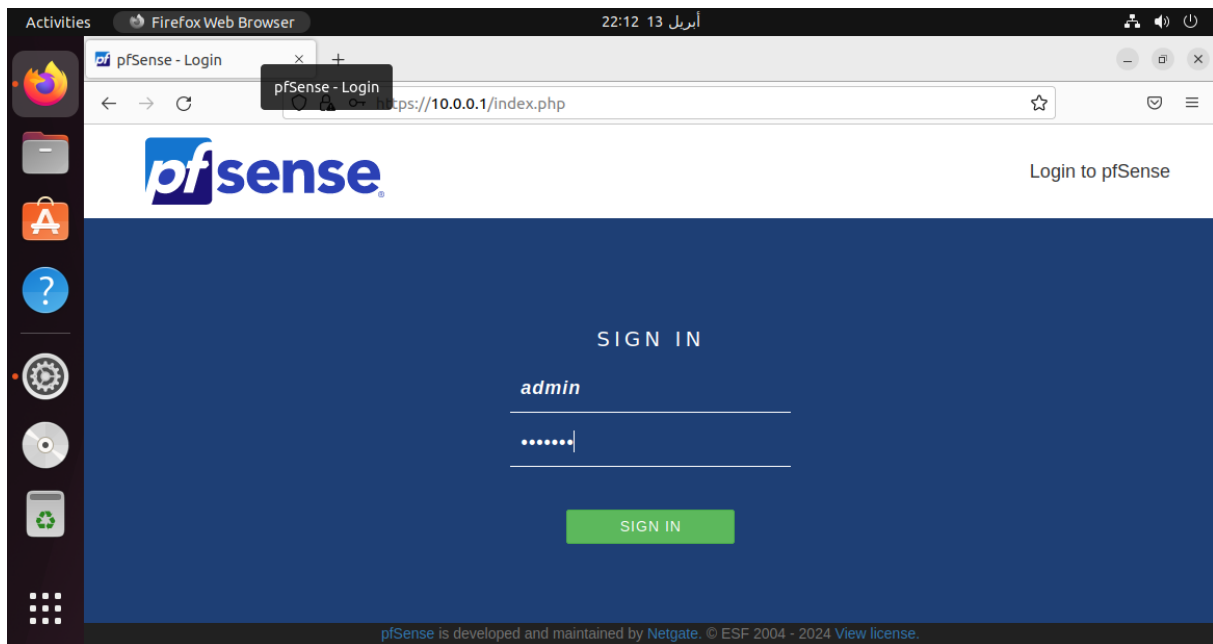


FIGURE 16 – interface GUI pfsense

Règles de Pare-feu dans pfSense

Les règles de pare-feu dans pfSense jouent un rôle crucial pour définir et contrôler le trafic réseau. Voici comment configurer et gérer les règles de pare-feu pour sécuriser votre infrastructure :

Création de Règles de Pare-feu

Pour créer une règle de pare-feu dans pfSense :

1. Aller à **Firewall > Rules**.
2. Sélectionner l'onglet correspondant à l'interface pour laquelle vous souhaitez ajouter une règle (par exemple, WAN, LAN, OpenVPN).
3. Cliquer sur **Add** pour ajouter une nouvelle règle.
4. Configurer les champs suivants :
 - **Action** : Choisir **Pass** pour permettre le trafic, **Block** pour bloquer le trafic, ou **Reject** pour rejeter le trafic avec un message d'erreur.
 - **Interface** : Sélectionner l'interface concernée (WAN, LAN, etc.).
 - **Address Family** : IPv4, IPv6 ou les deux.
 - **Protocol** : Choisir le protocole (TCP, UDP, ICMP, etc.).

- **Source** : Définir l'adresse source (any, réseau spécifique, adresse IP).
 - **Destination** : Définir l'adresse de destination (any, réseau spécifique, adresse IP).
 - **Port Range** : Spécifier la plage de ports (pour les protocoles TCP/UDP).
5. Configurer les options avancées si nécessaire et cliquer sur **Save**.

Exemples de Règles de Pare-feu

- **Autoriser le Trafic HTTP/HTTPS Sortant** :
 - Interface : LAN
 - Address Family : IPv4
 - Protocol : TCP
 - Source : any
 - Destination : any
 - Port Range : 80 (HTTP), 443 (HTTPS)
 - Action : Pass
- **Bloquer le Trafic ICMP Entrant sur l'Interface WAN** :
 - Interface : WAN
 - Address Family : IPv4
 - Protocol : ICMP
 - Source : any
 - Destination : WAN Address
 - Action : Block

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.40.40	*	192.168.106.2	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	192.168.40.40	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	✓ 0/32 KiB	IPv4 TCP	192.168.40.40	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 0/10 KiB	IPv4 TCP	192.168.40.40	*	*	3000 (HBCI)	*	none			
<input type="checkbox"/>	✓ 0/2 KiB	IPv4 TCP	192.168.30.30	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0/33 KiB	IPv4 TCP	192.168.30.30	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 10/268 KiB	IPv4 UDP	192.168.30.30	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.30.30	*	*	3000 (HBCI)	*	none			
<input type="checkbox"/>	✓ 0/852 B	IPv4 TCP	192.168.10.10	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.10.10	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	192.168.10.10	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.10.10	*	*	3000 (HBCI)	*	none			

FIGURE 17 – Règles de Pfsense

WAF :

Dans notre architecture, un WAF (Web Application Firewall) joue un rôle crucial en renforçant la sécurité des applications web présentes dans la DMZ externe. Cet article explique comment le WAF contribue à la sécurité et à la résilience de cette architecture.

Protection des Applications Web

Le WAF est positionné devant les serveurs web dans la DMZ externe, filtrant tout le trafic HTTP/HTTPS entrant et sortant. Cette configuration permet de protéger les applications web contre une variété de menaces, notamment les attaques courantes telles que les injections SQL, les scripts intersites (XSS), et les attaques de déni de service (DoS). En inspectant le trafic en temps réel, le WAF peut détecter et bloquer les requêtes malveillantes avant qu'elles n'atteignent les serveurs web.

Filtrage de Contenu et Contrôle d'Accès

Le WAF peut analyser le contenu des requêtes et des réponses HTTP/HTTPS pour détecter des anomalies ou des contenus malveillants. Il peut également appliquer des règles

strictes de contrôle d'accès, empêchant les utilisateurs non autorisés d'accéder à certaines parties de l'application web. Cette fonctionnalité est particulièrement utile pour protéger les pages d'administration ou les zones sensibles des applications web.

Protection Contre les Vulnérabilités Connues et Inconnues

Le WAF utilise des signatures de menace et des modèles de comportement pour identifier les tentatives d'exploitation des vulnérabilités connues. De plus, grâce à des techniques avancées telles que l'apprentissage automatique, il peut également détecter et bloquer des attaques inédites basées sur des comportements anormaux du trafic.

Journalisation et Monitoring

En intégrant le WAF dans l'architecture, vous bénéficiez d'une surveillance continue et d'une journalisation détaillée des activités du trafic web. Cela permet d'avoir une visibilité sur les tentatives d'attaque et de répondre rapidement aux incidents de sécurité. Les journaux générés par le WAF peuvent également être intégrés dans un SIEM (Security Information and Event Management) pour une analyse plus approfondie et une réponse aux incidents centralisée.

Renforcement de la Sécurité Globale

Le WAF renforce la sécurité globale de l'architecture en ajoutant une couche de défense en profondeur. Cette approche multi-couches combine les capacités de détection et de prévention du WAF avec d'autres mesures de sécurité telles que les pare-feu réseau, les IDS/IPS (Intrusion Detection/Prevention Systems), et les politiques de sécurité des applications.

Isolation des Attaques

En filtrant le trafic malveillant au niveau de la DMZ externe, le WAF empêche les attaques de se propager aux autres parties du réseau interne. Cela aide à contenir les incidents de sécurité et à limiter leur impact potentiel sur l'ensemble de l'infrastructure réseau.

Application des Politiques de Sécurité

Le WAF permet d'appliquer des politiques de sécurité spécifiques aux applications web, telles que le blocage des adresses IP suspectes, la limitation des taux de requêtes, et l'application de règles de sécurité basées sur les types de requêtes et de réponses. Ces politiques renforcent la protection contre les attaques ciblées et automatisées.

Masquage de la version de DNS :

Dans l'architecture réseau que nous avons mise en place, le masquage de la version du serveur DNS renforce la sécurité en rendant plus difficile pour un attaquant de déterminer les vulnérabilités spécifiques à exploiter. Cet article explique l'importance de cette pratique et comment nous l'avons réalisée.

Sécurité Renforcée par le Masquage de la Version DNS

Réduction des Risques d'Exploitation des Vulnérabilités

Chaque version de logiciel DNS peut avoir des vulnérabilités spécifiques connues. En masquant la version du serveur DNS, nous empêchons les attaquants d'identifier facilement ces vulnérabilités et de les exploiter pour lancer des attaques.

Obscurcissement des Informations

L'obscurcissement des informations, y compris les versions de logiciel, fait partie de notre stratégie de défense en profondeur. Moins un attaquant en sait sur notre infrastructure, plus il lui est difficile de planifier une attaque efficace.

Prévention des Attaques Automatisées

De nombreux outils de piratage et scripts automatisés recherchent des versions spécifiques de logiciels pour lancer des attaques. Masquer la version DNS nous aide à prévenir ces attaques automatisées.

Réalisation du Masquage de la Version DNS

Pour BIND (Berkeley Internet Name Domain)

1. **Modification du Fichier de Configuration** : Nous avons édité le fichier de configuration principal de BIND, situé à `/etc/bind/named.conf.options`.
2. **Ajout de l'Option version** : Nous avons ajouté la ligne suivante pour masquer la version :

```
options {  
    version "not-disclosed";  
};
```

3. **Redémarrage du Service BIND** : Nous avons appliqué les modifications en redémarrant le service BIND :

```
sudo systemctl restart bind9
```

Pour dnsmasq

1. **Modification du Fichier de Configuration** : Nous avons édité le fichier de configuration principal de dnsmasq, situé à `/etc/dnsmasq.conf`.
2. **Ajout de l'Option version** : Nous avons ajouté la ligne suivante pour masquer la version :

```
server=version=not-disclosed
```

3. **Redémarrage du Service dnsmasq** : Nous avons appliqué les modifications en redémarrant le service dnsmasq :

```
sudo systemctl restart dnsmasq
```


Gestion des Listes de Contrôle d'Accès (ACL)

Les listes de contrôle d'accès (ACL) sont utilisées pour définir les permissions sur les fichiers et les répertoires, offrant une granularité plus fine que les permissions traditionnelles. Voici un exemple de configuration d'ACL.

Exemple de Liste ACL

```
acl "trusted" {  
    192.168.200.2;    # dmz  
};  
options {  
    directory "/var/cache/bind";  
  
    recursion yes;                # enables recursive queries  
    allow-recursion { trusted; }; # allows recursive queries from "trusted"  
    listen-on { 192.168.200.2; }; # ns1 private IP address - listen on pr  
    allow-transfer { none; };  
    version "fake version";
```

FIGURE 18 – Exemple de configuration ACL

L'image ci-dessus montre une liste ACL appliquée à un fichier ou répertoire spécifique, définissant des permissions détaillées pour différents utilisateurs et groupes.

Configuration des Tâches Planifiées (crontab)

Les tâches planifiées permettent d'automatiser l'exécution des scripts et des commandes à des intervalles réguliers. Le fichier crontab contient ces tâches et leurs horaires. Voici un exemple de fichier crontab configuré dans notre infrastructure.

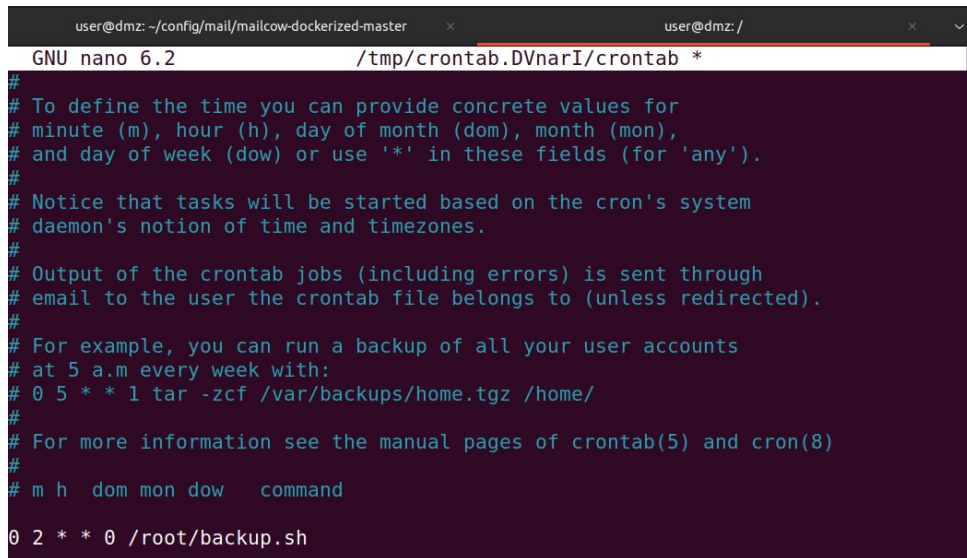
Exemple de crontab

/tmp/crontab.DVnarI/crontab

Le fichier ci-dessus montre une liste de tâches planifiées pour diverses opérations, telles que les sauvegardes et les mises à jour du système.

Backup Script (backup.sh)

Le script de sauvegarde, `backup.sh`, est utilisé pour créer des copies de sauvegarde des données importantes. Voici un aperçu de ce script :

A terminal window showing the configuration of a crontab file. The window title is 'user@dmz: ~/config/mail/mailcow-dockerized-master'. The editor is 'GNU nano 6.2' editing '/tmp/crontab.DVnari/crontab *'. The content includes comments about cron syntax and a cron job entry: '0 2 * * 0 /root/backup.sh'.

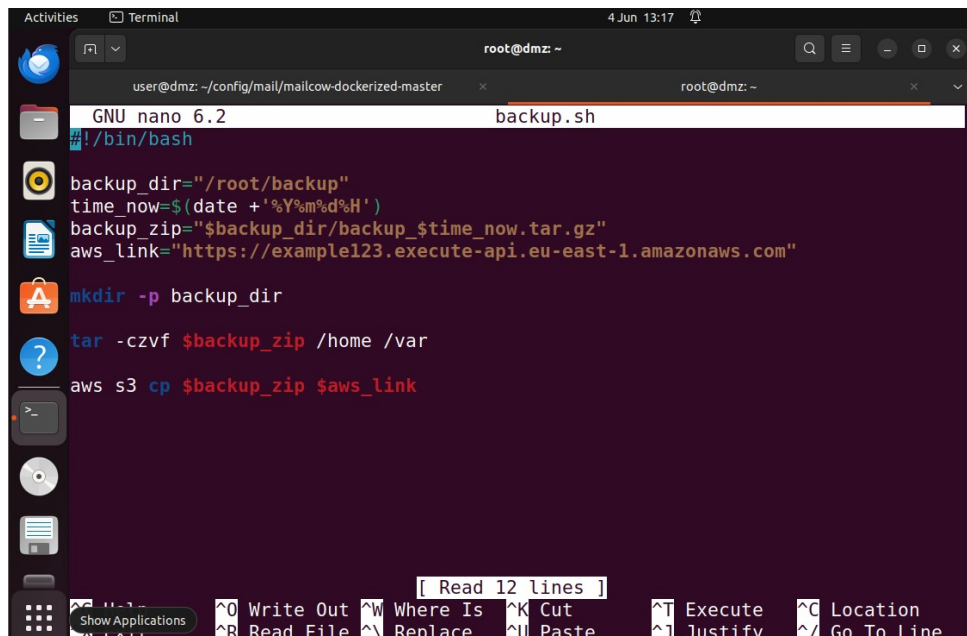
```
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 2 * * 0 /root/backup.sh
```

FIGURE 19 – Exemple de configuration crontab

```
#!/bin/bash
```

```
# Script de sauvegarde
```

```
tar -czvf /backup/mydata-$(date +%F).tar.gz /mydata
```

A terminal window showing the content of a script named 'backup.sh'. The window title is 'root@dmz: ~'. The script content includes variable assignments for backup directory, time, zip file name, and AWS link, followed by commands to create the directory, create a tar archive, and upload it to AWS S3.

```
#!/bin/bash
backup_dir="/root/backup"
time_now=$(date +%Y%m%d%H')
backup_zip="$backup_dir/backup_${time_now}.tar.gz"
aws_link="https://example123.execute-api.eu-east-1.amazonaws.com"
mkdir -p backup_dir
tar -czvf $backup_zip /home /var
aws s3 cp $backup_zip $aws_link
```

FIGURE 20 – Exemple de script de sauvegarde (backup.sh)

Ce script crée une archive compressée des données dans le répertoire `/mydata` et la stocke dans le répertoire `/backup` avec une date dans le nom du fichier.

Conclusion

En masquant la version de notre serveur DNS, nous avons augmenté la sécurité de notre architecture réseau en empêchant les attaquants d'identifier facilement les vulnérabilités spécifiques et en réduisant les risques d'attaques automatisées. Cette pratique est une partie essentielle de notre stratégie de sécurité globale visant à protéger les services critiques et à maintenir la résilience de notre infrastructure réseau.

Integration de la solution SIEM : ELK STACK

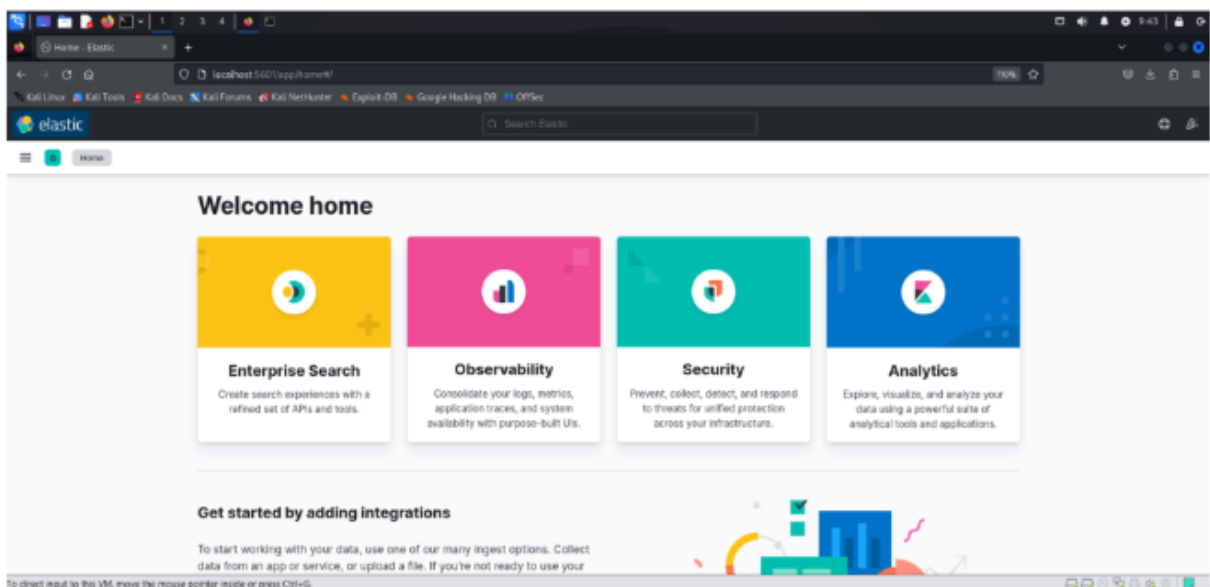


FIGURE 21 – ELK STACK

L'ELK Stack, composée d'Elasticsearch, Logstash, et Kibana, est une suite puissante de logiciels open-source pour la gestion et l'analyse des logs. Elle permet de collecter, stocker, analyser et visualiser de grandes quantités de données en temps réel.

- **Elasticsearch** : Moteur de recherche et d'analyse distribué, utilisé pour stocker et indexer les données collectées.
- **Logstash** : Pipeline de traitement de données qui ingère les données, les transforme, et les envoie à Elasticsearch.
- **Kibana** : Interface utilisateur pour visualiser les données stockées dans Elasticsearch et créer des tableaux de bord interactifs.

Utilité de l'ELK

L'ELK est employé dans de nombreux contextes :

- **Surveillance des applications et des infrastructures** : ELK permet une surveillance en temps réel des performances des applications et des infrastructures en analysant les journaux, les métriques et les données de suivi.
- **Analyse des journaux et débogage** : ELK aide à examiner les journaux des applications et des serveurs, facilitant ainsi la détection des problèmes, le diagnostic des erreurs et le débogage des systèmes.
- **Sécurité et conformité** : ELK est utilisé pour surveiller les activités suspectes, identifier les menaces de sécurité et satisfaire aux exigences de conformité.
- **Analyse des données opérationnelles** : ELK analyse des données opérationnelles comme les transactions, les événements et les indicateurs de performance, aidant ainsi à prendre des décisions commerciales éclairées.

Pourquoi choisir ELK ?

Plusieurs raisons expliquent pourquoi ELK est souvent préféré à d'autres solutions :

- **Efficacité** : ELK est extrêmement extensible et capable de traiter de grandes quantités de données rapidement, le rendant idéal pour des applications à grande échelle.
- **Flexibilité** : ELK supporte une large variété de sources de données, de formats et de types d'analyse, offrant une grande adaptabilité pour divers besoins.
- **Intégration** : ELK s'intègre facilement avec d'autres outils et technologies, permettant de créer des pipelines de données complets et des workflows automatisés.
- **Communauté et support** : ELK bénéficie d'une communauté active, de nombreuses ressources en ligne et d'un support commercial disponible pour les entreprises.

Décision et Installation d'ELK

Après avoir évalué plusieurs solutions pour nos besoins en surveillance, analyse de données et gestion des journaux, nous avons choisi ELK pour sa polyvalence, sa robustesse

et sa popularité dans l'industrie. ELK a été sélectionné pour sa capacité à gérer de grandes quantités de données efficacement, sa flexibilité pour s'adapter à différentes sources et types de données, et son intégration facile avec d'autres outils et technologies.

Avant de commencer l'installation, il est essentiel de s'assurer que toutes les dépendances nécessaires sont en place. Il est particulièrement important de vérifier que Java 8 est installé sur le système, car Elasticsearch et Kibana dépendent de cette version spécifique de Java. Pour vérifier la version actuelle de Java sur votre machine, exécutez la commande suivante dans votre terminal :

```
1 java -version
```

Suite à cette décision, nous avons installé ELK sur une machine Ubuntu en suivant les étapes décrites suivantes :

Installer Elasticsearch

1. Importer la clé GPG d'Elasticsearch :

```
1 wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo  
  ↪ apt-key add -
```

2. Ajouter le dépôt Elasticsearch à la liste des sources :

```
1 sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt  
  ↪ stable main" > /etc/apt/sources.list.d/elastic-7.x.list'
```

3. Mettre à jour la liste des paquets et installer Elasticsearch :

```
1 sudo apt-get update  
2 sudo apt-get install elasticsearch
```

4. Configurer Elasticsearch pour démarrer au boot :

```
1 sudo systemctl enable elasticsearch
```

5. Démarrer Elasticsearch :

```
1 sudo systemctl start elasticsearch
```

6. Vérifier qu'Elasticsearch fonctionne :

```
1 curl -X GET "localhost:9200/"
```

Installer Kibana

1. Installer Kibana :

```
1 sudo apt-get install kibana
```

2. Configurer Kibana pour démarrer au boot :

```
1 sudo systemctl enable kibana
```

3. Démarrer Kibana :

```
1 sudo systemctl start kibana
```

Installer Logstash

1. Installer Logstash :

```
1 sudo apt-get install logstash
```

2. Configurer Logstash :

```
1 sudo nano /etc/logstash/conf.d/logstash-simple.conf
```

3. Démarrer Logstash avec le fichier de configuration :

```
1 sudo systemctl start logstash
```

4. Configurer Logstash pour démarrer au boot :

```
1 sudo systemctl enable logstash
```

Collecte des Logs avec Filebeat, Packetbeat, et Winlogbeat

Introduction aux Beats

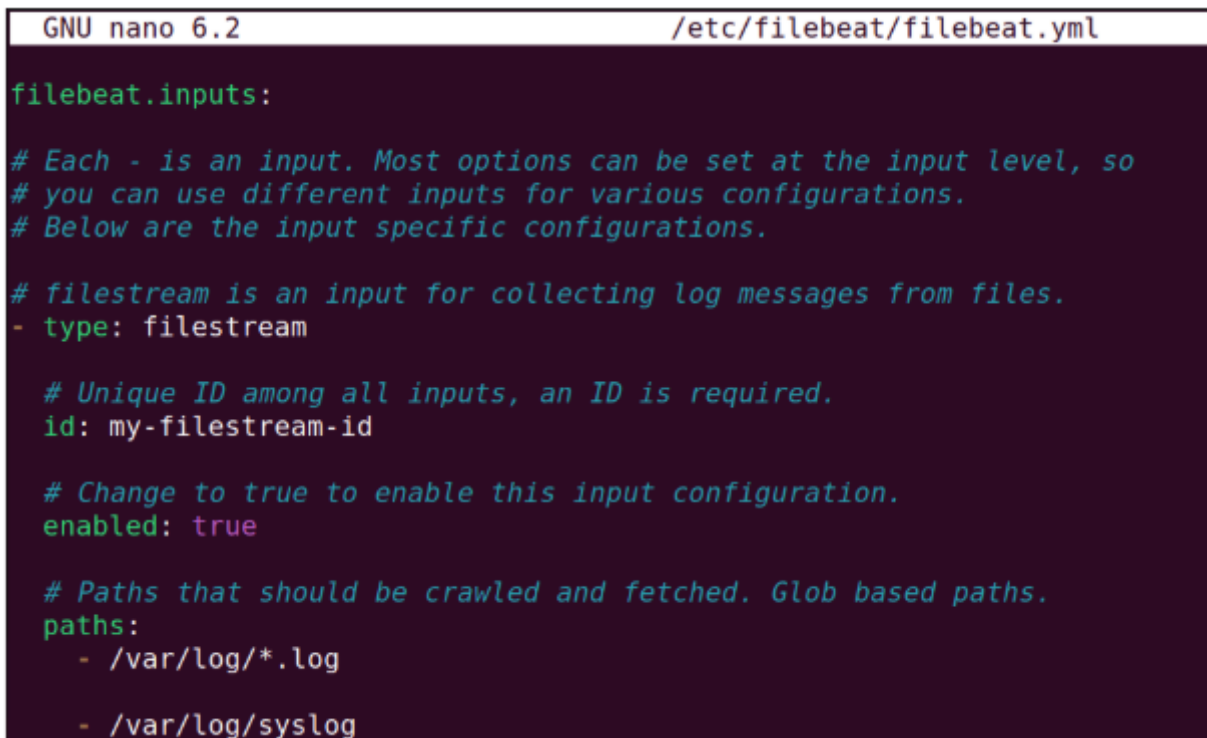
- **Filebeat** : Collecte les logs des fichiers spécifiés et les envoie à Elasticsearch. Il est léger, facile à déployer et consomme peu de ressources système.

- **Packetbeat** : Analyse le trafic réseau en temps réel et envoie les données à Elasticsearch. Il capture les paquets réseau et extrait des informations sur les transactions.
- **Winlogbeat** : Collecte les logs d'événements Windows et les envoie à Elasticsearch. Il est crucial pour la surveillance des événements système et des activités utilisateur sur les machines Windows.

Configuration de Filebeat

Fichier de Configuration : filebeat.yml

filebeat.inputs :



```
GNU nano 6.2 /etc/filebeat/filebeat.yml

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# filestream is an input for collecting log messages from files.
- type: filestream

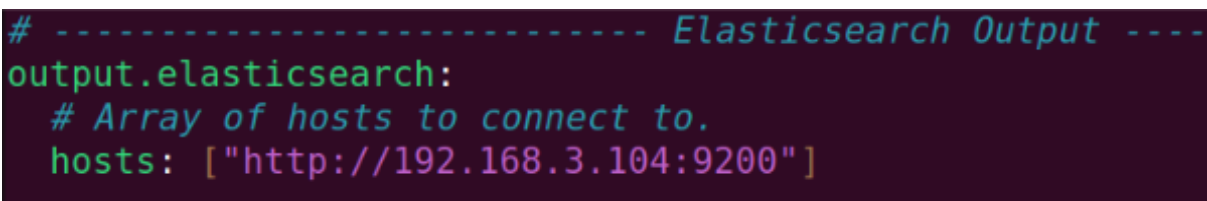
  # Unique ID among all inputs, an ID is required.
  id: my-filestream-id

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/*.log
    - /var/log/syslog
```

FIGURE 22 – filebeat.input

output.elasticsearch :



```
# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["http://192.168.3.104:9200"]
```

FIGURE 23 – output.elasticsearch

setup.kibana :

```
setup.kibana:
# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify and additional path, the scheme is required: http://localhost:5601/path
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "http://192.168.3.104:5601"
```

FIGURE 24 – output.elasticsearch

Explications :

- `filebeat.inputs` : Définit les fichiers de log à surveiller. Le chemin `/var/log/*.log` signifie que tous les fichiers de log dans le répertoire `/var/log` seront surveillés.
- `output.elasticsearch` : Spécifie que les logs collectés doivent être envoyés à un serveur Elasticsearch, à l'adresse IP 192.168.3.104 et au port 9200.

Connexion avec Elasticsearch

Les connexions à Elasticsearch et Kibana sont nécessaires pour configurer Filebeat. Définissez les informations de connexion dans `filebeat.yml`. Définissez l'hôte et le port où Filebeat peut trouver l'installation d'Elasticsearch, et définissez le nom d'utilisateur et le mot de passe d'un utilisateur autorisé à configurer Filebeat. Par exemple :

```
1 output.elasticsearch:
2   hosts: ["https://192.168.3.4:9200"]
3   username: "filebeat_internal"
4   password: "PASSWORD"
```

The screenshot displays the Elastic Search console interface. At the top, the browser address bar shows the URL `localhost:5601`. The main header includes the Elastic logo and a search bar. Below the header, the left sidebar contains navigation options like 'Discover', 'Visualize', and 'Dashboard'. The main content area shows a bar chart titled 'logstash.indexed.events' with a time range from 'Jun 9, 2024 @ 07:00:00.000Z' to 'Jun 9, 2024 @ 14:00:00.000Z'. The chart shows a sharp increase in events starting around 07:30, peaking at approximately 180,000 events per second around 08:00. Below the chart, a table of log entries is displayed, showing details like @timestamp, @version, and logstash.indexed.events.

```
setup.kibana:

# Kibana Host
# Scheme and port can be left out and will be
# In case you specify an additional path, the
# IPv6 addresses should always be defined as:
host: "http://192.168.3.104:5601"
```

FIGURE 28 – setup.kibana (packetbeat)

Explication :

- `packetbeat.interfaces.device` : Définit l'interface réseau à surveiller. `any` signifie toutes les interfaces.
- `packetbeat.protocols` : Définit les protocoles réseau à analyser. Les ports spécifiques des protocoles HTTP et MySQL sont listés ici.
- `output.elasticsearch` : Spécifie que les données collectées doivent être envoyées à un serveur Elasticsearch.

Connexion avec Elasticsearch :

Définissez l'hôte et le port où Packetbeat peut trouver l'installation d'Elasticsearch, et définissez le nom d'utilisateur et le mot de passe d'un utilisateur autorisé à configurer Packetbeat. Par exemple :

```
1 output.elasticsearch:
2   hosts: ["https://192.168.103.4:9200"]
3   username: "packetbeat_internal"
4   password: "YOUR_PASSWORD"
```

Collecte des logs (packetbeats) :

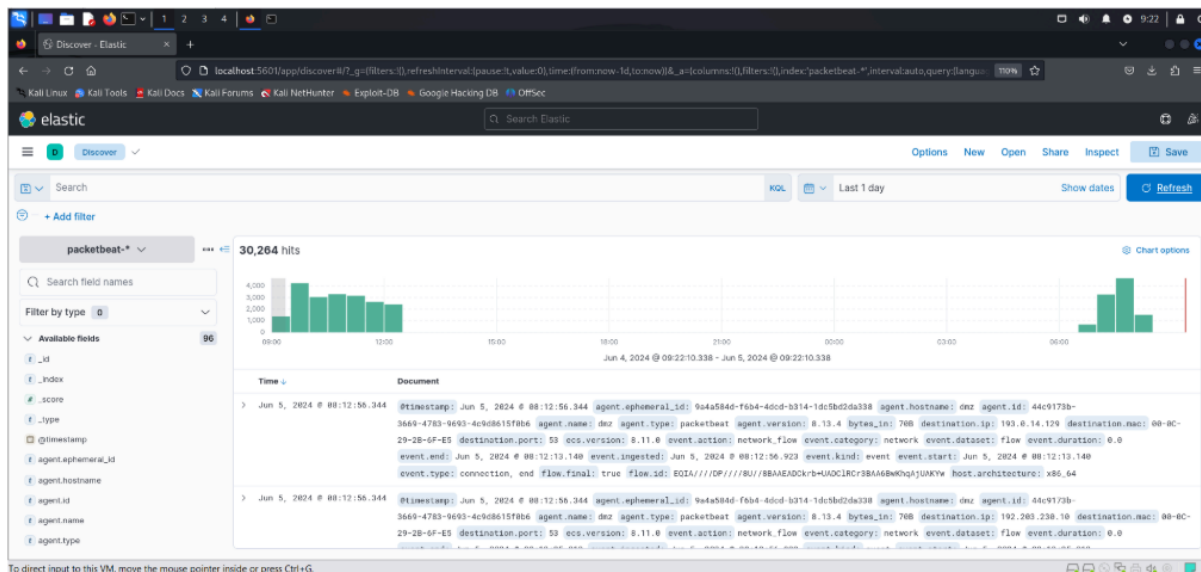


FIGURE 29 – collecte des logs (packetbeat)

Configuration de Winlogbeat

Fichier de Configuration : winlogbeat.yml

```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

  - name: Security

  - name: Microsoft-Windows-Sysmon/Operational

  - name: Windows PowerShell
    event_id: 400, 403, 600, 800

  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106

  - name: ForwardedEvents
    tags: [forwarded]
```

FIGURE 30 – winlogbeat.yml

output.Elasticsearch :

```
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["http://192.168.3.104:9200"]
```

FIGURE 31 – output.Elasticsearch (winlogbeat)

setup.kibana :

```
setup.kibana:
  # Kibana Host
  # Scheme and port can be left out and will be set to the
  default (http and 5601)
  # In case you specify an additional path, the scheme is
  required: http://localhost:5601/path
  # IPv6 addresses should always be defined as:
  https://[2001:db8::1]:5601
  host: "http://192.168.3.104:5601"
```

FIGURE 32 – setup.kibana (winlogbeat)

Explication :

- `winlogbeat.event_logs` : Définit les logs d'événements Windows à surveiller, comme les logs d'application, de sécurité et système. `ignore_older: 72h` signifie que les logs plus anciens que 72 heures ne seront pas collectés.
- `output.elasticsearch` : Spécifie que les logs collectés doivent être envoyés à un serveur Elasticsearch.

Connexion avec Elasticsearch :

Définissez l'hôte et le port où Winlogbeat peut trouver l'installation d'Elasticsearch, et définissez le nom d'utilisateur et le mot de passe d'un utilisateur autorisé à configurer Winlogbeat. Par exemple :

```
1 output.elasticsearch:
2   hosts: ["https://192.168.3.104:9200"]
3   username: "winlogbeat_internal"
```

4 password: "YOUR_PASSWORD"

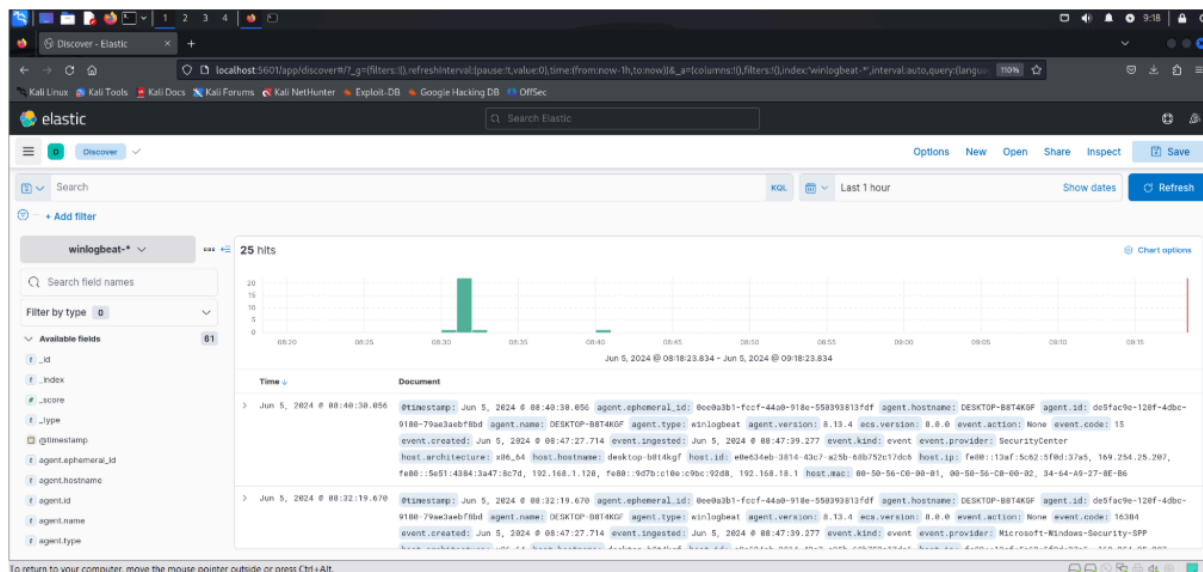


FIGURE 33 – collecte des logs (winlogbeat)

Intégration de pfSense avec Elasticsearch

Pour une gestion centralisée et une analyse approfondie des logs, nous avons configuré pfSense pour envoyer ses logs vers Elasticsearch via Filebeat. Cette section détaille les étapes nécessaires pour configurer cette intégration.

Configuration de pfSense pour l'envoi des logs

Pour que pfSense envoie ses logs à Elasticsearch, il est nécessaire de configurer pfSense pour envoyer les logs via syslog à une machine où Filebeat est configuré pour les recevoir et les expédier à Elasticsearch. Voici les étapes nécessaires pour cette configuration.

1. Accéder à l'Interface Web de pfSense :

- Ouvrir un navigateur web et entrer l'adresse IP de votre pfSense.
- Se connecter avec vos identifiants administrateur.

2. Accéder aux Paramètres de Logging :

- Aller à **Status > System Logs**.
- Sélectionner l'onglet **Settings**.

3. Configurer l'Envoi des Logs :

- Sous **Remote Logging Options**, cocher la case **Enable Remote Logging**.
- Dans le champ **Remote log servers**, entrer l'adresse IP de la machine où Filebeat est configuré pour recevoir les logs, suivi du port syslog (par défaut, 514). Par exemple : 192.168.1.100:514.
- Sélectionner les types de logs à envoyer (par exemple, **Firewall**, **System**, **DHCP**, **DNS**, etc.).

4. Sauvegarder et Appliquer :

- Cliquer sur **Save** pour enregistrer les modifications.



FIGURE 34 – Configuration de l'envoi des logs syslog sur pfSense

Envoi des Logs de pfSense vers Elasticsearch

Une fois Filebeat configuré et démarré, il commencera à surveiller les logs spécifiés et à les envoyer à Elasticsearch. Voici quelques points importants à considérer :

- **Format des Logs** : Assurez-vous que les logs de pfSense sont dans un format lisible par Filebeat. Utilisez les modules disponibles de Filebeat pour pfSense si nécessaire.
- **Filtrage et Parsing** : Utilisez Ingest Node ou Logstash pour parser et filtrer les logs avant de les indexer dans Elasticsearch.
- **Visualisation** : Utilisez Kibana pour créer des visualisations et des tableaux de bord afin de monitorer les logs et détecter les anomalies.

L'intégration de pfSense avec Elasticsearch via Filebeat permet une collecte centralisée et une analyse approfondie des logs de sécurité, facilitant ainsi la détection et la réponse aux incidents de sécurité.

Remote Logging Options

Enable Remote Logging

☒ Send log messages to remote syslog server

Source Address

Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog s must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol

IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address selected type is not found on the chosen interface, the other type will be tried.

Remote log servers

192.168.3.104:514

IP[:port]

IP[:port]

Remote Syslog Contents

☒ Everything

☐ System Events
☐ Firewall Events
☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
☐ General Authentication Events
☐ Captive Portal Events
☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
☐ Gateway Monitor Events
☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
☐ Network Time Protocol Events (NTP Daemon, NTP Client)

FIGURE 35 – L’envoi de Logs de Pfsense vers Elastitcsearch

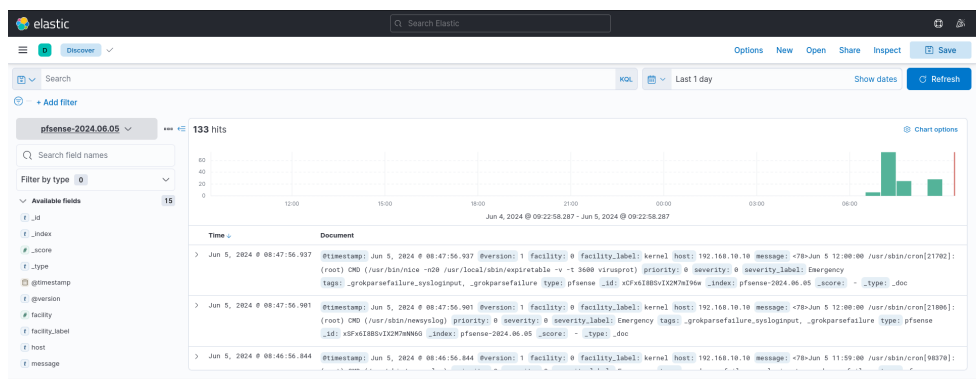


FIGURE 36 – Tableau de bord Kibana montrant les logs de pfSense

Analyse des Risques de Sécurité

Analyse de Sécurité, Identification de Menaces et Évaluation de Vulnérabilités

Dans cette section, nous détaillerons l'approche de notre analyse de sécurité, l'identification des menaces potentielles, et l'évaluation des vulnérabilités par le biais de tests de pénétration. Ces étapes sont essentielles pour garantir la robustesse et la sécurité de notre infrastructure réseau.

Analyse de Sécurité

L'analyse de sécurité consiste à examiner et évaluer la sécurité de notre infrastructure afin de détecter les éventuelles faiblesses exploitables. Les principales étapes de notre analyse de sécurité comprennent :

1. Identification des Actifs :

- Identifier tous les actifs critiques de l'infrastructure, y compris les serveurs, les applications, les bases de données, les réseaux, et les dispositifs de sécurité tels que pfSense et les machines de SIEM.

2. Identification des Menaces :

- Identifier les menaces potentielles qui pourraient affecter la sécurité de notre infrastructure. Ces menaces peuvent inclure des attaques par déni de service (DoS), des intrusions réseau, des malwares, des attaques par phishing, etc.

3. Évaluation des Vulnérabilités :

- Effectuer une évaluation des vulnérabilités pour identifier les faiblesses dans notre infrastructure. Cela inclut l'utilisation de scanners de vulnérabilités pour détecter les points faibles qui pourraient être exploités par des attaquants.

Identification des Menaces

L'identification des menaces est une étape cruciale pour comprendre les risques auxquels notre infrastructure est exposée. Les menaces peuvent être de diverses natures et provenir de différentes sources :

- **Menaces Interne** : Actions malveillantes ou non intentionnelles de la part des employés ou des utilisateurs ayant accès aux ressources internes.
- **Menaces Externes** : Attaques provenant de l'extérieur, telles que les pirates informatiques, les organisations criminelles, ou les acteurs étatiques.
- **Menaces Naturelles** : Catastrophes naturelles comme les inondations, les incendies, ou les tremblements de terre qui peuvent endommager l'infrastructure physique.

Évaluation des Vulnérabilités

L'évaluation des vulnérabilités permet de déterminer les faiblesses de sécurité présentes dans notre infrastructure. Pour ce faire, nous utilisons des outils et techniques spécialisés tels que :

1. **Tests de Pénétration** : Réalisation de tests de pénétration (pentests) pour simuler des attaques réelles et évaluer la résistance de notre infrastructure face à ces attaques.
2. **Analyse Manuelle** : Effectuer des analyses manuelles pour identifier des vulnérabilités qui pourraient ne pas être détectées par les outils automatisés.

Tests de Pénétration

Les tests de pénétration sont une méthode essentielle pour évaluer la sécurité de notre infrastructure. Ils consistent à simuler des attaques réelles pour identifier les faiblesses exploitables. Voici les étapes clés d'un test de pénétration :

1. **Planification et Préparation** :
 - Définir la portée du test, les objectifs, et les limites. Obtenir les autorisations nécessaires pour effectuer le test.
2. **Collecte d'Informations** :

- Rassembler des informations sur les cibles (adresses IP, noms de domaine, services en cours d'exécution, etc.) en utilisant des techniques de reconnaissance passive et active.

3. Analyse des Vulnérabilités :

- Utiliser des outils de scan pour identifier les vulnérabilités présentes sur les systèmes cibles.

4. Exploitation :

- Tenter d'exploiter les vulnérabilités identifiées pour évaluer leur impact réel. Cela inclut l'exécution de scripts d'exploitation et l'utilisation de frameworks tels que Metasploit.

5. Post-Exploitation :

- Évaluer les dommages potentiels après une exploitation réussie. Examiner les privilèges obtenus, les données accessibles, et les possibilités de mouvement latéral.

6. Rapport et Remédiation :

- Documenter les découvertes du test de pénétration, y compris les vulnérabilités exploitées, les données compromises, et les recommandations pour remédier aux failles.

Attaques et Réponse du WAF

Dans cette section, nous décrivons les attaques spécifiques que nous avons réalisées en utilisant OWASP Juice Shop, ainsi que les réponses observées du Web Application Firewall (WAF). Les attaques incluent l'injection SQL, le cross-site scripting (XSS), et l'injection de modèles côté serveur (SSTI).

Attaque par Injection SQL

L'injection SQL est une technique qui permet d'injecter des requêtes SQL malveillantes dans une application vulnérable. Voici les étapes et les résultats de notre test d'injection SQL sur OWASP Juice Shop.

1. Exécution de l'attaque :

- Nous avons identifié un champ de saisie vulnérable et injecté une requête SQL malveillante.

2. Capture d'écran de l'attaque :

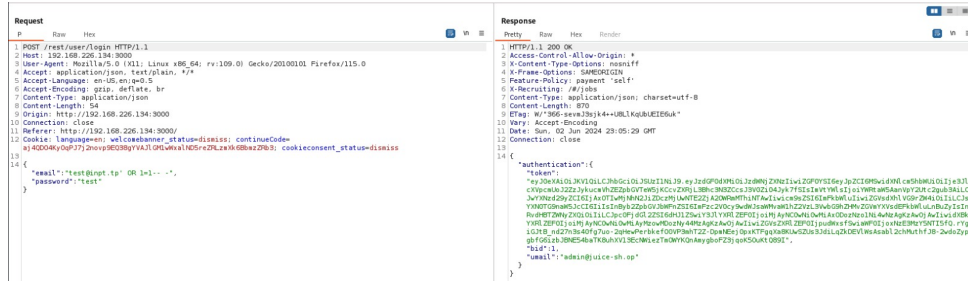


FIGURE 37 – Attaque par Injection SQL sur OWASP Juice Shop

3. Réponse du WAF :

- Le WAF a détecté et bloqué l'attaque d'injection SQL, empêchant l'exécution de la requête malveillante.

4. Capture d'écran de la réponse du WAF :

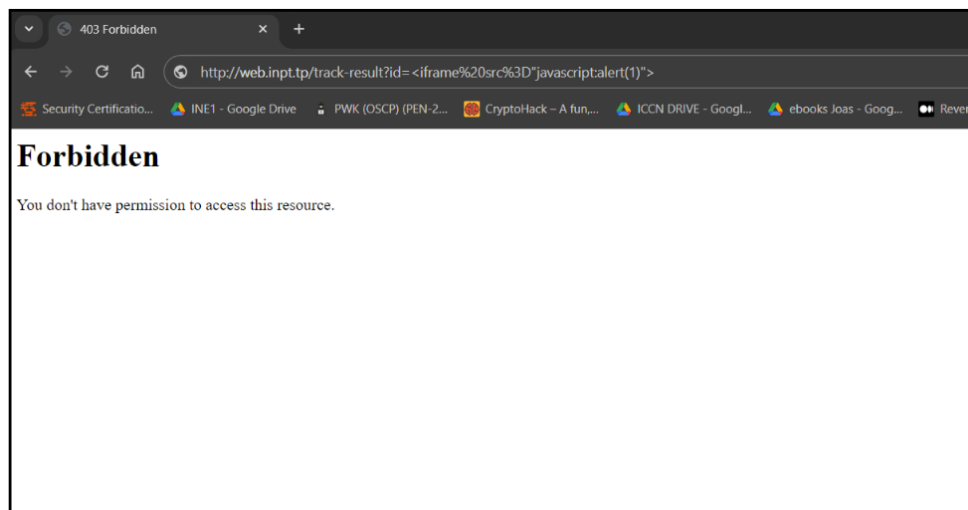


FIGURE 38 – Réponse du WAF à l'Attaque par Injection SQL

5. WAF Bypass :

- "WAF bypass" désigne les techniques et méthodes utilisées pour contourner ou échapper aux protections fournies par un Web Application Firewall (WAF)

6. Capture d'écran du WAF Bypass :

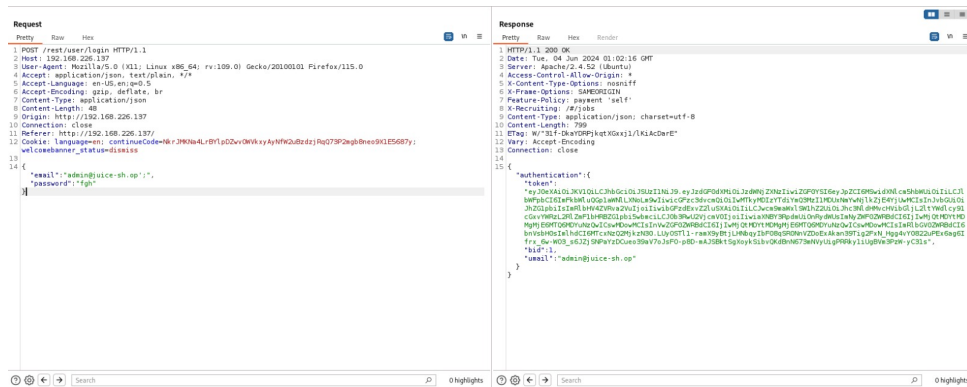


FIGURE 39 – WAF Bypass de l'Attaque par Injection SQL

Attaque par Cross-Site Scripting (XSS)

Le cross-site scripting (XSS) est une attaque qui injecte du code JavaScript malveillant dans une application web. Voici les étapes et les résultats de notre test XSS sur OWASP Juice Shop.

1. Exécution de l'attaque :

- Nous avons trouvé un champ vulnérable et injecté un script XSS.

2. Capture d'écran de l'attaque :

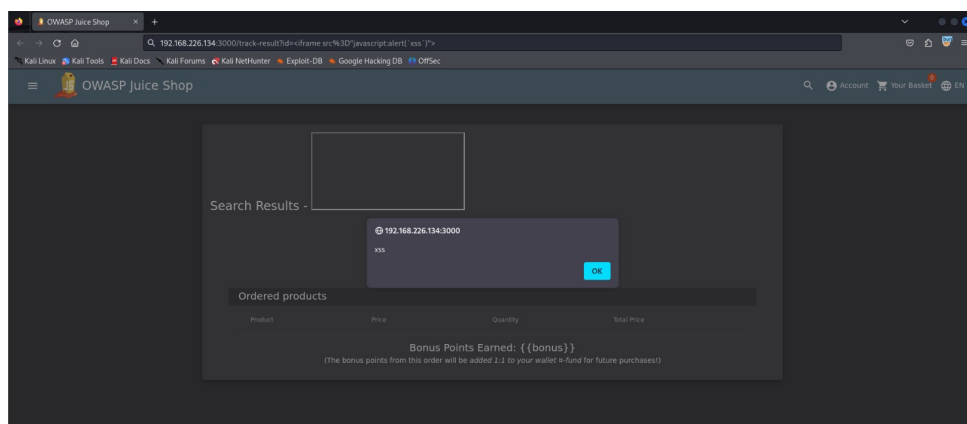


FIGURE 40 – Attaque par Cross-Site Scripting sur OWASP Juice Shop

3. Réponse du WAF :

- Le WAF a détecté l'injection de script et a bloqué l'exécution du code malveillant.

4. Capture d'écran de la réponse du WAF :

5. WAF Bypass :

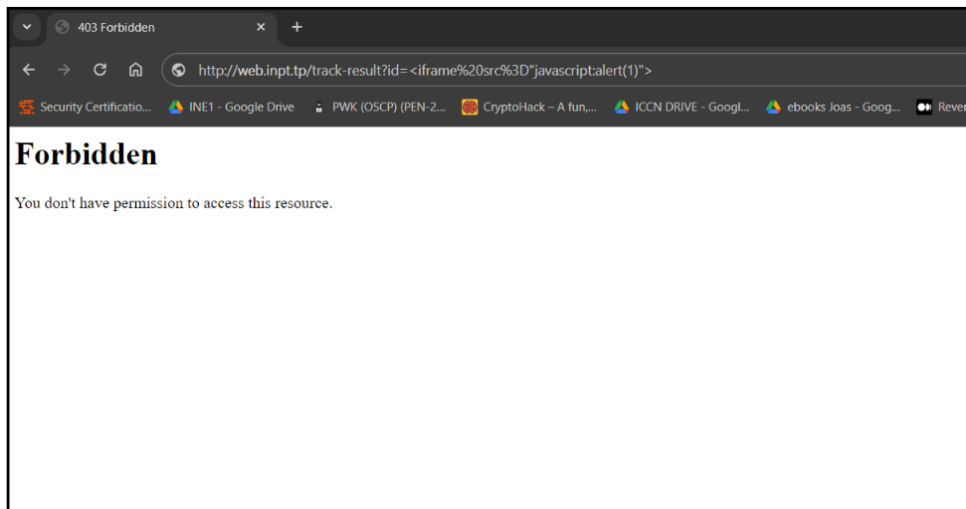


FIGURE 41 – Réponse du WAF à l'Attaque XSS

- "WAF bypass" désigne les techniques et méthodes utilisées pour contourner ou échapper aux protections fournies par un Web Application Firewall (WAF)

6. Capture d'écran du WAF Bypass :

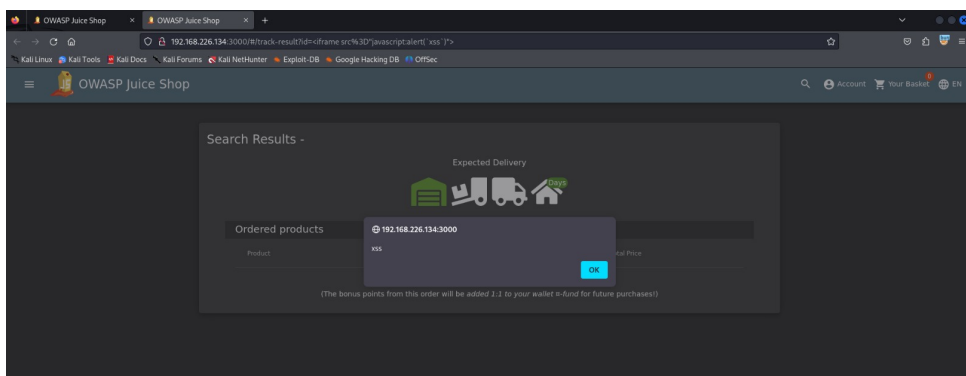


FIGURE 42 – WAF Bypass de l'Attaque par XSS

Attaque par Injection de Modèles Côté Serveur (SSTI)

L'injection de modèles côté serveur (SSTI) permet d'injecter du code malveillant dans des modèles utilisés par le serveur. Voici les étapes et les résultats de notre test SSTI sur OWASP Juice Shop.

1. Exécution de l'attaque :

- Nous avons injecté un code de modèle malveillant dans un champ vulnérable.

2. Capture d'écran de l'attaque :

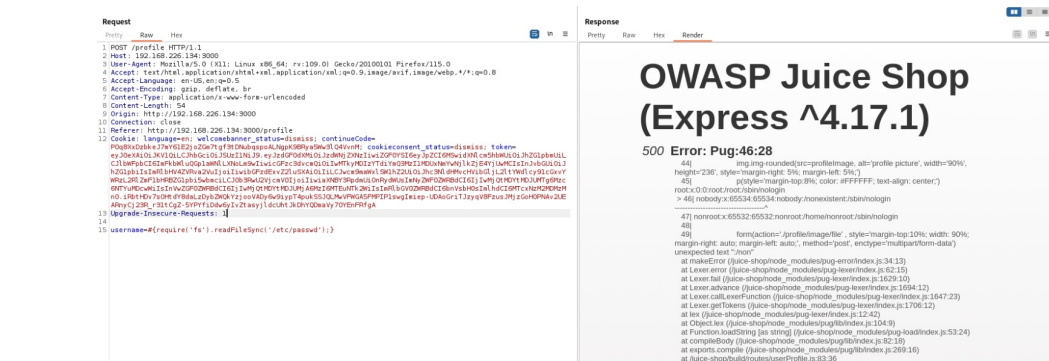


FIGURE 43 – Attaque par Injection de Modèles Côté Serveur sur OWASP Juice Shop

3. Réponse du WAF :

- Le WAF a détecté l'injection de modèle et a bloqué l'exécution du code malveillant.

4. Capture d'écran de la réponse du WAF :

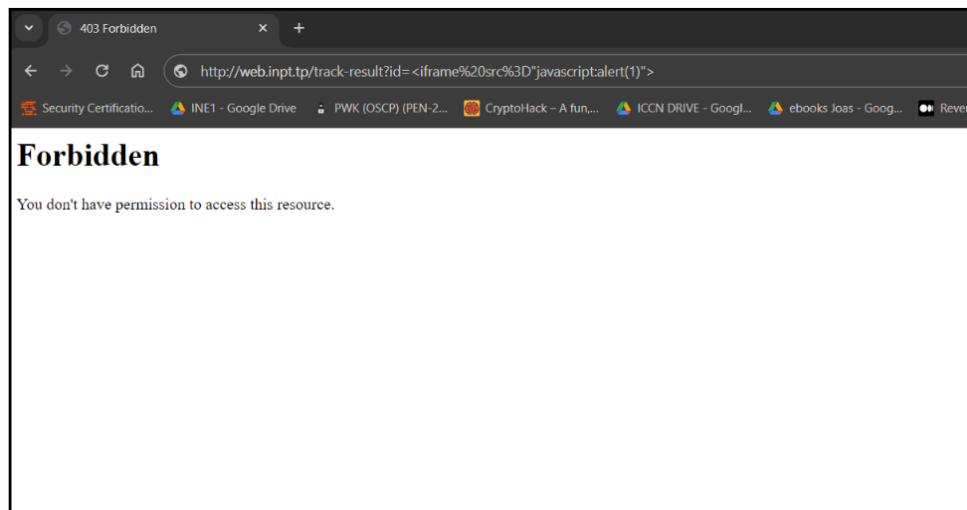


FIGURE 44 – Réponse du WAF à l'Attaque SSTI

5. WAF Bypass :

- "WAF bypass" désigne les techniques et méthodes utilisées pour contourner ou échapper aux protections fournies par un Web Application Firewall (WAF)

6. Capture d'écran du WAF Bypass :

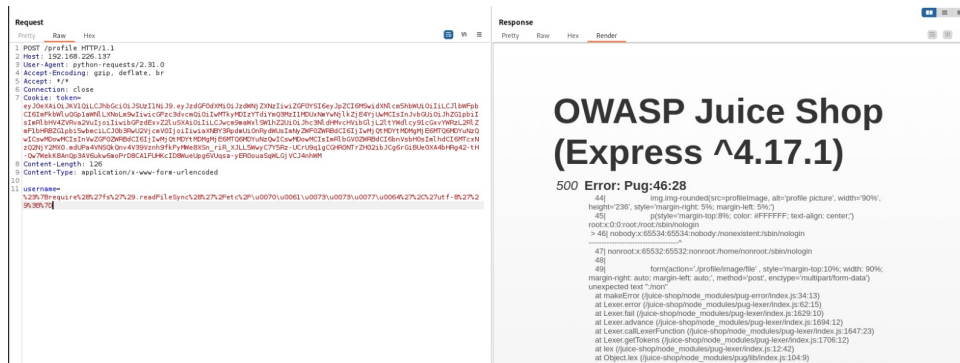


FIGURE 45 – WAF Bypass de l'Attaque SSII

Les attaques réalisées sur OWASP Juice Shop, notamment l'injection SQL, le XSS et le SSTI, ont permis de tester la robustesse de notre WAF. La réponse efficace du WAF à chaque attaque a montré sa capacité à détecter et à bloquer les tentatives malveillantes, assurant ainsi la sécurité de notre application web.

L'analyse de sécurité, l'identification des menaces, et l'évaluation des vulnérabilités sont des composants essentiels de la sécurisation de notre infrastructure réseau. Les tests de pénétration, en particulier, jouent un rôle crucial en simulant des attaques réelles pour découvrir et corriger les faiblesses avant qu'elles ne puissent être exploitées par des attaquants. En combinant ces approches, nous renforçons la sécurité et la résilience de notre infrastructure face aux menaces actuelles et futures.

Conclusion

Ce rapport a présenté une analyse exhaustive de l'implémentation de l'ELK Stack (Elasticsearch, Logstash, Kibana) pour la gestion et l'analyse des logs, ainsi que des mesures de sécurité avancées intégrées à notre infrastructure IT. L'ELK Stack s'est révélée être une solution performante et polyvalente, capable de collecter, stocker et analyser de grandes quantités de données en temps réel. Cette capacité a permis une surveillance approfondie de nos systèmes, une détection rapide des anomalies, et une analyse détaillée des événements critiques.

En complément, les tests de sécurité réguliers ont été essentiels pour identifier et remédier aux vulnérabilités potentielles. Ces tests ont renforcé notre architecture en assurant une protection accrue contre les menaces et en garantissant la conformité avec les meilleures pratiques de sécurité.

La combinaison de l'ELK Stack et des tests de sécurité proactifs a permis d'améliorer significativement notre visibilité sur les opérations IT, de renforcer la sécurité de notre infrastructure, et d'assurer une réactivité optimale face aux incidents. Cette approche intégrée a non seulement optimisé les performances de nos systèmes, mais a également renforcé la confiance de nos utilisateurs et partenaires.

En conclusion, l'implémentation de ces technologies et pratiques a permis d'établir une base solide pour une gestion efficace et sécurisée de notre infrastructure. Nous continuerons à surveiller et à améliorer notre environnement IT, en adoptant les innovations technologiques et les stratégies de sécurité les plus avancées pour maintenir notre position à la pointe de la performance et de la sécurité.