

## Projet - Sécurité des réseaux

Master 2 Cybersécurité

---

*Surveillance en temps réel avec*

---



Réalisé par :

HAMADOUCHE Rayane  
KHEMAMIL Sabrina  
AMRANE Lina

Travail demandé par :

M. Rida KHATOUN

## Table des matières

<b>Préface</b>	<b>3</b>
Chapitre 1 : Introduction à Splunk	4
1.1 Qu'est-ce que Splunk ?	5
1.2 Historique et évolution de Splunk	5
1.4 Fonctionnalités clés	5
1.4.1 Collecte et analyse des données	5
Collecte des données	5
Analyse avancée	6
1.4.2 Visualisation et tableaux de bord	6
1.4.3 Alertes et automatisation	6
1.4.4 Machine Learning et intelligence artificielle	6
1.5 Cas d'utilisation	6
Surveillance des systèmes IT	6
Sécurité et détection des menaces (SIEM)	7
Analyse des performances des applications	7
IoT et analyses prédictives	7
1.6 Architecture de Splunk	7
1.6.1 Composants principaux (figure 1)	7
1.6.2 Déploiement classique et architecture distribuée	8
1.6.3 Intégration avec les solutions Cloud	8
1.7 Avantages et limites	8
1.7.1 Points forts [7]	8
1.7.2 Challenges [7]	8
<b>Chapitre 2 : Implémentation de l'architecture réseau et mise en place de Splunk</b>	<b>9</b>
2.1 Architecture réseau	10
1. Présentation de l'architecture	10
2. Schéma de l'architecture réseau	10
3. Configuration de l'architecture réseau	11
3.1 Configuration des VLANs (LAN)	11
3.2 Configuration du pare-feu PfSense	12
3.2.1 Construction d'un réseau sécurisé avec les règles de pfSense	13
3.3 Déploiement de la DMZ	14
3.4 Configuration de snort:	14
2.2 Déploiement de Splunk	15
2.2.1 Installation de Splunk	15
2.2.2 Configuration de la récupération des logs	15
2.2.3 Création de tableaux de bord	17
2.2.4 Création des alertes	19
1. Détection des alertes Snort dans Splunk	20
2. Création de la recherche Splunk	20
3. Configuration de l'alerte dans Splunk	20
4. Amélioration de l'alerte	20

5. Démonstration	21
<b>Chapitre 3 : Simulation d'attaque et alerting Splunk</b>	<b>22</b>
3.1 Méthodologie de la simulation d'attaque	22
3.2 Mise en œuvre de l'attaque avec hping3	22
3.3 Surveillance et alertes sur Splunk	22
3.3.1 Monitoring des logs Snort	23
3.3.2 Visualisation du trafic web	23
3.3.3 Alertes automatiques générées par Splunk	24
<b>Conclusion</b>	<b>25</b>
<b>Références</b>	<b>26</b>

# Préface

La cybersécurité est devenue un enjeu stratégique incontournable dans le contexte actuel, où les menaces numériques ne cessent de croître et d'évoluer. Dans ce cadre, le choix d'outils performants pour la surveillance et l'analyse des événements réseau joue un rôle clé dans la prévention et la détection des attaques.

Ce rapport s'inscrit dans une démarche pédagogique et collective, réalisée en groupe, visant à approfondir la maîtrise des outils de sécurité, notamment **Splunk**, une solution puissante d'analyse de données. Ensemble, nous avons mis en pratique des compétences techniques, telles que la mise en place d'une architecture réseau sécurisée, la configuration d'outils comme pfSense, et l'utilisation de Splunk pour collecter, analyser et visualiser des données critiques.

Cette expérience collaborative nous a permis de renforcer nos connaissances techniques et d'explorer les aspects stratégiques de la cybersécurité, tout en développant nos aptitudes à travailler en équipe pour relever des défis complexes. Ce projet a été une opportunité précieuse pour allier théorie et pratique afin de répondre à des besoins réels en termes de surveillance et d'analyse de données.

Au-delà de l'aspect technique, ce projet nous a permis de développer une meilleure compréhension des enjeux liés à la gestion des risques et à la détection proactive des menaces. L'intégration de Splunk dans notre architecture réseau a illustré comment un outil bien configuré peut transformer des données brutes en informations exploitables pour la prise de décision rapide et efficace.

# Chapitre 1 : Introduction à Splunk

## 1.1 Qu'est-ce que Splunk ?

Splunk est une plateforme logicielle qui permet de collecter, d'indexer et d'analyser des données générées par des machines en temps réel. Initialement conçue pour l'analyse des journaux informatiques, elle s'est rapidement imposée comme un outil essentiel pour la surveillance des systèmes informatiques, la gestion des performances applicatives et la cybersécurité. Splunk offre une approche unifiée pour transformer des données complexes en informations exploitables et compréhensibles [1].

## 1.2 Historique et évolution de Splunk

### Fondation en 2003

Splunk a été fondé par **Michael Baum, Rob Das et Erik Swan** avec pour objectif de faciliter l'analyse des logs machine. L'idée était d'offrir un moteur de recherche puissant permettant aux équipes IT de diagnostiquer rapidement les problèmes système et d'optimiser la surveillance des infrastructures [2].

### Introduction en bourse en 2012

Après plusieurs années de croissance rapide, Splunk devient une société cotée en bourse (NASDAQ: SPLK) en 2012. Cette introduction marque un tournant stratégique, renforçant son expansion et lui permettant de diversifier ses solutions, notamment dans l'analyse des données en temps réel [2].

### Intégration de l'IA en 2017

Splunk intègre des fonctionnalités basées sur l'intelligence artificielle et le machine learning avec le **Machine Learning Toolkit (MLTK)**. Cette avancée permet d'automatiser la détection d'anomalies et d'optimiser les analyses prédictives, renforçant ainsi son rôle dans la cybersécurité et l'IT Ops [2].

### Élargissement de l'écosystème en 2019

Splunk élargit son écosystème en acquérant plusieurs entreprises clés comme SignalFx (monitoring cloud) et Phantom (automatisation en cybersécurité). Ces acquisitions renforcent ses capacités en **observabilité, automatisation et sécurité**, rendant sa plateforme encore plus complète [2].

### Splunk aujourd'hui

Aujourd'hui, Splunk est un acteur majeur de l'**observabilité, de la cybersécurité et de l'analyse de données**, utilisé par des milliers d'entreprises à travers le monde. Il continue d'évoluer avec le cloud et l'IA, tout en s'adaptant aux nouveaux défis des infrastructures modernes [2].

## 1.4 Fonctionnalités clés

### 1.4.1 Collecte et analyse des données

#### Collecte des données

Splunk peut ingérer des données à partir de nombreuses sources, telles que [4]:

- Journaux applicatifs.
- Flux réseaux (NetFlow, sFlow).

- Données d'appareils IoT.

Le moteur d'ingestion de Splunk utilise des agents appelés "Universal Forwarders" pour transmettre les données brutes vers les indexeurs. Ces données sont ensuite structurées et indexées pour une recherche rapide.

#### Analyse avancée

Le langage de recherche de Splunk (SPL) permet des analyses complexes. Par exemple, il est possible de corrélérer des événements issus de différentes sources pour identifier des anomalies ou des patterns récurrents [3].

#### 1.4.2 Visualisation et tableaux de bord

Splunk fournit des outils de visualisation puissants qui permettent de [1][5]:

- Créer des graphiques interactifs, des diagrammes à secteurs et des cartes thermiques.
- Configurer des tableaux de bord adaptés aux besoins spécifiques des utilisateurs.
- Partager les tableaux de bord avec les équipes pour favoriser la collaboration.

Ces visualisations sont également adaptées pour des présentations stratégiques.

#### 1.4.3 Alertes et automatisation

Splunk peut être configuré pour surveiller des événements en temps réel et générer des alertes lorsque des seuils critiques sont atteints. Ces alertes peuvent [5] :

- Envoyer des notifications par e-mail.
- Lancer des scripts automatisés pour résoudre les problèmes.
- S'intégrer à des systèmes de gestion des tickets comme ServiceNow.

#### 1.4.4 Machine Learning et intelligence artificielle

Splunk intègre des capacités de machine learning qui permettent [5]:

- De détecter des anomalies dans des séries temporelles.
- De prédire des événements futurs, tels que les pannes ou les pics de charge.
- D'automatiser l'identification de tendances et d'outils à travers des jeux de données volumineux.

L'application Splunk Machine Learning Toolkit (MLTK) fournit une interface intuitive pour appliquer des modèles pré-construits ou développer des algorithmes personnalisés.

### 1.5 Cas d'utilisation

#### Surveillance des systèmes IT

Les organisations utilisent Splunk pour surveiller les performances des serveurs, réseaux et applications. Il permet de [6]:

- Identifier les temps d'arrêt non prévus.
- Optimiser l'utilisation des ressources.

## Sécurité et détection des menaces (SIEM)

Splunk Enterprise Security (ES) est un outil dédié à la gestion des événements de sécurité. Il aide à :

- Déetecter les intrusions et les malwares.
- Surveiller les activités suspectes en temps réel.

## Analyse des performances des applications

Splunk APM (Application Performance Monitoring) permet de suivre les temps de réponse et les erreurs applicatives. Il aide à :

- Identifier les goulets d'étranglement.
- Améliorer l'expérience utilisateur.

## IoT et analyses prédictives

Avec l'intégration des appareils IoT, Splunk permet de [6] :

- Surveiller les données en provenance de capteurs en temps réel.
- Automatiser les réponses aux anomalies dans les environnements connectés.

# 1.6 Architecture de Splunk

## 1.6.1 Composants principaux (figure 1)

1. Universal Forwarder : Envoie les données des sources vers les indexeurs.
2. Indexer : Stocke et indexe les données ingérées.
3. Search Head : Fournit une interface pour exécuter des recherches et afficher des tableaux de bord.
4. Cluster Master : Gère la réPLICATION des données dans un environnement distribué.

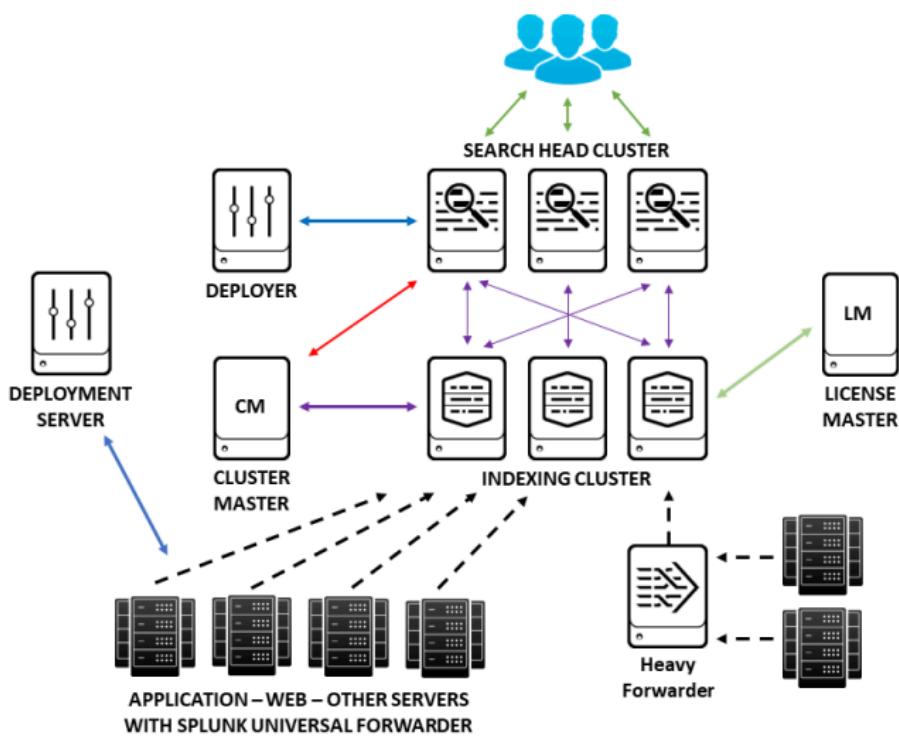


Figure 1 : Architecture intérieur de Splunk

### 1.6.2 Déploiement classique et architecture distribuée

Dans un déploiement simple, tous les composants peuvent fonctionner sur un seul serveur. Cependant, pour les grandes entreprises, une architecture distribuée est recommandée pour améliorer la scalabilité et la résilience [5][6].

### 1.6.3 Intégration avec les solutions Cloud

Splunk s'intègre parfaitement aux environnements cloud comme AWS, Azure et Google Cloud Platform. Avec Splunk Cloud, les organisations peuvent [5][7] :

- Éviter les coûts d'infrastructure locale.
- Profiter d'une évolutivité quasi illimitée.
- Accéder à leurs données depuis n'importe où.

## 1.7 Avantages et limites

### 1.7.1 Points forts [7]

1. Flexibilité : Adapté à divers cas d'utilisation (IT, sécurité, IoT).
2. Scalabilité : Peut traiter des volumes massifs de données.
3. Communauté active : Un large écosystème de plugins et de support.
4. Innovations continues : Ajout constant de nouvelles fonctionnalités.

### 1.7.2 Challenges [7]

1. Coûts élevés : Les licences Splunk sont basées sur le volume de données ingérées, ce qui peut être prohibitif.
2. Complexité initiale : L'apprentissage et la configuration peuvent prendre du temps.
3. Consommation de ressources : Les indexeurs nécessitent une infrastructure matérielle robuste pour des performances optimales.

# Chapitre 2 : Implémentation de l'architecture réseau et mise en place de Splunk

## 2.1 Architecture réseau

### 1. Présentation de l'architecture

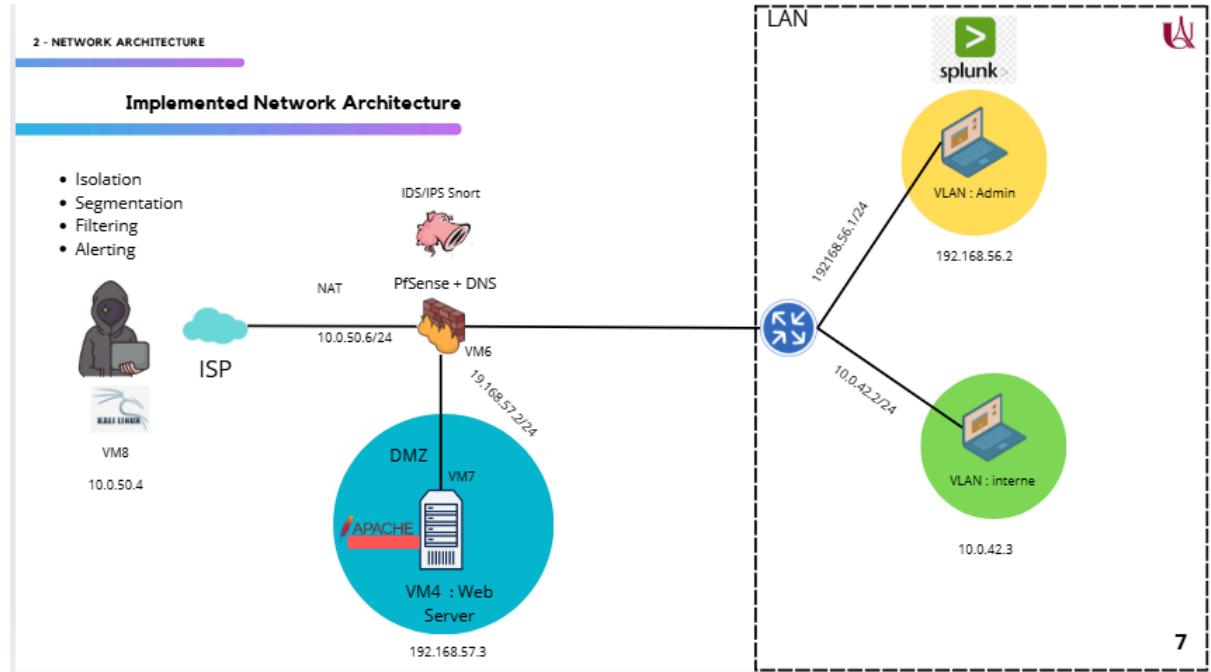
Pour assurer une surveillance en temps réel avec Splunk, nous avons opté pour une architecture réseau simple mais efficace, structurée autour des éléments suivants :

- Une DMZ : Cette zone héberge un serveur web Apache qui contient le site web de notre agence immobilière. Elle permet d'exposer ce service au public tout en protégeant le réseau interne contre d'éventuelles attaques.
- Un LAN : Le LAN est divisé en deux VLANs distincts :
  - Un premier VLAN dédié au poste administrateur, sur lequel Splunk a été installé pour collecter et analyser les logs du réseau.
  - Un second VLAN contenant un poste utilisateur, tel qu'un PC utilisé par le service RH, afin d'isoler les utilisateurs internes.
- Un pare-feu PfSense : Ce dispositif joue un double rôle de routeur et de pare-feu. Il assure la segmentation des réseaux et applique des règles de sécurité strictes pour protéger les différentes zones.
- Snort : Cet outil est installé sur PfSense pour analyser le trafic réseau, détecter les intrusions, et surveiller les activités malveillantes.
- La connexion au réseau WAN permet d'assurer l'accès au site web de l'agence immobilière depuis Internet. Elle représente également le point d'entrée potentiel des attaquants. Dans ce projet, un attaquant simulé, utilisant Kali Linux, a été connecté à ce réseau pour tester la sécurité et la détection des intrusions via Splunk et Snort.

Cette architecture garantit une séparation claire entre les zones exposées (DMZ) et les réseaux internes, tout en offrant une surveillance centralisée des activités réseau grâce à Splunk. Cela permet à la fois de sécuriser les communications et de répondre aux besoins opérationnels de notre agence immobilière.

### 2. Schéma de l'architecture réseau

Le schéma ci-dessous illustre l'architecture réseau mise en place pour ce projet. Il met en évidence les différentes zones du réseau, les équipements clés, ainsi que leurs interactions.



### 3. Configuration de l'architecture réseau

#### 3.1 Configuration des VLANs (LAN)

- Objectif : Segmentation du réseau pour séparer les zones critiques et limiter la portée des éventuelles intrusions.
- Chaque VLAN a été configuré comme suit :
  - VLAN 10 : Administrateur
    - IP : 192.168.56.2
    - Utilisé pour le poste administrateur, où Splunk est installé.
  - VLAN 20 : Utilisateurs internes
    - IP : 10.0.42.2
    - Contient des postes de travail, comme le PC du service RH.
- La configuration des VLANs a été réalisée sur PfSense .

#### 3.2 Configuration du pare-feu PfSense

Après avoir installer Pfsense en suivants les étapes de ce site suivant:  
<https://www.it-connect.fr/installation-de-pfsense%EF%BB%BF/>

La prochaine étape de la configuration de PfSense consiste à définir les adresses IP des interfaces pour les différentes zones du réseau : DMZ, WAN et LAN. Cela permet d'assurer la connectivité et de segmenter correctement le trafic entre ces zones.

La capture ci-dessous illustre la configuration des adresses IP pour chaque interface dans l'interface d'administration de PfSense :

```

pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: c7bf56e44b834dbc89a3

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

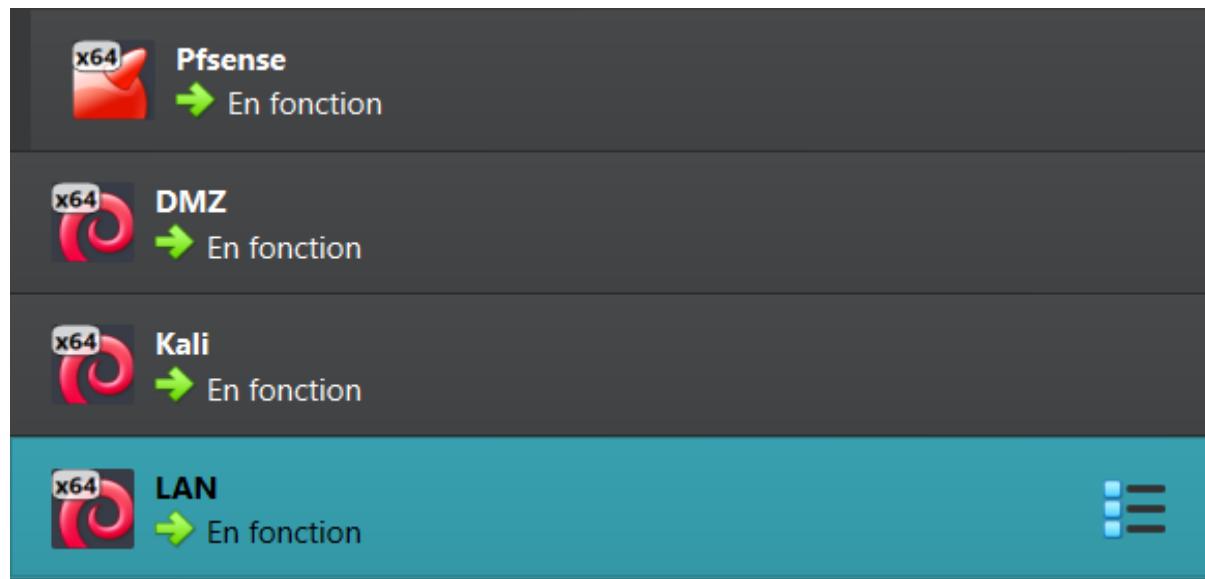
WAN (wan)      -> le0          -> v4/DHCP4: 10.0.50.6/24
LAN (lan)      -> le1          -> v4: 10.42.0.2/24
DMZ (opt1)     -> le2          -> v4: 192.168.57.2/24
ADMIN (opt2)   -> le1.1       -> v4: 192.168.58.1/24

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: ■

```

Cette architecture a été réalisée en utilisant des machines virtuelles (VMs) sur VirtualBox, ce qui permet une grande flexibilité et une gestion simplifiée des ressources réseau.



### 3.2.1 Construction d'un réseau sécurisé avec les règles de pfSense

Notre objectif est donc de rendre le serveur web accessible depuis Internet, tout en empêchant l'accès au LAN. En revanche, depuis le LAN, il doit être possible de se connecter au serveur web. Ce sont les principes de l'architecture DMZ .

Règles :

Tout d'abord, nous devons créer 3 règles pour bloquer l'accès de la DMZ au WAN, de la DMZ au LAN et du WAN au LAN :

- DMZ --> WAN : bloqué
- DMZ --> LAN : bloqué

- WAN --> LAN : bloqué

Ensuite, il faut établir rapidement la politique de sécurité de la DMZ, qui permet :

- Aux utilisateurs Internet d'accéder au serveur WEB.
- Au serveur web de pouvoir leur répondre.
- Que seuls les ports 80 et 443 (les ports HTTP et HTTPS) soient ouverts.

Règles à appliquer :

- WAN -> DMZ : HTTP/HTTPS autorisés
- LAN -> DMZ : HTTP/HTTPS/FTP autorisés

Le LAN doit pouvoir accéder au WAN, mais uniquement sur les ports HTTP et HTTPS :

- LAN -> WAN : HTTP/HTTPS autorisés

Enfin, il faut configurer une règle de redirection de port de l'adresse WAN et du port 80 vers l'adresse du serveur web et le port 80.

Voilà, les trois points de notre politique de sécurité sont respectés. Nous avons pu sécuriser notre architecture réseau grâce aux règles de notre pare-feu.

WAN:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0/0 B	IPv4 TCP	10.0.50.0/24	*	DMZ address	80 (HTTP)	*	none		
<input type="checkbox"/>		0/0 B	IPv4+6 *	DMZ address	*	WAN address	*	*	none	Block traffic from DMZ to WAN	
<input type="checkbox"/>		0/0 B	IPv4+6 TCP/ UDP	LAN address	*	WAN address	443 (HTTPS)	*	none	HTTP/HTTPS trafics are allowed in LAN to WAN	

LAN:

	2/139 KIB	*	*	*	LAN Address	443 80	*	*	Anti-Lockout Rule		
<input type="checkbox"/>		0/0 B	IPv4+6 *	WAN address	*	LAN address	*	*	none	Block traffic from WAN to LAN	
<input type="checkbox"/>		0/0 B	IPv4+6 *	DMZ address	*	LAN address	*	*	none	Block traffic from DMZ to LAN	
<input type="checkbox"/>		10/19 Kib	IPv4 TCP	10.42.0.0/24	*	*	80 (HTTP)	*	none	HTTP traffic passed from LAN	

DMZ:

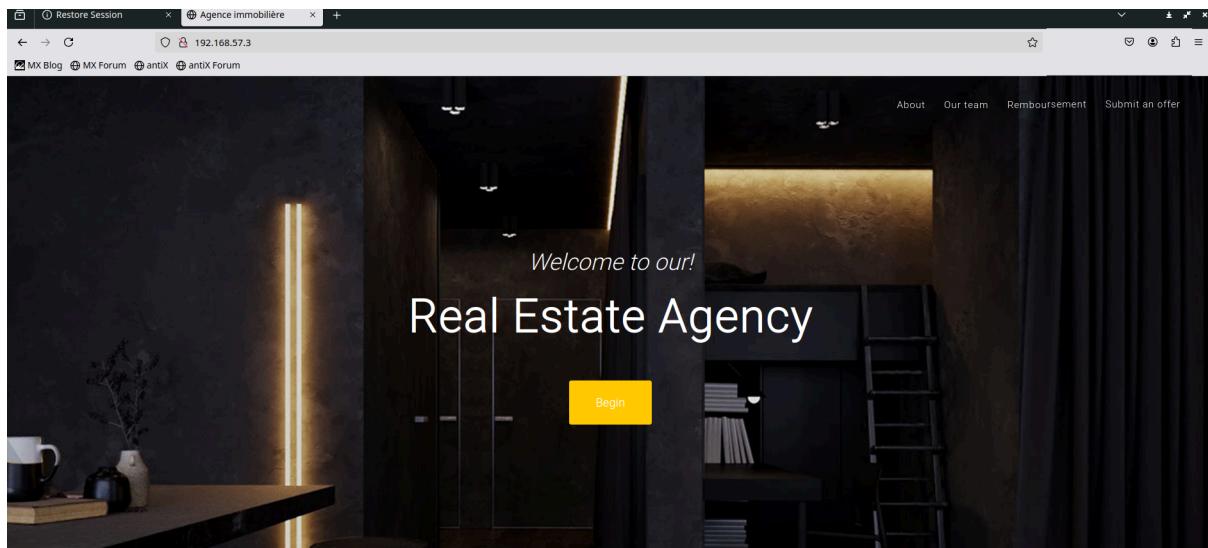
<input type="checkbox"/>		0/0 B	IPv4 TCP	10.0.50.0/24	*	DMZ address	80 (HTTP)	*	none	HTTP traffic allowed from WAN to DMZ	
<input type="checkbox"/>		0/0 B	IPv4 TCP	LAN address	*	DMZ address	80 (HTTP)	*	none	HTTP traffic allowed from LAN to DMZ	

### 3.3 Déploiement de la DMZ

Le sous-réseau 192.168.57.0/24 a été sélectionné pour notre DMZ afin de la différencier clairement du LAN interne.

Pour notre projet, l'installation et la configuration d'un serveur web Apache jouent un rôle essentiel dans l'établissement d'une infrastructure réseau solide.

Dans le cadre de notre projet, nous avons créé un site web immobilier où les visiteurs peuvent explorer des propriétés et trouver des informations pertinentes.



### 3.4 Configuration de snort:

Snort est configuré en tant que package supplémentaire sur pfSense, s'intégrant parfaitement aux fonctionnalités existantes du pare-feu. Grâce à l'interface web intuitive de pfSense, les ensembles de règles de Snort sont facilement téléchargés et mis à jour, garantissant ainsi une protection en temps réel contre les menaces émergentes. Les options de personnalisation permettent de configurer des règles spécifiques, ce qui permet une détection précise des activités réseau suspectes. En exploitant les fonctionnalités avancées de Snort, telles que l'analyse des protocoles et la détection basée sur des signatures, nous renforçons notre capacité à identifier et à atténuer les violations potentielles de sécurité.

A screenshot of the pfSense web interface showing the "Snort Interfaces" configuration screen. The top navigation bar includes "Services / Snort / Interfaces". Below the navigation, there is a toolbar with links: Snort Interfaces (highlighted), Global Settings, Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The main content area is titled "Interface Settings Overview" and displays a table with one row. The table columns are: Interface, Snort Status, Pattern Match, Blocking Mode, Description, and Actions. The single entry is "WAN (le0)" with status "ON", pattern match "AC-BNFA", blocking mode "DISABLED", description "WAN", and actions icons for edit, copy, and delete.

## 2.2 Déploiement de Splunk

Dans cette section, nous allons détailler les étapes pour installer Splunk, configurer la récupération des logs et créer des tableaux de bord afin de visualiser les données collectées.

### 2.2.1 Installation de Splunk

1. Téléchargement de Splunk
  - Rendez-vous sur le site officiel de Splunk (<https://www.splunk.com>).
  - Téléchargez la version gratuite ou d'essai pour votre système d'exploitation (Linux, Windows ou MacOS).
2. Premiers pas avec Splunk
  - Lancez le service Splunk :
 

```
sudo /opt/splunk/bin/splunk start
```
  - Acceptez les termes de la licence et créez un utilisateur administrateur (nom d'utilisateur et mot de passe).
3. Accès à l'interface Splunk
  - Accédez à l'interface via un navigateur à l'adresse suivante :
   
`http://localhost:8000`



## 2.2.2 Configuration de la récupération des logs

1. Installation de l'application Technology Add-on for pfSense
  - Depuis l'interface Splunk, accédez à :
    - Apps → Find More Apps.
  - Recherchez et installez l'application "Technology Add-on for pfSense".
  - Redémarrez Splunk pour appliquer les modifications.
2. Ajout d'une source de logs via TCP
  - Depuis l'interface Splunk, allez dans :
    - Settings → Data Inputs → UDP.
  - Configurez une nouvelle entrée UDP :
    - Port : 7001 (pour recevoir les logs envoyés depuis pfSense).
    - Source type : Spécifiez un type, par exemple pfsense\_logs.
    - Index : Utilisez un index existant ou créez-en un nouveau (par exemple : firewall\_logs).
3. Configuration de pfSense pour envoyer les logs
  - Connectez-vous à l'interface pfSense.
  - Allez dans Status → System Logs → Settings.

- Dans la section Remote Logging Options :
  - Activez l'envoi de logs vers un serveur distant.
  - Entrez l'adresse IP de votre serveur Splunk.
  - Configurez le port UDP : 7001.
  - Sélectionnez les types de logs à envoyer (par exemple : firewall, DHCP, etc.) dans notre cas on a choisi d'envoyer que les logs système et firewall.
- Sauvegardez la configuration et redémarrez les services si nécessaire.

**Remote Logging Options**

Enable Remote Logging  Send log messages to remote syslog server

Source Address

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 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

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

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)

#### 4. Vérification de la récupération des logs

- Accédez à l'onglet Search & Reporting dans Splunk.
  - Exécutez une recherche pour vérifier que les logs sont bien collectés :
- index=firewall

**splunk-enterprise Applications ▾** Administrateur ▾ Messages ▾ Paramètres ▾ Activité ▾ Aide ▾ Rechercher ▾

Vues par défaut ▾

Technology Add-on for pfSense

Nouvelle recherche

index=firewall

✓ 68 085 événement (avant 24/01/2025 21:59:25,000) Aucun échantillon d'événement ▾

Tâche ▾ Mode Intelligent ▾

Événements (68 085) Patterns Statistiques Visualisation

✓ Format de la chronologie ▾ - Zoom arrière + Zoom sur la sélection × Annuler la sélection

1 heure par colonne

Format ▾ Afficher : 50 par page ▾ Afficher : Liste ▾

Precedent 1 2 3 4 5 6 7 8 Suivant ▾

CHAMPS SÉLECTIONNÉS	i Durée	Événement
# Action 2 # field@100+ # host 1 # index 1 # interface 3 # IP_dst 38 # IP_src 12 # PORT_src 100+ # Protocol 6 # source 1 # sourcetype 1	23/01/2025 18:32:43,000	host = <b>10.42.0.2</b> index = <b>firewall</b>   source = <b>udp:7001</b>   sourcetype = <b>pfSense_firewall</b>
	23/01/2025 18:32:43,000	host = <b>10.42.0.2</b> index = <b>firewall</b>   source = <b>udp:7001</b>   sourcetype = <b>pfSense_firewall</b>
	23/01/2025 18:32:43,000	host = <b>10.42.0.2</b> index = <b>firewall</b>   source = <b>udp:7001</b>   sourcetype = <b>pfSense_firewall</b>
	23/01/2025 18:32:43,000	host = <b>10.42.0.2</b> index = <b>firewall</b>   source = <b>udp:7001</b>   sourcetype = <b>pfSense_firewall</b>
	23/01/2025 18:32:43,000	host = <b>10.42.0.2</b> index = <b>firewall</b>   source = <b>udp:7001</b>   sourcetype = <b>pfSense_firewall</b>
	23/01/2025 18:32:42,000	host = <b>10.42.0.2</b> index = <b>firewall</b>   source = <b>udp:7001</b>   sourcetype = <b>pfSense_firewall</b>
	23/01/2025 18:32:42,000	host = <b>10.42.0.2</b> index = <b>firewall</b>   source = <b>udp:7001</b>   sourcetype = <b>pfSense_firewall</b>

NB: dans notre démo on a dénommé l'index "firewall"

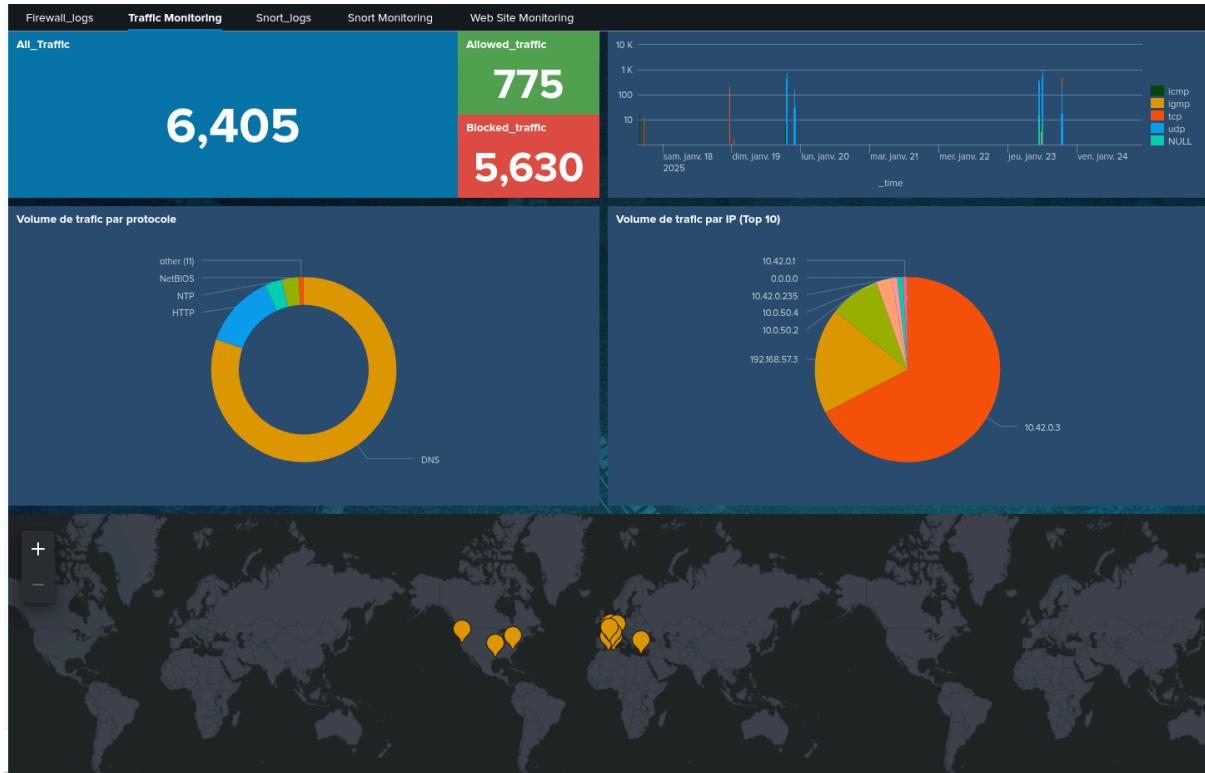
Remarque: comme vous constatez dans la recherche ci-dessus, les champs essentiels d'un log firewall ne sont pas automatiquement extraits. Subséquemment, pour éviter à chaque fois d'extraire ces derniers, on a créé ce qu'on appelle une requête SPL qui extrait les champs importants (tel que : src\_ip, dest\_ip, src\_port, ..etc) en utilisant des expressions régulières, voici une illustration d'un exemple concret:

NB: pour plus d'informations sur les requêtes SPL, consultez ce lien:  
<https://blog.alphorm.com/comprendre-langage-spl-commandes-pipelines>

### 2.2.3 Création de tableaux de bord

1. Accéder à l'outil de visualisation
  - Depuis l'interface Splunk, allez dans :
    - Dashboards → Create New Dashboard.
2. Ajout de graphiques
  - Sélectionnez un nom et une disposition (par exemple : grille simple, plusieurs colonnes, etc.).
  - Ajoutez des visualisations :
    - Utilisez les requêtes Splunk Processing Language (SPL), en utilisant les recherches sauvegardées comme mentionné ci-dessus.
    - Exemple de requête SPL pour visualiser le trafic réseau :  
`index=pfsense_logs sourcetype=firewall_logs | stats count by src_ip, dest_ip`
  - Sélectionnez le type de graphique (barres, courbes, camembert, etc.).
3. Enregistrement et partage
  - Sauvegardez le tableau de bord et configurez les droits d'accès (privé, public, etc.).

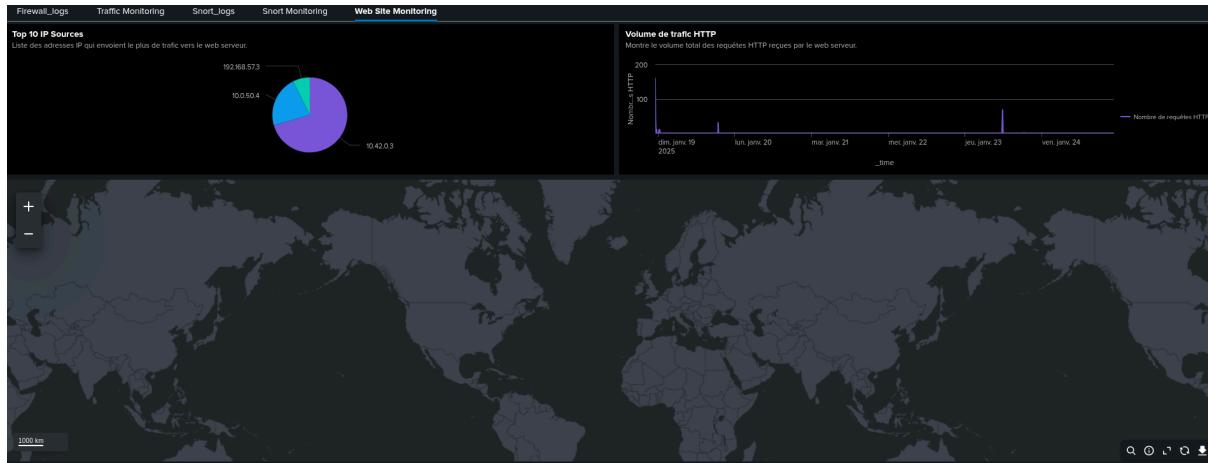
Un exemple de dashboard pour la surveillance du trafic firewall:



### Un exemple de dashboard pour la surveillance du trafic Snort:



## Un dernier exemple de dashboard pour la surveillance du trafic entrant vers la DMZ (site web):



### 2.2.4 Création des alertes

La création d'alertes dans Splunk permet de surveiller en temps réel les événements spécifiques dans les logs, tels que les anomalies de trafic ou les alertes générées par des systèmes de détection d'intrusion comme Snort. Cette section décrit le processus de création d'alertes basées sur des événements, avec un focus particulier sur les alertes Snort.

#### 1. Détection des alertes Snort dans Splunk

Snort, en tant que système de détection d'intrusions, génère des alertes pour chaque tentative d'attaque détectée. Ces alertes sont ensuite collectées et envoyées à Splunk, où elles sont indexées et peuvent être utilisées pour détecter des comportements malveillants en temps réel. La première étape consiste à s'assurer que les logs Snort sont correctement envoyés à Splunk. Cela peut être réalisé via :

- Fichiers de logs générés par Snort (ex. : /var/log/snort/alert).
- Envoi des logs via Syslog qui est notre cas.
- Récupération des logs depuis une base de données.

#### 2. Création de la recherche Splunk

Une fois les logs Snort intégrés, la recherche suivante permet d'identifier les alertes générées par Snort dans Splunk :

```
index=snort sourcetype=snort_alert  
| table _time src_ip dest_ip signature priority
```

Cette recherche extrait des informations pertinentes des alertes, telles que l'heure, les IP source et destination, la signature de l'attaque et la priorité. Cela permet de suivre les attaques détectées par Snort et d'analyser les patterns.

### 3. Configuration de l'alerte dans Splunk

Une fois la recherche définie, elle peut être transformée en alerte en suivant les étapes suivantes :

1. Enregistrement de la recherche comme alerte : La recherche est enregistrée sous forme d'alerte en temps réel ou planifiée.
2. Paramétrage des conditions de déclenchement : L'alerte se déclenche dès qu'un événement correspond à la recherche, par exemple, une alerte Snort détectée dans les logs.
3. Actions de l'alerte : Les actions incluent l'envoi d'un email à l'équipe de sécurité, l'exécution de scripts automatiques ou l'intégration avec des systèmes de communication tels que Slack ou Microsoft Teams.

Exemple de configuration d'une alerte par email pour une alerte Snort :

- Objet de l'email : "Alerte critique : Détection Snort"
- Contenu de l'email : Détails des alertes avec les informations clés (signature, IP source et destination).

### 4. Amélioration de l'alerte

Des filtres peuvent être ajoutés à la recherche pour affiner les alertes, par exemple en surveillant uniquement les alertes de haute priorité ou en filtrant les alertes répétées d'une même source IP. Ces ajouts permettent d'éviter les faux positifs et de se concentrer sur les événements les plus critiques.

### 5. Démonstration

- Création de l'alerte: Une fois qu'on a extrait les champs qui nous intéressent et définir dans notre cas c'est quoi un trafic anormal, on enregistre sous comme alerte.

## Enregistrer en tant qu'alerte

X

Titre	Trafic anormal détecté	
Description	Nombre anormal de trafic est détecté	
Permissions	Prive	Partagé dans l'app
Type d'alerte	Planifié	Temps réel
Expire	24	heure(s) ▾
<b>Conditions de déclenchement</b>		
Déclencher l'alerte quand	Nombre de résultats ▾	
	est supérieur à ▾	0
en	1	minute(s) ▾
Déclencher	Une fois	Pour chaque résultat
Throttle ?	<input type="checkbox"/>	
<b>Déclenchement d'Actions</b>		
Au déclenchement	<input checked="" type="checkbox"/> Ajouter aux alertes déclenchées <span style="float: right;">Retirer</span>	
	Gravité	Élevée ▾
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">Annuler</span> <span style="background-color: #28a745; color: white; border: 1px solid #28a745; padding: 2px 10px; font-weight: bold;">Enregistrer</span>		

# Chapitre 3 : Simulation d'attaque et alerting Splunk

## 3.1 Méthodologie de la simulation d'attaque

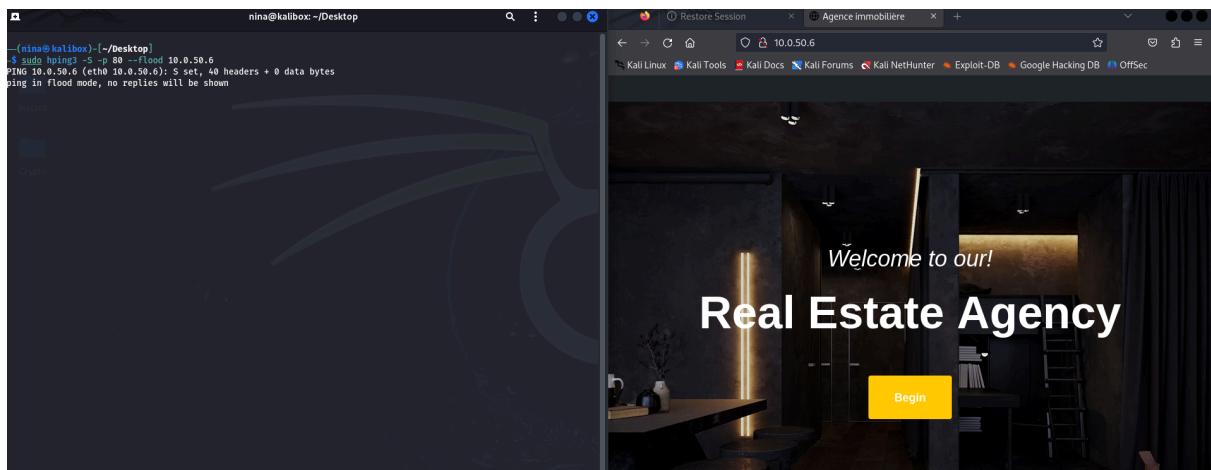
Dans le cadre de ce projet, nous avons simulé une attaque de type DoS (Denial of Service) pour évaluer l'efficacité de notre système de surveillance et d'alerting en temps réel configuré sur Splunk. L'objectif de cette simulation est de vérifier si l'attaque peut être détectée et analysée via les tableaux de bord que nous avons créés.

Pour cela, une machine virtuelle Kali Linux connectée au réseau WAN a été utilisée en tant qu'attaquant. Cette machine a lancé une attaque DoS contre le site web hébergé dans la DMZ. Nous avons choisi l'outil hping3, qui permet de générer un flux important de trafic malveillant, rendant le site web cible indisponible pour les utilisateurs légitimes.

## 3.2 Mise en œuvre de l'attaque avec hping3

Depuis la machine Kali, l'outil hping3 a été configuré pour cibler l'adresse IP du serveur web en utilisant l'attaque par synflood.

La commande utilisée permet de générer un trafic saturant les ressources du serveur web, provoquant ainsi une indisponibilité temporaire du site web..



## 3.3 Surveillance et alertes sur Splunk

Grâce à l'intégration de Splunk avec notre architecture réseau, nous avons pu visualiser et analyser l'attaque en temps réel. Voici comment nous avons procédé :

### 3.3.1 Monitoring des logs Snort

Une partie de nos tableaux de bord Splunk est consacrée à la visualisation des logs générés par Snort, permettant de détecter et d'analyser les activités suspectes. Lors de l'attaque DoS, nous avons pu identifier immédiatement l'activité malveillante grâce aux visualisations suivantes :

- Un camembert : Celui-ci met en évidence le top 10 des adresses IP ayant généré le plus de trafic. Nous avons constaté que l'adresse IP 10.0.50.4, correspondant à la machine de l'attaquant (Kali Linux), était la source principale des logs.
- Un diagramme en donut : Ce graphique regroupe les alertes par catégorie, notamment les types de menaces détectées par Snort. Lors de notre simulation, l'attaque DoS a été identifiée comme l'activité principale, ce qui a confirmé la nature malveillante de ce trafic.

Ces visualisations ont permis de détecter l'adresse IP de l'attaquant et de caractériser l'attaque en temps réel, facilitant une réponse rapide.



### 3.3.2 Visualisation du trafic web

Une autre section des tableaux de bord Splunk est dédiée à l'analyse du trafic web, collecté à partir des logs du serveur Apache. Ces outils nous permettent de surveiller l'activité sur le site web hébergé dans la DMZ et de détecter tout comportement anormal. Voici les éléments clés :

- Un diagramme linéaire : Il montre l'évolution du trafic web toutes les trois minutes. Lors de l'attaque DoS, nous avons observé un pic soudain et anormal de trafic correspondant à l'inondation du serveur par des requêtes malveillantes.
- Un camembert : Il affiche le top 10 des adresses IP générant le plus de trafic web. L'adresse IP 10.0.50.4 est apparue comme la principale source de trafic, confirmant son rôle dans l'attaque.

### 3.3.3 Alertes automatiques générées par Splunk

Grâce aux alertes automatiques configurées dans les étapes précédentes, nous avons pu identifier l'attaque DoS dès son déclenchement. Splunk, en analysant les logs en temps réel, a détecté un comportement anormal lié au trafic réseau et a immédiatement généré une alerte.

Voici une capture d'écran de l'alerte reçue au moment de l'attaque :

Cette fonctionnalité d'alerte en temps réel a renforcé notre capacité à réagir rapidement, en nous fournissant des informations clés sur l'incident dès qu'il s'est produit.

## Conclusion

Ce projet de surveillance en temps réel avec Splunk a permis de démontrer l'efficacité de l'architecture réseau mise en place, associée à des outils tels que pfSense et Snort, pour garantir la sécurité et la visibilité des activités réseau. À travers l'implémentation de VLANs, d'une DMZ sécurisée et de règles de pare-feu rigoureuses, nous avons pu segmenter efficacement le réseau et protéger les systèmes critiques contre les menaces potentielles.

L'intégration de Splunk a offert une vue centralisée et détaillée sur les logs réseau, permettant une analyse en temps réel et la détection proactive d'anomalies, comme en témoignent les tableaux de bord et les alertes automatiques. La simulation d'une attaque DoS a illustré la capacité de notre système à identifier rapidement les comportements malveillants et à fournir les informations nécessaires pour une réaction rapide.

En conclusion, ce projet met en lumière l'importance de combiner des solutions technologiques robustes avec des stratégies de sécurité bien pensées pour protéger les infrastructures réseau. Les résultats obtenus soulignent l'utilité de Splunk comme outil polyvalent pour la cybersécurité et la gestion des systèmes informatiques modernes.

## Références

- [1] S. Pilarski, *Data Science and Analytics in IT Management*, 2nd ed., Wiley, 2021, p. 123-126.
- [2] Splunk Inc., *Splunk Product Overview*, 2023.
- [3] K. Martinez, *Data Analytics in Modern Systems*, Springer, 2019, p. 45-48.
- [4] M. Richards, *Log Management Solutions*, CRC Press, 2020, p. 112-118.
- [5] R. Kelsey, *Visualization for Decision Making*, McGraw Hill, 2022, p. 110-112.
- [6] M. Hart, *IT Security Management Practices*, Academic Press, 2020, p. 90-102.
- [7] D. Brown, *Distributed Systems and Data Management*, Cambridge University Press, 2021, p. 56-62.