Département du Système d'Information

CONTEXTE	●	**Serveur Wazuh**
SUJET	●	**Mise en service**

Référence	●	*xxx - document d'architecture technique.docx*
Version	●	2
Statut	●	Terminé
Créé le	●	*06/06/2024 11:36:00*
Par	●	ISMAILI Yanisse
Mis à jour le	●	*17/06/2024 21:40:00*
Par	●	ISMAILI Yanisse
Validé le	●	*17/06/2024 21:40:00*
Par	●	ISMAILI Yanisse
Diffusé le	●	*10/06/2024*
À	●	Julien LALLEMAND
Péremption, archivage et restriction de diffusion	●	Diffusion interne

Nature de la restriction : confidentiel, diffusion restreinte, diffusion interne, restriction annulée

Table des mises à jour du document

version	date	objet de la mise à jour
01	06/06/2024	Version initiale
02	16/06/2024	Version finale
03	17/06/2024	Version Corrigée

Table des matières

Table des figures

Document d'architecture technique

1- Fonctionnalité et domaine applicatif

Cocher la case correspondante

Domaine Data Management/aide à la décision	
Domaine Investigation clinique	
Domaine Informatique scientifique	
Domaine Support aux départements	
Domaine Outils collaboratifs et audiovisuels	X
Secteur Infrastructure logicielle	
Secteur Infrastructure réseau	X
Secteur Ingénierie poste de travail	

2- Architecture matérielle

L'architecture matérielle pour le serveur wazuh comprend :

- **Serveur physique** : Un serveur dédié pour héberger l'infrastructure virtuelle.
- **Hyperviseur** : Utilisation de Oracle VM VirtualBox pour la virtualisation.
- **Switch** : Un switch 10Gb de 24 ports
- **Routeur** : routeur NetGate 4200
- **VM Serveur Wazuh**: Une VM dédiée à l'hébergement du service Wazuh.
- **VPN** : Utilisation de WireGuard pour la connexion à distance au service Wazuh
- **Stockage** : Disques SSD pour le stockage des données avec des sauvegardes répliquées sur un bucket s3.

3- Architecture logicielle

- **Système d'exploitation du serveur** : Windows 10
- **Wazuh**: Version 4.3.

- **système d'exploitation du routeur** : pfSense 1.7.2
- **hyperviseur:** Oracle VM VirtualBox 7.0.X
- **VPN:** WireGuard 1.0.X

4- Architecture réseau et sécurité

Schéma réseau :

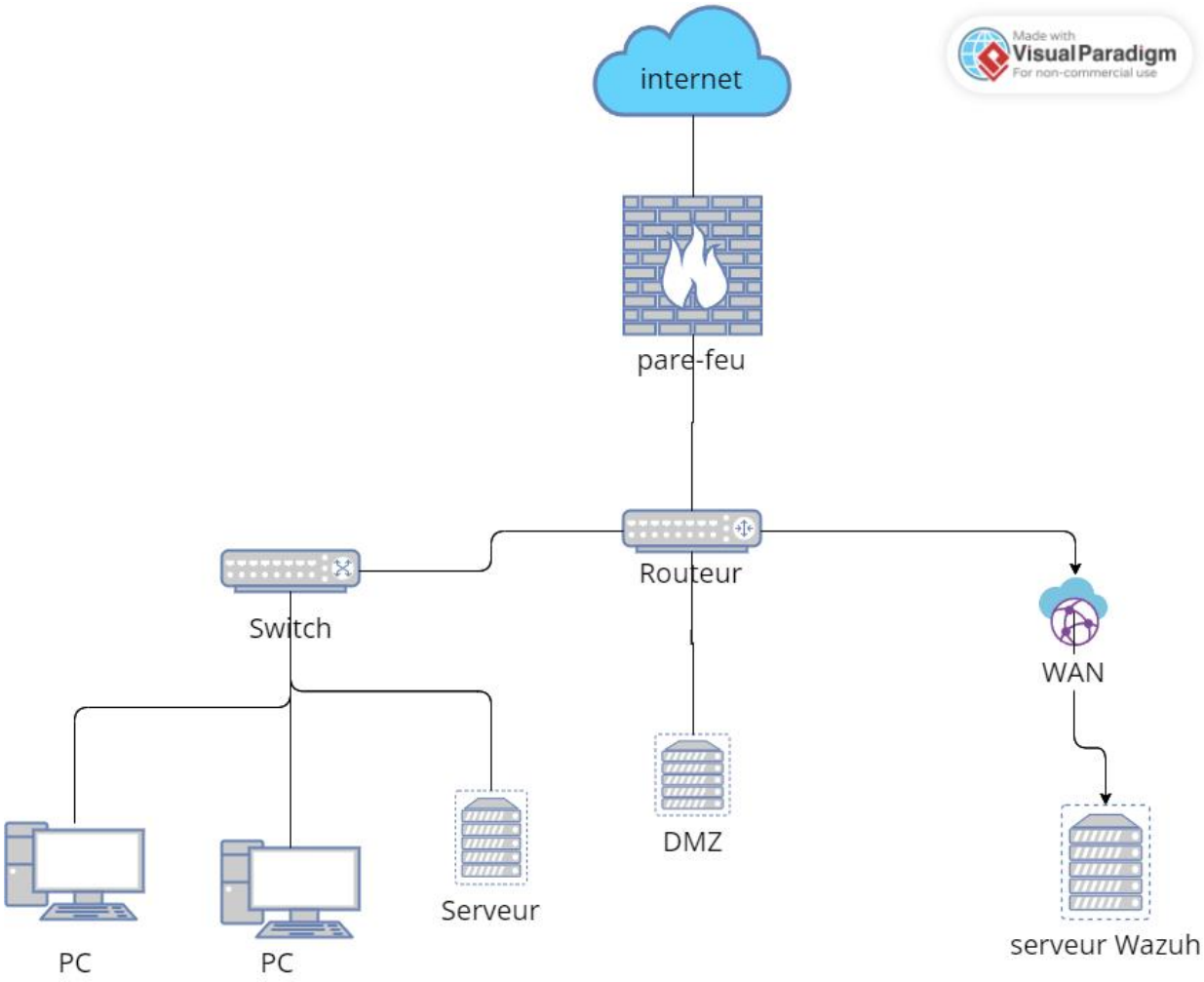

Figure 1 : Schéma réseau de la mise en place server Wazuh

Plan d'adressage IP :

Composant	Adresse IP	Remarques
Routeur (WAN)	203.0.113.20	Adresse IP publique
Routeur (LAN)	192.168.10.1	Passerelle par défaut
Routeur (DMZ)	192.168.20.1	Interface DMZ
Serveur Wazuh (DMZ)	192.168.20.10	Hébergement Wazuh
Postes de Travail (LAN)	192.168.10.100-199	DHCP
Serveurs Internes (LAN)	192.168.10.200-254	Adresses IP statiques
Pool VPN	192.168.30.0/24	Pour les utilisateurs VPN

Figure 2 : Plan d'adressage IP

Règles de sécurité du pare-feu :

- **Règles d'accès externe** : Seul le trafic HTTPS (port 443) est autorisé vers le serveur wazuh.
- **Règles internes** : Le trafic entre le LAN et le DMZ est restreint aux ports nécessaires (par exemple, 80, 443 pour le web).
- **VPN** : Accès VPN configuré pour les utilisateurs distants avec authentification forte (wireguard).

5- Organisation des données

- **Stockage principal** : Les fichiers utilisateurs sont stockés sur des disques SSD pour des performances optimales.

6- Installation

Installation de l'environnement

1. **Préparation de l'environnement** :
    - Installer Wazuh Manager sur la VM Windows 10.
    - Mettre à jour le système (Windows Update).

- Télécharger et installer l'agent Wazuh sur les systèmes à surveiller

Téléchargement et installation de Wazuh:

- Téléchargez le package Wazuh pour Windows depuis le site officiel de Wazuh
- Installez le Wazuh Manager en suivant les instructions fournies dans la documentation officielle.
- Installez l'agent Wazuh sur les autres machine que vous souhaiter surveiller

Configuration de base

1. Configurer le Wazuh Manager :

- Modifiez le fichier de configuration «ossec.conf» pour définir les règles de collecte des journaux.
- Exemple de configuration pour la collecte des logs système:

```
<localfile>
  <log_format>syslog</log_format>
  <location>C:\Windows\System32\winevt\Logs\Security.evtx</location>
</localfile>
```

2. **Démarrer le Wazuh Manager** :
   - Lancez le service du Wazuh Manager et assurez-vous qu'il fonctionne correctement.

3. **Configurer les agents wazuh :**
   - Éditez le fichier «ossec.conf» sur chaque agent pour définir les fichiers de journaux à surveiller
   - Assurez-vous que chaque agent est configuré pour communiquer avec le Wazuh Manager.

7- Configuration

1. Intégration avec Elastic stack

- Téléchargez et installez Elasticsearch et kibana depuis le site officiel d'Elastic.
- Configurez Elasticsearch pour recevoir les données de Wazuh.
- Configurez Kibana pour visualiser les données stockées dans Elasticsearch.

2. Configurer wazuh pour envoyer des log a Elasticsearch

output:

elasticsearch:

hosts: ['http://localhost:9200']

3. Configurer les alertes et notification

- Créez des règles d'alerte dans Wazuh pour détecter des événements spécifiques, tels que des tentatives de connexion échouées.
- Configurez des notifications par e-mail ou via des outils de communication comme slack ou Microsoft TEAMS.

Sécurisation et optimisation

1. Rotation et purge des logs

- Configurez des politiques de rotation des logs pour éviter l'accumulation excessive de données.
- Exemple de script de rotation :

logrotate -f /etc/logrotate.d/wazuh

2. Audits et rapports

- Programmez des audits réguliers des journaux pour verifier les configurations et détecter les anomalies.
- Génération de rapports périodiques pour l'analyse des tendances et la planification proactive des action correctives.

3. Optimisation des performances

- Ajustez les paramètres de collecte et de stockage des logs pour optimiser les performances (par exemple, taux de collecte, taille des index Elasticsearch).
- Utilisez des techniques de compression et d'archivage pour gérer efficacement l'espace de stockage.

8- Sources d'informations

- **Documentation officielle Wazuh:**

https://documentation.wazuh.com/current/index.html

- **Guide d'installation d'Elasticsearch et Kibana:**

https://www.elastic.co/guide/en/kibana/current/windows.html

https://www.elastic.co/guide/en/elasticsearch/reference/current/zip-windows.html

- **Guide d'installation de WireGuard :**

https://www.wireguard.com/install/

- **Documentation de pfSense :**

https://docs.netgate.com/pfsense/en/latest/

Remarque : Cette documentation vous guide à travers l'installation, la configuration et la gestion de Wazuh pour une surveillance efficace de votre infrastructure Windows 10. Si vous avez des questions ou besoin de clarifications supplémentaires, n'hésitez pas à demander.