SAÉ 5CYBER03

Sécurisation & Supervision avancée d'un système d'information

Dossier architecture technique

UNIVERSITÉ DE LA RÉUNION

BLUE WAVE LOGISTICCS

Sommaire :

Introduction..... 3
1 - Architecture Logique..... 4
1.1 Plan d'adressage Vlan :..... 4
1.2 Adressage des machines :..... 4
2 - Topologie réseau..... 5
2.1 Zone Technique..... 5
2.2 Zone de Service..... 6
2.3 Zone Frontale..... 6
2.4 Zone SOC (Security Operations Center)..... 6
2.5 Bastion..... 7
3 - Windows Server..... 7
3.1 Structure de l'Active Directory..... 7
3.1.1 Utilisateur, OU, tiering..... 7
3.2 Dossiers partagés..... 8
3.2.1 Description des dossiers partagés..... 8
4 - Wazuh Agent..... 10
5 - Firewall..... 11
5 - Liste des Connexions Guacamole..... 13
6 - Bibliographie..... 14

Introduction

Ce document technique a pour objectif de présenter l'architecture informatique mise en place. Il vise à fournir une vue d'ensemble claire et structurée des différents composants et configurations essentiels assurant le bon fonctionnement et la sécurité de notre infrastructure réseau.

Dans un premier temps, le plan d'adressage sera détaillé afin de clarifier l'organisation des adresses IP attribuées et leur répartition au sein des différents segments du réseau. Les VLAN seront également décrits pour optimiser la performance et renforcer la sécurité.

La configuration de l'Active Directory permettra de comprendre la gestion centralisée des utilisateurs et des ressources, facilitant ainsi l'administration et le contrôle des accès. Une section dédiée aux utilisateurs détaillera les différents types de comptes et leurs permissions, garantissant une gestion efficace des droits d'accès.

Les différentes couches de sécurité (tiers) mises en place seront exposées, mettant en lumière les mesures adoptées pour protéger l'infrastructure contre les menaces internes et externes. L'intégration des agents Wazuh sera aussi abordée, illustrant notre approche proactive en matière de surveillance et de détection des incidents de sécurité.

Enfin, les flux de firewall autorisés seront spécifiés, définissant les règles de trafic réseau autorisées et assurant une barrière fiable contre les accès non autorisés.

Ce document est destiné aux équipes techniques et aux parties prenantes impliquées dans la gestion et la maintenance de l'infrastructure informatique, leur fournissant les informations nécessaires pour comprendre, évaluer et optimiser l'architecture actuelle.

1 - Architecture Logique

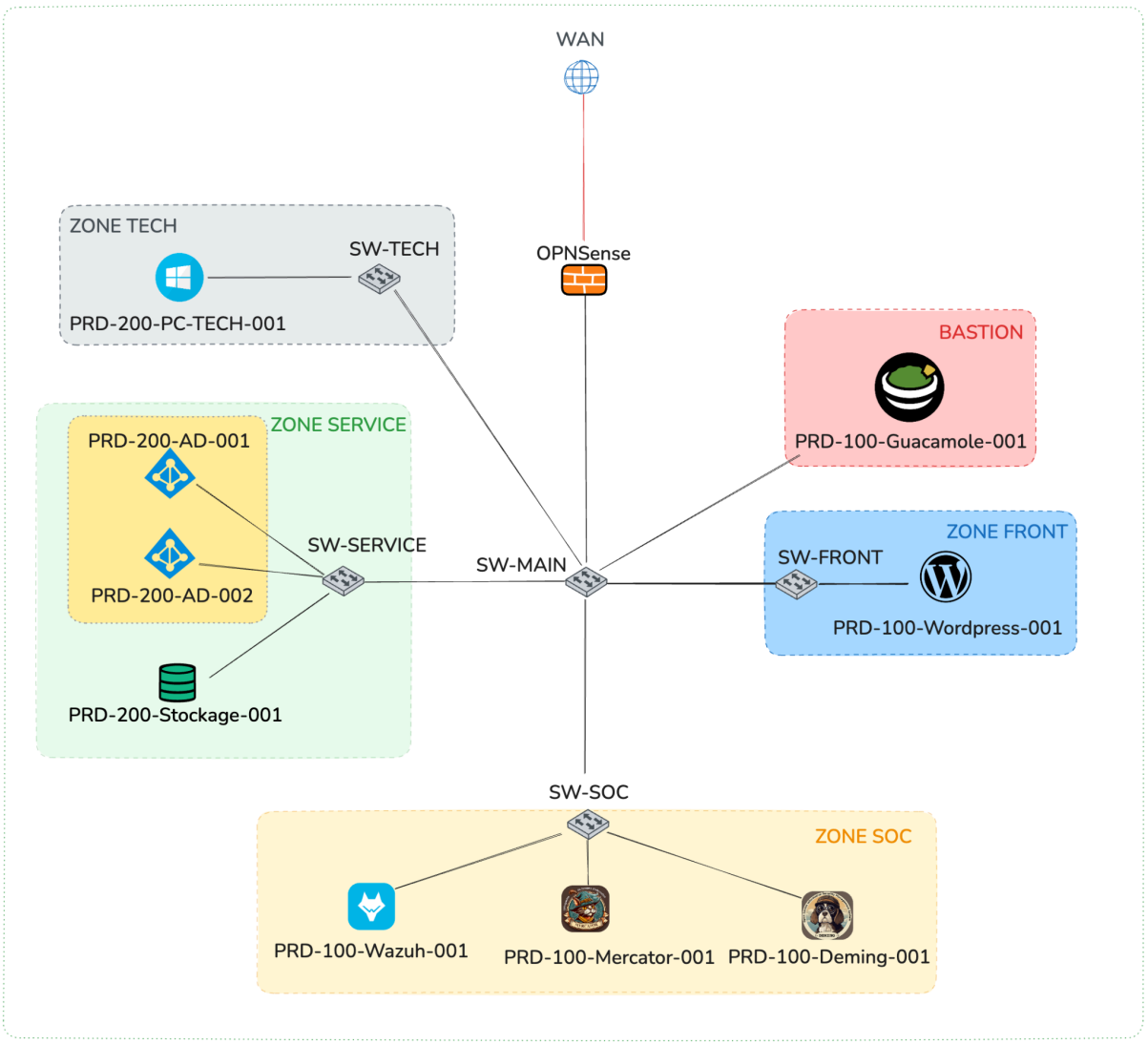
1.1 Plan d'adressage Vlan :

Vlan ID	Nom du VLAN	Sous-réseau (CIDR)	Passerelle
10	ZONE SOC	192.168.10.0/24	192.168.10.1
20	ZONE SERVICE	192.168.20.0/24	192.168.20.1
30	ZONE FRONT	192.168.30.0/24	192.168.30.1
40	BASTION	192.168.40.0/24	192.168.40.1
50	ZONE TECH	192.168.50.0/24	192.168.50.1

1.2 Adressage des machines :

Vlan ID	Machine	IP (CIDR)	Passerelle
10	PRD-100-Wazuh-001	192.168.10.254/24	192.168.10.1
10	PRD-100-Mercator-001	192.168.10.252/24	192.168.10.1
10	PRD-100-Deming-001	192.168.10.251/24	192.168.10.1
20	PRD-200-AD-001	192.168.20.254/24	192.168.20.1
20	PRD-200-AD-002	192.168.20.250/24	192.168.20.1
20	PRD-200-Stockage-001	192.168.20.252/24	192.168.20.1
30	PRD-100-Wordpress-001	192.168.30.254/24	192.168.30.1
40	PRD-100-Guacamole-001	192.168.40.254/24	192.168.40.1
50	PRD-200-Poste-TECH-001	192.1168.50.0/24	192.1168.50.1

2 - Topologie réseau



L'infrastructure est composée des zones suivantes

2.1 Zone Technique

- **Poste Windows des Techniciens**

  Poste de travail dédié aux techniciens pour la maintenance, la gestion et le support technique de l'infrastructure.

2.2 Zone de Service

- **Serveurs Windows avec Active Directory (AD)**
  Deux serveurs AD sont déployés pour assurer la redondance et garantir la disponibilité continue des services d'annuaire. Ils gèrent les identités, l'authentification des utilisateurs et les politiques de sécurité au sein du réseau, offrant ainsi une résilience accrue en cas de défaillance d'un serveur.

- **Serveur de stockage Windows Server**
  Permet l'accès, la centralisation et la gestion d'accès des ressources partagées des différents pôles de l'entreprise ainsi que le stockage des backup des serveurs ayant le rôle Active Directory

2.3 Zone Frontale

- **Serveur WordPress en DMZ**
  Héberge le site WordPress accessible depuis Internet, isolé du reste de l'infrastructure pour renforcer la sécurité.

2.4 Zone SOC (Security Operations Center)

- **Serveur WAZUH**
  Plateforme de détection des intrusions et de surveillance de la sécurité en temps réel.

- **Serveur de Monitoring (Deming)**
  Utilisé pour assurer la conformité avec les normes ISO27001. Ce serveur supervise les processus et les contrôles nécessaires pour répondre aux exigences de sécurité et de gestion des informations stipulées par la norme ISO27001, facilitant ainsi les audits et la maintenance de la conformité.

- **Serveur Mercator**

  Responsable de la cartographie de l'infrastructure. Mercator permet de visualiser et de gérer les différentes composantes de l'infrastructure et déterminer la criticité des actifs et applicatif

2.5 Bastion

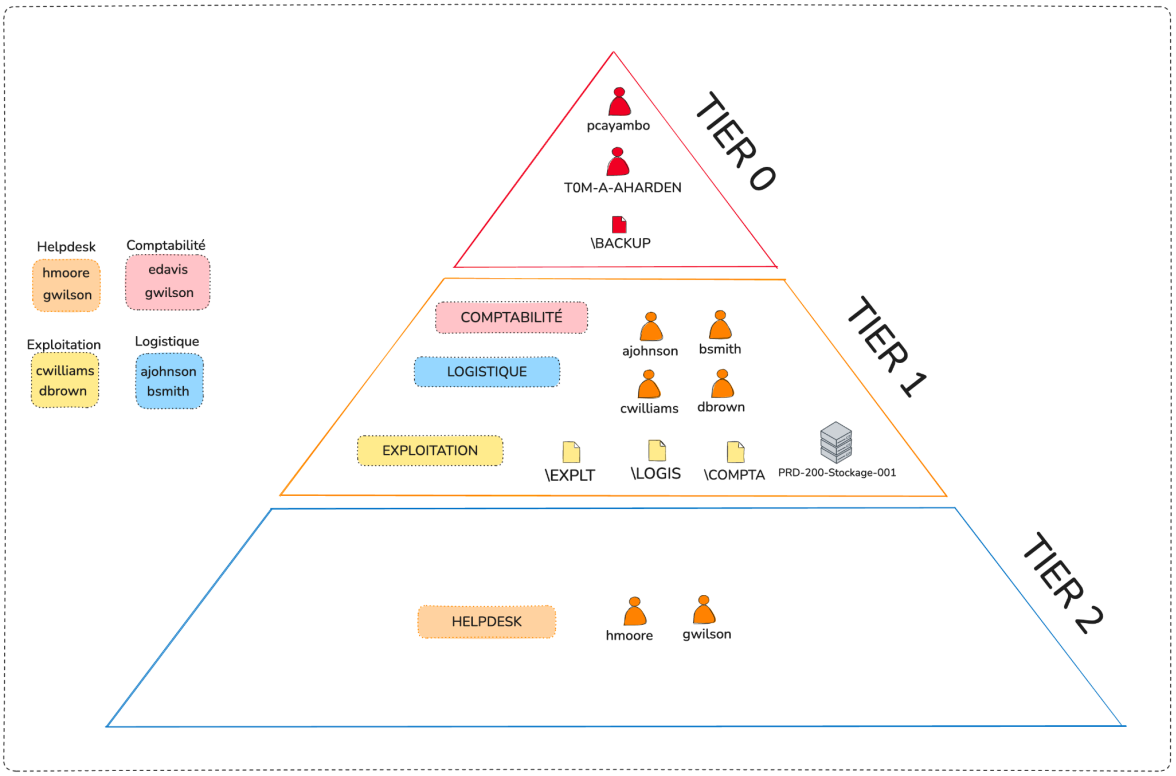
- **Apache Guacamole**
  Passerelle d'accès sécurisé permettant les connexions RDP et SSH aux serveurs via une interface web centralisée.

3 - Windows Server

3.1 Structure de l'Active Directory

3.1.1 Utilisateur, OU, tiering

L'annuaire Active Directory a été créé suivant le modèle de "tiering" suivant avec les utilisateurs et OU que sur le schéma ci-contre.



Tier 0 : Niveau Critique

Ressources : Contrôleurs de domaine, comptes administratifs hautement privilégiés

Rôle : Gestion de la sécurité globale et des accès principaux. Protection des infrastructures essentielles contre les compromissions.

Tier 1 : Niveau Serveurs et Applications

Ressources : Serveurs de fichiers (comme le serveur SMB), bases de données, applications métiers critiques.

Rôle : Administration et maintenance des serveurs et applications.

Tier 2 : Niveau Postes de Travail et Utilisateurs

Ressources : Ordinateurs de bureau, comptes utilisateurs, support, helpdesk.

Rôle : Gestion quotidienne des postes de travail et assistance aux utilisateurs. Limitation des privilèges pour réduire les risques de compromission.

3.2 Dossiers partagés

Les dossiers partagés suivants sont hébergés sur le serveur réseau **srv-stockage.pixelberry.com** et sont accessibles uniquement aux membres des groupes correspondants :

Nom du dossier	Groupe d'accès	Chemin d'accès
Comptabilité	Comptabilité	\\srv-stockage.pixelberry.com\COMPTA
Backup	T0-Admin	\\srv-stockage.pixelberry.com\BACKUP
Logistique	Logistique	\\srv-stockage.pixelberry.com\LOGIS
Exploitation	Exploitation	\\srv-stockage.pixelberry.com\EXPLT

3.2.1 Description des dossiers partagés

- **Comptabilité**
  Accessible uniquement aux membres du groupe Comptabilité. Ce dossier contient toutes les ressources nécessaires pour les opérations comptables.

- **Backup Active Directory**
  Réservé aux membres du groupe T0-Admin, ce dossier stocke les sauvegardes de l'Active Directory, assurant ainsi la restauration en cas de besoin.

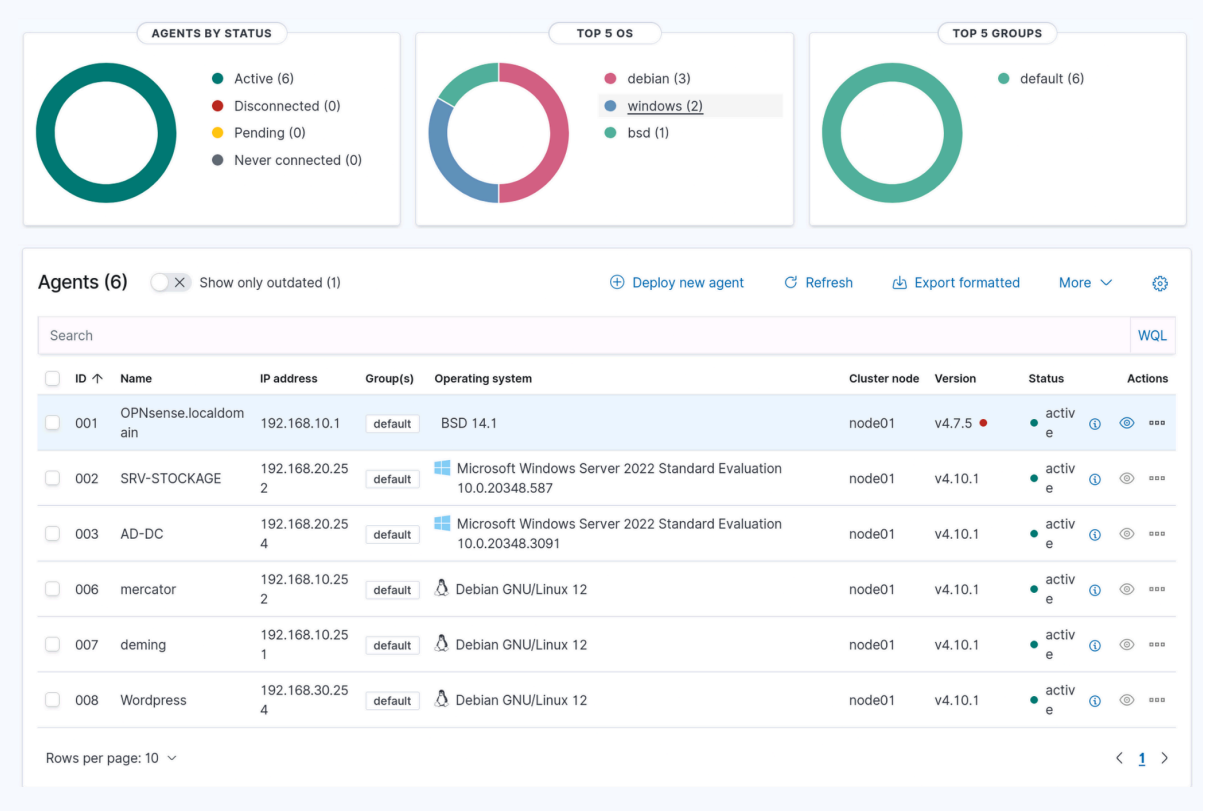
- **Logistique**

  Destiné aux membres du groupe Logistique, ce dossier centralise les documents et fichiers liés aux opérations logistiques de l'entreprise.

- **Exploitation**
  Accessible exclusivement aux membres du groupe Exploitation, ce dossier contient les informations et ressources nécessaires à la gestion des opérations quotidiennes.

4 - Wazuh Agent

Les agents wazuh sont installées sur les actifs suivants selon le dashboard de l'outil ci-dessous



Ces agents permettent de détecter et de remonter des alertes en cas d'intrusion comme le montre la capture ci-dessous

5 - Firewall

Un firewall OPNSense a été installé sur la topologie afin de filtrer les flux entrant, sortant et inter-zone. Les règles firewall sont disponibles dans le tableau ci-dessous

Interface USER				
Traffic	Source	Source Port	Destination	Dest Port
IN	USER net	Any	prd-200-ad-001 prd-200-ad-002	88/tcp+udp (kerberos)
IN	USER net	Any	prd-200-ad-001 prd-200-ad-002	389/tcp+udp (LDAP)
IN	USER net	Any	prd-200-ad-001 prd-200-ad-002	445/tcp+udp (SMB)

Interface SERVICE				
Trafic	Source	Source Port	Destination	Dest Port
IN	USER net	Any	prd-200-ad-001 prd-200-ad-002	389/tcp (LDAP)
IN	USER net	Any	prd-200-ad-001 prd-200-ad-002	445/tcp (SMB)
IN	prd-200-ad-001 prd-200-ad-002	Any	Any	53/tcp+udp (dns)
IN	prd-200-ad-001 prd-200-ad-002	Any	prd-100-wazuh-001	1514-1515/tcp+udp (Agent-Wazuh)
IN	prd-200-ad-001 prd-200-ad-002	Any	prd-100-wazuh-001	55000/tcp+udp (Api-Wazuh)

Interface FRONT				
Trafic	Source	Source Port	Destination	Dest Port
IN	prd-100-wordpress-001	Any	prd-100-wazuh-001	1514-1515/tcp+udp (Agent-Wazuh)
IN	prd-100-wordpress-001	Any	prd-100-wazuh-001	55000/tcp+udp (Api-Wazuh)

Interface WAN				
Trafic	Source	Source Port	Destination	Dest Port
IN	any	Any	prd-100-wordpress-001	80/tcp (http)
IN	any	Any	prd-100-wordpress-001	443/tcp (https)

Règle de NAT (port forward)				
Trafic	Source	Source Port	Destination	Dest Port
IN	wan address	Any	prd-100-wordpress-001	80/tcp (http)
IN	wan address	Any	prd-100-wordpress-001	443/tcp (https)

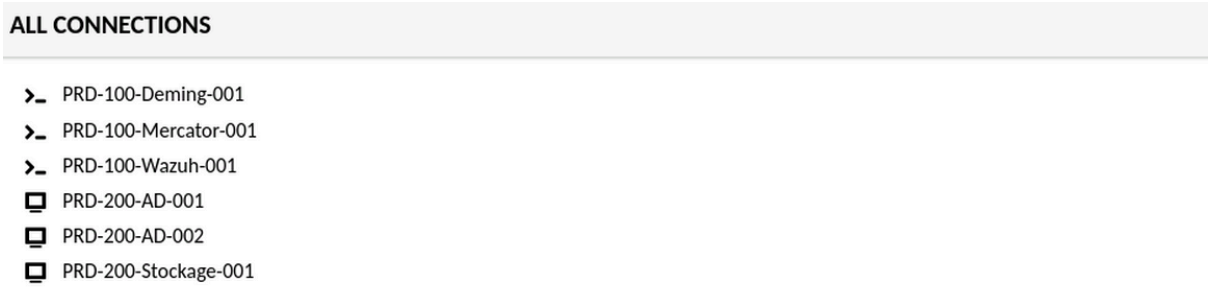
Floating				
Trafic	Source	Source Port	Destination	Dest Port
IN	USER net SOC net FRONT net SERVICE net	Any	Any	80/tcp (http)
IN	USER net SOC net FRONT net SERVICE net	Any	Any	443/tcp (https)
IN	USER net SOC net FRONT net SERVICE net	Any	prd-200-ad-001 prd-200-ad-002	53/udp+tcp (dns)

5 - Liste des Connexions Guacamole

Pour accéder aux différents serveurs, le poste autorisé pourrait utiliser les connexions suivantes.

: connexion SSH

: connexion RDP



Pour les connexions SSH, les utilisateurs sont contraints d'entrer les identifiants de chaque machine.

Dans le cas de l'utilisation d'une connexion RDP, les utilisateurs devront utiliser les identifiants de leur connexion Active Directory.

6 - Bibliographie

Mercator:
- Installation de mercator (documentation en français)

Deming:
- Installation de deming (documentation en français)

Apache guacamole:
- Documentation officielle
- Installation d'Apache Guacamole

Wazuh:
- Guide d'installation officiel

Wordpress:
- Guide d'installation officiel