DOSSIER TECHNIQUE

SAFEWAVE

IDRI NAHEL
FERAH JASSYM
DIMITRI BACOT
BACOT DIMITRI
GAMEZ ADRIEN
BOCHATON ALIZÉE

SOMMAIRE

1 - Fiche de contrôle du document

- *Caractéristiques du document :*

Synthèse	Description de l'infrastructure réseau et des dispositifs de sécurité configurés dans le cadre du projet "Techniques de sécurisation ISR"
Statut	En cours

- *Historique du document :*

Version	Date	Crée par	Modifications
1.1	20/02/2025	BOCHATON Alizée	Création du document

- *Liste de diffusion*

Nom	Contact
IDRI Nahel	nidri@guardiaschool.fr
BACOT Dimitri	dbacot@guardiaschool.fr
FERAH Jassym	jferah@guardiaschool.fr
GAMEZ Adrien	agamez@guardiaschool.fr
CIFELLI Damien	-
AKKOUCHE Adam	-

2 - Introduction

Ce document a été créé suite à la mise en place de l'infrastructure réseau demandée pour la réalisation du projet pédagogique "Techniques de sécurisation ISR" à Guardia Cybersecurity School.

2.1 *- Description générale*

L'infrastructure réseau est composée de 2 sous-réseaux, reliés par le firewall/routeur virtuel OPNsense:

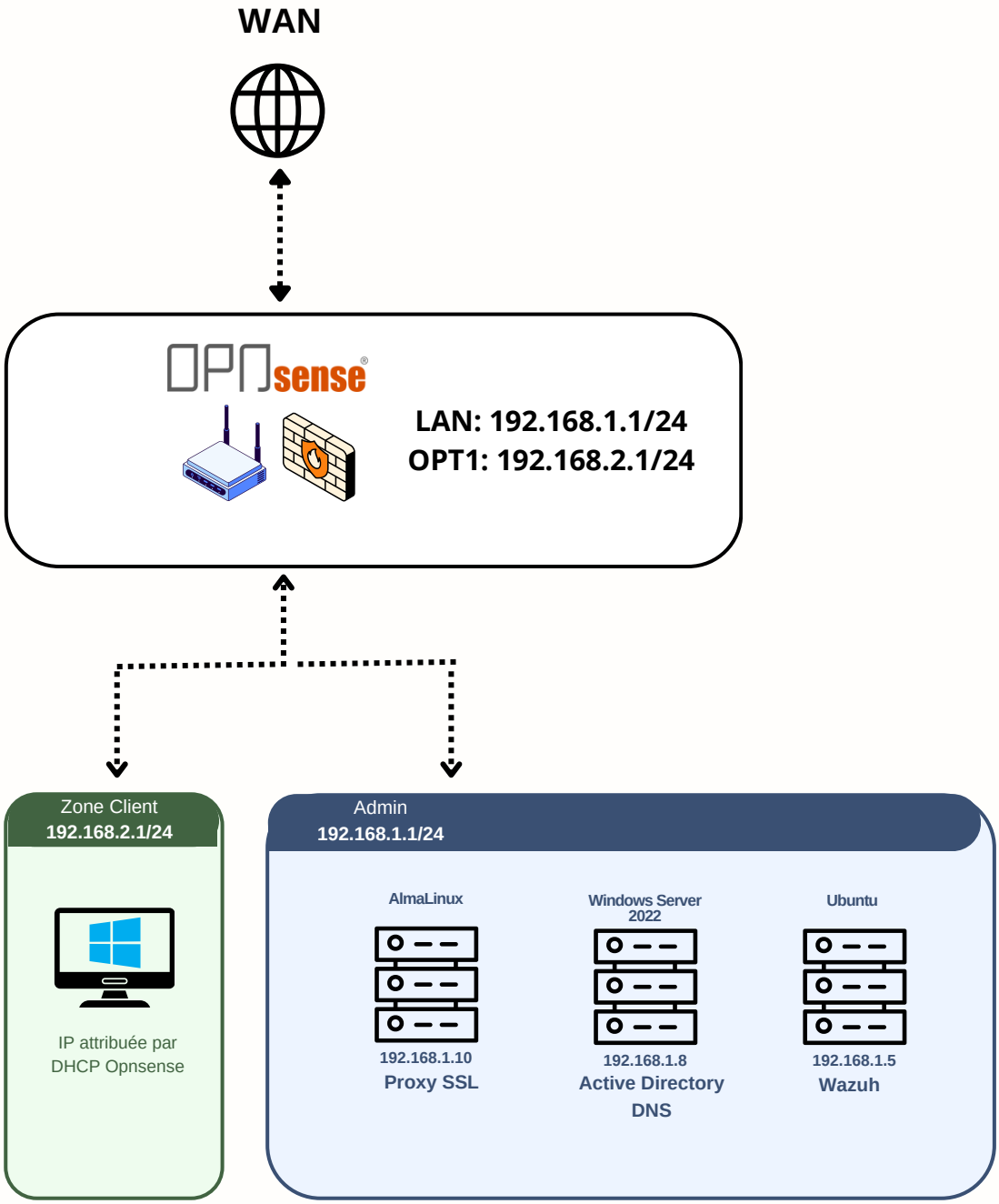
Sous-réseau	Ce qu'il contient	Interface réseau	IP de la passerelle
Zone Admin	• Une machine windows server (AD, DHCP, DNS) • Une machine Ubuntu (Wazuh) • Une machine AlmaLinux (Proxy Squid)	vmbr1	192.168.1.1/24
Zone Client	• Une machine Windows 10	vmbr0	192.168.2.1/24

2.2 - Périmètre du dossier

Ce document détaille les points suivants :

- Les caractéristiques des machines virtuelles mises en place
- L'ensemble de la configuration réseau
- Stratégie de sécurité mise en place
- Mise en place de Wazuh

3 - Schéma logique de l'infrastructure réseau



4 - Descriptif des machines virtuelles

L'infrastructure réseau est composée de 4 machines virtuelles :

4.1 *- Machine OPNSense*

Nom de la VM	100 (OPNSENSE)
Rôle	Firewall; routeur; proxy
OS	OPNSense
CPU	2 vCPU
RAM	2 Go
Stockage	16 Go
Adresse IP	192.168.1.1
Interface réseau	vmbr0 (bridge WAN); vmbr1; vmbr2
Logiciels et services	OPNSense

4.2 *- Machine Windows Server 1 - Administrateur*

Nom de la VM	101 (windowsserv1)
Rôle	DHCP; Active Directory
OS	Windows Server 2022
CPU	2 vCPU
RAM	2 Go
Stockage	32 Go
Adresse IP	192.168.1.8 (IP réservée)
Interface réseau	vmbr1
Logiciels et services	DHCP; Active Directory

4.3 *- Machine Windows 10 - Client*

Nom de la VM	103(WindowsClient)
Rôle	Poste utilisateur
OS	Windows 10
CPU	2 vCPU
RAM	2 Go
Stockage	32 Go
Adresse IP	192.168.2.2
Interface réseau	vmbr2
Logiciels et services	Navigateur, Session utlisateur

4.4 - Machine Ubuntu - Wazuh

Nom de la VM	102(Wazuh)
Rôle	Système de gestion des informations et des événements de sécurité
OS	Ubuntu
CPU	2 vCPU
RAM	4 Go
Stockage	100 Go
Adresse IP	192.168.1.5 (IP réservée)
Interface réseau	vmbr1
Logiciels et services	Wazuh

4.5 - Machine AlmaLinux - Proxy SSL

Nom de la VM	104(ServeurProxy)
Rôle	Proxy SSL
OS	AlmaLinux
CPU	3 vCPU
RAM	4 Go
Stockage	64 Go
Adresse IP	192.168.1.10 (IP réservée)
Interface réseau	vmbr1
Logiciels et services	Squid

5 - Descriptif des règles de pare-feu

5.1 - Règles de l'interface LAN

	Action	Interface	Direction	TCP/IP Version	Protocole	Source	Destination	Description
1	Pass	LAN	In	IPv4 + IPv6	any	any	any	Internet sur le LAN
2	Pass	LAN	Out	IPv4	any	any	192.168.1.5/24	Paquets vers Wazuh

5.2 - Règles de l'interface OPT1

	Action	Interface	Direction	TCP/IP Version	Protocole	Source	Destination	Description
1	Pass	OPT1	out	IPv4	any	OPT1 net	192.168.1.5/24	Paquets vers Wazuh
2	Pass	OPT1	in	IPv4 + IPv6	any	any	any	Autoriser Internet au client
3	Block	OPT1	in	IPv4	any	OPT1 net	205.251.207.238/32	Blocage d'amazon
4	Block	OPT1	in	IPv4	any	OPT1 net	66.254.114.41/32	Blocage d'un site pornographique

6 - Descriptif des services réseaux

6.1 - DHCP

Le DHCP distribue automatique une adresse IP au client lié à l'ad.

Pool d'adresse IP	192.168.2.1 - 192.168.2.244
Masque de sous-réseau	255.255.255.0
Durée du bail	8 jours

6.2 - Active directory

Nom du domaine	testserv.corp
Mode fonctionnel domaine	Windows server 2022
Mode fonctionnel forêt	Windows Server 2022
Nombre de contrôleurs de domaine	1

6.3 *- Wazuh*

Nous avons configuré des Wazuh-agent sur les machines windows server, client, et le proxy.

- Configuration des logs remontés par les Agents Wazuh

Canal d'événements	Emplacement	Format de log	Explication
1. Canal "Application"	Application	eventchannel	Événements relatifs eu fonctionnement des applications et des erreurs générées par celles-ci
2. Canal "Security"	Security	eventchannel	Tentatives de connexion, changements de mot de passe, accès aux ressources protégées • **Event ID exclus :** 5145; 5156; 5447; 4656; 4658; 4663; 4660; 4670; 4690; 4703; 4907; 5152; 5157
3. Canal "System"	System	eventchannel	Événements relatifs à l'OS (démarrages, arrêts, erreurs de services)
4. Canal "Microsoft-Windows-Powershell/Operational"	Microsoft-Windows-Powershell/Operational	eventchannel	Exécution de scripts Powershell (commandes, etc...)
5. Canal "Microsoft-Windows-Sysmon/Operational"	Microsoft-Windows-Sysmon/Operational	eventchannel	Processus de connexions réseau, modifications dans le système

L'accès du dashboard Wazuh se fait sur la machine Windows Server avec l'IP suivante:

192.168.1.5

Le dashboard permet de gérer la configuration de Wazuh et surveiller son état.

6.4 *- Proxy*

Element	Configuration
Réseaux internes autorisés	10.0.0.0/5 , 192.168.1.0/24
Ports autorisés	80, 443, 1025-65535
Sites bloqués	.youtube.com
Accès au cache	allow localhost manager
Accès par défaut	allow localhost manager
Limite de taille d'objet	50 MB
Configuration du port permettant la connexion au Proxy	192.168.1.10:3128