INFRA SI

HoneyPot

PentBox / honeypot

Mise en service

référence	*nils_jaudon_projet_infra_si.docx*
version	1.1
statut	
créé le	*13/06/2024 15:29:00*
par	Nils JAUDON
mis à jour le	*09/06/2024 17:21:00*
par	Nils JAUDON
validé le	*03/06/2024 17:21:00*
par	
diffusé le	16/06/2024
à	Jullien LALLEMAND
Péremption, archivage et restriction de diffusion	Usage interne

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

Table des matières

• Document d'architecture technique Projet Infra

• 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	
Secteur Infrastructure logicielle	X
Secteur Infrastructure réseau	X
Secteur Ingénierie poste de travail	

- ## Architecture matérielle

1. PC WINDOWS 10 (PHYSIQUE) (hôte)
1. VM VIRTUALBOX UBUNTU-LTS (virtuelle) (serveur)
1. VM VIRTUALBOX PFSENSE (Virtuelle) (pare feu)
1. VM VIRTUALBOX UBUNTU-LTS (virtuelle) (honeypot)

- ## Architecture logicielle

1. PC Windows 10
   - **Système d'exploitation :** Windows 10
   - **Rôle :** Utiliser l'administration et l'accès aux machines virtuelles.
   - **Logiciels :** Bureautique & VirtualBox.

Lien pour télécharger virtual box : https://www.virtualbox.org/

2. VM Virtual Box Ubuntu LTS (Miller)

   - **Système d'exploitation :** Ubuntu-LTS (64 bit)
   - **Rôle :** Machine interne principal de l'entreprise qui contient des informations confidentielles (base de données, site interne à l'entreprise, outil de gestion d'administration services de fichiers).
   - **Logiciels :**
     - Apache2 (serveur web)
     - Visual Studio Code : (Développement)
     - DataGrip : (Gestion de base de donnée)

3. VM Virtualbox Ubuntu LTS (Gargantua)

   - **Système d'exploitation :** Ubuntu-LTS (64 bit)
   - **Rôle :** Gargantua est une référence à interstellar, il agit comme un trou noir, configuré pour simuler des services et des vulnérabilités afin **d'attirer** les attaquants dedans. Il est conçu pour détecter et analyser les tentatives d'intrusions sans compromettre la sécurité du réseau interne. **ici il agira en tant que site web interne à l'entreprise (Portails d'Entreprise)**
   - **Logiciels :**

° Python3.12 (Gestion des librairies + Langage de programmation)
° PentBox (Outil pour configurer / crée un honeypot
° Git (Permet d'installer PentBox)
° Screen (Gestions des terminaux)

4. VM VirtualBox PFSENSE (Murphy)

- **Système d'exploitation :** Pfsense freebsd (64 bit)
- **Rôle :** Murphy est un pare feu, il sert à analyser le trafic réseau entrant et sortant, il sert à segmenter notre réseaux avec nos différentes interfaces réseaux, La mise en place d'un DHCP, Réseau Interne LAN / DMZ, Vlan
- **Logiciels :** Aucun à part l'installation de pfsense

• Architecture réseau et sécurité

Description de l'architecture réseau, les flux associés les règles de sécurité du pare-feu, ainsi que le rôle (ici le rôle des interface pfsense)

Nom de la machine	**Interface Pfsense**	**Adresse IP**	**VLAN**	**Fonctionnalité**	**Role**
Hôte (windows 10)	Ethernet	192.168.1.34	N/A	Ethernet	hôte
Miller (Ubuntu Desktop)	em1 (lan) 192.168.56.1/24	192.168.56.10	100	DHCP lan : 192.168.56.10 192.168.56.50	permet dhcp sur le réseau interne lan
Gargantua (honeypot)	em2 (DMZ) 192.168.100.1/24	192.168.100.10	150	DHCP dmz 192.168.100.10 192.168.100.50	permet dhcp sur le réseau interne dmz
Murphy (pfsense)	em0(wan) 192.168.1.16/24	192.168.1.16	N/A	filtrage/configuration interface	Pare Feu

DMZ :

- Limiter strictement le trafic sortant de la DMZ vers Internet.

LAN

- Autoriser le trafic interne entre Miller et Gargantua pour services internes.
- Bloquer le trafic sortant non autorisé vers Internet depuis le LAN.

WAN

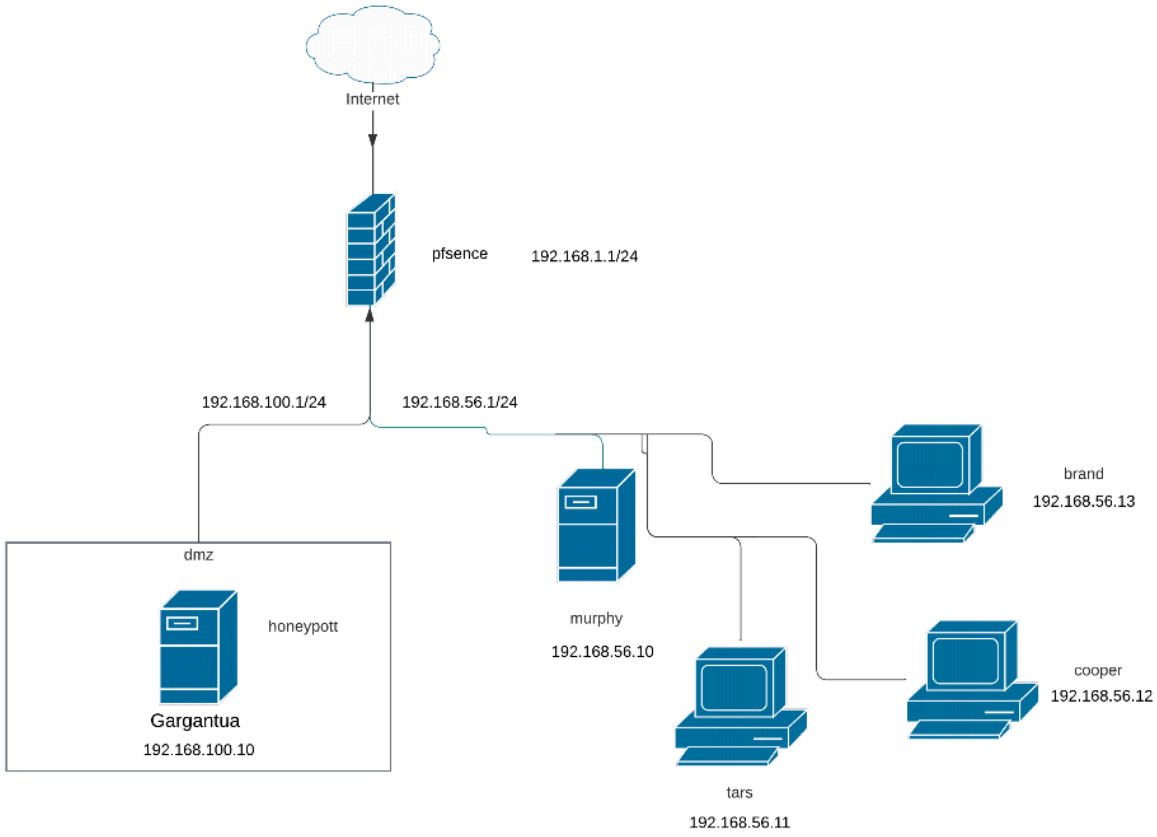
- Bloquer le trafic entrant non sollicité de l'Internet vers le LAN.
- Autoriser le trafic sortant nécessaire vers Internet depuis le LAN.

VLAN

- **Dans un futur il sera surement amené à avoir plusieurs services au seins d'un réseau interne, c'est pour cela que les vlans.**
- **pourquoi vlan 99? car le vlan 99 est en bonne pratique associé au PC Administration, et 150 est associé au vlan DMZ ^**

Schéma d’architecture & réseau :

schéma réseau d’un honeypot



Pourquoi avoir mis une dmz dans un réseau interne ?

1. Isolation des Services Exposés
2. Sécurité Renforcée
3. Analyse des Menaces
4. Meilleure Gestion des Ressources

Ici mes clients sont uniquement sur le schéma, et ne sont pas mis en place due à un manque de ressources de mon hôte windows 10, mais dans la réalité, il le serait.

Nous avons aussi fourni un document d’exploitation disponible sur le git suivant :

Il vous expliquera les démarches à suivre pour la maintenance, l’installation et la gestion des services.