

CONTEXTE ● **DNS Controller**

SUJET ● **Mise en service**

référence ● 340 - dossier d'exploitation.docx

version ● 1.4

statut ●

créé le ● 06/06/2024 11:03:00

par ● Julien BONNET

mis à jour le ● 17/06/2024 21:58:00

par ● Julien BONNET

validé le ● 17/06/2024 21:58:00

par ●

diffusé le ●

à ●

**Péréemption, archivage et
restriction de diffusion** ●

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



Pihole

Table des mises à jour du document

version	date	objet de la mise à jour
01	06/06/2024	Version initiale
02	10/06/2024	Complétion du document
03	16/06/2024	Finalisation du document

Table des matières

1	Document d'architecture technique (Nom Service concerné)	3
1.1	Fonctionnalité et domaine applicatif	3
1.2	Architecture matérielle	3
1.3	Architecture logicielle	4
1.4	Architecture réseau et sécurité	4
1.5	Organisation des données	5
1.6	Installer Windows Server et activer Hyper-V.	5
1.7	Créer les machines virtuelles pour pfSense et Ubuntu Server.	5
1.8	Installer pfSense sur la VM dédiée.	5
1.9	Installer Ubuntu Server sur la VM dédiée et installer Pi-hole.	5
1.9.1	Installation de ubuntu	5
1.9.2	Installation de Pihole	5
1.10	Configuration	9
1.10.1	Configuration de pfSense pour gérer le trafic WAN, LAN, et DMZ.	9
1.10.2	Configuration de Pi-hole pour filtrer le DNS et bloquer les publicités.	9
1.11	Sources d'informations	9

1 Document d'architecture technique (Nom Service concerné)

1.1 Fonctionnalité et domaine applicatif

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	

1.2 Architecture matérielle

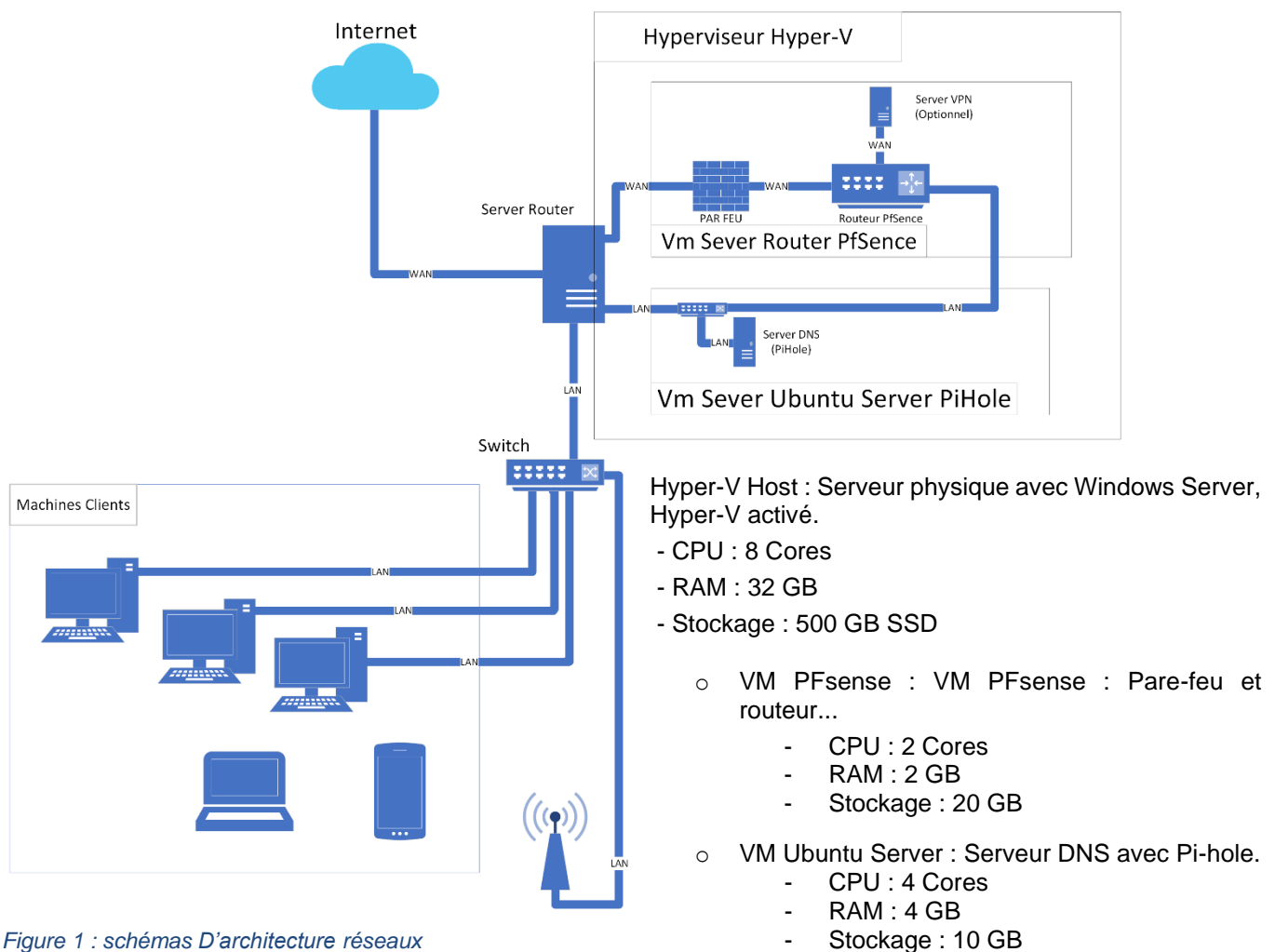


Figure 1 : schémas D'architecture réseaux

1.3 Architecture logicielle

Hyper-V Host : Windows Server avec Hyper-V activé.

VM PfSense : Système d'exploitation pfSense pour les fonctionnalités de pare-feu et de routage.

VM Ubuntu Server : Ubuntu Server avec Pi-hole installé pour le filtrage DNS.

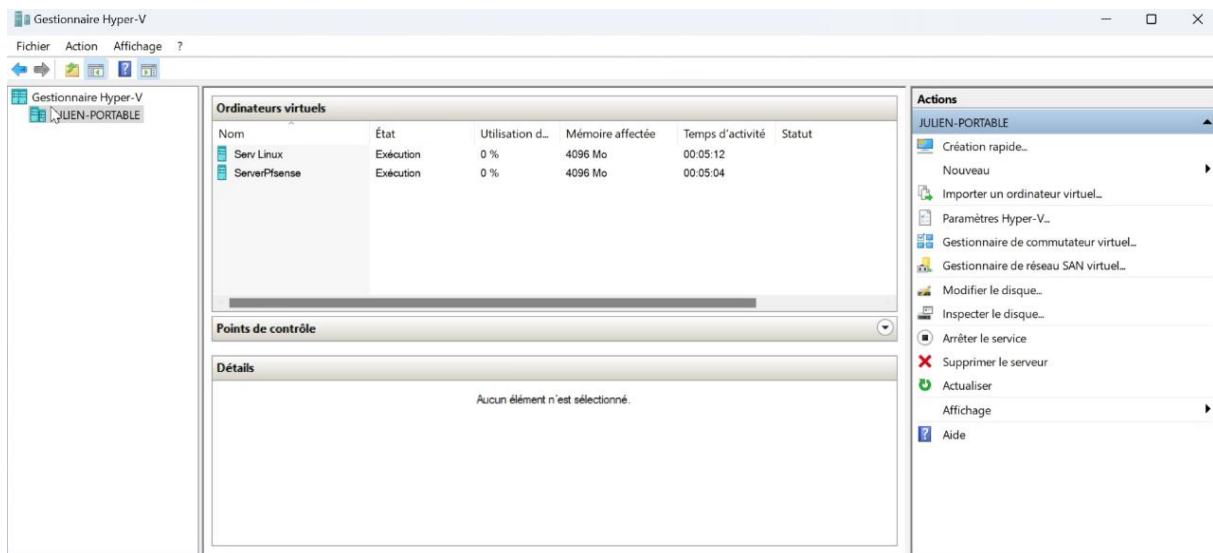


Figure 2 : Composition de l'hyperviseur

1.4 Architecture réseau et sécurité

Réseaux virtuels configurés sur Hyper-V :

- ExternalSwitch : Connecté à l'interface WAN.
- InternalSwitch : Connecté à l'interface LAN.
- DMZSwitch : Utilisé pour la zone DMZ.

Règles de sécurité du pare-feu pfSense :

- Filtrage du trafic entrant et sortant basé sur les règles définies.
- Portail captif pour contrôler l'accès au réseau.

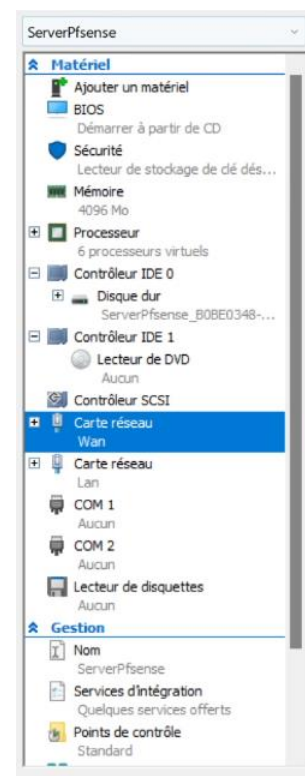


Figure 3 : vue conf PfSense

Suivre le SetupWizard de PiHole :

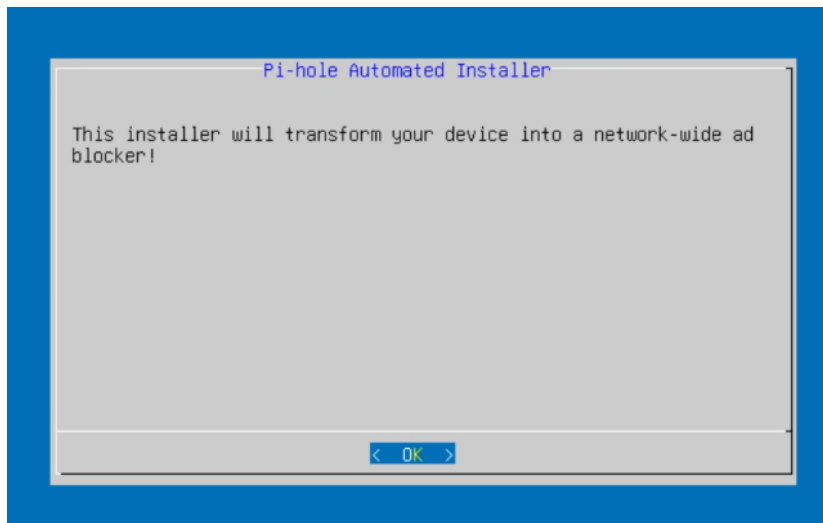


Figure 6 : PiHole Setup Wizzard

Paramétrage de L'ip de la VM ubuntu en mode Static :

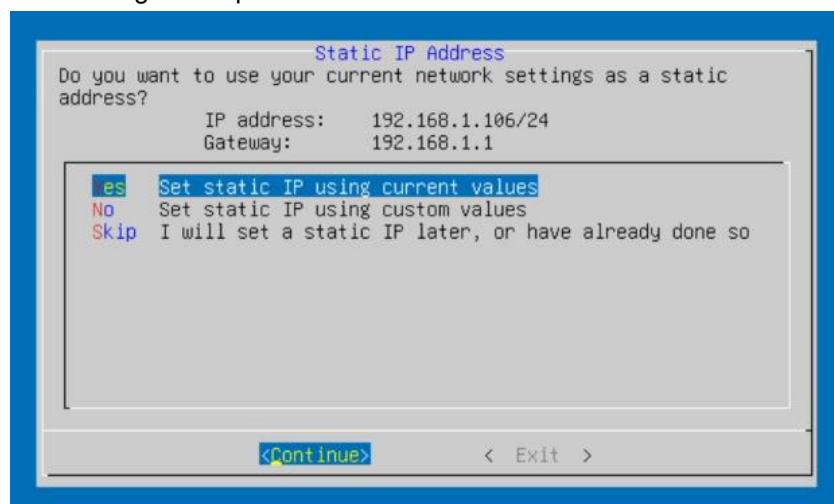


Figure 7 : Configuration IP Statique Server DNS

Acceptez l'installation du WebUI pour configuration du Server DNS :

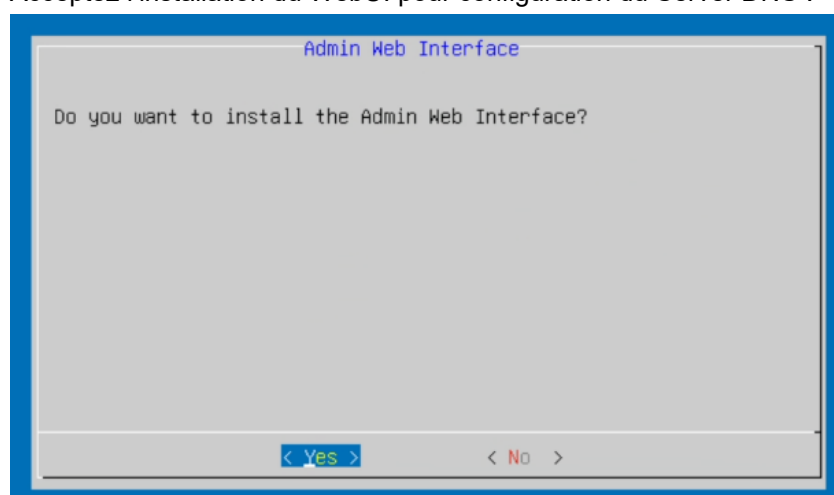


Figure 8 : Installation du WebUI

Étape importante choisir selon la politique de l'entreprise le mode de surveillance des requêtes DNS :

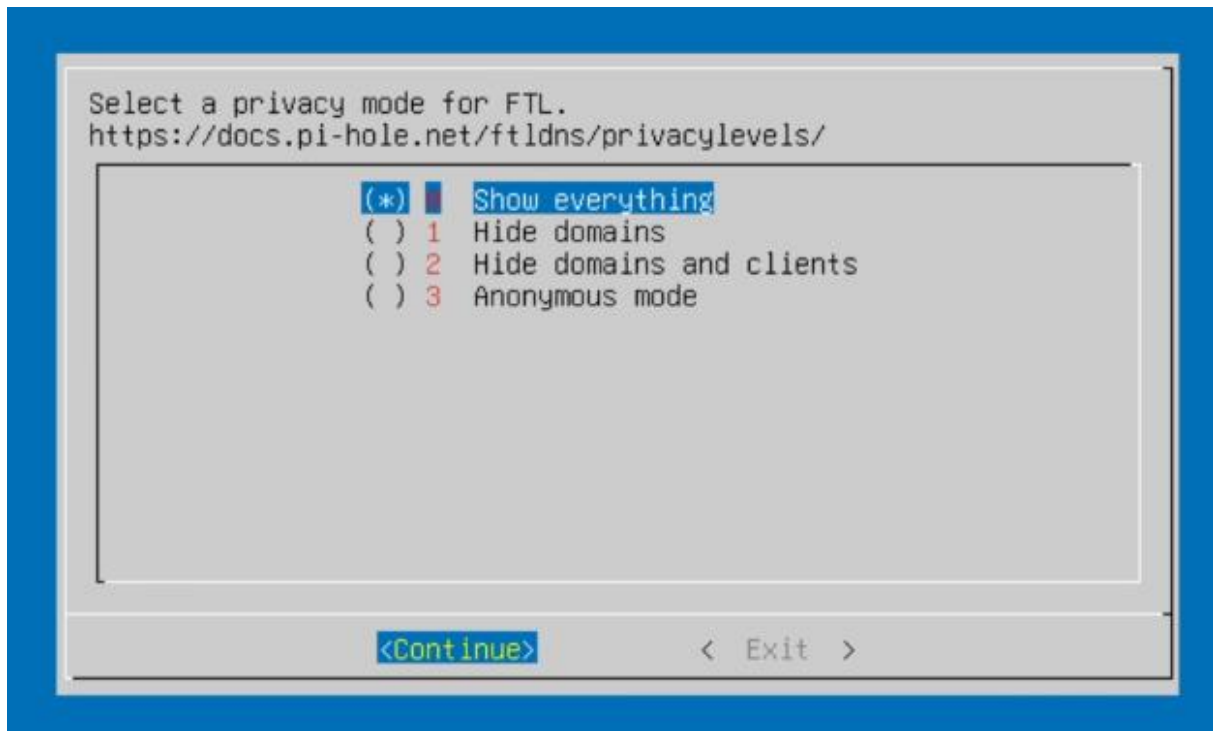


Figure 9 : Mise à Jour de La Politique de Confidentialité

Enfin résumé de l'installation :

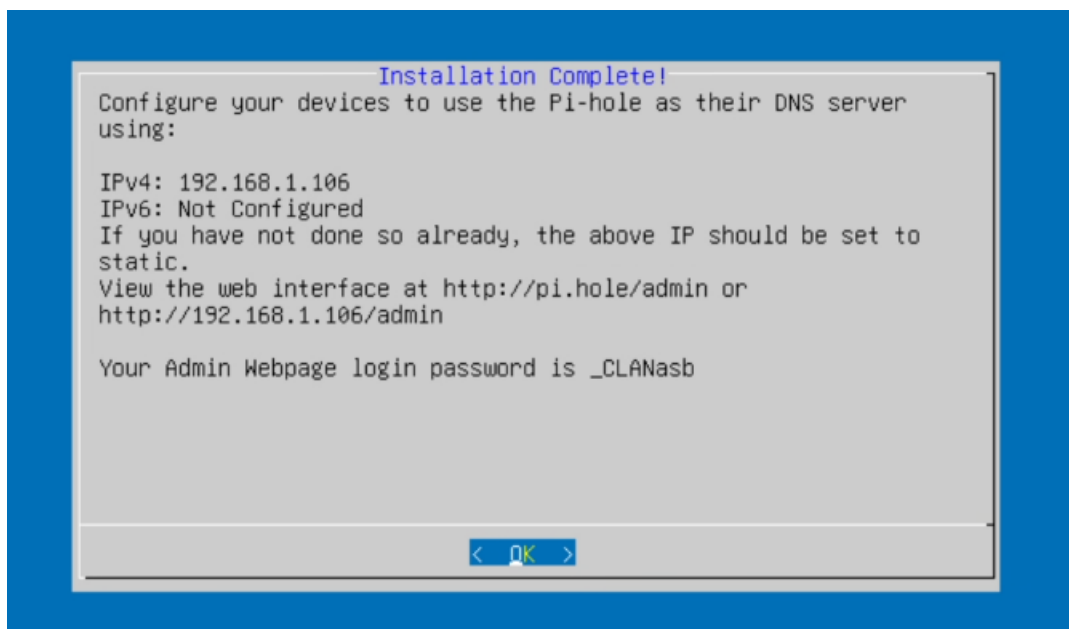


Figure 10 : Résumer de l'installation

Une fois Pi-hole installer se connecter a l'aide d'un navigateur de la machine physique sur le lien :
<http://192.168.0.106/admin/login.php>

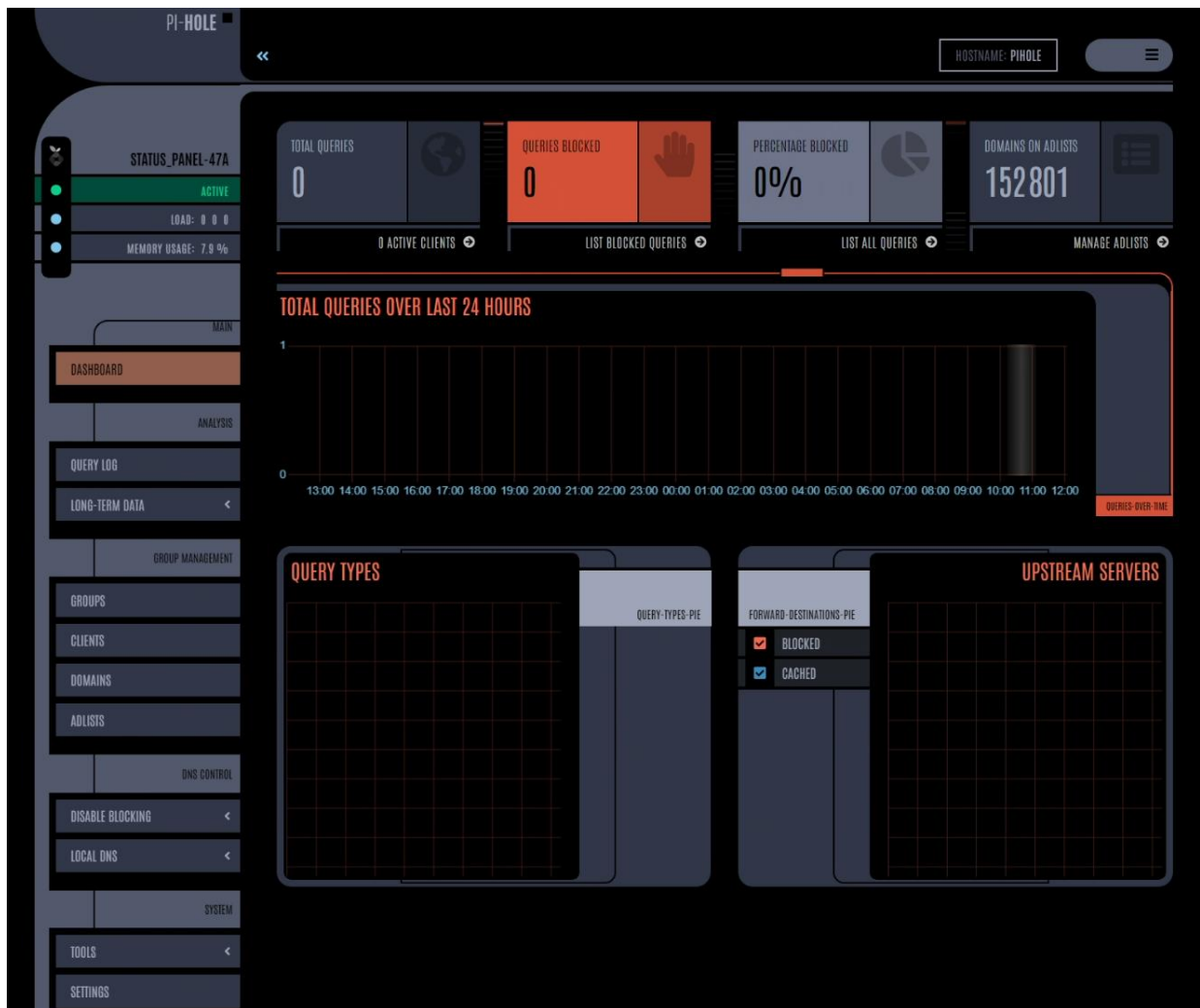


Figure 11 : Page d'accueil PiHole

1.10 Configuration

1.10.1 Configuration de pfSense pour gérer le trafic WAN, LAN, et DMZ.

1.10.2 Configuration de Pi-hole pour filtrer le DNS et bloquer les publicités.

A ce moment le Pihole est accessible sur le réseau LAN de HyperViseur, pour faire sa configuration :

- Par une autre VM quelque soit L'os (os avec navigateur internet) connecter au réseaux LAN.
- Par la Machine physique car celle-ci garde un accès sur ce réseau privé LAN,
- Par le VPN ; pour ce mode de configuration, il faut avoir déployer un server VPN sur PFsense)

1.11 Sources d'informations

Liens d'information :

- Documentation officielle pfSense : <https://docs.netgate.com/pfsense/en/latest/>
- Documentation officielle Pi-hole : <https://docs.pi-hole.net/>