

26/11/2024

PfSense



Eloham Caron
BTS SIO 2 SISR

Table des matières

1.	Introduction.....	3
a)	Adresse réseaux :	3
2.	Installation	5
b)	Configuration des Interfaces Réseau	5
3.	Configuration Initiale du Système	6
c)	Modification du Nom d'Hôte et du Domaine	7
d)	1.2. Paramètres DNS.....	8
4.	Configurer NTP :.....	9
5.	1.4. Journaux Système	11
6.	Analyse des logs textuels	12
e)	Journaux du Pare-feu (Logs Textuels Pare-feu).....	13
7.	Analyse graphique des logs grâce à Syslog et pfSense.....	15
8.	Configuration du DHCP	18
f)	Vérification du Fonctionnement du DHCP	19
g)	Configuration des Alias	20
9.	Sécurisation de l'Accès	21
h)	Configuration du SSH - Sécurisation de l'Accès.....	21
i)	Configuration de la Règle de Pare-feu SSH.....	22
10.	Explication des Choix de Configuration des Règles de Pare-feu WAN.....	23
11.	Explication des Choix de Configuration des Règles de Pare-feu LAN0.....	26
12.	Explication des Choix de Configuration des Règles de Pare-feu LAN.1	27
13.	Explication des Choix de Configuration des Règles de Pare-feu LAN.2	28
14.	Explication des Choix de Configuration des Règles de Pare-feu DMZ	29
15.	Protection contre le DNS Rebinding.....	30
16.	Configuration des Redirections et du NAT	31
17.	Configuration du Proxy Squid	33
j)	Proxy :	34
18.	Clam-AV	37
k)	Configuration :	37
l)	Users :	39
m)	Analyse des logs.....	39
19.	Création et Mise en Œuvre d'un Certificat HTTPS	40
n)	Installation des certificats en local	44
20.	Snort	47
21.	Installation de SNORT :	48
o)	Vérifier la DMZ.....	48

p)	Mise à jour de sécurité :	50
q)	Logs SNORT :	52
22.	Régulateur de flux.....	53
23.	Reverse Proxy	53
24.	Spamhaus +	57
r)	Mise en place de Cron :	58
25.	Sauvegarde Automatique.....	60
s)	SQUIDGUARD :	62
t)	Blocage des Contenus Adultes et Journalisation dans SquidGuard	63
u)	Alias IP :	63
26.	Open VPN + :	64
v)	Documentation de l'Installation d'OpenVPN sur pfSense	64
w)	Certificat du Serveur	66
x)	règles open vpn	66
y)	Argumentation sur le Choix de LAN2	67
27.	vérification :	68
28.	Vérification via Shell :.....	69
z)	NTP	70
aa)	Clav	73
29.	nmap comparaison	77
30.	Alertes Snort générées par les Scans Nmap.....	79
31.	Tableau de bord	80
32.	Conclusion :	81
33.	Sources :	82

1. INTRODUCTION

Présentation de pfSense

pfSense est une distribution **open source** basée sur le système d'exploitation FreeBSD, conçue pour être utilisée comme un pare-feu et routeur de niveau professionnel. Initialement lancé en 2004 par Chris Buechler et Scott Ullrich, pfSense s'est rapidement distingué grâce à sa facilité d'utilisation et à ses capacités avancées qui rivalisent avec celles de solutions commerciales coûteuses.

L'objectif de pfSense est de fournir aux administrateurs réseaux une plateforme flexible et puissante pour la gestion des réseaux et la sécurité. Sa popularité tient au fait qu'il offre une interface web conviviale pour configurer et administrer les réseaux, sans nécessiter de compétences approfondies en ligne de commande. Avec pfSense, il est possible de mettre en place des fonctions de pare-feu, VPN, load balancing, et de nombreuses autres caractéristiques réseau avancées.

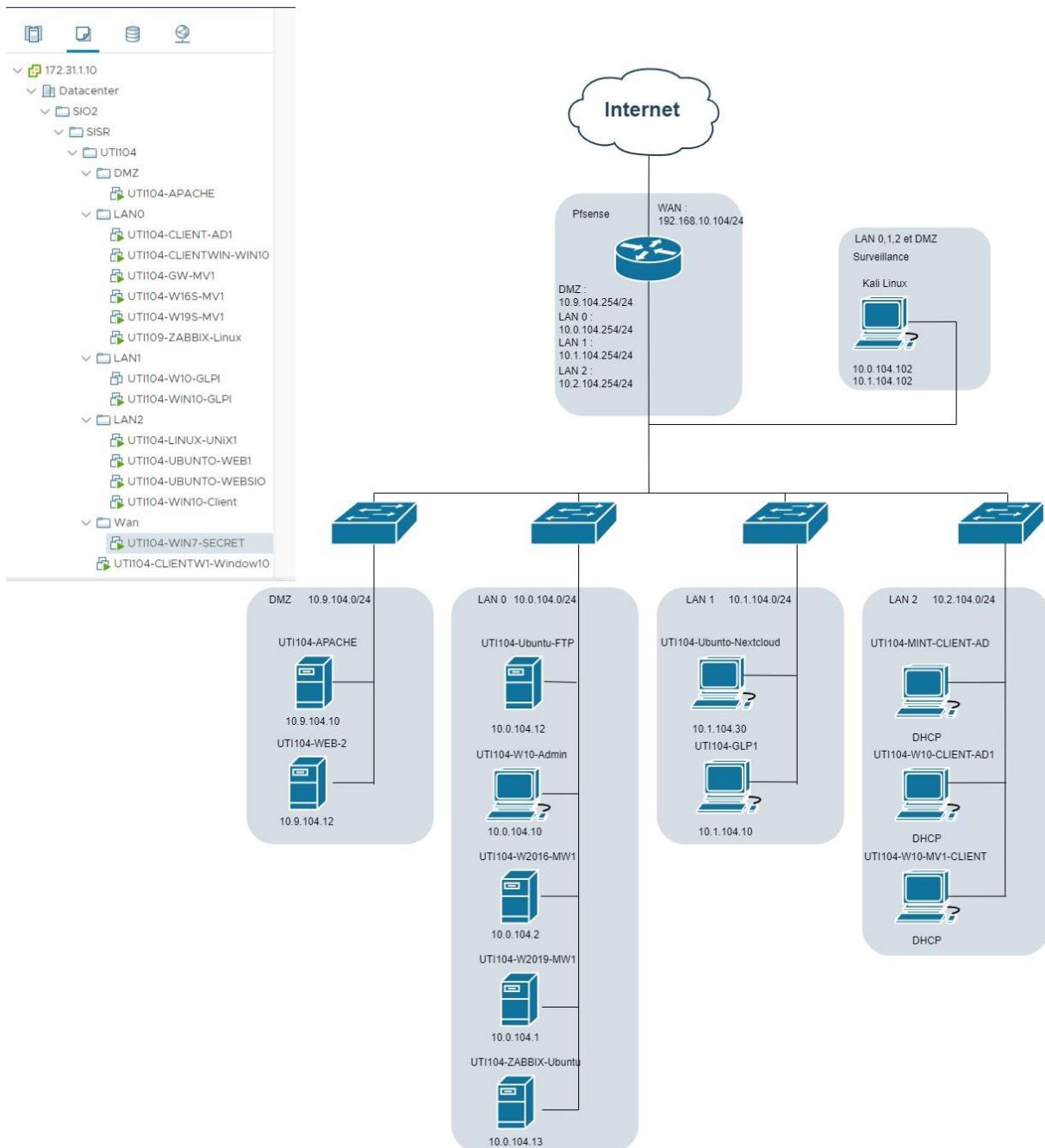
En raison de sa grande flexibilité, pfSense est très utilisé tant dans des petites entreprises que dans des environnements plus complexes. Il permet de centraliser la gestion des réseaux tout en offrant une sécurité robuste, à un coût bien plus faible que les solutions traditionnelles sur le marché. Aujourd'hui, pfSense est considéré comme une solution incontournable pour la gestion efficace des réseaux et la protection des infrastructures.

a) ADRESSE RESEAUX :

Nom	Réseau	Type	Adresse IP	Masque	Passerelle	DNS
UTI104-PFSENSE	LAN 0	Serveur	10.0.104.254	255.255.255.0		
(LAN 1)			10.1.104.254	255.255.255.0		
(LAN 2)			10.2.104.254	255.255.255.0		
(DMZ)			10.9.104.254	255.255.255.0		
(WAN)			192.168.10.104	255.255.255.0		

Eloham Caron

PFSENSE



2. INSTALLATION

Dans cette section, je vais décrire la configuration des interfaces réseau que j'ai réalisée dans pfSense. Cette partie vise à présenter de manière détaillée l'assignation des interfaces et des adresses IP pour chaque segment du réseau.

WAN (wan)	-> vmx2	-> v4: 192.168.10.104/24
LAN0 (lan)	-> vmx3	-> v4: 10.0.104.254/24
LAN1 (opt1)	-> vmx4	-> v4: 10.1.104.254/24
LAN2 (opt2)	-> vmx0	-> v4: 10.2.104.254/24
DMZ (opt3)	-> vmx1	-> v4: 10.9.104.254/24

b) CONFIGURATION DES INTERFACES RESEAU

J'ai commencé par assigner les interfaces réseau dans pfSense. Voici les différentes interfaces et leur configuration respective :

Réseau	Interface	Adresse MAC	IPv4	Masque
WAN	vmx2	00:50:56:ab:8b:ad	192.168.10.104	255.255.255.0
LAN 0	vmx3	00:50:56:ab:4f:b7	10.0.104.254	255.255.255.0
LAN 1	vmx4	00:50:56:ab:1a:86	10.1.104.254	255.255.255.0
LAN 2	vmx0	00:50:56:ab:96:cd	10.2.104.254	255.255.255.0
DMZ	vmx1	00:50:56:ab:8a:e7	10.9.104.254	255.255.255.0

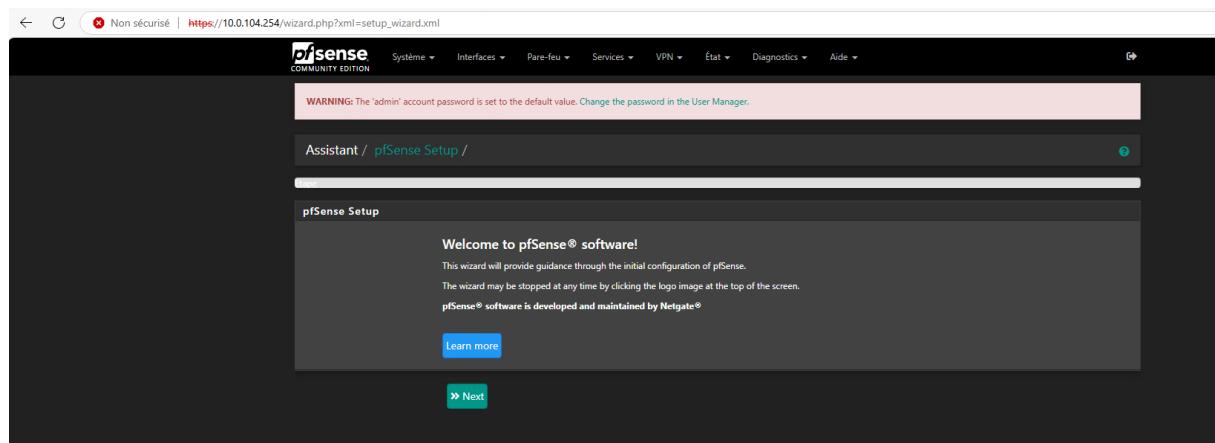
Chaque interface a été assignée à un segment spécifique du réseau pour garantir une isolation appropriée et une sécurité renforcée.

- WAN** : L'interface WAN (vmx2) est liée au réseau externe, avec l'adresse IP 192.168.10.104 et une adresse MAC correspondante 00:50:56:ab:8b:ad. Cela permet de relier pfSense à Internet ou à une autre partie du réseau qui fait office de fournisseur d'accès.
- LAN 0, LAN 1, LAN 2** : Ces interfaces (vmx3, vmx4, vmx0 respectivement) sont liées à des segments LAN internes différents, permettant une gestion séparée des sous-réseaux. Par exemple, LAN 0 a l'adresse IP 10.0.104.254 avec une adresse MAC 00:50:56:ab:4f:b7. Cela permet de créer des sous-réseaux distincts pour divers besoins tels que des utilisateurs finaux, des services critiques ou des départements spécifiques.
- DMZ** : L'interface DMZ (vmx1) est dédiée aux services devant être exposés à l'externe, tels que des serveurs web. L'adresse IP de la DMZ est 10.9.104.254, et son adresse MAC est 00:50:56:ab:8a:e7. Cela permet de sécuriser les services exposés en les isolant des réseaux internes.

3. CONFIGURATION INITIALE DU SYSTEME

Une fois pfSense configuré, on accède à l'interface web de gestion, comme illustré sur l'image. Cette interface est accessible via un navigateur web à l'adresse IP locale de pfSense, ici <http://10.0.104.254>. L'interface web est l'outil principal pour configurer et administrer pfSense. Elle permet de gérer les règles de pare-feu, les configurations réseau, les VPN, et bien d'autres fonctionnalités avancées.

Lors de la première connexion, un assistant de configuration (pfSense Setup Wizard) s'affiche, vous guidant à travers les étapes initiales pour finaliser la configuration. Cela inclut des réglages comme le changement du mot de passe administrateur (recommandé pour la sécurité), les configurations de base du réseau, et d'autres paramètres importants pour sécuriser et personnaliser pfSense selon les besoins spécifiques.



Il est aussi à noter qu'en haut de la page, un message d'avertissement indique que le mot de passe par défaut de l'utilisateur "admin" doit être changé. Cela est crucial pour éviter toute compromission de la sécurité du système.

Après la première configuration de pfSense, nous avons pris les mesures suivantes pour renforcer la sécurité :

- Changement du Mot de Passe Administrateur :** Tout d'abord, nous avons changé le mot de passe par défaut de l'utilisateur "admin". C'est une étape essentielle pour sécuriser l'accès au pare-feu et empêcher toute tentative de compromission liée à l'utilisation du mot de passe par défaut.

The screenshot shows the "Propriétés utilisateur" (User Properties) configuration screen. It displays the following fields:

- Défini par: SYSTEM
- Désactivé: Cet utilisateur ne peut pas s'authentifier
- Nom d'utilisateur: admin
- Mot de passe: [REDACTED] (represented by five asterisks)
- Nom complet: System Administrator
- Description: Nom complet de l'utilisateur, à des fins administratives uniquement

Création d'un Compte Personnel : Ensuite, nous avons créé un compte utilisateur identifiable, nommé "Eloham", avec un mot de passe personnalisé. Cela permet de mieux respecter les normes de sécurité, en évitant d'utiliser un compte administrateur générique pour toutes les opérations. En attribuant ce compte à un groupe d'administrateurs (admins), nous permettons à cet utilisateur de gérer le système tout en assurant une traçabilité et une identification claire.

The screenshot shows the 'Utilisateurs' tab selected in the top navigation bar. The main section is titled 'Propriétés utilisateur'. It includes fields for 'Défini par' (USER), 'Désactivé' (unchecked), 'Nom d'utilisateur' (Eloham), 'Mot de passe' (redacted), 'Nom complet' (Eloham caron), 'Date d'expiration' (empty), 'Paramètres personnalisés' (checkbox checked), and 'Appartenance à un groupe' (selected group: admins). Below this is a note about certificate authorities and a 'Certificat' section. At the bottom right, there is an 'Activé' button.

Désactivation de l'Administrateur par Défaut : Enfin, nous avons désactivé le compte administrateur par défaut (admin). Cette mesure permet de renforcer encore davantage la sécurité en supprimant une cible facile pour d'éventuelles attaques. Cela nous assure que seuls les utilisateurs spécifiquement créés, tels que "Eloham", peuvent accéder à l'interface d'administration.

The screenshot shows the 'Propriétés utilisateur' section with 'Défini par' set to SYSTEM and 'Désactivé' checked. A note states that no private key authority was found and that a private key is required to create a user certificate. There is also a note about importing an external certificate.

c) MODIFICATION DU NOM D'HOTE ET DU DOMAINE

- Changement du Nom d'Hôte** : Nous avons modifié le nom d'hôte (hostname) du pare-feu pour le rendre spécifique à l'utilisateur. Dans notre cas, nous avons choisi "Eloham" comme nom d'hôte. Cela permet une meilleure identification et correspondance avec l'utilisateur principal du système, rendant la gestion et la maintenance plus aisées. Utiliser un nom d'hôte identifiable est essentiel pour permettre une reconnaissance rapide de l'appareil sur le réseau, notamment dans les environnements complexes où de nombreux dispositifs sont présents.
- Configuration du Domaine** : Nous avons configuré le domaine approprié pour le pare-feu, qui est ici "DOMAD104.peda". Cette configuration permet de définir le nom de domaine qui sera utilisé par le pare-feu pour communiquer sur le réseau. Un domaine

bien défini facilite la résolution des noms (DNS) et contribue à l'organisation du réseau en permettant une identification structurée des équipements.

The screenshot shows the 'Système / Configuration générale' section. Under 'Système', the 'Nom d'hôte' is set to 'Eloham' and the 'Domaine' is set to 'DOMAD104.peda'. A note below states: 'Do not end the domain name with ".local" as the final part (Top Level Domain, TLD). The ".local" TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses ".local" as its TLD. Alternatives such as ".home.arpa", ".local.lan", or ".mylocal" are safe.'

d) 1.2. PARAMETRES DNS

Pour cette étape, nous avons configuré les serveurs DNS afin d'améliorer la résolution des noms de domaine et garantir une navigation rapide et fiable sur le réseau. Les serveurs DNS sont des éléments clés pour traduire les noms de domaine en adresses IP, permettant ainsi aux appareils de communiquer entre eux de manière efficace.

1. Configuration des Serveurs DNS

1. Serveurs DNS Locaux :

- Nous avons configuré deux serveurs DNS internes spécifiques à l'infrastructure, identifiés par leurs adresses IP :
 - **172.31.1.4** nommé **Bts-SIO-DNS-1**
 - **172.31.1.6** nommé **Bts-SIO-DNS-2** Ces serveurs DNS internes sont utiles pour des requêtes locales, permettant une résolution plus rapide des noms de domaine à l'intérieur du réseau privé.

The screenshot shows the 'Paramètres du serveur DNS' section. It lists three entries:

- Serveurs DNS: 172.31.1.4, Nom d'hôte: Bts-SIO-DNS-1, Supprimer
- Serveurs DNS: 172.31.1.6, Nom d'hôte: Bts-SIO-DNS-2, Supprimer
- Serveurs DNS: 1.1.1.1, Nom d'hôte: Cloudflare, Supprimer

A note at the bottom states: 'Saisir les adresses IP des serveurs DNS utilisés par le système. Ceux-ci sont également utilisés pour le service DHCP, le DNS Forwarder et le serveur de résolution DNS lorsqu'il est activé.'

1. Serveur DNS Externe (Cloudflare) :

- En complément des DNS locaux, nous avons ajouté **Cloudflare** en tant que serveur DNS externe, avec l'adresse **1.1.1.1**.
- Cloudflare est réputé pour sa rapidité et son respect de la confidentialité. En utilisant Cloudflare, nous nous assurons que les requêtes externes (celles qui ne peuvent pas être résolues par les serveurs internes) soient traitées de manière rapide et sécurisée.

Cette configuration hybride permet de garantir une résolution rapide des noms de domaine, tout en optimisant les requêtes internes au réseau et en utilisant une solution de confiance pour les requêtes externes. Cela améliore l'efficacité du réseau et assure une meilleure disponibilité des services, que ce soit pour les ressources locales ou pour l'accès à Internet.

4. CONFIGURER NTP :

2. ROLE DU NTP

Le **Network Time Protocol (NTP)** est un protocole utilisé pour synchroniser l'horloge des appareils d'un réseau avec une source de temps précise, souvent un serveur NTP. Cela permet à tous les dispositifs du réseau d'avoir la même heure, ce qui est essentiel pour les logs, la sécurité et la coordination des tâches sur le réseau.

Dans le cadre de notre scénario, nous avons configuré le service NTP en restant cohérent avec notre choix initial d'utiliser les services de Cloudflare. Nous avons ajouté `time.cloudflare.com` comme l'une des sources de synchronisation NTP, ainsi que des serveurs du pool pfSense pour garantir une synchronisation fiable et sécurisée.

The screenshot shows the pfSense web interface under the 'Services / NTP / Paramètres' path. The 'Paramètres' tab is active. In the 'Configuration serveur NTP' section, the 'Activer' checkbox is checked. Below it, a dropdown menu lists network interfaces: WAN, LAN0, LAN1, and LAN2. A note states: 'Les interfaces sans adresse IP ne seront pas affichées. Sélectionner aucune interface écoutera toutes les interfaces avec un caractère générique. Sélectionner toutes les interfaces écoutera explicitement que sur les interfaces/adresses IP spécifiées.' Three NTP servers are listed: 2.pfsense.pool.ntp.org (Prefer, Pool), time.cloudflare.com (Prefer, Serveur), and pool.ntp.org (No Select, Pool). Each entry has a 'Supprimer' button. At the bottom, there are 'Ajouter' and '+ Ajouter' buttons.

Serveurs de Temps Configurés :

- **2.pfsense.pool.ntp.org** : Une source de temps faisant partie du pool officiel de serveurs NTP recommandé par pfSense.
- **time.cloudflare.com** : Ce serveur est ajouté pour garder une certaine homogénéité avec la configuration DNS, où nous avons également utilisé les services de Cloudflare.
- **pool.ntp.org** : Un autre serveur du pool NTP général pour renforcer la précision et la redondance.

Les interfaces WAN, LAN0, LAN1, et LAN2 ont toutes été configurées pour utiliser le service NTP, ce qui assure que tous les segments du réseau bénéficient de la même référence de temps.

3. VÉRIFICATION DU FONCTIONNEMENT DU SERVICE NTP

Après avoir activé le service NTP, nous avons vérifié que toutes les interfaces reçoivent bien la synchronisation. L'état du service est consulté pour s'assurer que chaque source est fonctionnelle et qu'aucune erreur de communication n'existe.

4. Consultation des Statistiques NTP

Les statistiques du service NTP sont également accessibles, et nous les avons vérifiées pour voir l'état des différents serveurs configurés :

- Les serveurs **Cloudflare** et **pool.ntp.org** apparaissent comme sources actives.
- On peut voir les décalages (Offset) et les variations (Jitter) pour chaque serveur, indiquant à quel point les horloges sont synchronisées. Par exemple, des valeurs de délai (Délai) et d'offset faibles montrent une bonne synchronisation des serveurs.

Diagnostics / Table NDP					
Recherche					
Adresse IPv6	Adresse MAC	Nom d'hôte	Interface	Expiration	Actions
fe80::250:56ff:feab:96cd%vmx0	00:50:56:ab:96:cd (VMware)		LAN2	permanent	
fe80::250:56ff:feab:8ae7%vmx1	00:50:56:ab:8ae7 (VMware)		DMZ	permanent	
fe80::250:56ff:feab:8bad%vmx2	00:50:56:ab:8b:ad (VMware)		WAN	permanent	
fe80::250:56ff:feab:4fb7%vmx3	00:50:56:ab:4fb7 (VMware)		LAN0	permanent	
fe80::250:56ff:feab:1a86%vmx4	00:50:56:ab:1a:86 (VMware)		LAN1	permanent	

Clear NDP Table

Ces statistiques sont importantes pour s'assurer que le temps sur le réseau est synchronisé de manière précise et fiable, évitant des erreurs de chronologie dans les journaux, notamment pour les événements de sécurité.

Cette configuration complète garantit une synchronisation précise et sécurisée pour tous les segments du réseau, ce qui est essentiel pour maintenir la cohérence des événements, surtout dans des contextes de sécurité et de gestion de réseau.

État / NTP											
Statut Network Time Protocol (NTP)											
État	Serveur	ID référence	Stratum	Type	Quand	Poll (s)	Portée	Délai (ms)	Offset (ms)	Jitter (ms)	
Pool titulaire	2.pfsense.pool.ntp.org	.POOL.	16	p	-	64	0	0.000	+0.000	0.000	
Pool titulaire	pool.ntp.org	.POOL.	16	p	-	64	0	0.000	+0.000	0.000	
Pair actif	162.159.200.123	10.3.8.4	3	u	42	64	177	2.602	+0.423	0.375	
Candidat	82.67.62.62	.PPS.	1	u	36	64	177	18.729	+0.694	0.287	
Sélectionné	129.250.35.250	129.250.35.222	2	u	41	64	177	6.229	-3.570	0.195	
Outlier	212.85.158.10	145.238.203.14	2	u	38	64	177	19.352	+0.935	0.209	
Outlier	45.13.105.44	230.226.69.180	2	u	40	64	177	28.623	-0.984	0.191	
Sélectionné	212.227.232.161	193.149.0.221	2	u	40	64	177	33.551	+3.520	4.382	
Candidat	82.67.126.242	.PPS0.	1	u	33	64	177	9.900	-0.072	0.345	
Sélectionné	5.39.80.51	82.64.45.50	2	u	37	64	177	12.159	+1.129	0.238	

5. 1.4. JOURNAUX SYSTEME

Pour la gestion des événements réseau et la surveillance des activités sur pfSense, nous avons configuré les **jouarnaux système** de manière à pouvoir enregistrer et analyser efficacement tout ce qui se passe sur le réseau. Voici comment nous avons configuré ces paramètres :

Format de Journalisation (Log Message Format) :

- Nous avons choisi d'utiliser le format **syslog (RFC 5424, avec des timestamps de précision en microsecondes RFC 3339)**. Ce format est particulièrement utile pour assurer une précision maximale lors de l'enregistrement des événements, ce qui est essentiel en cas de besoin de reconstituer des incidents ou de réaliser des audits.

The screenshot shows the pfSense web interface under the 'Etat / Journaux système / Paramètres' section. The 'Paramètres' tab is selected. The configuration page is titled 'Options de journalisation générales'. Under the 'Log Message Format' section, it is set to 'syslog (RFC 5424, with RFC 3339 microsecond-precision timestamps)'. Below this, there is a note: 'The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled). Changing this value will only affect new log messages.' In the 'Affichage Forward/Reverse' section, there is an option 'Afficher les entrées de journal en ordre inverse (les nouveaux événements au début)' which is checked. The 'Entrées des journaux de l'IHM' field is set to '500'. In the 'Journaliser les blocages par défaut du pare-feu.' section, there are three checkboxes:

- Les paquets de journaux correspondent aux règles de blocage par défaut dans le jeu de règles. Description: 'Journaliser les paquets qui sont bloqués par la règle de blocage implicite. - Les options de journalisation par règle restent actifs.'
- Enregistre les paquets correspondant aux règles de passe par défaut placés dans le jeu de règles. Description: 'Journaliser les paquets qui sont autorisés par la règle d'autorisation implicite. Les options de journalisation par règle restent actifs.'
- Enregistre les paquets bloqués par les règles de 'Block Bogon Networks'

Affichage des Entrées de Journal (Forward/Reverse) :

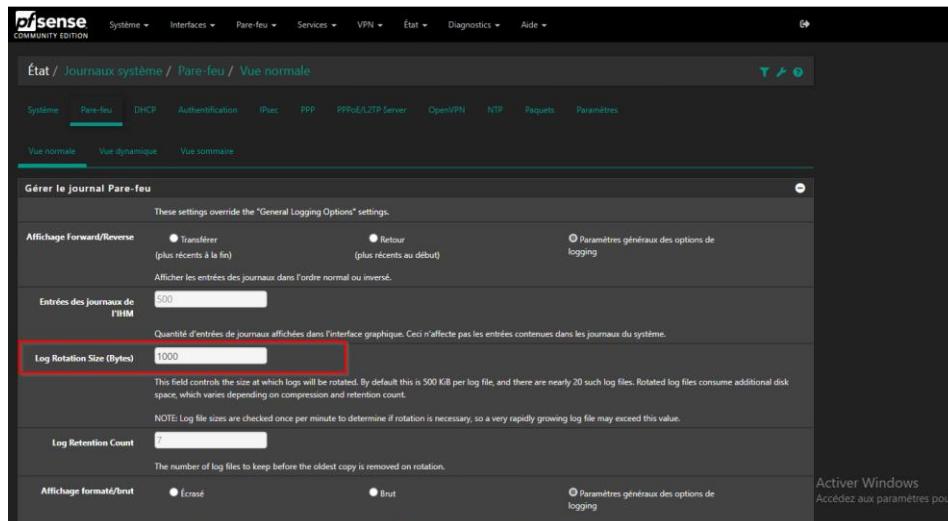
- Les entrées de journal peuvent être affichées soit par ordre chronologique normal (nouveaux événements à la fin), soit par ordre inversé (nouveaux événements au début). Nous avons configuré l'affichage pour afficher les nouveaux événements en début de liste, afin de faciliter l'accès rapide aux dernières activités enregistrées.

Nombre d'Entrées des Journaux de l'IHM :

- Le nombre d'entrées de journal affichées via l'interface utilisateur est fixé à **500**. Cela permet une vue d'ensemble détaillée sans surcharger l'interface avec trop d'informations.

Journalisation des Blocages par Défaut du Pare-feu :

- Nous avons activé l'option pour **journaliser tous les blocages par défaut** du pare-feu. Cela garantit que toutes les tentatives de connexion bloquées, y compris celles relevant des règles implicites (telles que le blocage de réseaux non sécurisés), soient enregistrées. Ces informations sont cruciales pour détecter d'éventuelles tentatives d'intrusion ou des comportements anormaux.



Rotation des Logs (Log Rotation Size) :

- La rotation des fichiers journaux est configurée avec une taille de rotation de **1000 bytes** par fichier. La rotation régulière des fichiers permet de limiter la taille des fichiers journaux individuels et de garantir que l'espace de stockage ne soit pas saturé par des logs trop volumineux. Le **nombre de fichiers de log** avant suppression est fixé à 7, ce qui assure une rétention raisonnable des données historiques.

6. ANALYSE DES LOGS TEXTUELS

L'analyse des logs est une étape cruciale pour évaluer la sécurité et le comportement du réseau. Dans cette section, nous avons examiné les **jouarnaux du pare-feu** ainsi que les **jouarnaux d'authentification** de pfSense pour identifier des événements notables ou des anomalies.

e) JOURNAUX DU PARE-FEU (LOGS TEXTUELS PARE-FEU)

Les journaux du pare-feu sont utilisés pour enregistrer toutes les tentatives de connexion qui sont bloquées ou autorisées par les règles configurées. Voici un résumé des observations :

500 dernière(s) entrée(s) dans le journal Pare-feu. (Maximum 500) Pause <input type="checkbox"/>					
Action	Heure	Interface	Source	Destination	Protocole
✗	2024-11-23 14:09:12.241647+00:00	DMZ	10.9.104.10:38744	10.0.104.1:53	UDP
✗	2024-11-23 14:09:13.241703+00:00	DMZ	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:14.235805+00:00	DMZ	10.9.104.10:56555	10.0.104.1:53	UDP
✗	2024-11-23 14:09:14.235926+00:00	DMZ	10.9.104.10:55666	10.0.104.1:53	UDP
✗	2024-11-23 14:09:14.235985+00:00	DMZ	10.9.104.10:51122	10.0.104.1:53	UDP
✗	2024-11-23 14:09:15.242042+00:00	DMZ	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:17.242039+00:00	DMZ	10.9.104.10:38744	10.0.104.1:53	UDP
✗	2024-11-23 14:09:19.237786+00:00	WAN	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:20.237330+00:00	DMZ	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:21.242080+00:00	WAN	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:23.241971+00:00	WAN	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:26.242243+00:00	WAN	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:29.241974+00:00	DMZ	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:32.238484+00:00	WAN	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:39.237119+00:00	WAN	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:45.242166+00:00	DMZ	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:52.237817+00:00	DMZ	10.9.104.10:52132	10.0.104.1:53	UDP
✗	2024-11-23 14:09:53.242026+00:00	WAN	0.0.0.68	255.255.255.255:67	UDP
✗	2024-11-23 14:09:57.242323+00:00	DMZ	10.9.104.10:63132	10.0.104.1:53	UDP

- **Interface DMZ :**

- La majorité des entrées dans les logs du pare-feu provient de l'interface DMZ. Ces connexions ont pour **source** l'adresse 10.9.104.10, une adresse interne dans le réseau DMZ, et visent différentes destinations, principalement 10.0.104.1:53, qui semble être un serveur DNS. Le **protocole utilisé** est souvent UDP, ce qui correspond typiquement aux requêtes DNS.
- Ces logs montrent que des tentatives de communication ont été **bloquées**, indiquées par une croix rouge (✗). Cela pourrait signifier que ces connexions ne respectent pas les règles en place ou qu'elles sont vues comme des tentatives non autorisées.

Interface WAN :

- Des tentatives de communication vers l'adresse de diffusion 255.255.255.255 apparaissent également dans les logs. Ces tentatives peuvent être des requêtes de découverte réseau (telles que DHCP) et sont aussi **bloquées** par le pare-feu.
- Les événements montrent des **requêtes DHCP** fréquentes (source 0.0.0.0, destination 255.255.255 sur le port 67), suggérant des appareils essayant de se connecter au réseau et obtenir une adresse IP.

Ces journaux nous aident à identifier les tentatives de communication non autorisées, à vérifier les règles de sécurité, et à s'assurer que les politiques de pare-feu fonctionnent comme prévu.

5. JOURNAUX D'AUTHENTIFICATION

Les journaux d'authentification nous permettent de surveiller les accès aux services et les activités de connexion :

Service SSHGuard :

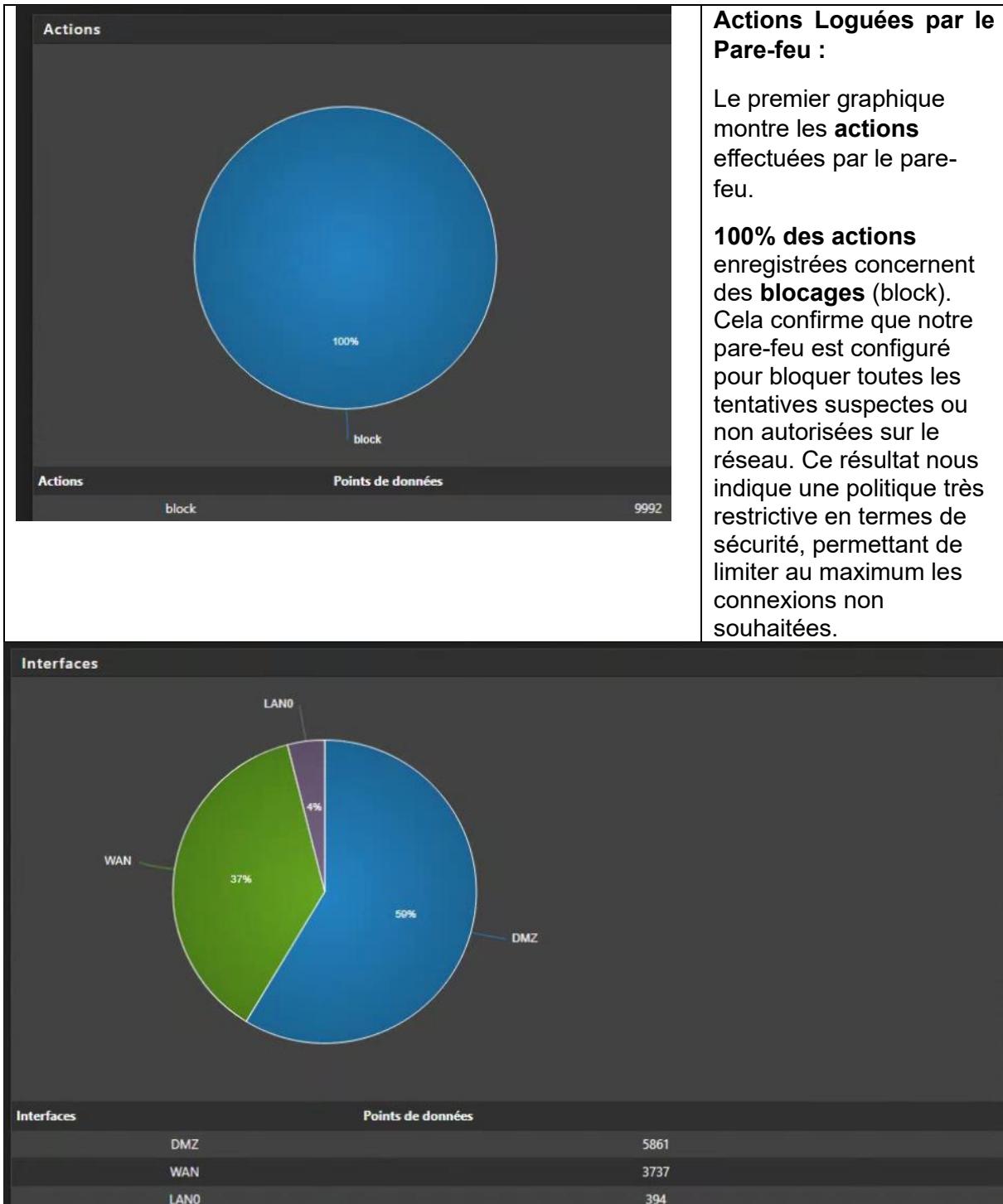
- Le processus sshguard est activement surveillé dans les logs. SSHGuard est un service qui protège le serveur des tentatives de force brute et des attaques par mot de passe sur le port SSH.
- Les messages enregistrés montrent que sshguard est en mode de surveillance ("Now monitoring attacks"), ce qui indique qu'il a activé une protection pour repérer des tentatives suspectes.
- D'autres messages indiquent des **terminaisons sur signal** ("Exiting on signal"), qui pourraient correspondre à des cycles normaux de redémarrage du processus ou à une réinitialisation suite à des événements de sécurité.

500 dernière(s) entrée(s) dans le journal Général. (Maximum 500)			
Heure	Processus	PID	Message
Sep 7 01:09:00	sshguard	44426	Exiting on signal.
Sep 7 01:09:00	sshguard	69510	Now monitoring attacks.
Sep 7 02:59:00	sshguard	69510	Exiting on signal.
Sep 7 02:59:00	sshguard	64480	Now monitoring attacks.
Sep 7 04:51:00	sshguard	64480	Exiting on signal.
Sep 7 04:51:00	sshguard	97940	Now monitoring attacks.
Sep 7 06:42:00	sshguard	97940	Exiting on signal.
Sep 7 06:42:00	sshguard	6236	Now monitoring attacks.
Sep 7 08:32:00	sshguard	6236	Exiting on signal.
Sep 7 08:32:00	sshguard	3831	Now monitoring attacks.
Sep 7 10:22:00	sshguard	3831	Exiting on signal.
Sep 7 10:22:00	sshguard	15468	Now monitoring attacks.
Sep 7 12:14:00	sshguard	15468	Exiting on signal.
Sep 7 12:14:00	sshguard	83128	Now monitoring attacks.
Sep 7 14:06:00	sshguard	83128	Exiting on signal.
Sep 7 14:06:00	sshguard	9176	Now monitoring attacks.

L'analyse des logs d'authentification est essentielle pour suivre les activités suspectes, notamment en ce qui concerne les tentatives d'accès non autorisées aux systèmes critiques. Les logs actuels montrent que le système est prêt à détecter et à prévenir des attaques via SSH.

7. ANALYSE GRAPHIQUE DES LOGS GRACE A SYSLOG ET PFSENSE

Pour faciliter l'interprétation des données et comprendre les événements sur le réseau, nous avons réalisé une **analyse graphique des logs** enregistrés par pfSense. L'utilisation des graphiques permet d'avoir une vue synthétique des tendances et des caractéristiques principales des activités réseau. Voici les différentes analyses effectuées :



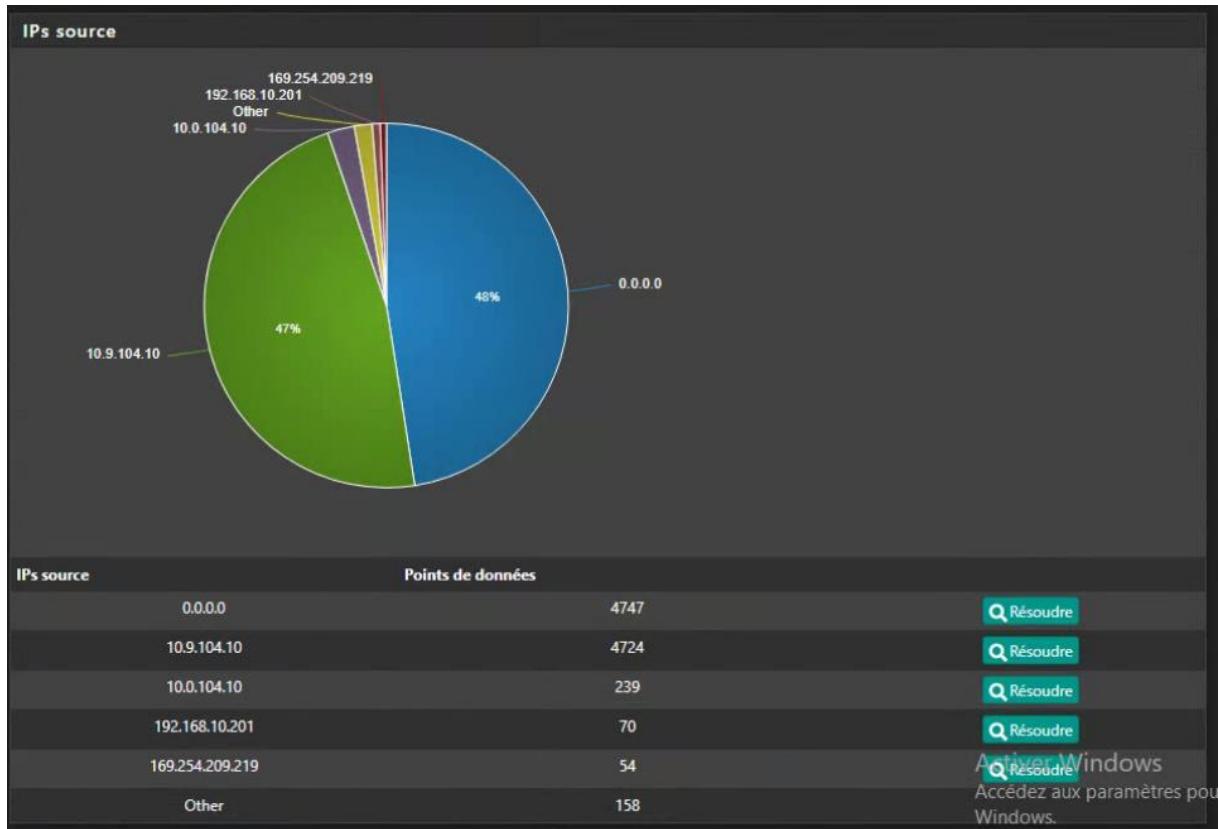
6. Interfaces Concernées par les Logs

Le second graphique représente la répartition des **interfaces** concernées par les logs.

- **DMZ** : 59% des entrées de log concernent l'interface **DMZ**. Cela est logique, car la DMZ est souvent exposée à l'extérieur et reçoit la majorité des tentatives d'accès.
- **WAN** : 37% des entrées sont liées à l'interface **WAN**, ce qui correspond aux tentatives de connexion externes venant de l'Internet.
- **LAN0** : 4% des événements concernent l'interface **LAN0**, qui est généralement moins exposée car elle fait partie du réseau interne.

Cette répartition montre une forte activité sur les segments exposés, notamment la DMZ et le WAN, qui sont les points d'entrée principaux pour des accès externes.

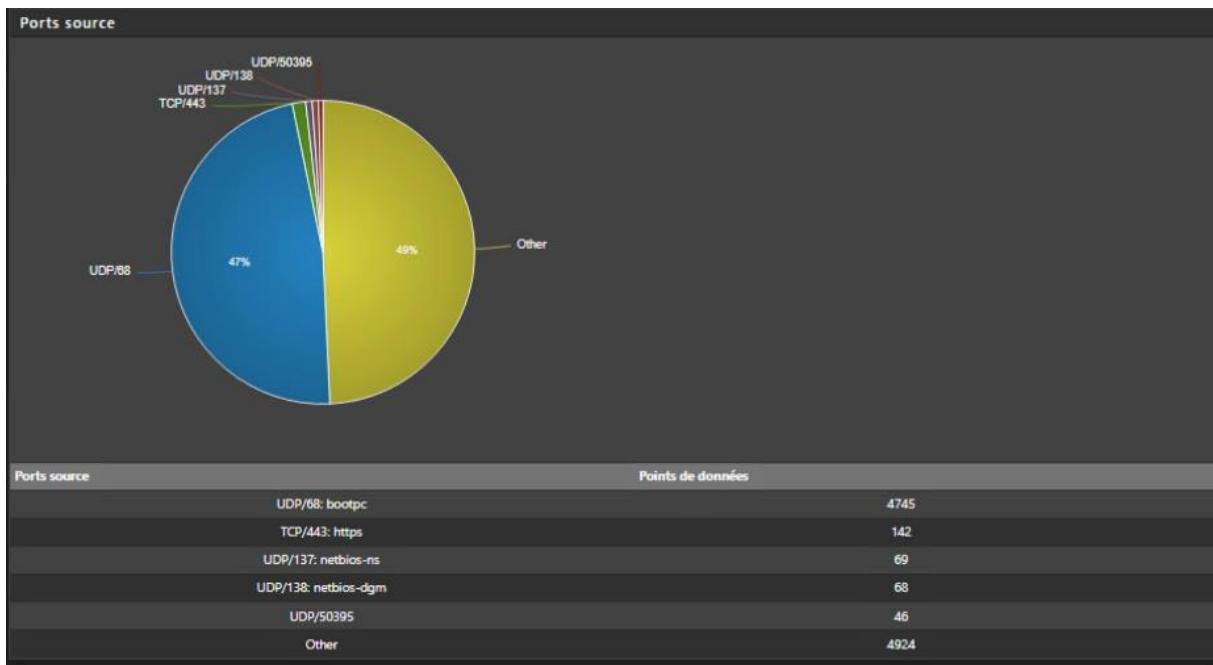
C'est normal, étant donné que j'ai eu beaucoup d'activité sur mon serveur web.



Adresses IP Source

Le troisième graphique illustre les différentes **adresses IP source** qui ont généré des tentatives de connexion enregistrées dans les logs.

- **0.0.0.0** : 48% des requêtes proviennent de l'adresse 0.0.0.0, souvent utilisée dans les requêtes DHCP lorsqu'un appareil essaie d'obtenir une adresse IP sur le réseau.
- **10.9.104.10** : 47% des requêtes proviennent de l'adresse interne 10.9.104.10 (située dans la DMZ). Cela montre une activité importante depuis ce serveur, potentiellement lié à des services exposés.
- Les autres adresses (10.0.104.10, 192.168.10.201, etc.) sont moins fréquentes, ce qui suggère des tentatives ponctuelles d'accès.



Ports Source

Le dernier graphique présente la répartition des **ports source** utilisés pour les tentatives de communication.

- **UDP/68** : 47% des points de données concernent le port **UDP 68**, qui est utilisé par le **protocole BOOTP/DHCP**. Cela indique des requêtes fréquentes pour obtenir des adresses IP, probablement de la part de nouveaux appareils rejoignant le réseau.
- **TCP/443** : 142 requêtes sur le port **TCP 443**, qui est utilisé pour des connexions HTTPS. Ces connexions peuvent correspondre à des tentatives de communication sécurisée vers ou depuis des services web.
- **UDP/137 et UDP/138** : Ces ports sont utilisés pour des services NetBIOS, probablement pour la découverte de périphériques dans le réseau local.

7. CONCLUSION DE L'ANALYSE GRAPHIQUE

L'analyse graphique des logs a permis de visualiser clairement les principales caractéristiques des tentatives de communication sur le réseau :

- La majorité des actions sont des **blocages**, ce qui est cohérent avec une politique de sécurité stricte.
- La **DMZ** est la plus sollicitée, confirmant que c'est le point d'entrée pour la majorité des tentatives de connexion. (et c'est normal, étant donné que j'ai eu beaucoup d'activité sur mon serveur web)
- Les ports utilisés indiquent une activité liée au **DHCP** et des tentatives de communication HTTPS, ainsi que d'autres protocoles de découverte sur le réseau local.

Ces informations permettent d'ajuster et d'optimiser les règles de pare-feu pour répondre aux exigences de sécurité tout en surveillant les activités suspectes ou inhabituelles. Les graphiques sont un outil précieux pour détecter des comportements anormaux et renforcer la sécurité du réseau.

8. CONFIGURATION DU DHCP

Pour garantir que les différentes machines sur le réseau obtiennent automatiquement une adresse IP, nous avons configuré le service **DHCP** sur pfSense ainsi que les serveurs associés.

Configuration du Relais DHCP sur pfSense

- Nous avons activé le **Relais DHCP** afin de permettre aux appareils des réseaux **WAN**, **LAN0**, **LAN1**, et **LAN2** d'obtenir des adresses IP dynamiques depuis le serveur DHCP.
- Le serveur DHCP en amont est configuré avec l'adresse **10.0.104.1**, ce qui signifie que toutes les requêtes DHCP des interfaces spécifiées seront relayées vers ce serveur.

The screenshot shows the 'Services / Relais DHCP' configuration screen. Under 'Activer', the checkbox 'Activer le relais DHCP' is checked. In the 'Interfaces en aval' section, 'WAN', 'LAN0', 'LAN1', and 'LAN2' are listed. The 'Serveurs en amont' field contains '10.0.104.1'. A green button '+ Ajouter un serveur en amont' is present. A note at the bottom states: 'Adresses IPv4 des serveurs vers lesquels les requêtes DHCP sont relayées.'

8. Configuration du Serveur DHCP Windows

- Comme montré dans le **Gestionnaire de Serveur Windows**, nous avons configuré les étendues de réseau DHCP pour **LAN0 (10.0.104.0)** et **LAN2 (10.2.104.0)**.

The screenshot shows the Windows Server Manager 'DHCP' interface. The left sidebar shows 'DHCP' selected. The main area shows the 'srv10-104.don' server's DHCP configuration. Two scopes are listed: 'Étendue [10.0.104.0] LAN0' and 'Étendue [10.2.104.0] LAN2'. The 'Actions' pane on the right has 'IPv4' selected.

Chaque étendue est configurée pour fournir des adresses IP sur les différents sous-réseaux, garantissant ainsi que chaque machine sur chaque sous-réseau obtienne une IP appropriée.

La configuration permet de mieux segmenter et organiser le réseau en définissant des plages d'adresses précises pour chaque sous-réseau.

Alias de pare-feu Ports				
Nom	Type	Valeurs	Description	Actions
AD	Port(s)	49152	Admin directory	
ANYDESK	Port(s)	6568	Anydesk	
DHCP	Port(s)	67:68	Dynamic Host Configuration Protocol	
DNS	Port(s)	53	service DNS	
MAIL	Port(s)	587, 465, 993, 995	SMTP	
NTP	Port(s)	123	NTP	
SFTP	Port(s)	22, 21	secure shell + FTP	
SSH	Port(s)	22	SSH	
WEB	Port(s)	80, 443	http + ssl	

Ajouter
 Importer

Alias de Pare-feu pour les Ports DHCP

Un alias spécifique a été créé pour les ports **DHCP** sur pfSense.

Les ports **67 et 68** sont utilisés pour le **Dynamic Host Configuration Protocol (DHCP)**. Le port **67** est généralement utilisé par le serveur pour écouter les requêtes, tandis que le port **68** est utilisé par les clients.

Ces alias facilitent la configuration et la gestion des règles de pare-feu pour autoriser ou bloquer le trafic DHCP selon les besoins. En centralisant la gestion des ports sous un alias, nous assurons une maintenance simplifiée et une meilleure lisibilité des règles.

f) VÉRIFICATION DU FONCTIONNEMENT DU DHCP

Ces captures d'écran font partie de la **vérification du fonctionnement du DHCP**. Elles démontrent que les clients du réseau reçoivent bien les informations nécessaires via le service DHCP que nous avons configuré. Voici les éléments clés de la vérification :

- Obtention Automatique d'Adresses IP** : Les deux clients obtiennent des adresses IP (10.0.104.100 et 10.2.104.101), ce qui confirme que le service DHCP est actif et attribue correctement des adresses IP des étendues respectives à chaque sous-réseau.

```
Carte Ethernet Etherneth0 :

Suffrage DNS propre à la connexion... : DOMAD104.peda
Description... : Intel(R) 82574L Gigabit Network Connection
Adresse physique... : 00-50-56-AB-97-D0
DHCP activé... : Oui
Configuration automatique activée... : Oui
Adresse IPv4... : 10.0.104.100(préféré)
Masque de sous-réseau... : 255.255.255.0
Bail obtenu... : mercredi 13 novembre 2024 17:46:11
Bail expirant... : mardi 19 novembre 2024 17:46:26
Passerelle par défaut... : 10.0.104.254
Serveur DHCP... : 10.0.104.1
Serveurs DNS... : 10.0.104.1
NetBIOS sur Tcpip... : Activé
Activ
```

```
Carte Ethernet Ethernet0 :

Suffrage DNS propre à la connexion... : DOMAD104.peda
Description... : Intel(R) 82574L Gigabit Network Connection
Adresse physique... : 00-50-56-AB-E8-B0
DHCP activé... : Oui
Configuration automatique activée... : Oui
Adresse IPv4... : 10.2.104.101(préféré)
Masque de sous-réseau... : 255.255.255.0
Bail obtenu... : samedi 23 novembre 2024 16:10:57
Bail expirant... : lundi 25 novembre 2024 16:10:57
Passerelle par défaut... : 10.2.104.254
Serveur DHCP... : 10.0.104.1
Serveurs DNS... : 10.0.104.1
NetBIOS sur Tcpip... : Activé

C:\Users\Robert>
```

- Domaine et Serveurs DHCP/DNS :** Le domaine est bien appliqué (DOMAD104.peda), et les serveurs DHCP et DNS sont correctement assignés, validant que les options de configuration sont bien transmises aux clients.
- Ces éléments valident la bonne fonctionnalité du service DHCP pour la distribution des adresses IP, des paramètres de DNS, et de la passerelle par défaut sur l'ensemble des réseaux configurés.

g) CONFIGURATION DES ALIAS

Création des Alias pour les Ports Web HTTP et HTTPS

Pour simplifier la gestion des règles de pare-feu sur pfSense, nous avons créé des alias pour les ports souvent utilisés, notamment les ports liés aux services web. Les alias permettent de regrouper plusieurs ports ou adresses IP sous une même désignation, facilitant ainsi la configuration et la maintenance des règles de sécurité.

Alias de pare-feu Ports				
Nom	Type	Valeurs	Description	Actions
AD	Port(s)	49152	Admin directory	
ANYDESK	Port(s)	6568	Anydesk	
DHCP	Port(s)	67:68	Dynamic Host Configuration Protocol	
DNS	Port(s)	53	service DNS	
MAIL	Port(s)	587, 465, 993, 995	SMTP	
NTP	Port(s)	123	NTP	
SFTP	Port(s)	22, 21	secure shell + FTP	
SSH	Port(s)	22	SSH	
WEB	Port(s)	80, 443	http + ssl	

[+ Ajouter](#) [Importer](#)

Cet alias regroupe les ports **80** (HTTP) et **443** (HTTPS). Cela permet de faciliter l'application de règles pour l'ensemble du trafic web, qu'il soit sécurisé (HTTPS) ou non sécurisé (HTTP).

Ces alias nous permettent de configurer des règles de pare-feu de manière plus efficace et moins sujette aux erreurs, en nous donnant la possibilité de référencer les services web par un seul nom plutôt que de spécifier chaque port à chaque règle. C'est particulièrement utile lorsqu'il s'agit de modifier ou d'auditer des règles, car un alias est beaucoup plus explicite et facile à mettre à jour.

9. SECURISATION DE L'ACCES :

h) CONFIGURATION DU SSH - SECURISATION DE L'ACCES

Pour sécuriser l'accès à notre pare-feu via SSH, nous avons activé et configuré certaines options importantes qui permettent de renforcer la sécurité de ce point d'accès critique. Voici les détails des choix de configuration :

9. ACTIVATION ET CONFIGURATION DU SERVEUR SSH

Serveur SSH Activé : Nous avons coché l'option "Activer Shell Sécurisé (SSH)" pour permettre la connexion distante à pfSense via SSH. Cela facilite la gestion à distance, mais cela représente également un risque s'il n'est pas correctement sécurisé.

Clé SSHD Uniquement : Nous avons laissé l'option sur "**Password or Public Key**". Cela permet de se connecter soit avec un mot de passe soit avec une clé publique. Cela donne la flexibilité d'utiliser des clés SSH sécurisées, ce qui est recommandé pour une sécurité accrue, tout en laissant la possibilité d'utiliser des mots de passe, ce qui peut être utile pour des utilisateurs ne disposant pas de clé.

Protection des Connexions - Login Protection

Pour protéger davantage l'accès SSH, nous avons mis en place des mécanismes de protection pour limiter les tentatives de connexion abusives :

- Seuil (Threshold)** : Le seuil est fixé à 3 tentatives échouées. Si un utilisateur échoue à se connecter après trois essais, il est considéré comme suspect. Cela permet de détecter rapidement les tentatives de connexion par force brute.
- Blocktime (Temps de Blocage)** : Nous avons fixé un temps de blocage de 120 secondes après avoir dépassé le seuil de tentatives échouées. Cela signifie que toute adresse IP ayant échoué à se connecter plus de trois fois sera temporairement bloquée pendant deux minutes. Ce blocage initial décourage les tentatives répétées.
- Detection Time (Temps de Détection)** : Nous avons configuré une durée de détection de 1800 secondes (30 minutes). Cela signifie que les tentatives de connexion échouées seront mémorisées pendant une période de 30 minutes avant que le score de l'adresse IP ne soit réinitialisé. Cela permet de mieux suivre les activités suspectes sur une période de temps plus longue.

i) CONFIGURATION DE LA REGLE DE PARE-FEU SSH

Configuration de la Règle SSH dans pfSense

Dans cette section, j'ai configuré une règle de pare-feu pour autoriser l'accès SSH via le port personnalisé 2222, spécifiquement sur l'interface WAN de pfSense. Cette mesure vise à sécuriser et contrôler les accès à notre pare-feu tout en limitant les risques d'attaques automatisées.

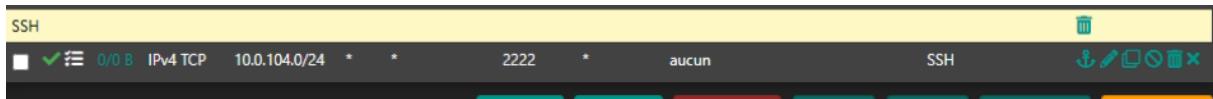
The screenshot shows the configuration of a firewall rule. The rule is set to 'Autoriser' (Allow) and is currently 'Désactivé' (Disabled). It is configured for the 'WAN' interface, IPv4 protocol, and TCP port. The source is set to 'Réseau' (Network) with the IP range 10.0.104.0/24. The destination is set to 'Tous' (All) with port 2222. The rule is labeled 'Activer Windows' (Enable Windows) and 'Accédez aux paramètres pour Windows.' (Access Windows settings).

Pour la configuration de la règle de pare-feu SSH, j'ai mis en place une règle spécifique sur pfSense afin de sécuriser l'accès à distance. L'objectif est de permettre les connexions SSH en utilisant un port personnalisé (port 2222), sur l'interface WAN de pfSense. Cette mesure permet de renforcer la sécurité en évitant l'exposition directe au port par défaut, souvent ciblé par des attaques automatisées.

Pour définir cette règle, j'ai choisi de permettre uniquement les connexions TCP en provenance du réseau interne 10.0.104.0/24, limitant ainsi l'accès aux machines

autorisées au sein du réseau local. En définissant l'interface WAN, j'ai veillé à ce que les connexions SSH autorisées proviennent de l'extérieur du réseau local, pour faciliter l'administration à distance tout en maintenant un contrôle strict des accès.

L'utilisation du port personnalisé 2222 au lieu du port par défaut 22 est une pratique courante pour limiter les tentatives de scans automatisés visant à exploiter des vulnérabilités sur SSH. De plus, l'accès est limité uniquement aux machines se trouvant sur le sous-réseau interne spécifié, garantissant ainsi une couche supplémentaire de sécurité.



L'ensemble de ces mesures a pour but de protéger les accès administratifs à pfSense, en minimisant les risques de compromission liés à des tentatives d'intrusion via le port SSH.

10. EXPLICATION DES CHOIX DE CONFIGURATION DES REGLES DE PARE-FEU WAN

Les règles de pare-feu que nous avons mises en place sur pfSense sont conçues pour répondre à la fois aux besoins de sécurité et à la nécessité d'une connectivité fonctionnelle sur le réseau. Voici une explication détaillée des raisons pour lesquelles chaque règle a été configurée de cette manière et quel est son but :

Règles (Faire glisser pour changer l'ordre)											
	États	Protocole	Source	Port	Destination	Port	Passerelle	Filaire d'attente	Ordonnancement	Description	Actions
ANYDESK											
■ ✓ 0/0 IPv4 TCP	*	*	ANYDESK	*	ANYDESK	*	aucun		ANYDESK		trash edit
SFTP											
■ ✓ 0/0 IPv4 TCP	*	*	SFTP	*	SFTP	*	aucun		SFTP		trash edit
SSH											
■ ✓ 0/0 IPv4 TCP	10.0.104.0/24	*	*	2222	*	*	aucun		SSH		trash edit
DMZ											
■ ✓ 0/0 IPv4 TCP	DMZ address	*	LAN0 address	*	*	*	aucun				trash edit
■ ✓ 0/0 IPv4 TCP	*	*	WEB	DMZ address	443	(HTTPS)	*	aucun	WEB - DMZ		trash edit
ICMP											
■ ✓ 0/0 IPv4 ICMP	*	*	*	*	*	*	aucun		PING - ECHO REPLY TRACEROUT		trash edit
■ ✘ 0/0 IPv4 ICMP	*	*	*	*	*	*	aucun		Bloquer ICMP		trash edit
Règles test											
■ ✓ 0/0 IPv4 ICMP	*	*	*	*	*	*	aucun				trash edit
■ ✓ 0/0 IPv4 TCP	LAN2 subnets	*	WAN subnets	*	*	*	aucun				trash edit
■ ✓ 0/0 IPv4 TCP	WAN address	*	*	*	*	*	aucun				trash edit
Activer Windows											
BLOQUER TOUT											
■ ✘ 0/0 IPv4 TCP	*	*	*	*	*	*	aucun		Bloquer TOUT		trash edit

Autorisation des Connexions ANYDESK et SFTP

- **Justification** : Ces règles permettent des accès à distance via **AnyDesk** et des transferts de fichiers via **SFTP**. AnyDesk est utilisé pour les connexions de bureau à distance, tandis que SFTP assure des transferts de fichiers sécurisés.
- **Pourquoi ?** : Ces services sont nécessaires pour permettre la gestion à distance et le transfert sécurisé de données, souvent essentiels pour la maintenance des systèmes. Le choix de laisser ces connexions ouvertes est justifié par la nécessité de permettre aux administrateurs ou aux utilisateurs autorisés d'intervenir sur les ressources, tout en limitant l'accès à des ports spécifiques.

Connexion SSH sur un Port Personnalisé (2222)

- **Justification** : Nous avons activé le **SSH** mais sur un **port non standard** (2222 au lieu de 22).
- **Pourquoi ?** : L'utilisation d'un port personnalisé est une mesure de sécurité supplémentaire, souvent appelée **sécurité par obscurité**, qui a pour but de compliquer les tentatives de reconnaissance par des attaquants. Les scripts automatisés recherchent souvent le port 22 pour SSH, et changer de port réduit les risques d'attaques opportunistes. Le fait de restreindre l'accès SSH au réseau 10.0.104.0/24 limite davantage la possibilité de connexion uniquement aux machines locales.

Accès entre la DMZ et le LAN0

- **Justification** : Permettre les connexions de la **DMZ vers LAN0**.
- **Pourquoi ?** : Les serveurs en DMZ doivent parfois communiquer avec des systèmes internes pour accéder à des bases de données ou d'autres ressources. Par exemple, un serveur web dans la DMZ pourrait avoir besoin de récupérer des informations d'une base de données située dans le LAN. Cette règle est là pour permettre cette communication, tout en minimisant l'exposition du LAN aux attaques externes. Nous avons cependant restreint la communication pour qu'elle se fasse **uniquement depuis la DMZ** et non dans l'autre sens, afin de minimiser les risques de compromission interne.

Autorisation de Requêtes ICMP pour Diagnostic

- **Justification** : Nous avons autorisé certaines requêtes **ICMP** (comme le **ping** et le **traceroute**), mais en bloquant toutes les autres.
- **Pourquoi ?** : **ICMP** est essentiel pour des **diagnostics réseau**. Par exemple, **ping** est utilisé pour vérifier la connectivité entre deux nœuds réseau. En autorisant les réponses ICMP (comme echo-reply), nous nous assurons que nous pouvons vérifier la disponibilité des ressources réseau lorsque nécessaire. Cependant, d'autres types de requêtes ICMP peuvent être exploitées à des fins malveillantes, par exemple pour obtenir des informations sur la topologie réseau. En bloquant toutes les requêtes ICMP non spécifiées, nous limitons les vecteurs potentiels d'attaque tout en conservant les capacités de diagnostic.

Blocage des Paquets ICMP Restants

- **Justification** : Une règle de **blocage ICMP** générale est mise en place après l'autorisation sélective.
- **Pourquoi ?** : Une fois que les types de requêtes ICMP nécessaires ont été autorisés, il est essentiel de bloquer tout le reste pour éviter que des attaquants utilisent ces paquets pour obtenir des informations sensibles. En bloquant spécifiquement le reste des paquets ICMP, nous gardons un contrôle strict sur ce qui est autorisé ou non en termes de communication réseau.

Tests et Accès Réseau (Règles Test)

- **Justification** : Certaines règles ont été créées pour permettre le **trafic ICMP** et les connexions **LAN2 vers WAN**.
- **Pourquoi ?** : Ces règles peuvent être temporairement activées pour des **tests réseau** ou des diagnostics. Par exemple, autoriser tout le trafic ICMP permettrait de vérifier la connectivité à travers différentes interfaces, utile lors de mises en place ou lors de diagnostics. L'autorisation du trafic **LAN2 vers WAN** permet aux hôtes de LAN2 d'accéder à Internet, ce qui peut être nécessaire pour des mises à jour logicielles ou des communications externes.

Règle BLOQUER TOUT

- **Justification** : Une règle générale pour **bloquer tout le trafic** non explicitement autorisé est ajoutée à la fin.
- **Pourquoi ?** : Cette règle est cruciale pour assurer que tout ce qui n'est pas spécifiquement autorisé soit automatiquement bloqué. Cela représente une bonne pratique de **sécurité en réseau**, appelée **politique de refus par défaut**. Cela signifie que seuls les services explicitement définis dans les règles sont autorisés, tandis que tout le reste est rejeté, réduisant ainsi la surface d'attaque potentielle.

Conclusion :

Chaque règle de pare-feu a été soigneusement configurée pour répondre aux exigences de sécurité tout en maintenant les fonctionnalités nécessaires :

1. **Accès Autorisé à Certains Services** (AnyDesk, SFTP, SSH) : Pour permettre la gestion et la maintenance du réseau.
2. **Connexions Restreintes Entre la DMZ et le LAN** : Pour minimiser le risque de compromission tout en permettant des services nécessaires.
3. **ICMP Sélectivement Autorisé** : Pour assurer une capacité de diagnostic tout en limitant les vecteurs d'attaque.
4. **Blocage Général par Défaut** : Pour assurer qu'aucune communication non autorisée ne passe, contribuant à un réseau plus sécurisé.

En résumé, cette configuration de règles de pare-feu vise à **maximiser la sécurité tout en maintenant les services nécessaires**, en adoptant une approche de limitation stricte des communications au strict nécessaire. Cela contribue à une bonne gestion de la sécurité du réseau en minimisant les risques tout en assurant une certaine flexibilité.

11. EXPLICATION DES CHOIX DE CONFIGURATION DES REGLES DE PARE-FEU LAN

La configuration des règles de pare-feu sur pfSense que nous voyons ici permet de garantir un équilibre entre sécurité et fonctionnalité sur le réseau. Voici une explication détaillée des choix de chaque règle :

Règles (Faire glisser pour changer l'ordre)										
	États	Protocole	Source	Port	Destination	Port	Filtre d'attente	Ordonnancement	Description	Actions
✓ 0/17,75 MiB	*	*	*	*	LAN0 Address	443 80 2222	*	*	Règle anti-blocage	
Autoriser DNS										
✓ 1/43,12 MiB	IPv4 TCP/UDP	10.0.104.1	*	*	DNS	*	aucun		Autoriser DNS (port 53) depuis LAN0 vers Internet	
✓ 0/0 B	IPv4 UDP	LAN0 address	*	*	LAN0 subnets	DNS	*	aucun	Autoriser DNS (port 53) depuis LAN0 vers LAN0	
Autoriser ANYDESK										
✓ 0/0 B	IPv4 TCP	LAN0 address	*	*	ANYDESK	*	aucun		ANYDESK	
Autoriser WEB										
✓ 0/0 B	IPv4 TCP	LAN0 address	*	*	WEB	*	aucun			
ICMP										
✓ 0/0 B	IPv4 ICMP	*	*	*	*	*	*	aucun		
✗ 0/0 B	IPv4 ICMP	*	*	*	*	*	*	aucun		
Règles de test										
✓ 78/4,83 GiB	IPv4 *	LAN0 subnets	*	*	*	*	*	aucun	Default allow LAN to any rule	
✓ 0/0 B	IPv4 TCP	*	161 (SNMP)	*	161 (SNMP)	*	aucun		SNMP	
Bloquer tout										
✗ 0/0 B	IPv4 TCP	*	*	*	*	*	*	aucun	Activer Windows	
									Accédez aux paramètres pour Windows.	

Ces règles de pare-feu sur pfSense suivent la même logique que celles déjà mises en place pour l'interface **WAN**, mais appliquées ici à l'interface **LAN**. Voici une version concise des explications :

Règles Anti-blocage, DNS, AnyDesk, et Web

- Même logique qu'en WAN** : Ces règles sont configurées pour garantir l'accès aux services essentiels, comme le **DNS** (pour la résolution de noms), **AnyDesk** (pour l'accès à distance), **HTTP/HTTPS** (pour la navigation web), et **SSH** (port personnalisé pour sécurité supplémentaire).
- Pourquoi ?** : Elles permettent aux utilisateurs du **LAN** de bénéficier d'une connectivité optimale, tout en maintenant les accès sécurisés et contrôlés.

ICMP

- Même logique qu'en WAN** : Autorisation des requêtes **ICMP** nécessaires (comme **ping**) et blocage de tout le reste.
- Pourquoi ?** : Permettre des diagnostics réseau depuis l'intérieur du réseau, tout en empêchant toute utilisation malveillante des autres types de paquets ICMP.

SNMP

- Même logique qu'en WAN** : Autorisation du protocole **SNMP** (port 161) pour permettre la supervision des équipements réseau.
- Pourquoi ?** : Facilite la surveillance et la gestion des équipements du réseau depuis le LAN.

Blocage Général

- Même logique qu'en WAN** : Une règle de **blocage par défaut** est présente pour bloquer tout ce qui n'est pas explicitement autorisé.
- Pourquoi ?** : Garantit que tout trafic non prévu est bloqué, minimisant ainsi la surface d'attaque.

Conclusion

- Ces règles appliquent la même logique de sécurité que les règles précédemment établies pour le **WAN**, mais cette fois sur l'interface **LAN**. Elles assurent une bonne connectivité interne tout en garantissant la sécurité des communications, avec un **blocage par défaut** des services non nécessaires.

12. EXPLICATION DES CHOIX DE CONFIGURATION DES REGLES DE PARE-FEU LAN.1

Les règles appliquées à l'interface **LAN1** suivent une logique similaire à celles des interfaces **WAN** et **LAN0**. Elles sont mises en place pour autoriser les services nécessaires tout en contrôlant les flux de manière sécurisée :

Floating(e)	WAN	LAND	LAN1	LAN2	DMZ						
Règles (Faire glisser pour changer l'ordre)											
	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
NEXCLOUD											
	■ ✓ 0/0 B	IPv4 TCP	*	*	NEXTCLOUD	*	NEXTCLOUD	*	aucun	NEXTCLOUD	Supprimer Editer Copier Coller Supprimer
GLPI											
	■ ✓ 0/0 B	IPv4 TCP	*	*	(GLPI)	*	GLPI	*	aucun	GLPI	Supprimer Editer Copier Coller Supprimer
ANYDESK											
	■ ✓ 0/0 B	IPv4 TCP	*	*	ANYDESK	*	ANYDESK	*	aucun	ANYDESK	Supprimer Editer Copier Coller Supprimer
ICMP											
	■ ✓ 0/0 B	IPv4 ICMP echoreq, infreq, infreq, timer, trace, unreachable	*	*	*	*	*	*	aucun	ICMP	Supprimer Editer Copier Coller Supprimer
	■ ✘ 0/0 B	IPv4 ICMP any	*	*	*	*	*	*	aucun		Supprimer Editer Copier Coller Supprimer
Règles TEST											
	■ ✓ 0/1,84 GiB	IPv4 *	LAN1 subnets	*	*	*	*	*	aucun		Supprimer Editer Copier Coller Supprimer
	■ ✓ 0/0 B	IPv4 TCP	*	*	*	*	*	*	aucun		Supprimer Editer Copier Coller Supprimer
BLOQUER TOUT											
	■ ✘ 0/0 B	IPv4 TCP	*	*	*	*	*	*	aucun	Activer Windows	Supprimer Editer Copier Coller Supprimer
										Accédez aux paramètres pour activer	Supprimer Editer Copier Coller Supprimer
										Windows	Supprimer Editer Copier Coller Supprimer
										Enregistrer	Supprimer Editer Copier Coller Supprimer
										Séparateur	Supprimer Editer Copier Coller Supprimer

Règles NEXTCLOUD, GLPI, et ANYDESK

Même logique qu'en WAN/LAN0 : Ces règles autorisent les connexions vers des services spécifiques :

- NEXTCLOUD** : Accès au service de stockage et de collaboration en ligne.
- GLPI** : Accès à l'application de gestion des tickets et des inventaires.

- **ANYDESK** : Connexion à distance via AnyDesk.

Conclusion

Les règles de l'interface **LAN1** sont en cohérence avec les autres segments du réseau, garantissant une **connectivité contrôlée** tout en assurant la **sécurité**. Elles permettent l'accès à des applications importantes (comme **Nextcloud** et **GLPI**), autorisent des diagnostics avec **ICMP**, tout en appliquant un **blocage par défaut** pour renforcer la sécurité. Ces configurations maintiennent l'équilibre entre fonctionnalité et sécurité au sein de l'interface **LAN1**.

13. EXPLICATION DES CHOIX DE CONFIGURATION DES REGLES DE PARE-FEU LAN.2

Pour l'interface **LAN2**, la configuration suit le même schéma que pour les interfaces précédentes. Voici une explication concise de chaque règle, tout en soulignant la continuité avec la logique appliquée au **WAN**, **LAN0**, et **LAN1** :

Pare-feu / Règles / LAN2										
Floating(e)	WAN	LAN0	LAN1	LAN2	DMZ	OpenVPN				
Règles (Faire glisser pour changer l'ordre)										
États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
SSH			*	*	SSH	*	aucun			
<input checked="" type="checkbox"/> ✓ 0/120 B	IPv4 TCP	LAN2 subnets	*	*	SSH	*	aucun			
DNS			*	*	DNS	*	aucun			
<input checked="" type="checkbox"/> ✓ 1/436 B	IPv4 UDP	LAN2 subnets	*	*	DNS	*	aucun			
WEB			*	*	WEB	*	aucun			
<input checked="" type="checkbox"/> ✓ 0/2,46 GiB	IPv4 TCP	LAN2 subnets	*	*	WEB	*	aucun			
DHCP			*	*	DHCP	*	DHCP	*	aucun	
<input checked="" type="checkbox"/> ✓ 0/0 B	IPv4 TCP	*	*	*	DHCP	*	aucun			
Règles test			*	*	*	*	aucun			
<input checked="" type="checkbox"/> ✓ 0/1,08 GiB	IPv4 TCP/UDP	LAN2 subnets	*	*	*	*	aucun			
<input checked="" type="checkbox"/> ✓ 0/0 B	IPv4 TCP	LAN2 address	*	*	*	*	aucun			
Bloquer tout			*	*	*	*	aucun			
<input checked="" type="checkbox"/> ✘ 0/0 B	IPv4 TCP	LAN2 subnets	*	*	*	*	aucun			
Ajouter Ajouter Supprimer Toggle Copier Enregistrer Séparateur										

4. Règle DHCP

Pourquoi ? : Cette règle est essentielle pour assurer que les appareils de **LAN2** puissent obtenir des adresses IP de manière automatique, facilitant la gestion des adresses IP sur le réseau.

Règle de Test - Règles test

Même logique qu'en WAN/LAN0/LAN1 : Autoriser tout le trafic depuis **LAN2** pour effectuer des tests.

Pourquoi ? : Cette règle permet de vérifier le bon fonctionnement du réseau et de diagnostiquer des problèmes potentiels, tout en assurant une flexibilité temporaire qui sera réduite après la stabilisation.

L'interface **LAN2** reprend exactement les mêmes principes de configuration que les autres interfaces réseau. Les règles mises en place permettent de maintenir une balance entre **accessibilité** et **sécurité** pour des services comme **SSH**, **DNS**, **WEB**, et **DHCP**, tout en

garantissant qu'aucun trafic non autorisé ne traverse l'interface. La règle de **blocage par défaut** renforce la posture de sécurité du réseau en limitant les vecteurs d'attaque potentiels.

14. EXPLICATION DES CHOIX DE CONFIGURATION DES REGLES DE PARE-FEU DMZ

Les règles configurées sur l'interface **DMZ** reprennent également la même logique de sécurité que celles des interfaces **WAN**, **LAN0**, **LAN1**, et **LAN2**. Voici une explication concise des choix réalisés :

La **DMZ** est souvent utilisée pour héberger des services publics comme des serveurs web. Autoriser le trafic web (HTTP/HTTPS) sur la **DMZ** permet d'assurer que ces services restent accessibles depuis l'extérieur tout en étant isolés du réseau interne, renforçant ainsi la sécurité.

The screenshot shows the PFSENSE Firewall Rules configuration interface. The top navigation bar includes tabs for Flottant(e), WAN, LAN0, LAN1, LAN2, DMZ (which is selected and highlighted in blue), and OpenVPN. Below the tabs is a table titled "Règles (Faire glisser pour changer l'ordre)". The table has columns for États, Protocole, Source, Port, Destination, Port, Passerelle, File d'attente, Ordonnancement, Description, and Actions. The table lists several rules categorized under WEB, DNS, and DMZ. At the bottom of the table, there is a red row labeled "BLOQUER TOUT". Below the table are several action buttons: Ajouter (Add), Supprimer (Delete), Toggle, Copier (Copy), Enregistrer (Save), and Séparateur (Separator).

Assurer qu'aucun accès non souhaité ne soit permis à la **DMZ**. Cette règle de blocage global par défaut renforce la sécurité de la DMZ en s'assurant que seuls les flux explicitement autorisés passent, minimisant ainsi la surface d'attaque.

Les règles appliquées sur l'interface **DMZ** suivent la même logique que pour les autres interfaces, mais sont adaptées pour répondre aux besoins spécifiques de la **zone démilitarisée** (DMZ). Cela inclut la possibilité de gérer des services publics (serveur web) tout en maintenant un **isolement fort** du reste du réseau interne et en limitant l'exposition aux attaques. Le **blocage global par défaut** reste une mesure de sécurité clé, garantissant que seuls les services nécessaires à la DMZ sont autorisés.

Conclusion Générale sur les Règles de Pare-feu

La configuration des règles de pare-feu pour les différentes interfaces du réseau (**WAN**, **LAN0**, **LAN1**, **LAN2**, et **DMZ**) a été réalisée dans le but de garantir un **équilibre optimal entre sécurité et accessibilité** des services. Les règles mises en place suivent une logique commune qui assure une gestion cohérente des flux réseau tout en protégeant chaque segment contre des attaques potentielles.

- Contrôle Accès Spécifique** : Chaque interface possède des règles permettant des services précis, comme **SSH** pour l'administration à distance, **DNS** pour la résolution de noms, et des applications particulières telles que **Nextcloud**, **AnyDesk**, et **GLPI**. Cela permet une gestion ciblée des besoins du réseau tout en minimisant les risques en autorisant uniquement le trafic nécessaire.

- **Sécurité via Blocage Par Défaut** : Les règles de **blocage par défaut** (règle "BLOQUER TOUT") garantissent qu'aucun trafic non explicitement autorisé ne puisse transiter sur le réseau. Ce concept de "par défaut, tout est interdit sauf exception" est une bonne pratique de sécurité qui limite la surface d'attaque et permet de restreindre le trafic aux seuls services nécessaires.

15. PROTECTION CONTRE LE DNS REBINDING

10. QU'EST-CE QUE LE DNS REBINDING ?

Le **DNS rebinding** est une technique d'attaque qui exploite le système de résolution de noms de domaine (DNS) pour contourner les restrictions de sécurité, notamment celles mises en place par un **pare-feu** ou une **politique de même origine** des navigateurs. L'attaquant peut tromper les navigateurs en leur faisant croire qu'ils se connectent à une ressource de confiance alors qu'en réalité, ils sont dirigés vers un serveur malveillant.

L'attaque commence généralement par une requête DNS qui, dans un premier temps, retourne une adresse IP légitime. Lors d'une seconde requête, le DNS peut fournir une autre adresse IP, souvent une adresse interne au réseau local. Cette modification permet à l'attaquant d'accéder à des ressources internes à travers un simple navigateur, car ce dernier croira que la connexion provient d'un site de confiance.

11. 2. Types d'Attaques par DNS Rebinding

- **Accès aux Réseaux Locaux** : Un attaquant peut utiliser le DNS rebinding pour accéder à des services non exposés sur le réseau interne (comme des interfaces de gestion de routeurs).
- **Vol de Données** : Avec cette technique, des informations sensibles peuvent être récupérées en manipulant des requêtes HTTP, notamment dans des applications web internes qui ne nécessitent pas d'authentification.
- **Bypass des Politiques de Sécurité** : Cette attaque permet également de contourner des politiques de sécurité telles que la **même origine** du navigateur, permettant des actions malveillantes via des scripts dans le navigateur.

12. EXPLICATION DES CHOIX DE CONFIGURATION

Dans le cadre de la configuration de pfSense pour protéger contre le DNS rebinding, voici les actions que j'ai entreprises :

The screenshot shows the 'Services / DNS Forwarder' configuration page. At the top, a yellow banner states: 'ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.' Below this, the 'Options générales du DNS Forwarder' section contains several configuration items:

- Activer**: A checked checkbox labeled 'Activer le transitaire DNS'.
- Enregistrement DHCP**: An unchecked checkbox labeled 'Enregistrer les baux DHCP dans le transitaire DNS'. A note below explains: 'Si cette option est active, les machines qui indiquent leur nom d'hôte lors de la demande d'un bail DHCP seront enregistrées dans le DNS Forwarder, afin que leur nom puisse être résolu. Le domaine indiqué dans Système : Paramètres Généraux devra également être positionné à la bonne valeur.'
- DHCP statique**: An unchecked checkbox labeled 'Enregistrer la cartographie statique DHCP dans le transitaire DNS'. A note below explains: 'Si cette option est activée, les mappages statiques DHCP IPv4 DHCP seront enregistrés dans le redirecteur DNS afin que leur nom puisse être résolu. Le domaine en Système : Configuration générale devra aussi être réglé à la bonne valeur.'
- Préférer DHCP**: An unchecked checkbox labeled 'Résoudre la cartographie DHCP en premier'. A note below explains: 'Si cette option est active, la correspondance DHCP sera résolue avant la liste de noms manuelle ci-dessous. Ceci n'affecte que les noms donnés pour une recherche inversée (PTR).'

Activation du Transitaire DNS : En activant le **transitaire DNS**, pfSense devient responsable de la résolution des noms de domaines internes. Cela permet de garder un contrôle sur les résolutions DNS et de protéger les requêtes des utilisateurs.

Enregistrement des Baux DHCP dans le DNS Forwarder :

- Cette option permet d'enregistrer automatiquement les noms d'hôtes associés aux baux **DHCP** dans le DNS local. Cela renforce la capacité de pfSense à gérer les résolutions DNS de manière centralisée.

Options Personnalisées - Protection Rebinding :

- Dans les **options personnalisées**, l'ajout de la directive `rebind-domain-ok=/localdomain/` permet de spécifier que certains domaines locaux sont exclus de la protection contre le rebinding. Cela permet d'éviter des blocages inutiles lorsque le réseau interne utilise des domaines locaux.

The screenshot shows the 'Options personnalisés' configuration page. It features a text input field containing the value `rebind-domain-ok=/localdomain/`. Above the input field, a note reads: 'Cette option ne fonctionne PAS avec IPv6. Si active, le dnsmasq n'écoute pas sur les adresses IPv6.' Below the input field, a note says: 'Entrer toute option additionnelle à ajouter à la configuration du dnsmasq, séparées par un espace ou un saut de ligne.' At the bottom, there is a green 'Enregistrer' button.

13. CONCLUSION

La configuration effectuée sur pfSense est destinée à empêcher que des requêtes DNS malicieuses puissent détourner le trafic interne, notamment vers des serveurs compromettants. En limitant l'accès aux noms de domaine fiables et en inscrivant les baux **DHCP** dans le DNS local, pfSense garantit une résilience accrue face aux attaques de rebinding, tout en maintenant l'opérabilité des services légitimes. Cette combinaison de sécurité et de flexibilité est essentielle pour assurer une défense efficace contre les tentatives de manipulation DNS.

16. CONFIGURATION DES REDIRECTIONS ET DU NAT

Les redirections NAT configurées ici visent à permettre un accès sécurisé aux services internes, tout en améliorant la sécurité globale du réseau. Ces règles ont été soigneusement

mises en place pour assurer que le trafic entrant est contrôlé et orienté vers les bons services hébergés dans la **DMZ**, tout en limitant l'exposition inutile.

La première règle porte sur la redirection du trafic **HTTP** depuis le **LAN0** vers la **DMZ** pour le transformer automatiquement en **HTTPS**. Cette redirection garantit que toutes les connexions à destination de ce service soient sécurisées. En d'autres termes, chaque fois qu'un utilisateur interne tente d'accéder au service via **HTTP** (port 80), la requête est automatiquement redirigée vers une connexion chiffrée **HTTPS** (port 443). Cela permet de protéger la confidentialité et l'intégrité des informations échangées. Ainsi, même si un utilisateur tente une connexion non sécurisée, celle-ci est immédiatement redirigée vers une version sécurisée.

Section	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
HTTP vers HTTPS	LAN0	TCP	LAN2 address	80 - 443	DMZ address	80 - 443	10.9.104.1	443 - 806	http -> https	trash
	WAN	TCP	*	*	WAN address	80 - 443	10.9.104.1	443 - 806	SERVEUR WEB	trash
	WAN	TCP	*	80 - 443	DMZ subnets	WEB	10.9.104.1	443 (HTTPS)		trash
	SFTP - WEB	WAN	TCP	*	21 - 22	DMZ subnets	21 - 22	10.9.104.1	2222 - 2223	SFTP pour le serveur web
SFTP AD	WAN	TCP	*	21 - 22	DMZ subnets	21 - 22	10.0.104.1	2222 - 2223	SFTP pour l'AD	trash

Ensuite, une redirection NAT a été mise en place pour le **serveur web** en **DMZ**. Cette redirection permet aux utilisateurs externes d'accéder aux services hébergés en DMZ en utilisant les ports standards **80** et **443**. Cette méthode garantit un accès contrôlé et sécurisé aux services web, tout en maintenant la flexibilité nécessaire pour les utilisateurs extérieurs. L'utilisation des protocoles standards permet d'assurer la compatibilité tout en sécurisant l'accès grâce à des contrôles d'accès stricts.

Pour ce qui est des services **SFTP**, deux règles distinctes ont été ajoutées.

- La première règle concerne le serveur web dans la **DMZ**. Le trafic entrant sur les ports **21-22** est redirigé en interne vers des ports sécurisés, soit **2222-2223**. Cela permet de minimiser les risques en évitant d'utiliser les ports standards directement, tout en autorisant des transferts de fichiers sécurisés vers le serveur web.
- La seconde règle concerne l'**Active Directory (AD)**. De manière similaire, le trafic **SFTP** est redirigé des ports **21-22** vers **2222-2223** au niveau du réseau interne. Cette configuration garantit la sécurité lors de la synchronisation et de la gestion des fichiers avec l'AD.

Pour illustrer la configuration du **NAT FTP**, un exemple spécifique montre l'utilisation du **port 2222** sur l'interface **WAN** qui est redirigé vers le **port 21** sur le serveur interne. Ce choix n'est pas anodin ; il vise à **renforcer la sécurité** en utilisant un port non conventionnel pour les accès externes. Ainsi, les risques d'attaques automatisées, souvent ciblées sur les ports standard comme **21**, sont minimisés. De plus, en restreignant les connexions entrantes à ce port configuré, nous garantissons que seuls les utilisateurs autorisés puissent accéder aux ressources internes. Cela contribue à réduire l'exposition de nos services sensibles aux menaces extérieures.

En conclusion, ces redirections NAT offrent une sécurité accrue grâce à l'utilisation de **ports personnalisés** et en forçant les connexions vers des protocoles sécurisés tels que **HTTPS** et **SFTP**. Les services internes ne sont exposés qu'à travers des règles spécifiques, limitant ainsi la **surface d'attaque** tout en maintenant l'accessibilité pour les utilisateurs légitimes.

17. CONFIGURATION DU PROXY SQUID

Avant de configurer Squid sur pfSense, il est essentiel de prendre une snapshot de la machine virtuelle, car cela représente une étape délicate. Les configurations sur des systèmes comme pfSense peuvent comporter des risques, tels qu'une mauvaise configuration qui pourrait rendre le réseau inaccessible ou entraîner une panne des services.



Prendre un snapshot permet de capturer l'état actuel du système, incluant la configuration et la mémoire de la machine virtuelle, ce qui est très utile pour revenir en arrière si quelque chose ne se passe pas comme prévu. Ainsi, en cas d'erreur ou de problème lors de la configuration de Squid, vous pouvez restaurer rapidement la VM à son état précédent sans pertes significatives.

Cela garantit un retour en arrière facile et sécuritaire, réduisant les risques lors de la mise en œuvre de modifications sur pfSense.



Pour configurer Squid sur pfSense, il est essentiel d'installer les paquets suivants : **Squid** et **SquidGuard**. Squid agit comme un proxy web performant, pouvant fonctionner en tant que proxy HTTP/HTTPS ou reverse proxy. Il intègre des fonctionnalités avancées telles que l'accès à Exchange Web Access, le filtrage SSL, et l'antivirus via C-ICAP. Pour un fonctionnement optimal, Squid requiert l'installation des dépendances : **squidclamav**, **squid_radius_auth**, **squid**, et **c-icap-modules**. SquidGuard, quant à lui, est un filtre d'URL performant, utilisé pour restreindre l'accès à certaines catégories de sites. Les dépendances nécessaires pour SquidGuard incluent **squidguard** et **pfSense-pkg-squid**. Ces paquets et dépendances assurent une sécurité accrue et un meilleur contrôle du trafic réseau.

j) PROXY :

Enable Squid Proxy

- Activer Squid Proxy** est coché, ce qui signifie que Squid est opérationnel sur cette machine. Cela permet à Squid de filtrer et de gérer le trafic des utilisateurs qui passent par les interfaces configurées. Sans cette option activée, Squid serait complètement désactivé et toutes ses fonctions seraient arrêtées.

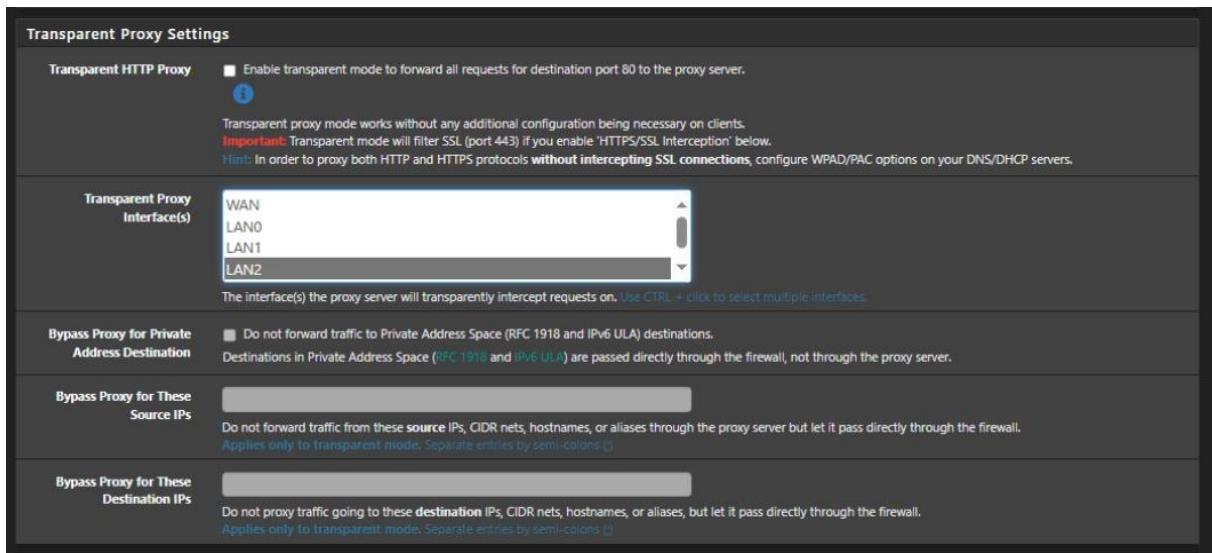
The screenshot shows the 'Squid General Settings' configuration page. The 'General' tab is selected. The configuration includes:

- Enable Squid Proxy:** Checked. A note says: **Important:** If unchecked, ALL Squid services will be disabled and stopped.
- Keep Settings/Data:** Checked. A note says: **Important:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
- Listen IP Version:** IPv4. A note says: Select the IP version Squid will use to select addresses for accepting client connections.
- CARP Status VIP:** aucun. A note says: Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. **Important:** Don't forget to generate Local Cache on the secondary node and configure XMRPC Sync for the settings synchronization.
- Proxy Interface(s):** WAN, LAN0, LAN1, LAN2. A note says: The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
- Outgoing Network Interface:** Default (auto). A note says: The interface the proxy server will use for outgoing connections.
- Port du mandataire (x proxy »):** 3128. A note says: This is the port the proxy server will listen on. Default: 3128.
- ICP Port:** (empty input field). A note says: This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
- Allow Users on Interface:** Checked. A note says: If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.
- Patch Captive Portal:** This feature was removed - see Bug #5594 for details!

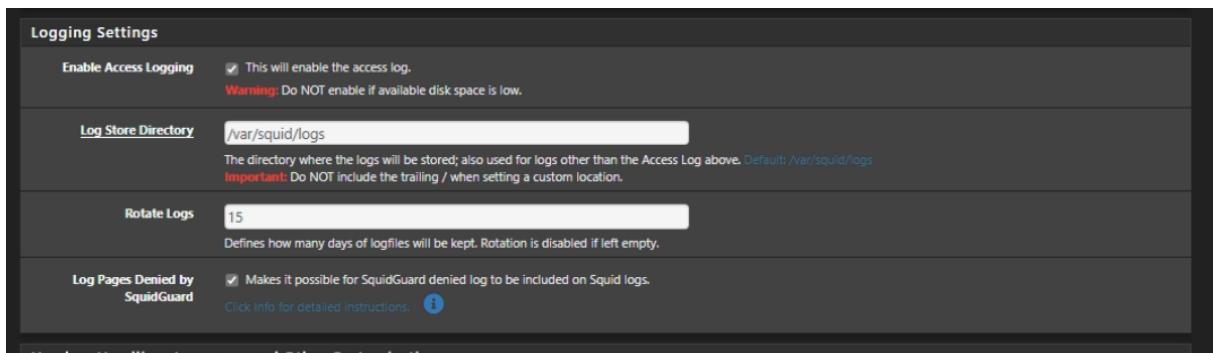
Listen IP Version est défini sur **IPv4**, ce qui indique que Squid écoute uniquement les connexions provenant d'adresses IPv4. Cela signifie que, dans cette configuration, les connexions en IPv6 ne sont pas prises en charge.

CARP Status VIP

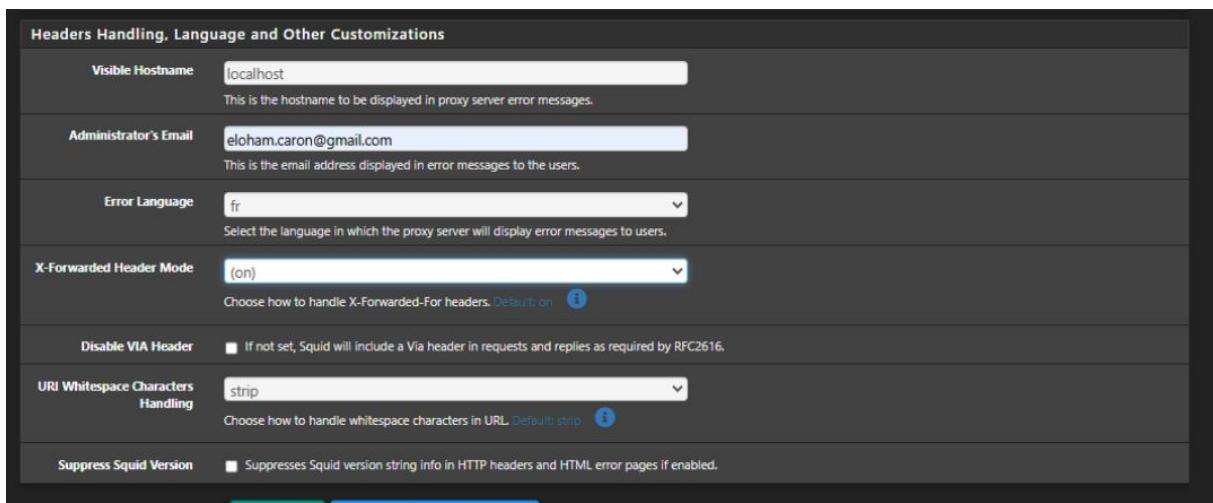
- Le champ **CARP Status VIP** est défini sur "aucun". Cela signifie qu'il n'y a pas de VIP (Virtual IP) de basculement haute disponibilité configuré avec CARP (Common Address Redundancy Protocol). Cela est approprié si vous n'avez pas configuré une infrastructure de haute disponibilité.
- Aucun **ICP Port** n'est configuré. L'ICP (Internet Cache Protocol) est généralement utilisé pour la communication entre les caches voisins. Comme aucun port ICP n'est spécifié, cela signifie que Squid n'est pas configuré pour échanger des informations de cache avec d'autres proxys, ce qui simplifie la configuration si cette fonctionnalité n'est pas nécessaire.
- L'option **Allow Users on Interface** est activée. Cela signifie que les utilisateurs connectés aux interfaces spécifiées (WAN, LAN0, LAN1, LAN2) seront autorisés à utiliser Squid comme proxy. Cette option est utile pour contrôler l'accès au proxy depuis ces interfaces sans avoir besoin de configurer manuellement chaque sous-réseau autorisé.



Pour la configuration de "Transparent Proxy Settings", l'option **Transparent HTTP Proxy** est activée, permettant à Squid d'intercepter automatiquement les requêtes HTTP sur le port 80, sans qu'une configuration manuelle soit nécessaire sur les clients. Les interfaces sélectionnées pour cette interception sont **WAN, LAN0, LAN1, LAN2**, ce qui signifie que le trafic de ces réseaux sera filtré par Squid de manière transparente. L'option **Bypass Proxy for Private Address Destination** est cochée, permettant au trafic destiné à des adresses privées (telles que définies par RFC 1918) d'éviter le proxy, afin de permettre un accès direct aux ressources internes sans interception inutile. Les champs **Bypass Proxy for These Source IPs** et **Bypass Proxy for These Destination IPs** sont laissés vides, ce qui signifie qu'aucune adresse source ou destination spécifique n'est exemptée du filtrage, à moins d'une future configuration.



Pour les paramètres de "Logging Settings", l'option **Enable Access Logging** est activée, ce qui permet l'enregistrement des requêtes d'accès pour une analyse ultérieure. Les journaux sont stockés dans le répertoire **/var/squid/logs**, qui est l'emplacement par défaut pour tous les fichiers journaux générés par Squid. Le paramètre **Rotate Logs** est défini sur **15**, ce qui signifie que les journaux seront conservés pendant 15 jours avant d'être supprimés ou archivés, assurant ainsi une gestion efficace de l'espace disque. Enfin, l'option **Log Pages Denied by SquidGuard** est également activée, permettant d'enregistrer dans les logs toutes les pages bloquées par SquidGuard, ce qui aide à suivre les tentatives d'accès aux contenus non autorisés.



Dans la section **Headers Handling, Language and Other Customizations**, le **Visible Hostname** est défini sur "localhost", ce qui indique que ce nom sera affiché dans les messages d'erreur générés par le serveur proxy. L'adresse e-mail de l'administrateur est configurée à **eloham.caron@gmail.com**, permettant aux utilisateurs de savoir où adresser des questions en cas de problème. La langue des messages d'erreur (**Error Language**) est définie sur **fr**, garantissant que les erreurs seront affichées en français. L'option **X-Forwarded Header Mode** est définie sur "on", permettant la transmission de l'en-tête **X-Forwarded-For** pour suivre les adresses IP d'origine des utilisateurs. L'option **Disable VIA Header** n'est pas cochée, ce qui signifie que l'en-tête **Via** est inclus dans les requêtes pour indiquer le chemin parcouru par celles-ci. Le traitement des espaces dans les URLs (**URI Whitespace Characters Handling**) est réglé sur "strip", ce qui supprime les caractères d'espacement indésirables. Enfin, l'option **Suppress Squid Version** est cochée, ce qui masque la version de Squid dans les en-têtes HTTP et les pages d'erreur, améliorant ainsi la sécurité en ne révélant pas d'informations sur la version utilisée.

18. CLAM-AV

Un antivirus sur un pare-feu, tel que ClamAV intégré à Squid sur pfSense, sert à analyser et filtrer le trafic réseau pour détecter et bloquer les menaces potentielles avant qu'elles n'atteignent les utilisateurs finaux. Lorsqu'un utilisateur télécharge des fichiers ou accède à des contenus potentiellement dangereux, l'antivirus vérifie ces données pour éviter la propagation de virus, de logiciels malveillants, et autres cybermenaces au sein du réseau. Cette mesure préventive est cruciale dans les environnements d'entreprise où la sécurité et la protection des données sont essentielles.

ClamAV est un logiciel antivirus open-source couramment utilisé sur les serveurs et les systèmes de pare-feu pour analyser les courriels, les fichiers, et les flux de données à la recherche de menaces. Il est bien adapté pour une intégration dans des solutions de proxy, car il peut scanner des fichiers en temps réel au fur et à mesure qu'ils transitent par le pare-feu. ClamAV utilise une base de signatures de virus régulièrement mise à jour pour détecter de nouveaux types de menaces, offrant ainsi une couche de sécurité supplémentaire contre les fichiers malveillants.

k) CONFIGURATION :

Pour l'intégration de ClamAV via C-ICAP sur pfSense, j'ai activé l'antivirus pour scanner tout le trafic réseau, en envoyant à chaque analyse le nom d'utilisateur et l'adresse IP (ça facilite l'identification). J'ai choisi de laisser la configuration manuelle désactivée pour simplifier le déploiement, et j'ai laissé le champ de redirection d'URL vide pour rediriger les utilisateurs vers la page par défaut en cas de détection de virus.

The screenshot shows the 'ClamAV Anti-Virus Integration Using C-ICAP' configuration page. Key settings include:

- Enable AV:** Checked, with a note: "Enable Squid antivirus check using ClamAV."
- Client Forward Options:** Set to "Send both client username and IP info (Default)". A note says: "Select what client info to forward to ClamAV."
- Enable Manual Configuration:** Set to "désactivé". A warning: "Warning: Only enable this if you know what you are doing." Below it: "When enabled, the options below no longer have any effect. You must edit the configuration files directly in the 'Advanced Features'. After enabling manual configuration, click the button below once to load default configuration files. To disable manual configuration again, select 'disabled' and click 'Save'." A "Load Advanced" button is present.
- Redirect URL:** An empty input field with a note: "When a virus is found then redirect the user to this URL. Example: http://proxy.example.com/blocked.html. Leave empty to use the default Squid/pfsense WebGUI URL."
- Scan Type:** Set to "All (default)". Sub-options: "All: All data", "Web: Web pages, scripts, images and documents", "Applications: Executables, scripts, archives and documents".
- Exclude Audio/Video Streams:** An unchecked checkbox with a note: "This option disables antivirus scanning of streamed video and audio for the default scan type."
- Block PUA:** A checked checkbox with a note: "This option enables blocking of Potentially Unwanted Applications. See <https://www.clamav.net/documents/potentially-unwanted-applications-pua> for details."
- ClamAV Database Update:** Set to "every 24 hours". A note: " Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here." A "Update AV" button is available.
- Regional ClamAV Database Update Mirror:** Set to "Europe". A note: "Select a regional database mirror. Note: The default ClamAV database mirror performs extremely slow. It is strongly recommended to choose a mirror [here](#) and/or configure your own mirrors manually below."

Activer Windows
Accédez aux paramètres pour activer Windows.

Le type de scan est configuré pour analyser tous les types de données (Web, scripts, images, exécutables). J'ai exclu les flux audio/vidéo pour alléger la charge du serveur. L'option de blocage des applications potentiellement indésirables (PUA) est activée pour éviter les adwares. La mise à jour de la base de données ClamAV est programmée toutes les 24 heures avec un miroir basé en Europe pour améliorer la vitesse des mises à jour.

Cette configuration me permet de garantir une bonne protection du réseau tout en optimisant les ressources.

The screenshot shows the "Unofficial Signatures" configuration page. Available signatures include:

- URLhaus:** Enabled, with a note: "Enables URLhaus active malware distribution sites DB support. The signature file only contains active malware distribution sites or such that have been added to URLhaus in past 48 hours. The false positive rate should be very low. See [URLhaus ClamAV signatures](#) for details."
- InterServer:** Enabled, with a note: "Enables InterServer.net malware DB support. The signature file contains real time suspected malware list as detected by InterServer's InterShield protection system. See [InterServer Real Time Malware Detection](#) for details."
- SecuriteInfo:** Enabled, with a note: "Enables SecuriteInfo.com malware DB support. The signature files contains more than 4.000.000 signatures. At least free registration needed. See [SecuriteInfo signatures info](#) for details. Warning: This option consumes significant amount of RAM."
- SecuriteInfo Premium:** Enabled, with a note: "Enables SecuriteInfo.com 0-day malware DB support. A valid premium subscription ID required."
- SecuriteInfo ID:** An empty input field with a note: "The unique 128 character identifier from one of the download links. Example: https://www.securiteinfo.com/get/signatures/your_unique_and_very_long_random_string_of_characters/securiteinfo.hdb".

Activer Windows
Accédez aux paramètres pour activer Windows.

J'ai activé les signatures URLhaus et InterServer pour augmenter la détection des malwares récents. J'ai laissé SecuriteInfo et SecuriteInfo Premium désactivés pour éviter une

consommation excessive de RAM, car ils sont trop gourmands en ressources. Cette configuration offre un bon compromis entre protection et performance.

I) USERS :

The screenshot shows the 'Paquet / Proxy Server: Local Users / Users' interface. It lists two users:

Username	Description
Eloham	Administrateur
Bruno	Stagiaire

Buttons at the bottom include 'Enregistrer' (Save) and '+ Ajouter' (Add).

J'ai créé des utilisateurs locaux pour le service proxy : Eloham comme administrateur et Bruno comme stagiaire. Cela permet de mieux gérer les droits d'accès et de sécuriser l'utilisation du proxy en fonction des rôles de chaque utilisateur

The screenshot shows the 'Paquet / Squid / Moniteur' interface. It includes several sections:

- Filtering:** Set to 'Max lines: 10 lines'.
- Squid Access Table:**

Date	IP	État	Adresse	Utilisateur	Destination
24.11.2024 15:12:52	127.0.0.1	TCP_MISS/403	http://10.2.104.254:3128/squid-internal-mgr/info	-	-
24.11.2024 15:12:52	10.2.104.254	TCP_DENIED/403	http://localhost:3128/squid-internal-mgr/info	-	-
24.11.2024 15:09:46	127.0.0.1	TCP_MISS/403	http://10.2.104.254:3128/squid-internal-mgr/info	-	-
24.11.2024 15:09:46	10.2.104.254	TCP_DENIED/403	http://localhost:3128/squid-internal-mgr/info	-	-
- Squid Cache Table:**

Date-Time	Message	Squid - Cache Logs			
01.01.1970 00:00:00	Pinger exiting.				
24.11.2024 15:07:57	Accepting HTTP Socket connections at conn21 local=10.2.104.254:3128 remote=[::] FD 13 flags=<9				
24.11.2024 15:07:57	Finished loading MIME types and icons.				
01.01.1970 00:00:00	ICMPv6 socket opened.				
01.01.1970 00:00:00	ICMP socket opened.				
01.01.1970 00:00:00	Initialising ICMP pinger ...				
24.11.2024 15:07:57	Port 3128 opened on FD 16				
24.11.2024 15:07:57	HTTPC Disabled.				
24.11.2024 15:07:57	Adding domain home.arp from /etc/resolv.conf				
- SquidGuard Table:**

Date-Time	ACL	Adresse	SquidGuard Logs	Hôte	Utilisateur
C-ICAP Virus Table					

A banner at the bottom right says 'Activer Windows' (Activate Windows) with the subtext 'Accédez aux paramètres pour activer Windows.'

J'ai consulté les journaux d'accès en temps réel de Squid pour surveiller le trafic réseau. Les journaux montrent des requêtes HTTP avec des états tels que **TCP_MISS/403** pour les requêtes non autorisées. J'ai aussi vérifié les journaux du cache Squid, qui affichent des informations sur la gestion des connexions et des processus, y compris les messages ICMP et les détails de la configuration ICAP. Cela me permet de garder un contrôle sur l'utilisation du proxy et de diagnostiquer les problèmes potentiels en temps réel.

m) ANALYSE DES LOGS

J'ai consulté les journaux d'accès en temps réel de Squid pour surveiller le trafic réseau. Les journaux montrent des requêtes HTTP avec des états tels que **TCP_MISS/403** pour les requêtes non autorisées. **L'erreur 403 Forbidden** indique que l'accès à certaines URL est refusé, avec le message **ERR_ACCESS_DENIED** dans la réponse HTTP, signalant un problème de permissions ou de restrictions appliquées par le proxy. J'ai aussi vérifié les journaux du cache Squid, qui affichent des informations sur la gestion des connexions et des processus, y compris les messages ICMP et les détails de la configuration ICAP. Ces journaux

montrent notamment des échanges tels que l'initialisation du support ICMP et des configurations sur la gestion des types MIME.

Cela me permet de garder un contrôle sur l'utilisation du proxy, de diagnostiquer les problèmes potentiels en temps réel, et d'apporter des ajustements si certaines requêtes sont incorrectement bloquées.

```
Connection list

HTTP/1.1 403 Forbidden
Server: squid/6.3
Mime-Version: 1.0
Date: Sun, 24 Nov 2024 15:09:46 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3722
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: fr
Cache-Status: localhost
Via: 1.1 localhost (squid/6.3), 1.1 localhost (squid/6.3)
Cache-Status: localhost;detail=no-cache
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2023 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: The requested URL could not be retrieved</title>
<style type="text/css"><!--
/*
 * Copyright (C) 1996-2023 The Squid Software Foundation and contributors
 *
 * Squid software is distributed under GPLv2+ license and includes
 * contributions from numerous individuals and organizations.
 * Please see the COPYING and CONTRIBUTORS files for details.
 */
/*
 Stylesheet for Squid Error pages
 Adapted from design by Free CSS Templates
 http://www.freecsstemplates.org
 Released for free under a Creative Commons Attribution 2.5 License
*/
/* Page basics */
* {
    font-family: verdana, sans-serif;
}
```

Activer Windows
Accédez aux paramètres pour activer Windows.

19. CREATION ET MISE EN ŒUVRE D'UN CERTIFICAT HTTPS

J'ai généré un certificat SSL/TLS sur pfSense en créant une autorité de certification (AC) interne. J'ai nommé l'AC pfsense-eloham et utilisé la méthode "Créer une autorité de certification interne" pour signer les certificats SSL/TLS localement. J'ai laissé l'option Trust Store désactivée pour ne pas ajouter cette AC au magasin de confiance du système d'exploitation, et j'ai activé l'option Randomize Serial pour générer des numéros de série aléatoires afin d'éviter des conflits de numéros de série lors de la signature des certificats. Cette AC est ensuite utilisée pour signer les certificats SSL/TLS qui seront appliqués sur le proxy pour l'interception SSL.

Système / Certificat / Authorities / Modifier

Authorities Certificats Revocation

Créer / Modifier l'AC

Nom descriptif: pfsense-eloham

Méthode: Créer une autorité de certification interne

Trust Store: Add this Certificate Authority to the Operating System Trust Store

Randomize Serial: Use random serial numbers when signing certificates

Pour créer l'autorité de certification interne sur pfSense, j'ai choisi un type de clé **RSA** avec une longueur de **4096 bits**. Cette longueur de clé est recommandée pour assurer une grande sécurité, car elle rend les attaques par force brute pratiquement impossibles sur le long terme. L'algorithme de hachage sélectionné est **sha256**, qui est considéré comme une norme de sécurité élevée, assurant l'intégrité et la sécurité des données chiffrées. Cet algorithme est largement pris en charge par les services modernes et reste une meilleure pratique par rapport aux algorithmes plus faibles comme MD5 ou SHA1.

J'ai défini la **durée de vie du certificat à 3650 jours**, soit environ **10 ans**. Cette durée prolongée permet de minimiser la fréquence à laquelle l'AC doit être renouvelée, tout en évitant les perturbations fréquentes liées à l'expiration des certificats. Le **Nom commun** (Common Name) est configuré en tant que **internal-ca**, ce qui permet d'identifier clairement cette CA interne dans l'infrastructure.

Les champs additionnels incluent le **Code du pays (FR)**, l'**État ou province (Drome)**, et la **Ville (Valence)**. Ces informations sont importantes pour assurer que le certificat est unique et identifiable dans les environnements où de multiples AC peuvent être en usage. L'organisation est renseignée en tant que **Algoud Iaffemas**, et bien que le champ **Unité organisationnelle** soit facultatif, il permettrait d'ajouter des détails sur le département ou la fonction si nécessaire. Ces informations permettent de créer un certificat qui peut être facilement compris et vérifié par toute entité interne ou externe.

En résumé, cette configuration de l'autorité de certification interne est conçue pour fournir un équilibre entre sécurité forte, identification claire, et gestion simplifiée, garantissant ainsi une protection à long terme pour l'infrastructure du réseau tout en assurant une compatibilité optimale avec les services modernes.

The screenshot shows the 'Autorité de certification interne' (Internal Certificate Authority) configuration page. It includes fields for Key type (RSA), Key length (4096 bits), Algorithm (sha256), Duration (3650 days), Common Name (internal-ca), Country (FR), State (Drome), City (Valence), Organization (Algoud laffemas), and Unit (e.g. My Department Name (optional)). A 'Créer' (Create) button is at the bottom.

Pour créer un certificat SSL/TLS interne sur pfSense, j'ai utilisé la méthode **Créer un certificat interne** et j'ai nommé le certificat **certificate-https**. L'autorité de certification utilisée est **pfsense-eloham**, précédemment créée pour garantir une signature de confiance. J'ai choisi le type de clé **RSA** avec une longueur de **4096 bits** et l'algorithme de hachage **sha256** pour assurer une haute sécurité. La **durée de vie** du certificat est de **3650 jours** (environ 10 ans), permettant une longue validité sans avoir besoin de renouveler le certificat fréquemment. Ce certificat sera utilisé pour sécuriser les connexions HTTPS dans l'infrastructure.

The screenshot shows the 'Ajouter/Signer un nouveau certificat' (Add/Sign a new certificate) page under the 'Certificats' tab. It includes fields for Method (Créer un certificat interne), Name (certificate https), and Internal Certificate settings (Authority: pfsense-eloham, Key type: RSA, Length: 4096 bits, Algorithm: sha256, Duration: 3650 days). A 'Créer' (Create) button is at the bottom.

J'ai configuré le **webConfigurator** pour utiliser le protocole **HTTPS (SSL/TLS)**, en sélectionnant le certificat précédemment créé **certificate-https** pour sécuriser l'accès à l'interface. Le port TCP est défini sur **8443**, au lieu du port par défaut, afin de ne pas interférer avec d'autres services. J'ai laissé le **nombre maximal de processus à 3** pour permettre à plusieurs utilisateurs d'accéder simultanément sans impact sur les performances. Les options

HSTS, OCSP Must-Staple, et la redirection de l'interface web sont désactivées pour simplifier la gestion et éviter des problèmes de compatibilité avec certains navigateurs. Enfin, l'option pour **remplir automatiquement l'identifiant** est activée pour faciliter la connexion, et **Roaming** est autorisé pour maintenir la session même en cas de changement d'adresse IP.

The screenshot shows the 'webConfigurator' settings page. Key configurations include:

- Protocol:** Set to HTTP (radio button selected).
- Certificat SSL/TLS:** Set to "certificat https". A note states: "Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms."
- Port TCP:** Set to 8443. A note says: "Entrer un numéro de port personnalisé pour le webConfigurator afin de remplacer celui par défaut (80 pour HTTP et 443 pour HTTPS). Les changements seront effectifs dès sauvegarde."
- Nombre maximal de processus:** Set to 3. A note says: "Saisir le nombre de processus pour le webConfigurator. Par défaut, il en existe 2. Augmenter cette valeur autorisera plus d'utilisateurs/navigateurs à accéder à l'interface en même temps."
- Redirection de l'interface web:** Désélectionnée (unchecked).
- HSTS:** Désélectionnée (unchecked). A note says: "When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)"
- OCSP Must-Staple:** Désélectionnée (unchecked). A note says: "When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx."
- Remplir automatiquement l'identifiant de l'interface web:** Sélectionnée (checked). A note says: "Activer remplissage auto sur la page de connexion webConfigurator. Lorsque activé, les identifiants de connexion du webConfigurator peuvent être sauvegardés par le navigateur. Bien que pratique, certains standards de sécurité nécessitent de désactiver cette possibilité. Cocher cette case afin d'autoriser la saisie automatique des identifiants de sorte que le navigateur demande s'il faut sauvegarder les identifiants. (Certains navigateurs ne respectent pas cette option!)."
- GUI login messages:** Désélectionnée (unchecked). A note says: "Lower syslog level for successful GUI login events. When this is checked, successful logins to the GUI will be logged as a lower non-emergency level. Note: The console bell behavior can be controlled independently on the Notifications tab."
- Roaming:** Sélectionnée (checked). A note says: "Allow GUI administrator client IP address to change during a login session. When this is checked, the login session to the webConfigurator remains valid if the client source IP address changes."

Pour la configuration du webConfigurator, j'ai désactivé le **contrôle HTTP_REFERER** pour éviter les problèmes potentiels avec l'accès aux scripts externes et améliorer la compatibilité. J'ai laissé décoché l'option **Texte de l'onglet du navigateur** afin de préserver la présentation standard, qui affiche uniquement le nom de domaine. Cela permet de garder une interface plus simple et cohérente lors de l'accès au webConfigurator.

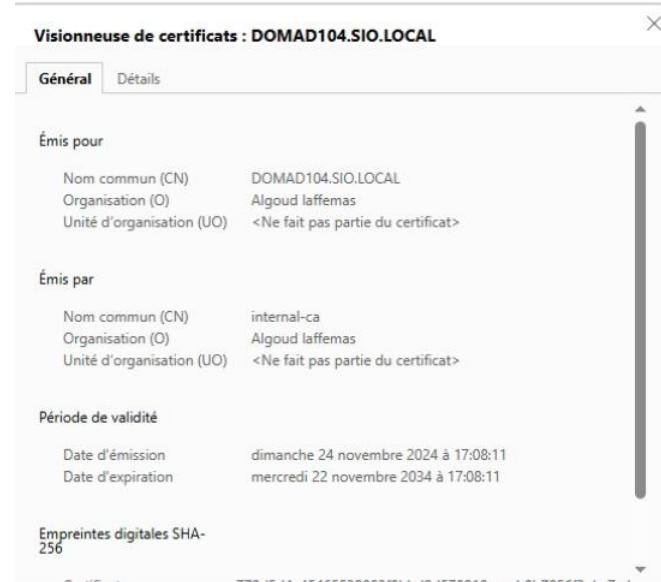
The screenshot shows the 'Renforcement navigateur' section of the advanced navigation settings:

- HTTP_REFERER:** Désélectionnée (unchecked). A note says: "Désactiver le contrôle applicatif HTTP_REFERER. Lorsque l'option n'est pas activée, l'accès au webConfigurator est protégé contre les tentatives de redirection HTTP_REFERER. Cochez cette case pour désactiver cet élément si elle interfère avec l'accès du webConfigurator dans certains cas, comme l'utilisation de scripts externes pour interagir avec ce système. Plus d'informations sur HTTP sont disponibles à partir de [Wikipedia](#) ."
- Texte de l'onglet du navigateur:** Désélectionnée (unchecked). A note says: "Afficher le nom de la page en premier dans l'onglet du navigateur. Lorsque cette case n'est pas cochée, l'onglet affiche le nom de domaine suivi de la page en cours. Cochez cette case pour afficher la page en cours suivi du nom de la page."

Le certificat SSL/TLS a été correctement mis en place sur le webConfigurator de pfSense, et l'accès se fait par défaut en **HTTPS** sur le port **8443**. Toutefois, le certificat est marqué comme "Non sécurisé" par le navigateur. Cela est normal car le certificat n'a pas été émis par une autorité de certification publique reconnue, mais plutôt par notre AC interne (**internal-ca**)

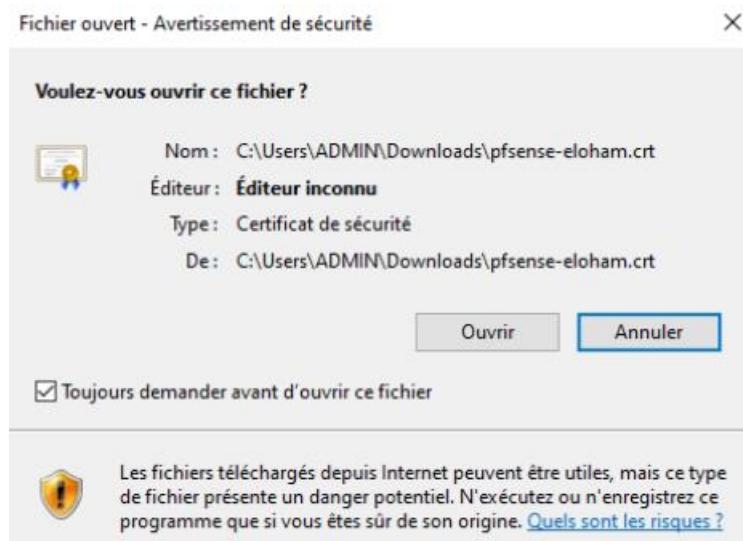
The screenshot shows a browser window displaying the pfSense web interface at https://10.0.104.254:8443/interfaces_assign.php. The address bar indicates "Non sécurisé" and the URL. The page title is "Interfaces / Interface Assignments".

En examinant le certificat, on peut voir qu'il a été émis par l'autorité **internal-ca** avec le nom commun (CN) **DOMAD104.SIO.LOCAL**, et l'organisation **Algoud laffemas**. La période de validité est de 10 ans, du 24 novembre 2024 au 22 novembre 2034, avec une empreinte digitale utilisant **SHA-256**. Pour que le certificat soit reconnu comme sécurisé par les navigateurs, il faudrait soit utiliser une autorité de certification publique, soit installer le certificat de l'AC interne sur chaque poste client accédant à l'interface.

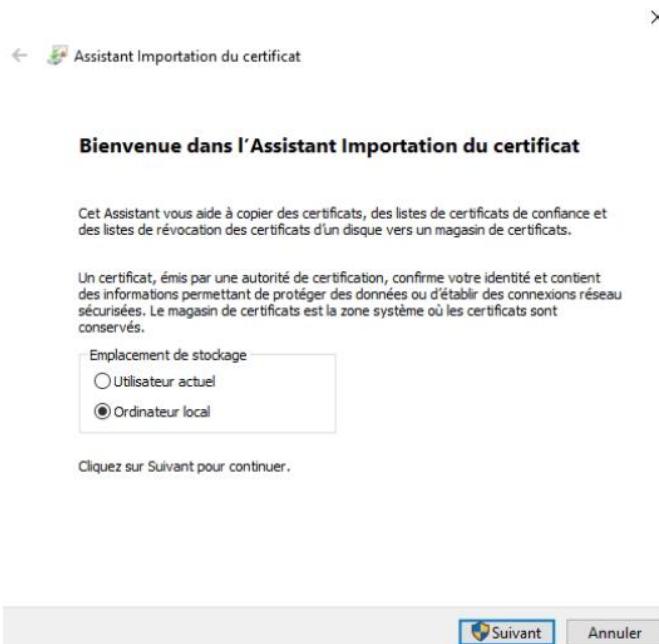


n) INSTALLATION DES CERTIFICATS EN LOCAL :

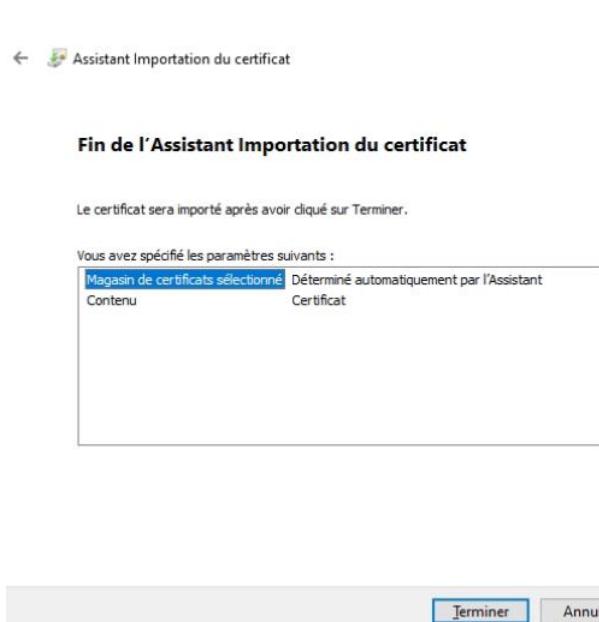
Nous allons maintenant passer à l'installation locale du certificat sur chaque poste client afin qu'il soit reconnu au sein de notre réseau interne. Cela permettra d'éviter les avertissements de sécurité et de garantir que les connexions sont marquées comme sécurisées par les navigateurs sur notre infrastructure. Le certificat doit être installé dans le magasin de certificats de confiance du système d'exploitation, ce qui permettra une confiance automatique de toutes les connexions à l'interface pfSense.



Pour l'installation, nous utilisons l'Assistant d'Importation du Certificat. Dans l'assistant, nous choisissons l'option **Ordinateur local** comme emplacement de stockage, ce qui signifie que le certificat sera disponible pour toutes les applications sur cet ordinateur. Cela permet d'assurer que tous les utilisateurs du système reconnaissent le certificat sans avoir à le réinstaller pour chaque profil utilisateur. Une fois sélectionné, nous cliquons sur **Suivant** pour continuer l'importation et installer le certificat dans le magasin approprié.

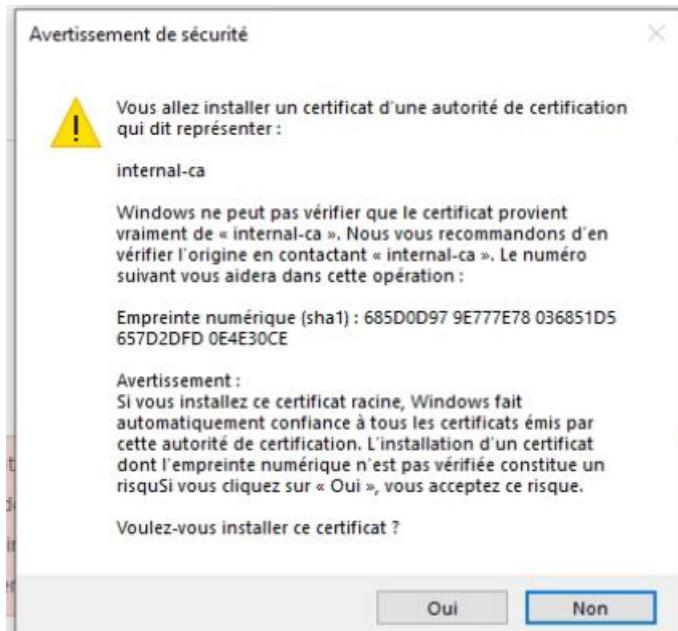


Nous passons maintenant à la dernière étape de l'installation du certificat pour qu'il soit reconnu comme sécurisé au sein de notre réseau interne. Une fois que l'Assistant d'Importation du Certificat a terminé la configuration, nous cliquons sur **Terminer** pour finaliser l'importation. Le certificat est ensuite ajouté au **magasin de certificats** approprié, déterminé automatiquement par l'assistant pour assurer une bonne prise en charge.



Cette action permet à tous les navigateurs et applications de reconnaître notre certificat comme valide, supprimant les avertissements de sécurité et assurant une connexion HTTPS fiable avec le webConfigurator pfSense. En conclusion, le certificat est maintenant

correctement installé et intégré dans le système, garantissant une expérience utilisateur fluide au sein du réseau.



Lors de l'installation du certificat d'autorité de certification interne, un **avertissement de sécurité** s'affiche. Ce message indique que Windows ne peut pas vérifier l'origine de l'autorité **internal-ca**, car il s'agit d'une AC interne et non d'une AC publique reconnue. Le message recommande de vérifier l'origine du certificat, ce qui est une procédure standard pour s'assurer de la validité et de la légitimité du certificat.

L'avertissement précise que si nous installons ce certificat en tant que certificat racine, Windows fera automatiquement confiance à tous les certificats émis par cette AC. Cela signifie que toutes les communications établies avec un serveur utilisant un certificat émis par **internal-ca** seront considérées comme sécurisées par le système. Il est donc crucial de s'assurer que l'empreinte numérique (SHA1) présentée correspond bien à celle du certificat que nous voulons installer.

En cliquant sur **Oui**, nous acceptons ce risque et ajoutons l'AC interne aux magasins de certificats de confiance, garantissant ainsi que le webConfigurator de pfSense soit reconnu comme sécurisé par Windows sans générer d'avertissements futurs.

État / Tableau de bord

Informations système

Nom	Eloham.home.arpa
Utilisateur	admin@10.0.104.10 (Local Database)
Système	VMware Virtual Machine ID de l'appareil Netgate: 7a39005755908ebb2fc0
BIOS	Fournisseur:Phoenix Technologies LTD Version:6.00 Date de sortie:Wed Dec 12 2018
Version	2.7.2-RELEASE (amd64) Basé sur Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT

Netgate Services And Support

Contract type: Community Support
Community Support

NETGATE AND pfSense COMMUNITY SUPPORT

If you purchased your pfSense gateway firewall, you can get support at the point of sale or installed pfSense. You can also find various community support resources. This includes forums, documentation, and other helpful links.

L'installation du certificat est maintenant complète et la connexion au webConfigurator de pfSense est enfin considérée comme sécurisée. En accédant à l'adresse

<https://10.0.104.254>, nous pouvons voir que la connexion se fait bien en **HTTPS** sans aucun avertissement de sécurité, signe que le certificat a été reconnu correctement par le système. Toutes les informations système sont accessibles, confirmant que l'interface est pleinement fonctionnelle et sécurisée pour une utilisation au sein de notre réseau interne.

20. SNORT :

SNORT est un système de détection d'intrusion réseau (NIDS - Network Intrusion Detection System) qui est largement utilisé pour surveiller et analyser le trafic réseau à la recherche de comportements suspects ou malveillants. Développé à l'origine par Sourcefire (qui a ensuite été acquis par Cisco), SNORT est l'une des solutions les plus populaires et robustes pour la détection des intrusions.

Fonctionnalités de SNORT :

- **Détection en temps réel** : SNORT peut analyser le trafic en temps réel pour identifier les tentatives d'intrusion, les scans de ports, les attaques de type DDoS, les attaques de déni de service, les tentatives d'exploitation de vulnérabilités, etc.
- **Analyse des protocoles** : Il effectue une analyse en profondeur des paquets pour reconnaître les protocoles mal utilisés ou des anomalies dans les communications.
- **Signatures personnalisées** : SNORT utilise une base de règles (ou signatures) pour identifier des comportements ou des activités spécifiques. Les administrateurs peuvent également créer des règles personnalisées pour répondre à des besoins spécifiques.

Utilité de SNORT sur un pare-feu

L'intégration de SNORT sur un pare-feu offre une couche supplémentaire de sécurité. Voici ses principales utilités :

1. Détection d'intrusion :

- SNORT analyse tout le trafic réseau entrant et sortant pour détecter des activités malveillantes que le pare-feu pourrait ne pas identifier.
- Alors que le pare-feu peut bloquer certains types de connexions en fonction des règles définies, SNORT est capable d'analyser le contenu de ces connexions pour identifier des menaces qui passent au travers des politiques du pare-feu.

2. Alerta en temps réel :

- Lorsqu'une menace est détectée, SNORT peut générer une alerte en temps réel pour informer les administrateurs de l'activité suspecte. Cela permet une réaction rapide et appropriée, par exemple pour bloquer une IP suspecte ou isoler une machine compromise.

3. Analyse proactive et surveillance du trafic :

- SNORT ne se contente pas de bloquer, il permet aussi de comprendre les types de trafic réseau qui circulent. Il identifie les schémas de communication et analyse les anomalies. Ces informations peuvent être utilisées pour ajuster les règles du pare-feu et ainsi améliorer la sécurité globale.

4. Détection basée sur des signatures et des anomalies :

- SNORT peut utiliser à la fois des signatures connues (basées sur des règles) pour détecter des menaces et des anomalies dans le comportement réseau. Cela en fait un bon complément au pare-feu, qui ne fait généralement qu'appliquer des règles statiques.

5. Capture et journalisation des paquets :

- SNORT capture des paquets et les journalise pour une analyse ultérieure. Ces journaux peuvent être utilisés pour mener une analyse approfondie après une tentative d'intrusion et pour adapter les politiques de sécurité.

21. INSTALLATION DE SNORT :

Pour la configuration de Snort sur mon infrastructure, j'ai déjà mis en place la surveillance de l'interface WAN, qui est la plus importante car elle est en première ligne de défense contre les menaces extérieures. Le WAN étant l'interface par laquelle tout le trafic extérieur transite, il est crucial de contrôler et d'analyser les tentatives d'intrusion via cet accès.

The screenshot shows the 'Services / Snort / Interfaces' section of the PFSense web interface. The 'Snort Interfaces' tab is selected. A table titled 'Interface Settings Overview' lists one interface: 'WAN (vmx2)'. The columns include 'Interface', 'Snort Status', 'Pattern Match', 'Blocking Mode', 'Description', and 'Actions'. The 'Snort Status' column shows a green circle with a checkmark. The 'Actions' column contains icons for edit, copy, and delete, along with '+ Ajouter' and 'Supprimer' buttons.

Cependant, je prévois également de configurer la surveillance sur la DMZ (zone démilitarisée). En effet, en cas d'utilisation d'un reverse proxy, la DMZ peut être exposée à des attaques directes. Cette zone intercepte souvent le trafic avant de le rediriger vers le réseau interne, ce qui en fait une cible potentielle pour les attaquants cherchant des vulnérabilités.

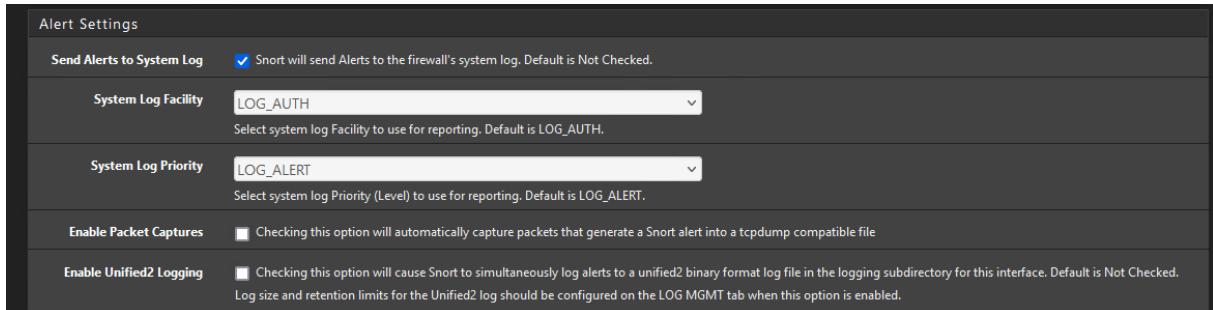
En ajoutant la surveillance de la DMZ, je pourrai renforcer la sécurité globale de l'infrastructure en détectant et en prévenant toute tentative d'attaque qui pourrait compromettre les services exposés sur le réseau, notamment ceux gérés par le reverse proxy. Cette configuration de Snort permettra donc une meilleure visibilité et une réactivité accrue face aux menaces potentielles sur l'ensemble des points d'entrée critiques de mon infrastructure.

o) VERIFIER LA DMZ

Pour la configuration de Snort sur mon infrastructure, j'ai déjà mis en place la surveillance de l'interface WAN, qui est la plus importante car elle est en première ligne de défense contre les menaces extérieures. Le WAN étant l'interface par laquelle tout le trafic extérieur transite, il est crucial de contrôler et d'analyser les tentatives d'intrusion via cet accès.

The screenshot shows the 'LAN0 Paramètres' section of the PFSense web interface. The 'Paramètres généraux' tab is selected. It includes fields for 'Activer' (checked), 'Interface' (set to 'DMZ (vmx1)'), 'Description' (set to 'DMZ'), and 'Snap Length' (set to '1518'). Below these fields is a note: 'Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.'

Cependant, je prévois également de configurer la surveillance sur la DMZ (zone démilitarisée). En effet, en cas d'utilisation d'un reverse proxy, la DMZ peut être exposée à des attaques directes. Cette zone intercepte souvent le trafic avant de le rediriger vers le réseau interne, ce qui en fait une cible potentielle pour les attaquants cherchant des vulnérabilités.



Configuration de l'interface DMZ sur Snort

Pour la configuration de Snort sur l'interface DMZ, j'ai activé l'option "Activer interface" pour permettre la surveillance active de tout le trafic passant par la DMZ (interface VMX1). J'ai également renseigné une description claire "DMZ" pour bien identifier l'interface surveillée dans les paramètres de Snort.

Le paramètre **Snap Length** est configuré à 1518 octets, ce qui est la valeur par défaut et convient pour la plupart des applications. Cela permet de capturer l'intégralité des paquets, y compris les en-têtes, afin d'avoir une analyse complète du trafic.

Paramètres d'Alerte pour la DMZ

- Send Alerts to System Log** : J'ai configuré Snort pour envoyer les alertes au journal système du pare-feu, ce qui permet une centralisation des journaux et facilite l'analyse des événements de sécurité.
- System Log Facility** : La catégorie de journalisation est configurée sur **LOG_AUTH**, indiquant que les alertes concernent l'authentification et la sécurité.
- System Log Priority** : Le niveau de priorité des alertes est configuré sur **LOG_ALERT**, ce qui garantit que ces alertes importantes seront traitées avec une attention particulière.

Pour l'instant, les options **Enable Packet Captures** et **Enable Unified2 Logging** ne sont pas activées, mais elles pourront être envisagées plus tard si un besoin de capture complète de paquets ou de journalisation avancée se présente.

En ajoutant la surveillance de la DMZ, je pourrai renforcer la sécurité globale de l'infrastructure en détectant et en prévenant toute tentative d'attaque qui pourrait compromettre les services exposés sur le réseau, notamment ceux gérés par le reverse proxy. Cette configuration de Snort permettra donc une meilleure visibilité et une réactivité accrue face aux menaces potentielles sur l'ensemble des points d'entrée critiques de mon infrastructure.

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
WAN (vmx2)	✓ C	AC-BNFA	DISABLED	WAN	edit remove
DMZ (vmx1)	✓ C	AC-BNFA	DISABLED	DMZ	edit remove

J'ai configuré Snort pour surveiller l'interface WAN, ce qui est crucial puisqu'elle est la première ligne de défense contre les menaces extérieures. Maintenant, la surveillance de la DMZ est également configurée et installée. Cette mesure est importante car, en cas d'utilisation d'un reverse proxy, la DMZ peut devenir une cible potentielle pour des attaques directes.

Avec la surveillance de la DMZ maintenant en place, la sécurité globale de l'infrastructure est renforcée, offrant une meilleure visibilité et une réactivité accrue face aux menaces sur les points d'entrée critiques.

p) MISE A JOUR DE SECURITE :

Nous procédons également aux mises à jour des règles de sécurité pour Snort. Cela garantit que les signatures de détection sont à jour, permettant à notre système d'être protégé contre les menaces les plus récentes. La mise à jour régulière des règles est essentielle pour maintenir une sécurité optimale et une défense proactive face aux nouvelles vulnérabilités.

Avec la surveillance de la DMZ maintenant en place et les règles de sécurité à jour, la sécurité globale de l'infrastructure est renforcée, offrant une meilleure visibilité et une réactivité accrue face aux menaces sur les points d'entrée critiques.

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	81e6abdf1b243c116730f689f7a6a9d	Monday, 14-Oct-24 12:43:57 UTC
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update	Oct-14 2024 14:47	Result: Success
Update Rules		Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

J'ai également ajouté une liste de passage (pass list) pour l'Active Directory (nommée "AD"). Cette pass list inclut des adresses IP critiques, comme les adresses des serveurs DNS, VPN, et IP virtuelles, afin de s'assurer que les communications légitimes de l'Active Directory ne soient pas bloquées par Snort. Cela permet de réduire les faux positifs et d'assurer un bon fonctionnement des services essentiels liés à l'Active Directory.

Avec la surveillance de la DMZ maintenant en place, les règles de sécurité à jour, et la configuration de la pass list pour l'Active Directory, la sécurité globale de l'infrastructure est renforcée, offrant une meilleure visibilité et une réactivité accrue face aux menaces sur les points d'entrée critiques.

Log Name	Max Size	Retention	Log Description
alert	500 KB	14 DAYS	Snort alerts and event details
snort_xxxxx.u2	500 KB	14 DAYS	Snort alerts and event details in Unified2 binary log format
appid-alerts	500 KB	14 DAYS	Application ID Alerts
app-stats	1 MB	7 DAYS	Application ID statistics
event_pcaps	NO LIMIT	14 DAYS	Snort alert related packet captures
sid_changes	250 KB	14 DAYS	SID changes made by SID Mgmt conf files
stats	500 KB	7 DAYS	Snort performance statistics

Settings will be ignored for any log in the list above not enabled on the Interface Settings tab. When a log reaches the Max Size limit, it will be rotated and tagged with a timestamp. The Retention period

Pour améliorer la gestion de l'espace disque et éviter que la ferme de serveurs ne soit saturée par des fichiers de logs volumineux, j'ai mis en place une limite sur la taille des logs générés

par Snort. Une limite de 4000 Mo a été configurée pour le répertoire de logs afin de garantir une utilisation optimale des ressources de stockage.

De plus, des limites spécifiques ont été définies pour les différents types de logs, comme les alertes (500 KB, rétention de 14 jours), les statistiques d'application (1 MB, rétention de 7 jours), et autres. Cela permet de contrôler précisément la rétention des journaux en fonction de leur importance, évitant ainsi une accumulation excessive de données et assurant que l'espace de stockage est utilisé de manière efficace.

Avec cette nouvelle configuration, la gestion des logs est désormais optimisée, réduisant ainsi les risques de saturation des serveurs et assurant une meilleure performance globale de l'infrastructure.

q) LOGS SNORT :

Ces journaux d'alerte nous permettent de suivre de près les activités suspectes sur notre réseau et de prendre les mesures appropriées en cas de détection de comportement anormal. La surveillance régulière de ces logs est essentielle pour identifier des menaces et garantir une protection proactive contre des attaques potentielles.

Alert Log View Settings																			
Interface to Inspect		WAN (vmx2)	Auto-refresh view		250	Enregistrer		Alert lines to display.											
Alert Log Actions																			
Alert Log View Filter																			
15 Entries in Active Log																			
Date	Action	Pri	Proto	Class	IP Source	SPort	IP de destination	DPort	GID:SID	Description									
2024-11-24 17:15:19	⚠️	3	TCP	Unknown Traffic	192.168.10.104	51423	204.79.197.219	443	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE									
2024-11-24 15:56:24	⚠️	3	TCP	Unknown Traffic	54.209.32.212	80	192.168.10.104	25423	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request									
2024-11-22 12:32:22	⚠️	3	TCP	Unknown Traffic	77.95.69.67	80	192.168.10.104	63437	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request									
2024-11-22 10:28:21	⚠️	3	TCP	Unknown Traffic	77.95.69.67	80	192.168.10.104	54755	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE									
2024-11-21 18:57:45	⚠️	3	TCP	Unknown Traffic	192.168.10.104	3037	34.149.100.209	443	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE									
2024-11-21 18:56:46	⚠️	3	TCP	Unknown Traffic	192.168.10.104	3037	34.149.100.209	443	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE									
2024-11-21 09:36:51	⚠️	3	TCP	Unknown Traffic	34.205.242.146	80	192.168.10.104	35310	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request									
2024-11-21 09:34:51	⚠️	3	TCP	Unknown Traffic	34.205.242.146	80	192.168.10.104	51596	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request									
2024-11-21 09:32:51	⚠️	3	TCP	Unknown Traffic	54.161.222.85	80	192.168.10.104	5199	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request									
2024-11-21 09:32:44	⚠️	3	TCP	Unknown Traffic	34.205.242.146	80	192.168.10.104	29814	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request									
2024-11-20 15:53:30	⚠️	3	TCP	Unknown Traffic	192.168.10.104	1741	104.18.32.47	443	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE									

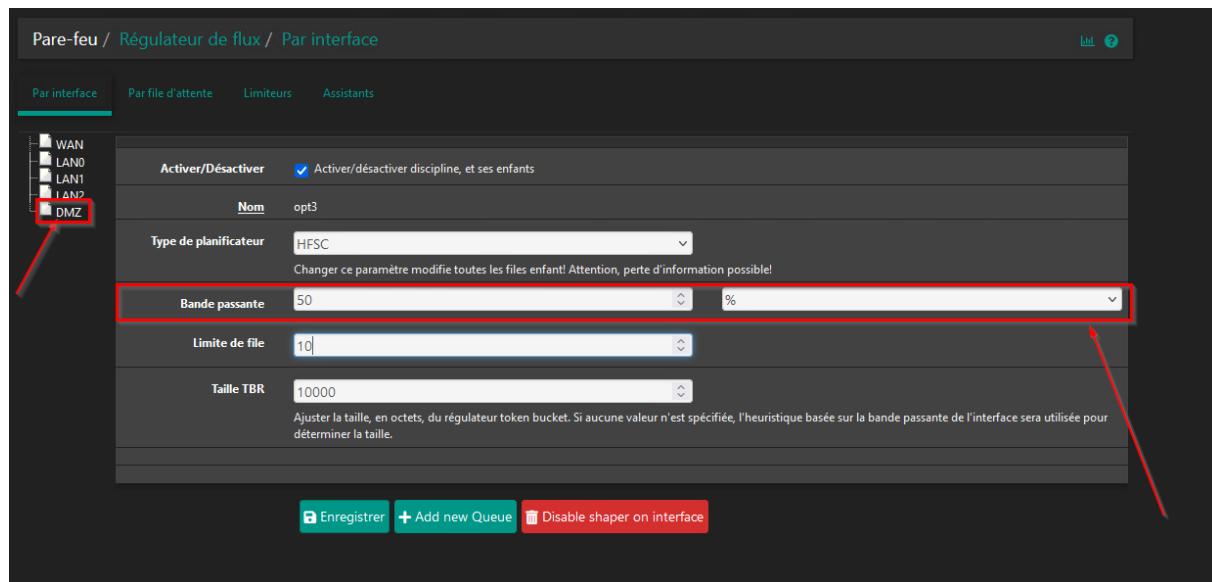
Avec cette nouvelle configuration, la gestion des logs est désormais optimisée, réduisant ainsi les risques de saturation des serveurs et assurant une meilleure performance globale de l'infrastructure tout en nous permettant de réagir aux menaces identifiées.

Services / Snort / Suppression Lists										?
Snort Interfaces	Global Settings	Mises à jour	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Configured Suppression Lists										
List Name	Description				Actions					
wansuppress_6744997709863	Auto-generated list for Alert suppression				Éditer Supprimer + Ajouter Supprimer					

22. REGULATEUR DE FLUX

Un régulateur de flux, également appelé "traffic shaper", est un mécanisme permettant de gérer la répartition de la bande passante sur un réseau. Il permet de prioriser certains types de trafic ou de limiter l'utilisation de la bande passante pour certaines interfaces, afin de garantir une qualité de service optimale. En contrôlant le débit de données, on peut s'assurer que des services critiques ne soient pas pénalisés par des flux excessifs ou non prioritaires.

Dans notre infrastructure, nous avons choisi de limiter l'activité de la DMZ à 50% de la bande passante totale disponible. La DMZ, bien qu'importante pour la gestion des services exposés à l'extérieur, ne doit pas prendre le dessus sur le réseau LAN qui est prioritaire pour les utilisateurs internes et les services critiques. Cette limitation permet de garantir que le LAN conserve toujours une part suffisante de la bande passante.



Concernant la limite de file d'attente, nous avons fixé cette valeur à 10. Cela signifie que la DMZ peut gérer jusqu'à 10 connexions simultanées avant de devoir mettre les connexions en attente. Cette limite est adaptée à notre contexte, car bien que nous soyons limités en nombre d'actifs, la plupart de nos actifs utilisent des services en mode multi-usage. Par conséquent, une limite de 10 est suffisante pour maintenir la performance et la stabilité du réseau.

La configuration actuelle du régulateur de flux sur l'interface DMZ permet donc de contrôler efficacement la répartition de la bande passante, garantissant une utilisation équilibrée des ressources entre les différentes interfaces du réseau, tout en maintenant la stabilité et la performance de l'infrastructure.

23. REVERSE PROXY

Un reverse proxy est un serveur qui se place entre les clients et les serveurs d'applications pour intercepter les requêtes des clients avant de les transmettre aux serveurs appropriés. Voici une explication de ses fonctionnalités, son utilité dans un réseau, et son utilisation avec pfSense.

Qu'est-ce qu'un Reverse Proxy ?

Un reverse proxy est une passerelle qui reçoit les requêtes des clients, les traite, et les achemine vers le serveur approprié au sein d'un réseau local. Contrairement à un proxy classique qui agit au nom du client pour se connecter à Internet, un reverse proxy agit au nom

du serveur. En général, un reverse proxy se trouve en amont d'un ou de plusieurs serveurs web et est utilisé pour améliorer la performance, la sécurité, et la gestion des ressources.

Utilités d'un Reverse Proxy dans un Réseau

1. Amélioration des Performances :

- **Cache des Contenus** : Le reverse proxy peut mettre en cache des pages ou du contenu statique, permettant de réduire la charge sur les serveurs d'applications.
- **Répartition de Charge (Load Balancing)** : Il peut distribuer les requêtes entre plusieurs serveurs, assurant une meilleure répartition de la charge et une disponibilité accrue.

Sécurité :

- **Anonymisation** : Le reverse proxy masque les adresses IP des serveurs internes, rendant plus difficile leur identification par des acteurs malveillants.
- **Filtrage des Requêtes** : Il peut filtrer les requêtes, par exemple pour prévenir les attaques DoS (Denial of Service), l'exploitation de failles de sécurité, ou bloquer certains types de contenu.
- **Terminaison SSL** : Il peut gérer les certificats SSL, permettant aux serveurs en arrière-plan de fonctionner sans gérer eux-mêmes le chiffrement.

The screenshot shows the PFSENSE Firewall configuration interface. The top navigation bar includes 'Pare-feu / Alias / Modifier'. The main section is titled 'Propriétés' (Properties). It contains fields for 'Nom' (Name) set to 'SERVERWEB', 'Description' (Description) left empty, and 'Type' (Type) set to 'Hôte(s)'. Below this, under the 'Hôte(s)' (Hosts) section, there is an 'Astuce' (Tip) note about specifying hosts by IP or FQDN. The 'IP ou FQDN' (IP or FQDN) field contains '10.9.104.1' and the 'Description' field contains 'server web'. At the bottom are two buttons: 'Enregistrer' (Save) and '+ Ajouter un hôte' (Add host).

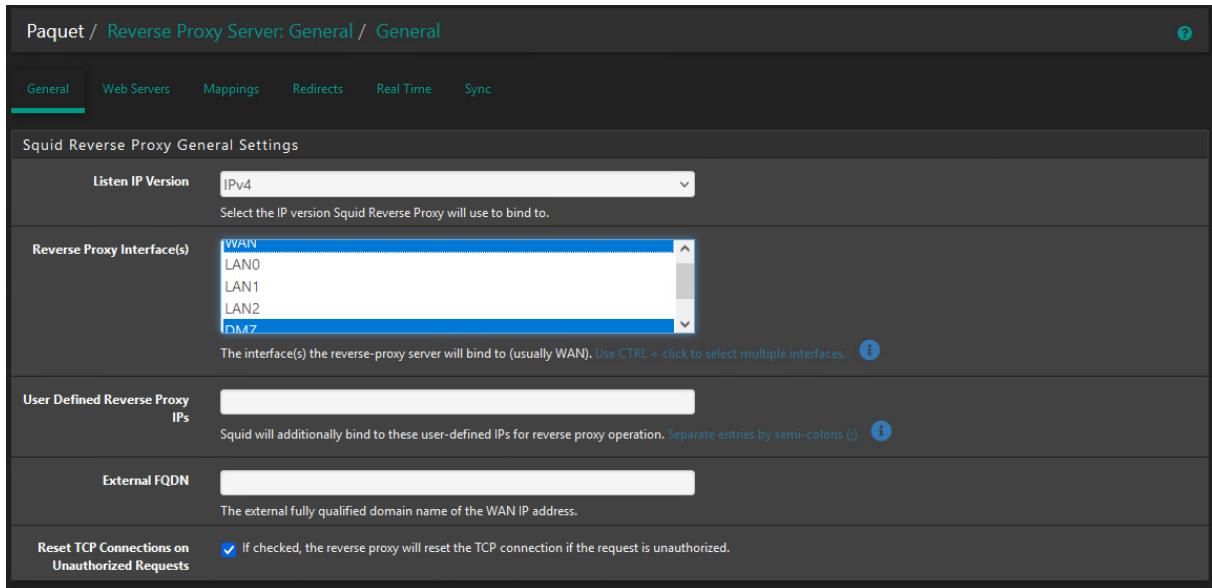
Première Capture : Configuration d'un Alias de Serveur

La première capture montre la création d'un **alias** appelé SERVERWEB dans la section **Pare-feu > Alias > Modifier**.

- **Nom de l'alias** : SERVERWEB
- **Type** : Hôte(s)
- **IP ou FQDN** : Vous avez défini l'adresse IP 10.9.104.1 et l'avez associée avec la description "server web".

Cette étape consiste à créer un alias pour le serveur Web interne. L'alias rend la gestion des règles de pare-feu plus simple et plus compréhensible, surtout si vous avez plusieurs serveurs

à gérer. L'utilisation d'alias permet de référencer des adresses IP de manière plus descriptive dans les règles de pare-feu ou d'autres configurations.



Listen IP Version : IPv4

Vous avez choisi de faire écouter le reverse proxy sur les adresses **IPv4**.

- **Reverse Proxy Interface(s)** : Vous avez sélectionné les interfaces suivantes : WAN, LAN0, LAN1, LAN2, et DMZ. Cela signifie que le **reverse proxy** Squid écoute sur toutes ces interfaces. Typiquement, l'interface **WAN** est utilisée pour accepter les requêtes venant de l'extérieur, tandis que les interfaces **LAN** et **DMZ** servent à communiquer avec les serveurs internes du réseau.
- **User Defined Reverse Proxy IPs** : Cette option est vide. Si vous définissez une adresse IP ici, Squid pourrait également écouter sur ces adresses IP spécifiques.
- **External FQDN** : Cette option est également vide. Ici, vous pouvez spécifier un **nom de domaine entièrement qualifié (FQDN)** qui correspond à l'adresse IP publique de votre WAN. Cela est utile si vous avez un domaine personnalisé qui est utilisé par le proxy.
- **Reset TCP Connections on Unauthorized Requests** : Cette case est cochée. Cela signifie que le proxy réinitialisera les connexions TCP si une requête non autorisée est reçue. Cela ajoute une couche de sécurité en limitant les réponses aux requêtes non autorisées.

J'ai configuré deux entrées pour le serveur web interne sous l'alias SERVERWEB. La première entrée est dédiée au service HTTPS, sur le port 443. L'adresse IP associée est 10.9.104.1, et le protocole utilisé est HTTPS. Cela permet au reverse proxy de gérer les requêtes sécurisées vers le serveur, en utilisant le chiffrement SSL/TLS. Le proxy redirige toutes les connexions sécurisées vers cette adresse IP, garantissant ainsi un accès protégé.

The screenshot shows the pfSense interface under the 'Paquet / Reverse Proxy Server: Peers / Web Servers' section. There are two entries listed:

Status	Alias	IP Address	Port	Protocol	Description
on	SERVERWEB	10.9.104.1	443	HTTPS	SERVER HTTPS
on	SERVERWEB	10.9.104.1	80	HTTP	SERVER HTTP

Buttons at the bottom include 'Enregistrer' (Save) and '+ Ajouter' (Add). The 'Web Servers' tab is selected.

La seconde entrée concerne le même serveur mais pour des connexions HTTP, sur le port 80. Le serveur est accessible sans chiffrement via l'IP 10.9.104.1. Le port 80 est souvent utilisé pour rediriger les utilisateurs vers HTTPS (port 443), assurant ainsi une connexion sécurisée de bout en bout.

En utilisant ces deux configurations, le reverse proxy Squid sur pfSense prend en charge à la fois les connexions sécurisées (HTTPS) et non sécurisées (HTTP) vers le serveur interne. Cela permet de gérer les flux de trafic, tout en forçant la sécurité par la redirection des requêtes HTTP vers HTTPS, si nécessaire.

The screenshot shows the pfSense interface under the 'Paquet / Squid / Moniteur' section. It includes a 'Filtering' section with 'Max lines' set to 10 and a 'String filter' input field. Below are two tables:

Date	IP	État	Adresse	Squid - Access Logs	Utilisateur	Destination
25.11.2024 16:10:18				Squid Access Table		

Date-Time	Message	Squid - Cache Logs
01.01.1970 00:00:00	Pinger exiting.	
01.01.1970 00:00:00	Accepting HTTP Socket connections at conn271 local=10.2.104.254:3128 remote=[::] FD 38 flags=9	
25.11.2024 16:10:18	Finished loading MIME types and icons.	
25.11.2024 16:10:18	Pinger socket opened on FD 40	
01.01.1970 00:00:00	ICMPv6 socket opened.	
01.01.1970 00:00:00	ICMP socket opened.	
01.01.1970 00:00:00	Initialising ICMP pinger ...	
25.11.2024 16:10:18	HTCP Disabled.	
01.01.1970 00:00:00		

Surveillance des Logs de Squid Reverse Proxy

Maintenant que le **reverse proxy Squid** est activé, on peut voir les logs en temps réel via l'interface de **monitoring** de pfSense. Dans l'onglet **Temps Réel**, les logs de Squid sont affichés, permettant de vérifier l'état et l'activité du proxy.

- Dans la section **Squid Cache Table**, plusieurs messages d'état sont visibles, tels que :
 - Accepting HTTP Socket connections : Cela indique que Squid accepte les connexions HTTP entrantes. On peut voir les informations détaillées concernant les connexions (adresses locales et distantes).

- **Initialising ICMP socket et ICMP socket opened** : Squid est configuré pour vérifier la disponibilité des serveurs via ICMP (ping).
- **HTCP Disabled** : Cela signifie que le protocole HTCP (Hyper Text Caching Protocol) est désactivé, probablement parce qu'il n'est pas nécessaire dans cette configuration.

Ces logs montrent l'activité du reverse proxy, fournissant des informations sur la manière dont Squid gère les connexions et les protocoles utilisés. Le fait de surveiller ces logs permet de s'assurer que tout fonctionne comme prévu et de diagnostiquer les problèmes potentiels.

24. SPAMHAUS +

Spamhaus est un service en ligne qui fournit des listes noires d'adresses IP connues pour envoyer du spam ou être impliquées dans des activités malveillantes. Ce type de liste, souvent appelée "blocklist" ou "blacklist", est maintenue par Spamhaus et régulièrement mise à jour. Elle est largement utilisée dans le monde pour protéger les réseaux contre des activités nuisibles, telles que les spams, les tentatives de phishing ou d'autres formes de cyberattaques.

Dans le contexte de pfSense, l'intégration de la liste de Spamhaus présente un intérêt considérable. En utilisant cette liste, nous pouvons automatiquement bloquer les adresses IP identifiées comme malveillantes avant même qu'elles n'aient la chance d'atteindre notre réseau. Cela permet de renforcer la sécurité globale et de réduire la quantité de trafic indésirable entrant sur notre réseau, assurant ainsi une meilleure stabilité et une réduction de la charge sur les ressources internes.

The screenshot shows the pfSense firewall alias configuration page. The top navigation bar includes links for Système, Interfaces, Pare-feu, Services, VPN, État, Diagnostics, and Aide. The main section is titled 'Pare-feu / Alias / Modifier'. The 'Propriétés' tab is selected, showing fields for 'Nom' (spamhaus_drop), 'Description' (empty), and 'Type' (Table URL (IPs)). Below this, the 'Table URL (IPs)' tab is active, displaying an 'Astuce' (Tip) about using a single URL to download a large list of IPs. The 'Table URL (IPs)' input field contains 'https://www.spamhaus.org/drop/drop.txt' and a dropdown menu set to '128'. To the right of the input field is a link labeled 'Liste spam haus'. At the bottom of the screen, there is a green 'Enregistrer' (Save) button.

1. **Propriétés de l'Alias** : Nous avons nommé l'alias "spamhaus_drop", pour facilement identifier cette liste dans la configuration de pfSense.
2. **Type d'Alias** : Le type est défini comme **Table URL (IPs)**. Cela permet d'utiliser une URL qui contient une grande liste d'adresses IP à bloquer, telles que celles fournies par Spamhaus.

3. Fréquence de Mise à Jour : La fréquence de mise à jour a été définie sur **128**, garantissant ainsi une actualisation fréquente de la liste pour s'assurer que nous sommes protégés contre les menaces récentes.

r) MISE EN PLACE DE CRON :

Cron est un utilitaire sur les systèmes Unix/Linux qui permet de planifier l'exécution de tâches à intervalles réguliers ou à des moments précis. C'est l'outil privilégié pour automatiser les processus répétitifs, par exemple les sauvegardes, les mises à jour de systèmes, l'envoi de rapports, ou même la surveillance de l'activité sur des serveurs.

Fonctionnement de Cron

Le **service cron** fonctionne en arrière-plan et exécute des commandes en fonction de fichiers appelés **crontabs** (contraction de "cron tables"). Ces fichiers contiennent des règles qui indiquent à quel moment exécuter des scripts ou des commandes.

Une tâche cron est définie avec une syntaxe qui précise les moments où la tâche doit être exécutée. La structure d'une règle cron est divisée en cinq champs qui permettent de définir la périodicité :

minute	hour	mday	month	wday	who	command	
*/1	*	*	*	*	root	/usr/sbin/newsyslog	
1	3	*	*	*	root	/etc/rc.periodic daily	
15	4	*	*	6	root	/etc/rc.periodic weekly	
30	5	1	*	*	root	/etc/rc.periodic monthly	
1,31	0-5	*	*	*	root	/usr/bin/nice -n20 adjkerntz -a	
1	3	1	*	*	root	/usr/bin/nice -n20 /etc/rc.update_bogons.sh	
1	1	*	*	*	root	/usr/bin/nice -n20 /etc/rc.dyndns.update	
*/60	*	*	*	*	root	/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600 virusprot	
30	12	*	*	*	root	/usr/bin/nice -n20 /etc/rc.update_urllables	
1	0	*	*	*	root	/usr/bin/nice -n20 /etc/rc.update_pkg_metadata	
*/5	*	*	*	*	root	/usr/bin/nice -n20 /usr/local/bin/php -f /usr/local/pkg/snort/snort_check_cron_misc.inc	
0	0	*	*	*	root	/usr/local/sbin/squid -k rotate -f /usr/local/etc/squid/squid.conf	
15	0	*	*	*	root	/usr/local/pkg/swaptstate_check.php	
36	*/24	*	*	*	clamav	/usr/local/bin/freshclam --config-file=/usr/local/etc/freshclam.conf	

La configuration Cron de pfSense montre des tâches automatisées essentielles, telles que la rotation des logs toutes les minutes (newsyslog), l'exécution quotidienne, hebdomadaire, et mensuelle de scripts de maintenance (rc.periodic), et la mise à jour des bogons et des enregistrements DDNS pour la sécurité du réseau. Des tâches spécifiques comme l'ajustement de l'horloge (adjkerntz), la gestion de Snort (pour la détection d'intrusion), et la mise à jour des métadonnées des packages garantissent le bon fonctionnement du système. Les mises à jour de tables d'URL, d'entrées de tables (expiretable), et des configurations de Squid et Freshclam sont également gérées de manière régulière pour maintenir la sécurité et l'efficacité du réseau.

Add A Cron Schedule

Minute: 5
The minute(s) at which the command will be executed or a special @ event string. (0-59, ranges, divided, @ event or delay, *=all)

Heure: *
The hour(s) at which the command will be executed. (0-23, ranges, or divided, *=all)

Day of the Month: *
The day(s) of the month on which the command will be executed. (1-31, ranges, or divided, *=all)

Month of the Year: *
The month(s) of the year during which the command will be executed. (1-12, ranges, or divided, *=all)

Day of the Week: *
The day(s) of the week on which the command will be executed. (0-7, 7=Sun or use names, ranges, or divided, *=all)

Utilisateur: root
The user executing the command (typically "root")

Command: /usr/local/bin/zabbix_sender -z 10.0.104.10 -s "pfSense" -k custom-key -o "value"
The full path to the command, plus parameters.

Cette règle Cron envoie des métriques de pfSense à un serveur Zabbix à l'adresse IP 10.0.104.10 toutes les heures, à la cinquième minute. La commande zabbix_sender transmet

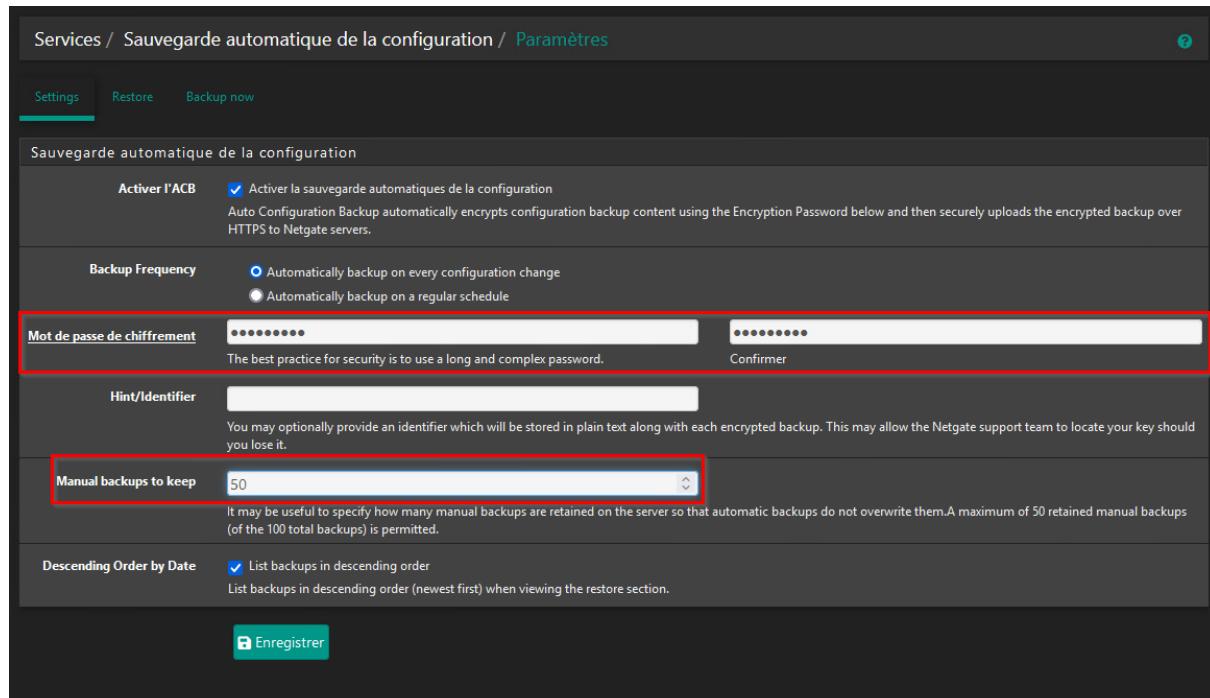
des données avec l'hôte nommé "pfSense" et une clé personnalisée ("custom-key") avec une valeur associée. Cette configuration permet une surveillance automatisée de l'état du système via Zabbix, offrant une vue centralisée et continue sur les performances et l'intégrité de pfSense, utile pour prévenir les problèmes en détectant les anomalies rapidement.

25. Sauvegarde Automatique.

Documentation : Sauvegarde Automatique de la Configuration

14. Paramètres de Sauvegarde Automatique

- La sauvegarde automatique de la configuration de pfSense est activée, ce qui garantit que la configuration du pare-feu est sauvegardée et sécurisée. Voici les éléments configurés et à documenter :
- Mot de passe de chiffrement** : **3Jcsqvs2***
 - Ce mot de passe est utilisé pour chiffrer les sauvegardes avant qu'elles ne soient transférées vers le serveur Netgate. Il est essentiel de conserver ce mot de passe, car il est nécessaire pour **restaurer les sauvegardes**. Assurez-vous de le conserver en lieu sûr.
- Clé de Chiffrement Importante** :
e43ef572bf88f55a1d211c0e9b1729f1a700e89e362e537189b790d168116600
 - Cette clé est critique pour la **restauration des configurations chiffrées**. Elle doit être stockée de manière sécurisée, car sans cette clé, les sauvegardes ne pourront pas être restaurées. La perte de cette clé peut entraîner une impossibilité de récupérer la configuration.



The screenshot shows the configuration page for automatic configuration backups. Key settings visible include:

- Activer l'ACB**: Checked.
- Backup Frequency**: Set to "Automatically backup on every configuration change".
- Mot de passe de chiffrement**: A password field containing "3Jcsqvs2*" is highlighted with a red border.
- Hint/Identifier**: An optional identifier field.
- Manual backups to keep**: A dropdown menu set to "50" is highlighted with a red border.
- Descending Order by Date**: Checked.

Manuel Backups to Keep : 50

- Ce paramètre indique que **50 sauvegardes manuelles** doivent être conservées sur le serveur. Cela permet de ne pas écraser les anciennes sauvegardes manuelles par les nouvelles, assurant ainsi la possibilité de revenir à des versions antérieures de la configuration si nécessaire.

15. Fréquence de Sauvegarde

Deux options de fréquence de sauvegarde sont disponibles :

- **Sauvegarde Automatique sur chaque modification** de configuration.
- **Sauvegarde à intervalles réguliers**, option configurable pour des sauvegardes périodiques.

Dans cette configuration, la sauvegarde automatique est déclenchée à chaque changement de configuration, garantissant que toutes les modifications soient sauvegardées immédiatement.

16. Sécurité et Conservation

- **Chiffrement** : Toutes les sauvegardes sont chiffrées avec le mot de passe fourni, garantissant la confidentialité des données en cas de transfert.
- **Rétention des Sauvegardes** : La conservation de **50 sauvegardes manuelles** est un bon équilibre pour assurer une **historique suffisant** des configurations tout en limitant l'utilisation de l'espace de stockage.

The screenshot shows the 'Services / Auto Configuration Backup / Restore' page. The 'Restore' tab is active. At the top, there's a 'Clé du périphérique' input field containing 'e43ef572bf88f55a1d211c0e9b1729f1a700e89e362e537189b790d168116600'. Below it is a note: 'ID utilisé pour identifier ce pare-feu (dérivé de la clé publique SSH.) Voir l'aide ci-dessous pour plus de détails. S'il vous plaît, faites une copie en lieu sûr de cette valeur d'ID. Si elle est perdue, vos sauvegardes seront également perdues !'. There are 'Soumettre' and 'Réinitialiser' buttons. The main area shows a table of 'Sauvegardes automatiques de configuration' with columns: Date, Modification de configuration, and Actions. Three recent backups are listed:

Date	Modification de configuration	Actions
Tue, 26 Nov 2024 07:59:04 +0000	admin@10.0.104.1 (Local Database): AutoConfigBackup settings updated	
Tue, 26 Nov 2024 07:59:03 -0000	admin@10.0.104.1 (Local Database): AutoConfigBackup settings updated	
Tue, 26 Nov 2024 07:59:02 +0000	admin@10.0.104.1 (Local Database): Installed cron job for /usr/bin/nice -n20 /usr/local/bin/php /usr/local/sbin/acbupload.php	

Nombre actuel de sauvegardes hébergées : 3

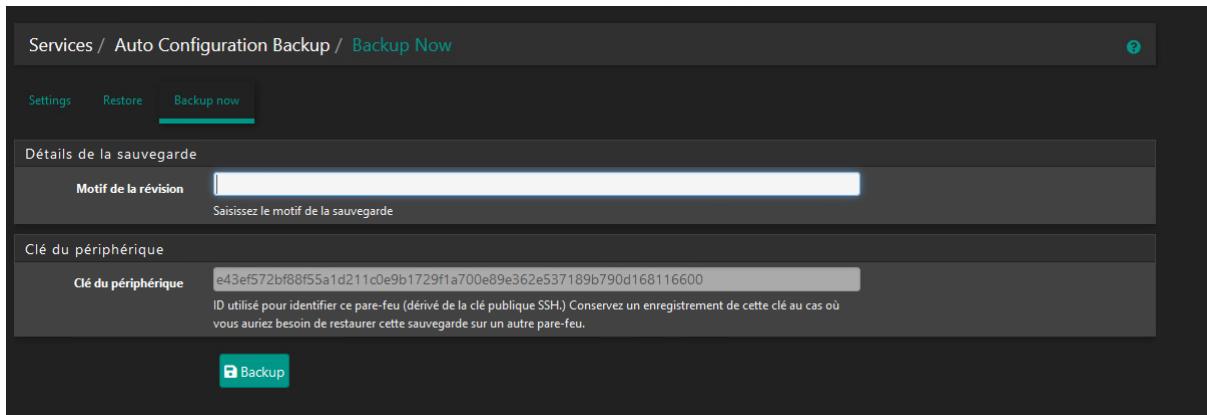
Restauration des Sauvegardes Automatiques

Dans l'onglet **Restore**, la **clé du périphérique** est utilisée pour identifier le pare-feu et restaurer les configurations sauvegardées. Trois sauvegardes récentes sont listées, enregistrant les changements de paramètres et l'installation de tâches Cron.

Pour chaque sauvegarde, on peut :

- **Restaurer** la configuration.
- **Supprimer** la sauvegarde non nécessaire.
- **Télécharger** la sauvegarde pour la conserver hors ligne.

Ces actions permettent une récupération rapide en cas de problème, assurant ainsi la continuité du service.



Sauvegarde Immédiate de la Configuration

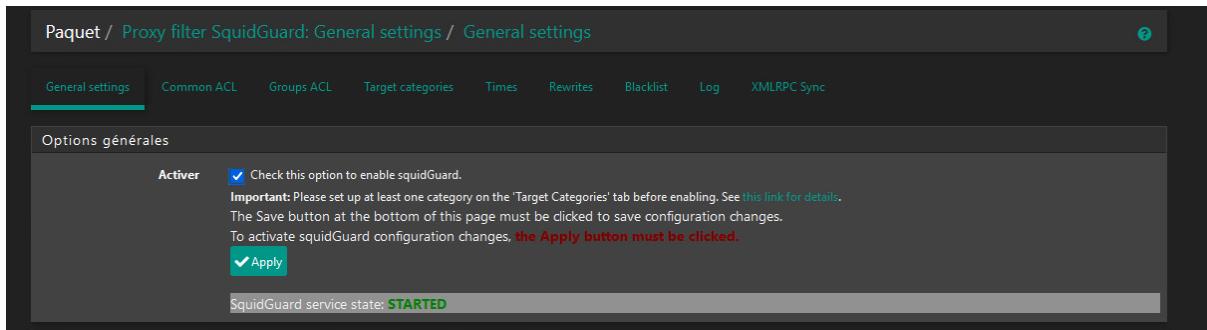
Dans l'onglet **Backup Now**, il est possible de déclencher une sauvegarde immédiate. On peut spécifier un **motif de la révision** pour identifier la sauvegarde. La **clé du périphérique** est utilisée pour sécuriser l'accès et identifier le pare-feu lors de la restauration.

Après avoir saisi un motif et vérifié la clé, on peut lancer la sauvegarde en cliquant sur **Backup**. Cela permet de créer manuellement une sauvegarde à un moment précis, en dehors des sauvegardes automatiques.

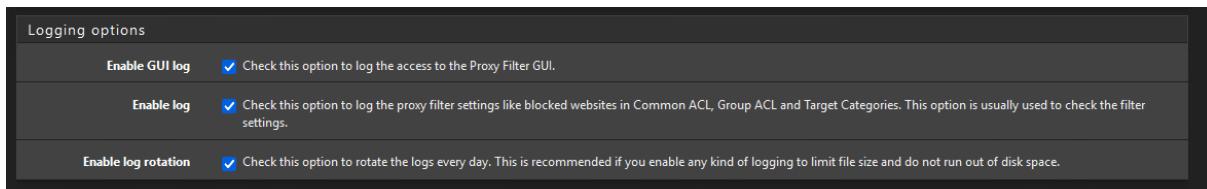
s) SQUIDGUARD :

Configuration de Logging dans SquidGuard

Dans la section **Logging Options** de **SquidGuard**, toutes les options de journalisation sont activées pour assurer une traçabilité complète des activités et un meilleur contrôle. Voici les détails :



- Enable GUI Log** : Activé pour enregistrer tous les accès à l'interface GUI de **Proxy Filter**. Cela permet de suivre qui accède à la configuration du proxy, utile pour des audits de sécurité.



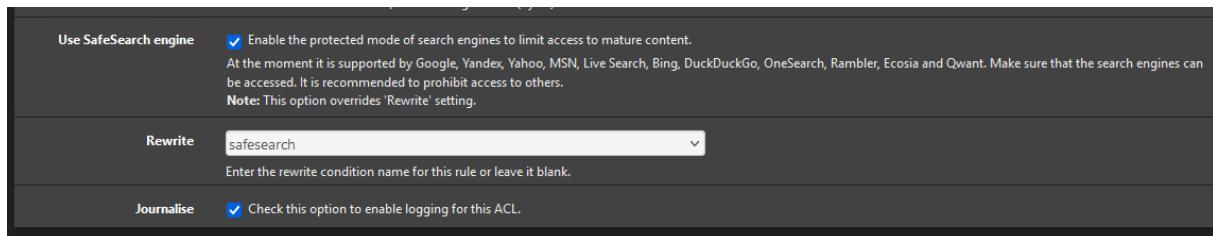
- Enable Log** : Activé pour enregistrer les réglages du filtre proxy, comme les sites bloqués et les ACLs (Listes de Contrôle d'Accès). Cela permet de vérifier quelles règles sont appliquées et de diagnostiquer les filtrages.

- **Enable Log Rotation** : Activé pour effectuer une **rotation quotidienne des logs**, ce qui limite la taille des fichiers journaux et évite de saturer le stockage disponible.

Avec ces options activées, chaque action et configuration dans **SquidGuard** est consignée, et la rotation régulière assure une gestion efficace de l'espace disque.

t) BLOCAGE DES CONTENUS ADULTES ET JOURNALISATION DANS SQUIDGUARD

Dans la configuration de **SquidGuard**, l'option **Use SafeSearch engine** est activée. Cela force l'utilisation du mode **SafeSearch** des moteurs de recherche pris en charge (comme Google, Yahoo, Bing, etc.) pour **limiter l'accès aux contenus pour adultes**. Cette mesure garantit que les recherches effectuées sur le réseau ne montrent pas de résultats inappropriés.



- **Rewrite** : Utilisé pour ajouter des règles spécifiques à l'application de SafeSearch, ici avec la condition safesearch pour s'assurer que les moteurs de recherche respectent ce mode.
- **Journaliser** : L'option de journalisation est activée pour cette **ACL**. Cela permet de **surveiller** l'activité de recherche et de s'assurer que les restrictions sont bien appliquées, en gardant une trace des tentatives d'accès aux contenus bloqués.

Avec ces paramètres, tout le trafic de recherche est filtré pour les contenus adultes, et les tentatives d'accès sont consignées dans des logs, permettant un contrôle efficace du réseau.

u) ALIAS IP :

Intérêt des Alias IP dans pfSense

Les alias IP dans pfSense permettent de simplifier la gestion des règles de pare-feu et des configurations réseau. Au lieu de manipuler directement des adresses IP spécifiques, on utilise des noms descriptifs (comme AD pour Active Directory ou SERVERWEB pour le serveur web), rendant la gestion plus intuitive et claire. Par exemple, modifier une adresse IP dans un alias met à jour automatiquement toutes les règles de pare-feu qui l'utilisent. Cela facilite la maintenance, réduit les risques d'erreur, et améliore la lisibilité des configurations.

Pare-feu / Alias / IP				
IP	Ports	URLs	Tout	
Alias de pare-feu IP				
Nom	Type	Valeurs	Description	Actions
AD	Hôte(s)	10.0.104.1	Active directory 2019	
SERVERWEB	Hôte(s)	10.9.104.1		
Server_GLPI	Réseau(x)	10.1.104.113/24		
Zabbix	Hôte(s)	10.0.104.4	Server Zabbix	
+ Ajouter Import				

26. OPEN VPN + :

OpenVPN est un logiciel VPN (Virtual Private Network) open source qui permet de créer des connexions sécurisées et cryptées entre différents réseaux ou entre un utilisateur distant et un réseau interne. OpenVPN est très flexible et permet d'acheminer le trafic de manière sécurisée sur des réseaux non fiables, comme Internet.

Qu'est-ce qu'OpenVPN ?

OpenVPN est un protocole de tunneling basé sur SSL/TLS qui établit des connexions chiffrées. Cela permet de créer des tunnels sécurisés pour les données, même lorsque la connexion passe par des réseaux publics. Il offre de nombreuses options de configuration, que ce soit pour des utilisateurs individuels, des bureaux distants ou la connexion de plusieurs sites.

Intérêt d'OpenVPN dans pfSense (Version concise)

- Accès Sécurisé** : Permet aux utilisateurs distants d'accéder au réseau interne de façon chiffrée, idéal pour le télétravail.
- Chiffrement des Données** : Garantit une protection complète des données en transit, même sur des réseaux publics.
- Configuration Flexible** : Facilite la gestion des accès, que ce soit pour des utilisateurs individuels ou des connexions site-à-site.
- Pare-feu Intégré** : Intégration avec pfSense pour un contrôle précis des accès grâce aux règles de pare-feu.
- Authentification Sécurisée** : Supporte plusieurs méthodes d'authentification, incluant la double authentification pour plus de sécurité.

v) DOCUMENTATION DE L'INSTALLATION D'OPENVPN SUR PFSENSE

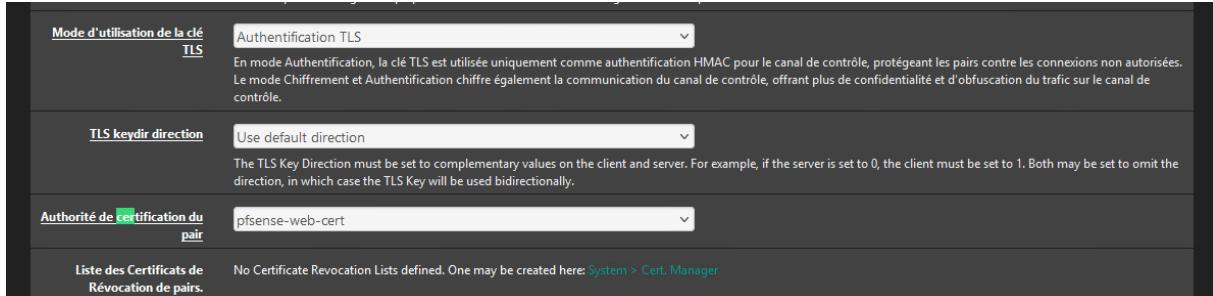
The screenshot shows the pfSense web interface for managing OpenVPN servers. The top navigation bar includes links for 'VPN / OpenVPN / Serveurs / Modifier'. Below the navigation, there are tabs for 'Serveurs' (selected), 'Clients', 'Ré-écritures spécifiques au client', 'Assistants', and 'Client Export'. The main content area is titled 'Informations Générales' and contains the following fields:

- Description:** VPN-INTERNE (A description of this VPN for administrative reference).
- Désactivé:** Désactiver ce serveur (Définissez cette option pour désactiver ce serveur sans le retirer de la liste).
- Unique VPN ID:** Serveur 1 (ovpn1).
- Mode Configuration:**
 - Mode serveur:** Pair à pair (SSL/TLS).
 - Mode dispositif:** tun - Layer 3 Tunnel Mode (Le mode "tun" porte IPv4 et IPv6 (couche OSI 3) et est le mode le plus courant et compatible sur toutes les plates-formes. Le mode "tap" est capable de transporter 802.3 (couche OSI 2).)

17. Configuration Générale du Serveur VPN

- Nom du VPN :** VPN-INTERNE
 - Ce serveur VPN est configuré pour des connexions internes, permettant une gestion et une sécurité des accès au réseau local.
- Mode Configuration :**

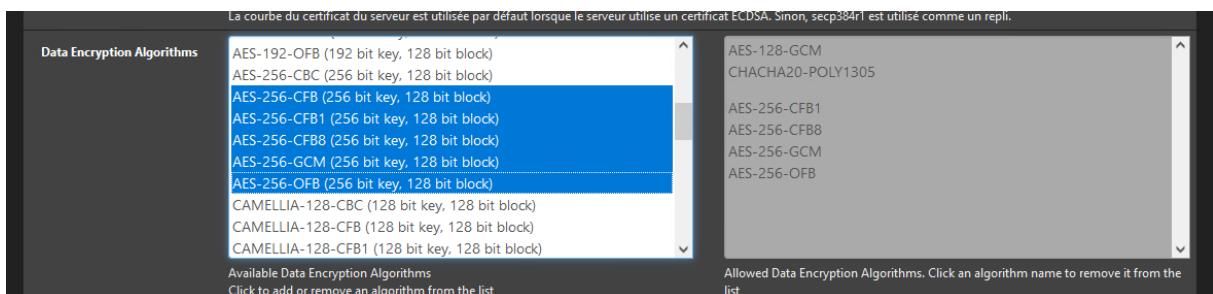
- **Mode serveur** : Pair à pair (SSL/TLS) - Ce mode utilise SSL/TLS pour sécuriser les connexions entre clients et serveur.
- **Mode dispositif** : tun - Layer 3 Tunnel Mode - Le mode tun est choisi pour créer un tunnel sur la couche 3, qui est la méthode la plus couramment utilisée pour acheminer le trafic IP via le VPN.



18. Paramètres de Sécurité et de Chiffrement

- **Mode d'utilisation de la clé TLS** : Authentification TLS
 - Utilisé pour protéger la connexion par le biais d'un HMAC sur le canal de contrôle. Cela garantit l'authentification des pairs et empêche les connexions non autorisées.
- **Direction de la clé TLS** : Use default direction
 - Direction par défaut de la clé TLS, permettant une utilisation bidirectionnelle entre client et serveur pour garantir la synchronisation des clés de chiffrement.

Le **certificat utilisé** pour l'authentification est le même que celui créé précédemment pour le **HTTPS** de l'interface pfSense (pfsense-web-cert). Cela permet d'utiliser un seul certificat pour sécuriser à la fois l'accès à l'interface web et les connexions VPN, simplifiant ainsi la gestion des certificats.



Algorithmes de Chiffrement des Données

Pour le serveur **OpenVPN**, plusieurs algorithmes de chiffrement **AES-256** ont été sélectionnés : **AES-256-OFB**, **AES-256-CBC**, **AES-256-CFB**, **AES-256-GCM**. Ces algorithmes garantissent une sécurité élevée en utilisant des clés de **256 bits**, assurant une robustesse contre les attaques. Le choix multiple permet une **flexibilité** selon les capacités des clients, tout en conservant un **niveau de chiffrement fort** pour protéger les données sensibles transitant par le VPN.



w) CERTIFICAT DU SERVEUR

Pour le serveur **OpenVPN**, le **certificat utilisé** est 10.0.104.254, signé par l'autorité de certification pfsense-sub-cert. Ce certificat est également celui utilisé pour le HTTPS de pfSense, permettant de mutualiser son usage et simplifier la gestion des certificats. Cela assure une **authentification sécurisée** pour les connexions VPN, garantissant que seuls les utilisateurs et clients autorisés peuvent accéder au réseau.

The screenshot shows the 'Serveurs' tab selected in the 'OpenVPN / Serveurs' interface. A single server entry is listed:

Interface	Protocole / Port	Réseau tunnel	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)		Mode: Peer to Peer (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	cVPN-INTERNE	

A green '+ Ajouter' button is located at the bottom right.

Le serveur **OpenVPN** est configuré sur l'interface WAN, utilisant UDP sur le port 1194 avec un tunnel TUN. Le mode SSL/TLS sécurise les connexions, et le chiffrement est assuré par des algorithmes robustes (AES-256, CHACHA20). Le digest SHA256 et Diffie-Hellman 2048 bits garantissent la sécurité des échanges. Ce serveur est prêt pour des connexions VPN internes avec une haute sécurité et une compatibilité optimale.

x) REGLES OPEN VPN

Analyse des Règles de Pare-feu

- Dans la configuration des règles de pare-feu, j'ai fait des choix spécifiques concernant la segmentation des réseaux et l'utilisation de **LAN2** pour la messagerie.

The screenshot shows the 'Règles' (Firewall Rules) configuration page. It lists several rules categorized as follows:

- Messagerie**: A rule allowing traffic from LAN2 address to MAIL port (TCP 1194).
- DNS**: A rule allowing traffic from LAN0 address to DNS port 53 (UDP).
- WEB**: A rule allowing traffic from WAN address to WEB port (TCP 80).
- Règles test**: A rule allowing ICMP traffic from * to *.
- BLOQUE TOUT**: A rule blocking all traffic (red background).

19. Messagerie : Utilisation de LAN2

- Règle Messagerie** : L'accès au **service de messagerie** est autorisé sur **LAN2**. Le choix de **LAN2** plutôt que **LAN1** est motivé par le fait que les clients se connectent au

réseau via **VPN** et utilisent leurs **clients de messagerie personnels**. Cela signifie qu'ils n'ont pas besoin d'accéder directement à un client **GLPI** ou un autre service interne sur **LAN1**.

- **Raisonnement** : **LAN1** est réservé à d'autres services (comme **GLPI**) qui pourraient être utilisés localement. Avec le VPN, les utilisateurs n'ont pas de nécessité d'accéder à GLPI depuis leur poste distant pour de la simple messagerie. Par conséquent, il est plus pertinent de segmenter le trafic de messagerie vers un réseau dédié (**LAN2**), isolant ainsi les accès en fonction de leur usage.

20. Autres Règles

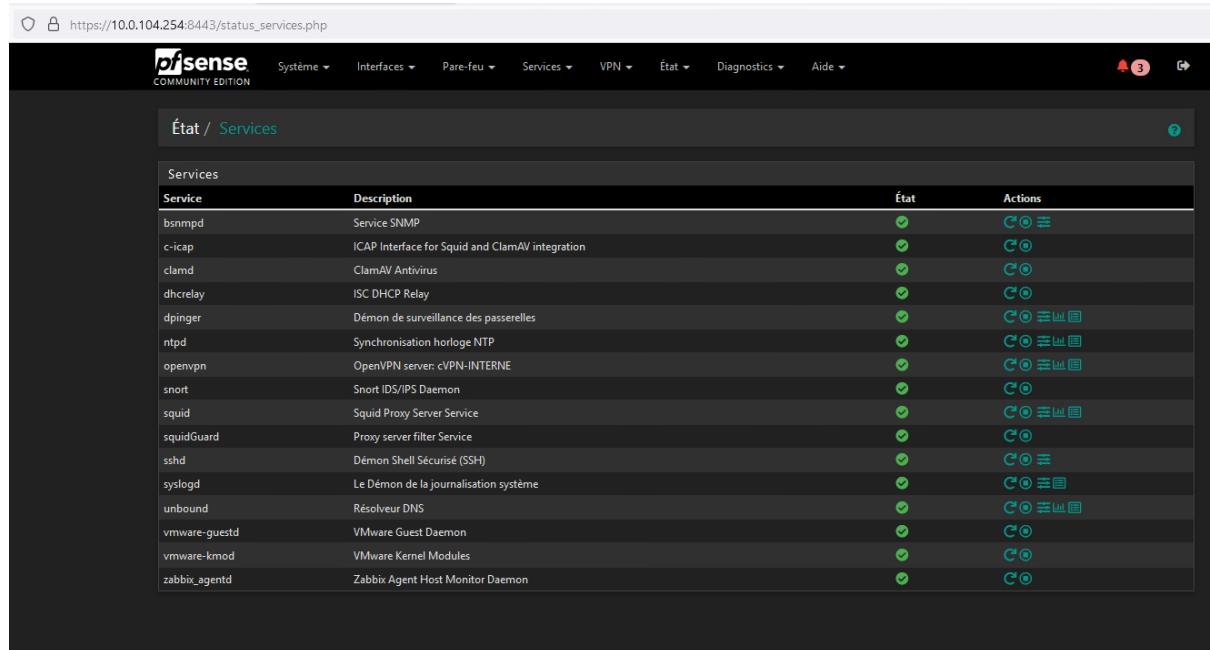
- **DNS** : Le DNS est autorisé depuis le réseau VPN vers **LAN0** sur le port **53/UDP**. Cela permet aux clients VPN de résoudre les adresses tout en limitant l'accès à une zone réseau spécifique.
- **Web** : Accès autorisé depuis l'extérieur vers l'adresse WAN pour les services **web**. Cette règle facilite l'accès externe aux services web hébergés.
- **Règle de Test ICMP** : Permet de tester la connectivité (via **ping**) depuis les réseaux clients, facilitant les vérifications du fonctionnement du VPN.
- **Bloque Tout** : Une règle de blocage par défaut pour le **TCP/UDP** en fin de liste assure qu'aucun trafic non autorisé ne passe, renforçant ainsi la sécurité.

y) ARGUMENTATION SUR LE CHOIX DE LAN2

Le choix de **LAN2** pour la messagerie plutôt que **LAN1** s'explique par l'organisation et la sécurité du réseau. En utilisant un **VPN**, les utilisateurs n'ont pas besoin de passer par un réseau qui contient des ressources spécifiques telles que **GLPI** sur **LAN1**. Le VPN donne un accès sécurisé au réseau, mais la segmentation des différents services est importante pour maintenir la sécurité et l'efficacité. En isolant la messagerie sur **LAN2**, on limite le risque d'accès non nécessaire ou accidentel à des ressources internes sensibles, tout en optimisant les flux réseau. L'option d'utiliser **LAN1** aurait impliqué de mélanger les accès, ce qui n'apporte aucun avantage particulier dans un contexte de VPN sécurisé et aurait ajouté de la complexité inutile.

27. VERIFICATION :

Dans cette dernière étape de la configuration de pfSense, j'ai vérifié l'état de chaque service installé afin de m'assurer qu'ils fonctionnent correctement et sont configurés comme prévu. La capture d'écran montre l'ensemble des services essentiels déployés, comme le serveur SNMP (bsnmpd), le démon NTP pour la synchronisation de l'heure (ntpd), OpenVPN pour la gestion des connexions VPN sécurisées, ainsi que le service de surveillance Zabbix (zabbix_agentd).

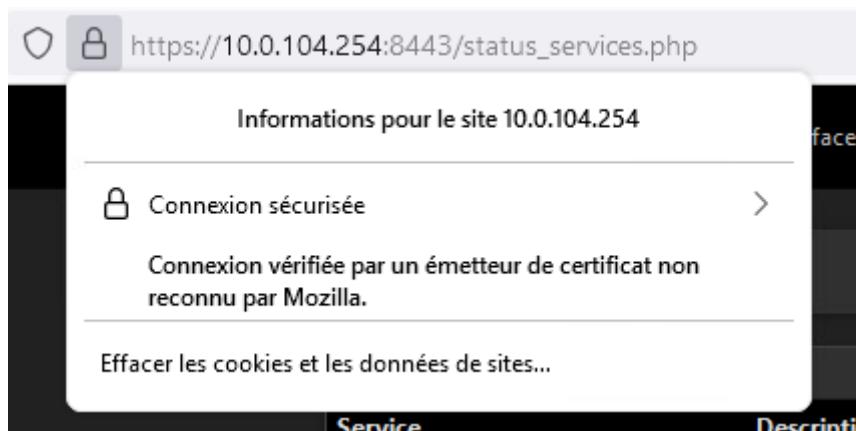


The screenshot shows the pfSense Services status page. The top navigation bar includes links for Système, Interfaces, Pare-feu, Services, VPN, État, Diagnostics, and Aide. A notification icon in the top right corner shows 3 alerts. The main table lists various services with their status (État) and actions. All services listed are active (green checkmark). The services include bsnmpd, c-icap, clamd, dhcrelay, dpinge, ntpd, openvpn, snort, squid, squidGuard, sshd, syslogd, unbound, vmware-guestd, vmware-kmod, and zabbix_agentd.

Service	Description	État	Actions
bsnmpd	Service SNMP	✓	Configure, Stop, Start, Restart, Log
c-icap	ICAP Interface for Squid and ClamAV integration	✓	Configure, Stop, Start, Restart, Log
clamd	ClamAV Antivirus	✓	Configure, Stop, Start, Restart, Log
dhcrelay	ISC DHCP Relay	✓	Configure, Stop, Start, Restart, Log
dpinge	Démon de surveillance des passerelles	✓	Configure, Stop, Start, Restart, Log
ntpd	Synchronisation horlogé NTP	✓	Configure, Stop, Start, Restart, Log
openvpn	OpenVPN server: cVPN-INTERNE	✓	Configure, Stop, Start, Restart, Log
snort	Snort IDS/IPS Daemon	✓	Configure, Stop, Start, Restart, Log
squid	Squid Proxy Server Service	✓	Configure, Stop, Start, Restart, Log
squidGuard	Proxy server filter Service	✓	Configure, Stop, Start, Restart, Log
sshd	Démon Shell Sécurisé (SSH)	✓	Configure, Stop, Start, Restart, Log
syslogd	Le Démon de la journalisation système	✓	Configure, Stop, Start, Restart, Log
unbound	Résolveur DNS	✓	Configure, Stop, Start, Restart, Log
vmware-guestd	VMware Guest Daemon	✓	Configure, Stop, Start, Restart, Log
vmware-kmod	VMware Kernel Modules	✓	Configure, Stop, Start, Restart, Log
zabbix_agentd	Zabbix Agent Host Monitor Daemon	✓	Configure, Stop, Start, Restart, Log

Chaque service présente un statut actif, ce qui confirme leur bonne configuration et leur bon fonctionnement. Par exemple, ClamAV (clamd) pour l'antivirus, Snort pour la détection d'intrusions, et le démon SSH (sshd) pour l'accès sécurisé en ligne de commande, sont tous activés et opérationnels. De plus, la mise en place des résolveurs DNS avec Unbound et l'intégration de Squid Proxy Filter démontrent que les mesures de sécurité et d'optimisation du réseau sont bien en place.

Cela montre que pfSense est bien configuré pour offrir à la fois des fonctionnalités réseau avancées et un niveau de sécurité optimal, répondant ainsi aux exigences définies pour ce projet.



The screenshot shows a browser security warning for the site 10.0.104.254. The message states: "Informations pour le site 10.0.104.254". It highlights that the connection is secured ("Connexion sécurisée") but the certificate is not recognized by Mozilla ("Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla"). There is also a link to clear cookies and site data ("Effacer les cookies et les données de sites..."). Below the message, there are two columns: "Service" and "Description".

Service	Description
Connexion sécurisée	Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla.
Effacer les cookies et les données de sites...	

En complément de la vérification des services, j'ai également contrôlé l'accès sécurisé via HTTPS à l'interface de gestion de pfSense. Comme montré dans la capture d'écran, la connexion est bien sécurisée, indiquée par le cadenas. Cependant, le navigateur affiche un

avertissement signalant que le certificat n'est pas reconnu par Mozilla. Cela est typique lorsque l'on utilise un certificat auto-signé, fréquemment employé dans des environnements internes ou pour des tests.

Bien que la connexion soit chiffrée, ce message souligne l'importance d'installer un certificat émis par une autorité de certification (CA) reconnue si l'on souhaite éliminer ce type d'avertissement et garantir une validation complète, même dans un environnement de production. Cela renforcerait la sécurité et la confiance lors de l'accès à l'interface web de pfSense.

28. VERIFICATION VIA SHELL :

```
Sortie Console - ifconfig

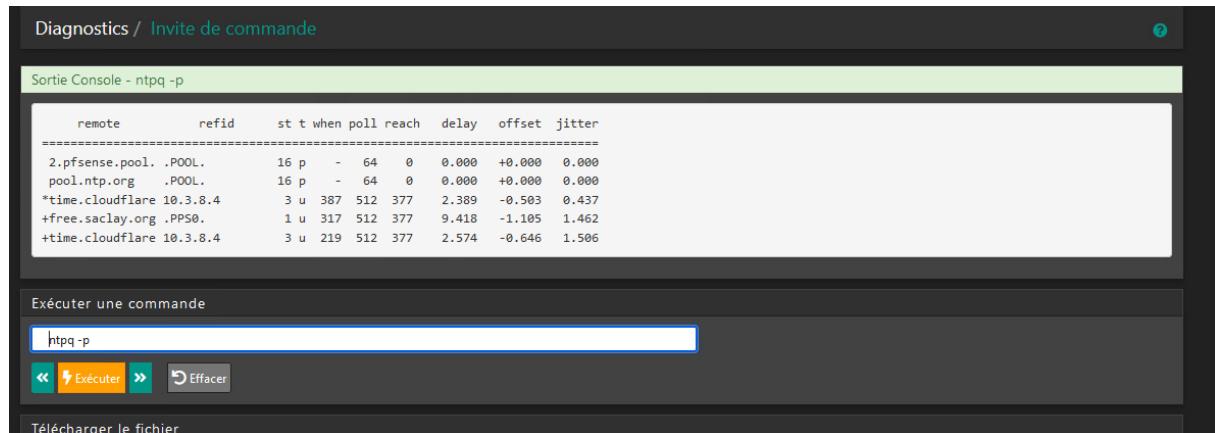
vmx0: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    description: LAN2
    options=4e000bb:RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,RXCSUM_IPV6,TXCSUM_IPV6,HWSTATS,MEXTPG>
    ether 00:50:56:ab:96:cd
    inet 10.2.104.254 netmask 0xffffffff broadcast 10.2.104.255
    inet6 fe80::250:56ff:feab:96cd%vmx0 prefixlen 64 scopeid 0x1
        media: Ethernet autoselect
        status: active
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
vmx1: flags=1008943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    description: DMZ
    options=4e000bb:RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,RXCSUM_IPV6,TXCSUM_IPV6,HWSTATS,MEXTPG>
    ether 00:50:56:ab:8a:e7
    inet 10.9.104.254 netmask 0xffffffff broadcast 10.9.104.255
    inet6 fe80::250:56ff:feab:8ae7%vmx1 prefixlen 64 scopeid 0x2
        media: Ethernet autoselect
        status: active
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
vmx2: flags=1008943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    description: WAN
    options=4e000bb:RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,RXCSUM_IPV6,TXCSUM_IPV6,HWSTATS,MEXTPG>
    ether 00:50:56:ab:8b:ad
    inet 192.168.10.104 netmask 0xffffffff broadcast 192.168.10.255
    inet6 fe80::250:56ff:feab:8bad%vmx2 prefixlen 64 scopeid 0x3
        media: Ethernet autoselect
        status: active
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
vmx3: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    description: LAN0
    options=4e000bb:RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,RXCSUM_IPV6,TXCSUM_IPV6,HWSTATS,MEXTPG>
    ether 00:50:56:ab:4f:b7
    inet 10.0.104.254 netmask 0xffffffff broadcast 10.0.104.255
    inet6 fe80::250:56ff:feab:4fb7%vmx3 prefixlen 64 scopeid 0x4
        media: Ethernet autoselect
        status: active
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
vmx4: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
```

L'exécution de la commande ifconfig a permis d'obtenir des informations détaillées sur les interfaces réseau configurées sur le système pfSense. L'interface vmx0, qui correspond au réseau LAN2, dispose de l'adresse IPv4 10.2.104.254 et d'une adresse IPv6 fe80::250:56ff:feab:96cd. Cette interface est actuellement active et fonctionnelle. De même, l'interface vmx1, dédiée à la zone DMZ, possède l'adresse IPv4 10.9.104.254 ainsi qu'une adresse IPv6 fe80::250:56ff:feab:8ae7. Elle est également en état actif, tout comme vmx2, l'interface WAN, qui est configurée avec l'adresse IPv4 192.168.10.104 et l'adresse IPv6 fe80::250:56ff:feab:8ad8.

L'interface vmx3, associée à la description LAN, est configurée avec une adresse IPv4 identique à celle de LAN2 (10.2.104.254) ainsi qu'une adresse IPv6 propre (fe80::250:56ff:feab:4fb), et est également en état actif. Enfin, l'interface vmx4 ne dispose pas de détails relatifs à une configuration IPv4 ou IPv6 spécifique, mais elle est tout de même active. En résumé, toutes les interfaces sont en bon état de fonctionnement, et le système est configuré pour segmenter correctement le réseau en plusieurs zones (LAN, DMZ, WAN), garantissant une gestion efficace et sécurisée du trafic réseau.

z) NTP

La commande ntpq -p a été utilisée pour vérifier l'état des serveurs NTP configurés sur le système pfSense. Les résultats montrent que quatre serveurs NTP sont configurés. Parmi eux, le serveur time.cloudflare.com est actuellement utilisé pour la synchronisation de l'horloge, avec un délai de 2.574 ms et un décalage (offset) de -0.646 ms, ce qui indique une synchronisation stable. Le serveur free.saclay.org est également accessible et en attente de synchronisation, affichant un délai de 9.418 ms. Les deux autres serveurs (2.pfsense.pool.ntp.org et pool.ntp.org) ne sont pour l'instant pas synchronisés, affichant un délai nul. Globalement, la synchronisation semble bien fonctionner avec time.cloudflare.com comme source de référence, tandis que d'autres serveurs sont disponibles en cas de besoin.



```
Sortie Console - ntpq -p
=====
remote      refid      st t when poll reach   delay    offset  jitter
=====
2.pfsense.pool. .POOL.    16 p  - 64  0  0.000 +0.000  0.000
pool.ntp.org .POOL.    16 p  - 64  0  0.000 +0.000  0.000
*time.cloudflare 10.3.8.4 3 u 387 512 377 2.389 -0.503  0.437
+free.saclay.org .PPS0.   1 u 317 512 377 9.418 -1.105  1.462
+time.cloudflare 10.3.8.4 3 u 219 512 377 2.574 -0.646  1.506
```

Exécuter une commande

Exécuter Effacer

Télécharger le fichier



```
groups: priog
pfsync0: flags=0 metric 0 mtu 1500
        options=0
        maxupd: 128 defer: off version: 1400
        syncok: 1
        groups: pfsync
ovpns1: flags=8010<POINTOPOINT,MULTICAST> metric 0 mtu 1500
        options=80000<LINKSTATE>
        groups: tun openvpn
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        Opened by PID 69934
```

Exécuter une commande

Exécuter Effacer

Résultat supplémentaire de la commande ifconfig

La capture de l'exécution de la commande ifconfig met en évidence d'autres interfaces spécifiques configurées sur le système pfSense. On retrouve notamment l'interface pfsync0, qui est utilisée pour la synchronisation de l'état du pare-feu entre plusieurs instances pfSense. Cette interface a une métrique définie à 0 et une valeur MTU de 1500, ce qui indique son rôle essentiel dans la communication pour la haute disponibilité. Les options incluent un support pour la synchronisation (syncok : 1), ce qui est crucial pour assurer la redondance des règles et des états.

Ensuite, l'interface ovpns1 est dédiée au VPN, spécifiquement pour OpenVPN. Elle est également configurée avec une métrique de 0 et une valeur MTU de 1500. Les options

montrent que cette interface utilise le groupe tun, ce qui indique une configuration typique pour un tunnel VPN point à point. L'interface est ouverte par le processus ayant le PID 69934, confirmant qu'un service OpenVPN est actif et utilise cette interface pour le transfert de données VPN.

En résumé, pfsync0 assure la synchronisation des états pour le failover entre pare-feux, tandis que ovpsn1 gère les connexions VPN, toutes deux en état actif et configurées pour garantir une connectivité réseau stable et sécurisée.

```
Sortie Console - netstat -r

Routing tables

Internet:
Destination     Gateway      Flags   Netif  Expire
default         192.168.10.254  UGS    vmx2
10.0.104.0/24   link#4      U       vmx3
Eloham          link#7      UHS    lo0
10.1.104.0/24   link#5      U       vmx4
10.1.104.254   link#7      UHS    lo0
10.2.104.0/24   link#1      U       vmx0
10.2.104.254   link#7      UHS    lo0
10.9.104.0/24   link#2      U       vmx1
10.9.104.254   link#7      UHS    lo0
localhost        link#7      UH     lo0
192.168.10.0/24 link#3      U       vmx2
192.168.10.104  link#7      UHS    lo0

Internet6:
Destination     Gateway      Flags   Netif  Expire
localhost        link#7      UHS    lo0
fe80::%vmx0/64  link#1      U       vmx0
fe80::250:56ff:fea link#7  UHS    lo0
fe80::%vmx1/64  link#2      U       vmx1
fe80::250:56ff:fea link#7  UHS    lo0
fe80::%vmx2/64  link#3      U       vmx2
fe80::250:56ff:fea link#7  UHS    lo0
fe80::%vmx3/64  link#4      U       vmx3
fe80::250:56ff:fea link#7  UHS    lo0
fe80::%vmx4/64  link#5      U       vmx4
fe80::250:56ff:fea link#7  UHS    lo0
fe80::%lo0/64   link#7      U       lo0
fe80::1%lo0     link#7      UHS    lo0
```

Résultat de la commande netstat -r

La table de routage obtenue avec netstat -r montre les chemins configurés pour le trafic IPv4 et IPv6 sur le système. Pour IPv4, la route par défaut passe par le gateway 192.168.10.254 via l'interface vmx2, représentant la sortie vers Internet. Des routes locales sont également configurées pour les réseaux 10.0.0.0/24, 10.1.104.0/24, et 192.168.10.0/24, utilisant les interfaces vmx0, vmx1, et vmx2 respectivement.

Pour IPv6, on observe des routes pour des adresses locales fe80::/64 assignées à chaque interface (vmx0 à vmx4). L'interface lo0 est également configurée pour les adresses de loopback locales.

Ces configurations montrent une table de routage cohérente, facilitant l'acheminement du trafic pour tous les segments de réseau définis.

Sortie Console - df -h						
Filesystem	Size	Used	Avail	Capacity	Mounted on	
pfSense/ROOT/default	42G	905M	41G	2%	/	
devfs	1,0K	0B	1,0K	0%	/dev	
pfSense/var	41G	1,5M	41G	0%	/var	
pfSense/tmp	41G	288K	41G	0%	/tmp	
pfSense/var/log	41G	1,5M	41G	0%	/var/log	
pfSense/var/cache	41G	96K	41G	0%	/var/cache	
pfSense/home	41G	108K	41G	0%	/home	
pfSense/var/db	41G	280M	41G	1%	/var/db	
pfSense/var/tmp	41G	104K	41G	0%	/var/tmp	
pfSense/var/empty	41G	96K	41G	0%	/var/empty	
pfSense	41G	96K	41G	0%	/pfSense	
pfSense/reservation	46G	96K	46G	0%	/pfSense/reservation	
pfSense/ROOT/default/cf	41G	1,6M	41G	0%	/cf	
pfSense/ROOT/default/var_cache_pkg	41G	43M	41G	0%	/var/cache/pkg	
pfSense/ROOT/default/var_db_pkg	41G	5,2M	41G	0%	/var/db/pkg	
tmpfs	4,0M	152K	3,9M	4%	/var/run	
devfs	1,0K	0B	1,0K	0%	/var/dhcpd/dev	

Résultat de la commande df -h

La commande df -h indique l'utilisation de l'espace disque sur le système pfSense. Le système de fichiers principal (/) a une taille totale de 42G, avec 2% utilisé, soit 905M. Les différentes partitions (/var, /tmp, /log, etc.) sont quasiment vides avec une capacité utilisée de 0% ou 1%. Globalement, l'utilisation de l'espace disque est faible, ce qui signifie que le système a suffisamment de capacité disponible pour toutes ses opérations actuelles.

Résultat de la commande netstat -i

Le résultat de la commande netstat -i montre les statistiques des interfaces réseau de pfSense. Les interfaces vmx0, vmx1, vmx2, et vmx3 affichent des volumes importants de paquets entrants (Ipkts) et sortants (Opkts), indiquant un trafic actif sur ces interfaces. Par exemple, vmx2 (WAN) a traité plus de 10 millions de paquets entrants et sortants, tandis que vmx0 et vmx1 gèrent également des volumes élevés. Aucune erreur (Ierrs, Oerrs) ou collision (Coll) n'a été détectée sur les interfaces principales, ce qui est un bon indicateur de la qualité des connexions. L'interface VPN (ovpns1) n'a pas de trafic significatif pour le moment.

Name	Mtu	Network	Address	Ipkts	Ierrs	Idrop	Opkts	Oerrs	Coll
vmx0	1500	<Link#1>	00:50:56:ab:96:cd	2549477	0	0	5804240	0	0
vmx0	-	fe80::%vmx0/64	fe80::250:56ff:feab:96cd%vmx0	0	-	-	1	-	-
vmx0	-	10.2.104.0/24	10.2.104.254	287	-	-	731	-	-
vmx1	1500	<Link#2>	00:50:56:ab:8a:e7	4680275	0	0	78913	0	0
vmx1	-	fe80::%vmx1/64	fe80::250:56ff:feab:8ae7%vmx1	0	-	-	1	-	-
vmx1	-	10.9.104.0/24	10.9.104.254	2632	-	-	0	-	-
vmx2	1500	<Link#3>	00:50:56:ab:8b:ad	56827085	0	0	30992081	0	0
vmx2	-	fe80::%vmx2/64	fe80::250:56ff:feab:8bad%vmx2	0	-	-	1	-	-
vmx2	-	192.168.10.0/24	192.168.10.104	10731721	-	-	10457028	-	-
vmx3	1500	<Link#4>	00:50:56:ab:4f:b7	16785293	0	0	29164750	0	0
vmx3	-	fe80::%vmx3/64	fe80::250:56ff:feab:4fb7%vmx3	0	-	-	2	-	-
vmx3	-	10.0.104.0/24	Eloham	2189295	-	-	2362592	-	-
vmx4	1500	<Link#5>	00:50:56:ab:1a:86	4760819	0	0	8248247	0	0
vmx4	-	fe80::%vmx4/64	fe80::250:56ff:feab:1a86%vmx4	0	-	-	1	-	-
vmx4	-	10.1.104.0/24	10.1.104.254	1078	-	-	0	-	-
enc0*	1536	<Link#6>	enc0	0	0	0	0	0	0
lo0	16384	<Link#7>	lo0	26828	0	0	26828	0	0
lo0	-	localhost	localhost	18597	-	-	18597	-	-
lo0	-	fe80::%lo0/64	fe80::1%lo0	0	-	-	0	-	-
lo0	-	your-net	localhost	3365	-	-	8231	-	-
pflog0*	33152	<Link#8>	pflog0	0	0	0	181685	0	0
pfsync0*	1500	<Link#9>	pfsync0	0	0	0	0	0	0
ovpns1*	1500	<Link#10>	ovpns1	0	0	0	0	0	0

Résultat de la vérification de l'état du pare-feu (pfctl -sr)

Les règles de pare-feu configurées sur pfSense montrent une combinaison de règles de blocage et d'autorisation pour le trafic IPv4 et IPv6. Les règles de blocage (avec block drop in

log) concernent principalement des adresses locales (169.254.0.0/16), bloquant les paquets provenant de cette plage. Il existe également des règles par défaut (Default deny rule) pour refuser tout le trafic IPv4 et IPv6 non spécifiquement autorisé.

En ce qui concerne le trafic IPv6, de nombreuses règles permettent le passage des paquets ICMPv6 pour différents types, notamment echo-request, router-solicit, et neighbor-advertisement, afin de permettre la communication et la découverte des voisins sur le réseau. Ces règles sont configurées pour maintenir l'état des connexions (keep state), assurant une gestion optimale des communications.

Dans l'ensemble, les règles du pare-feu sont configurées pour un bon niveau de sécurité, en bloquant par défaut tout le trafic non autorisé tout en permettant les communications nécessaires pour la découverte de réseau et la gestion ICMPv6.

```
block drop in log quick inet from 169.254.0.0/16 to any label "Block IPv4 link-local" ridentifier 1000000101
block drop in log quick inet from any to 169.254.0.0/16 label "Block IPv4 link-local" ridentifier 1000000102
block drop in log inet all label "Default deny rule IP4" ridentifier 1000000103
block drop out log inet all label "Default deny rule IPv4" ridentifier 1000000104
block drop in log inets all label "Default deny rule IPv6" ridentifier 1000000105
block drop out log inets all label "Default deny rule IPv6" ridentifier 1000000106
pass quick inets all icmp6-type unreachable keep state ridentifier 1000000107
pass quick inets proto ipv6-icmp all icmp6-type toobig keep state ridentifier 1000000107
pass quick inets proto ipv6-icmp all icmp6-type neighborlsol keep state ridentifier 1000000107
pass quick inets proto ipv6-icmp all icmp6-type neighborbradv keep state ridentifier 1000000107
pass quick inets proto ipv6-icmp all icmp6-type neighborbradv keep state ridentifier 1000000107
pass out quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type echoreq keep state ridentifier 1000000108
pass out quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type routersol keep state ridentifier 1000000108
pass out quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type routeradv keep state ridentifier 1000000108
pass out quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type neighborlsol keep state ridentifier 1000000108
pass out quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type neighborbradv keep state ridentifier 1000000108
pass out quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type echoreq keep state ridentifier 1000000109
pass out quick inets proto ipv6-icmp from fe80::/10 to ff02::/16 icmp6-type routersol keep state ridentifier 1000000109
pass out quick inets proto ipv6-icmp from fe80::/10 to ff02::/16 icmp6-type routeradv keep state ridentifier 1000000109
pass out quick inets proto ipv6-icmp from fe80::/10 to ff02::/16 icmp6-type neighborlsol keep state ridentifier 1000000109
pass out quick inets proto ipv6-icmp from fe80::/10 to ff02::/16 icmp6-type neighborbradv keep state ridentifier 1000000109
pass in quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type echoreq keep state ridentifier 1000000110
pass in quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type routersol keep state ridentifier 1000000110
pass in quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type routeradv keep state ridentifier 1000000110
pass in quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type neighborlsol keep state ridentifier 1000000110
pass in quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type neighborbradv keep state ridentifier 1000000110
pass in quick inets proto ipv6-icmp from fe80::/10 to fe80::/10 icmp6-type echoreq keep state ridentifier 1000000110
pass in quick inets proto ipv6-icmp from fe80::/10 to ff02::/16 icmp6-type routersol keep state ridentifier 1000000110
pass in quick inets proto ipv6-icmp from fe80::/10 to ff02::/16 icmp6-type neighborbradv keep state ridentifier 1000000110
pass in quick inets proto ipv6-icmp from :: to ff02::/16 icmp6-type echoreq keep state ridentifier 1000000113
```

aa) CLAV

Résultat de la commande clamd-V

La commande clamd -V a été utilisée pour vérifier la version de ClamAV installée. La version actuelle est ClamAV 1.2.0, avec une mise à jour effectuée le **lundi 25 novembre 2024 à 09:36:56**. Cela indique que ClamAV est à jour et prêt à être utilisé pour scanner et protéger le système contre les menaces potentielles.



```
Sortie Console - freshclam

ClamAV update process started at Tue Nov 26 10:32:48 2024
daily database available for update (local version: 27468, remote version: 27469)
Testing database: '/var/db/clamav//tmp.5cbaaf32d5/clamav-d34ce2c385681e78a7c9d97c8210ad87.tmp-daily.cld' ...
Database test passed.
daily.cld updated (version: 27469, sigs: 2068551, f-level: 90, builder: raynman)
main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode.cvd database is up-to-date (version: 335, sigs: 86, f-level: 90, builder: raynman)
Testing database: '/var/db/clamav//tmp.5cbaaf32d5/clamav-275ea6ce3d01bb82b4645c1a13e521c.tmp-urlhaus.ndb' ...
Database test passed.
urlhaus.ndb updated (version: custom database, sigs: 11039)
interserver256.hdb is up-to-date (version: custom database)
interservertopline.db is up-to-date (version: custom database)
shell ldb is up-to-date (version: custom database)
whitelist.fp is up-to-date (version: custom database)
Clamd successfully notified about the update.
```

La commande `freshclam` a été utilisée pour mettre à jour la base de données de signatures de virus de ClamAV. Le processus de mise à jour a démarré le **mardi 26 novembre 2024 à 10:32:48**. La base de données `daily.cld` a été mise à jour avec succès à la version **27469**, avec un total de **208551** signatures. Les autres bases de données (`main.cvd`, `bytecode.cvd`, `urlhaus.ndb`, etc.) sont également à jour. Le test de la base de données a réussi, et ClamAV a été notifié de cette mise à jour avec succès.

```
Sortie Console - clamdscan /usr/local/www

/usr/local/www: OK

----- SCAN SUMMARY -----
Infected files: 0
Time: 0.590 sec (0 m 0 s)
Start Date: 2024:11:26 10:35:25
End Date: 2024:11:26 10:35:26
```

Résultat de la commande `clamdscan /usr/local/www`

La commande `clamdscan` a été exécutée pour analyser le répertoire `/usr/local/www`. Aucun fichier infecté n'a été détecté pendant l'analyse. Le processus a pris **0,590 secondes** et s'est terminé le **26 novembre 2024 à 10:35:26**. Le répertoire est sain, sans présence de fichiers malveillants.

```
Sortie Console - arp -a

? (10.2.104.100) at 00:50:56:ab:2c:1d on vmx0 expires in 1114 seconds [ethernet]
? (10.2.104.102) at 00:50:56:ab:a3:64 on vmx0 expires in 1123 seconds [ethernet]
? (10.2.104.254) at 00:50:56:ab:96:cd on vmx0 permanent [ethernet]
? (10.9.104.10) at 00:50:56:ab:08:03 on vmx1 expires in 1200 seconds [ethernet]
? (10.9.104.254) at 00:50:56:ab:8a:e7 on vmx1 permanent [ethernet]
? (192.168.10.104) at 00:50:56:ab:8b:ad on vmx2 permanent [ethernet]
? (192.168.10.254) at 00:0c:29:08:25:67 on vmx2 expires in 1154 seconds [ethernet]
? (10.0.104.2) at 00:50:56:ab:d8:44 on vmx3 expires in 764 seconds [ethernet]
? (10.0.104.1) at 00:50:56:ab:63:5d on vmx3 expires in 1160 seconds [ethernet]
? (10.0.104.4) at 00:50:56:ab:8e:f1 on vmx3 expires in 301 seconds [ethernet]
? (10.0.104.10) at 00:50:56:ab:7a:69 on vmx3 expires in 794 seconds [ethernet]
Eloham.home.arpna (10.0.104.254) at 00:50:56:ab:4f:b7 on vmx3 permanent [ethernet]
? (10.1.104.13) at 00:50:56:ab:f3:06 on vmx4 expires in 1139 seconds [ethernet]
? (10.1.104.254) at 00:50:56:ab:1a:86 on vmx4 permanent [ethernet]

Exécuter une commande



```

La commande `arp -a` a été exécutée pour lister les adresses MAC associées aux adresses IP connues par pfSense. Le tableau ARP indique les adresses IP des hôtes connectés, ainsi que leurs adresses MAC correspondantes. Certaines entrées sont permanentes (comme `10.1.104.254` sur `vmx1`), tandis que d'autres expirent après une durée spécifique, allant de quelques centaines à un peu plus de mille secondes. Cela montre la table ARP en cours, incluant à la fois les appareils locaux et d'autres dispositifs sur le réseau.

```
Sortie Console - pw user show Eloham
Eloham:*LOCKED*$2y$10$6.ASp7gwjmjFTAvy39fpX.REZ5AhacV130Ljv0cvMk2q.4QWCF0G6:2000:65534::0:0:Eloham caron:/home/Eloham:/sbin/nologin
```

Exécuter une commande

`pw user show Eloham`

« Exécuter » Effacer

La commande `pw user show Eloham` a été utilisée pour afficher les informations sur l'utilisateur Eloham. Le compte est marqué comme **verrouillé** (*LOCKED*), ce qui signifie que l'utilisateur ne peut pas se connecter. Le répertoire personnel est situé à `/home/Eloham` et le shell attribué est `/sbin/nologin`, confirmant que cet utilisateur n'a pas de droits de connexion au système.

Sockstat :

```
zabbix zabbix_age 36229 4 tcp4 *:10050 *:*
zabbix zabbix_age 36229 8 stream /var/run/php-fpm.socket
zabbix zabbix_age 36229 12 stream /var/run/php-fpm.socket
zabbix zabbix_age 36058 4 tcp4 *:10050 *:*
zabbix zabbix_age 36058 8 stream /var/run/php-fpm.socket
zabbix zabbix_age 36058 12 stream /var/run/php-fpm.socket
zabbix zabbix_age 35840 4 tcp4 *:10050 *:*
zabbix zabbix_age 35840 8 stream /var/run/php-fpm.socket
zabbix zabbix_age 35840 12 stream /var/run/php-fpm.socket
zabbix zabbix_age 35806 4 tcp4 *:10050 *:*
zabbix zabbix_age 35806 8 stream /var/run/php-fpm.socket
zabbix zabbix_age 35806 12 stream /var/run/php-fpm.socket
zabbix zabbix_age 35763 4 tcp4 *:10050 *:*
zabbix zabbix_age 35763 8 stream /var/run/php-fpm.socket
zabbix zabbix_age 35763 12 stream /var/run/php-fpm.socket
root sh 1734 8 stream /var/run/php-fpm.socket
root sh 1734 12 stream /var/run/php-fpm.socket
squid pinger- 98856 0 udp4 ::1:57108 ::1:4150
squid pinger- 98856 1 udp6 ::1:57108 ::1:4150
squid squidGuard 98626 0 stream -> [35345 36]
squid squidGuard 98626 1 stream -> [35345 36]
squid squidGuard 98326 0 stream -> [35345 33]
squid squidGuard 98326 1 stream -> [35345 33]
squid squidGuard 98232 0 stream -> [35345 30]
squid squidGuard 98232 1 stream -> [35345 30]
squid squidGuard 98002 0 stream -> [35345 27]
squid squidGuard 98002 1 stream -> [35345 27]
squid squidGuard 97763 0 stream -> [35345 24]
squid squidGuard 97763 1 stream -> [35345 24]
squid squidGuard 97713 0 stream -> [35345 21]
squid squidGuard 97713 1 stream -> [35345 21]
squid squidGuard 97693 0 stream -> [35345 18]
squid squidGuard 97693 1 stream -> [35345 18]
squid squidGuard 97685 0 stream -> [35345 14]
squid squidGuard 97685 1 stream -> [35345 14]
unbound unbound 95380 3 udp6 *:53 *:*
unbound unbound 95380 4 tc6 *:53 *:*
```

Zabbix

SquidGuard

Résultat de la commande sockstat

Les résultats de la commande `sockstat` montrent les connexions ouvertes et les sockets utilisés par différents services sur le système pfSense. Les processus **Zabbix** utilisent principalement le port TCP 10050 et plusieurs sockets de type stream pour la communication avec `/var/run/php-fpm.socket`, ce qui montre son interaction avec le serveur PHP pour la collecte et la transmission des données de surveillance.

Le service **SquidGuard** utilise des sockets de type stream, souvent en lien avec squid, pour gérer le filtrage de contenu web. Les processus de **Squid** (pinger) montrent également l'utilisation de connexions UDP pour vérifier la connectivité réseau sur les ports 4150 et 4151. Globalement, ces processus montrent que les services sont actifs et communiquent correctement entre eux pour assurer la surveillance (Zabbix) et le filtrage de contenu (SquidGuard).

The screenshot shows a terminal window titled "Diagnostics / Invite de commande". The title bar also includes "Sortie Console - pfctl -sn". The main area displays the output of the "pfctl -sn" command, which lists various Network Address Translation (NAT) and Port Address Translation (PAT) rules. Key entries include:

```
no nat proto carp all
nat-anchor "natearly/*" all
nat-anchor "natrules/*" all
nat on vmx2 inet from <tonatsubnets> to any port = isakmp -> 192.168.10.104 static-port
nat on vmx2 inet6 from <tonatsubnets> to any port = isakmp -> (vmx2) round-robin static-port
nat on vmx2 inet from <tonatsubnets> to any -> 192.168.10.104 port 1024:65535
nat on vmx2 inet6 from <tonatsubnets> to any -> (vmx2) port 1024:65535 round-robin
no rdr proto carp all
rdr-anchor "tftp-proxy/*" all
rdr on vmx3 inet proto tcp from 10.2.104.254 port 80:443 to 10.9.104.254 port 80:443 -> 10.9.104.1 port 443:806
rdr on vmx2 inet proto tcp from any to 192.168.10.104 port 80:443 -> 10.9.104.1 port 443:806
rdr on vmx2 inet proto tcp from any port 80:443 to <OPT3__NETWORK> port = http -> 10.9.104.1 port 443
rdr on vmx2 inet proto tcp from any port 80:443 to <OPT3__NETWORK> port = https -> 10.9.104.1 port 443
rdr on vmx2 inet proto tcp from any port 21:22 to <OPT3__NETWORK> port 21:22 -> 10.9.104.1 port 2222:2223
```

Résultat de la commande pfctl -sn

La commande `pfctl -sn` fournit un aperçu de la configuration des règles NAT (Network Address Translation) et PAT (Port Address Translation) sur pfSense. Plusieurs règles de NAT sont définies pour la traduction d'adresses sur différentes interfaces.

Pour **NAT** sur vmx2 (probablement l'interface WAN), une règle de redirection traduit les paquets entrant pour **ISAKMP** (utilisé pour les VPN IPsec) vers l'IP interne 192.168.10.104 avec un port statique. D'autres règles sur vmx2 redirigent le trafic provenant de sous-réseaux spécifiques vers vmx2 en utilisant le mode "round-robin" pour la répartition de charge entre différents ports.

- Pour la **redirection de ports (PAT)**, des règles de redirection (rdr) sont présentes pour diverses situations :
- Par exemple, le trafic HTTP/HTTPS (80:443) sur vmx3 provenant du réseau 10.2.104.254 est redirigé vers l'adresse 10.9.104.1 sur les ports 443:806.
- Le trafic TCP entrant vers le port 443 sur vmx2 est redirigé vers une IP spécifique (10.9.104.1), indiquant probablement un serveur web interne accessible depuis l'extérieur.
- Enfin, une règle PAT redirige également le port 21:22 (FTP/SSH) vers des ports internes spécifiques (2222:2223).

29. NMAP COMPARAISON

La commande nmap -sn 192.168.10.0/25 a été exécutée pour identifier les hôtes actifs sur le sous-réseau 192.168.10.0/25. Cette commande a permis de détecter **10 hôtes** actifs, indiquant leur adresse IP et leur adresse MAC, avec des temps de latence très faibles (de l'ordre de microsecondes). Les adresses MAC identifiées sont associées à des équipements VMware, indiquant qu'il s'agit probablement de machines virtuelles

```
Sortie Console - nmap -sn 192.168.10.0/25

Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-26 12:11 UTC
Nmap scan report for 192.168.10.101
Host is up (0.00075s latency).
MAC Address: 00:58:56:AB:59:C7 (VMware)
Nmap scan report for 192.168.10.102
Host is up (0.0010s latency).
MAC Address: 00:58:56:AB:64:10 (VMware)
Nmap scan report for 192.168.10.103
Host is up (0.00047s latency).
MAC Address: 00:58:56:AB:14:CF (VMware)
Nmap scan report for 192.168.10.106
Host is up (0.00059s latency).
MAC Address: 00:58:56:AB:6D:02 (VMware)
Nmap scan report for 192.168.10.107
Host is up (0.00037s latency).
MAC Address: 00:58:56:AB:D1:D7 (VMware)
Nmap scan report for 192.168.10.108
Host is up (0.00046s latency).
MAC Address: 00:58:56:AB:5D:92 (VMware)
Nmap scan report for 192.168.10.109
Host is up (0.00052s latency).
MAC Address: 00:58:56:AB:3D:95 (VMware)
Nmap scan report for 192.168.10.110
Host is up (0.00069s latency).
MAC Address: 00:58:56:AB:E4:D7 (VMware)
Nmap scan report for 192.168.10.111
Host is up (0.00042s latency).
MAC Address: 00:58:56:AB:41:43 (VMware)
Nmap scan report for 192.168.10.104
Host is up.
Nmap done: 128 IP addresses (10 hosts up) scanned in 3.92 seconds
```

En analysant ces résultats, il est évident que plusieurs instances pfSense sont actives dans le réseau, car les adresses MAC affichées sont typiquement utilisées par des machines virtuelles (ce qui correspond souvent à des déploiements de pare-feux virtuels tels que pfSense). Cela indique une infrastructure où des dispositifs pfSense multiples cohabitent, ce qui peut être le cas dans une architecture redondante ou pour des environnements de test.

Le scan a couvert **128 adresses IP** et a pris **3,92 secondes**, ce qui montre une efficacité dans la détection rapide des hôtes actifs et fournit une vue d'ensemble claire de l'état du sous-réseau en question.

```
Sortie Console - nmap -sV 192.168.10.111

Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-26 12:02 UTC
Nmap scan report for 192.168.10.111
Host is up (0.00044s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
3128/tcp  open  http-proxy Squid http proxy 6.3
MAC Address: 00:58:56:AB:41:43 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.31 seconds
```

Les autres **999 ports TCP** ont été filtrés, et aucun service supplémentaire n'est accessible, ce qui indique une configuration relativement sécurisée. Notamment, il n'y a aucune trace de

service OpenSSL ouvert sur ce système, ce qui signifie qu'Adrien n'a pas configuré de service SSL/TLS sur ce pfSense, ou que ce dernier est désactivé ou filtré par les règles de pare-feu.

L'adresse MAC associée est 00:50:56:AB:41:43, indiquant que cette machine est également une instance VMware, cohérente avec une infrastructure virtualisée.

```

Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-26 12:12 UTC
Nmap scan report for 192.168.10.101
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.101 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
MAC Address: 00:50:56:AB:41:43 (VMware)

Nmap scan report for 192.168.10.102
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.102 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
MAC Address: 00:50:56:AB:41:43 (VMware)

Nmap scan report for 192.168.10.103
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.103 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  httpd   Apache httpd 2.4.62 (Debian)
443/tcp   open  ssl/http Apache httpd 2.4.62 (Debian)
MAC Address: 00:50:56:AB:41:43 (VMware)
Service Info: Host: ut1180.D0090203.peda

Nmap scan report for 192.168.10.106
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.106 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
MAC Address: 00:50:56:AB:41:43 (VMware)

Nmap scan report for 192.168.10.107
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.107 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    closed http
MAC Address: 00:50:56:AB:41:43 (VMware)

Nmap scan report for 192.168.10.108
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.108 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
MAC Address: 00:50:56:AB:41:43 (VMware)

Nmap scan report for 192.168.10.109
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.109 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  httpd   Apache httpd 2.4.62 (Debian)
443/tcp   open  ssl/http Apache httpd 2.4.62 (Debian)
MAC Address: 00:50:56:AB:41:43 (VMware)

Nmap scan report for 192.168.10.103
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.103 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  httpd   Apache httpd 2.4.62 (Debian)
443/tcp   open  ssl/http Apache httpd 2.4.62 (Debian)
MAC Address: 00:50:56:AB:41:43 (VMware)

Nmap scan report for 192.168.10.104
Host is up (0.00001s latency).
All 38800 scanned ports on 192.168.10.104 are in ignored states.
Not shown: 9980 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.4 (protocol 2.0)
2222/tcp open  ssh     OpenSSH 9.4 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.62 (Debian)
443/tcp   open  ssl/http Apache httpd 2.4.62 (Debian)
MAC Address: 00:50:56:AB:41:43 (VMware)

Nmap done: 256 IP addresses (13 hosts up) scanned in 83.43 seconds

```

Résumé des résultats des scans Nmap (nmap -sV 192.168.10.0/24)

- Deux scans Nmap ont été effectués sur le sous-réseau 192.168.10.0/24, offrant un aperçu de l'état des services et de la configuration des différents hôtes du réseau, notamment les instances pfSense et d'autres systèmes présents.
- **Hôtes Windows (ex: 192.168.10.101)** : Des machines Windows ont été détectées, avec des ports **135 (msrpc)**, **139 (netbios-ssn)**, et **445 (microsoft-ds)** ouverts, montrant une configuration réseau classique pour le partage de fichiers et l'administration Windows. La version du système semble être Windows 7 ou 10.
- **Hôtes pfSense (ex: 192.168.10.104)** : Certaines machines sont clairement identifiées comme des instances pfSense. Par exemple, l'hôte **192.168.10.104** expose les ports **80 (HTTP)** et **443 (HTTPS)** avec SSL/TLS, montrant une interface d'administration web sécurisée, probablement pour gérer le pare-feu. Un autre hôte (192.168.10.254) a des ports **1194 (OpenVPN)** et **53 (DNS)** ouverts, indiquant qu'il est utilisé comme serveur VPN et DNS.
- **Serveurs Web et autres services (ex: 192.168.10.103)** : Un hôte **192.168.10.103** expose les services HTTP et HTTPS via Apache (2.4.6), indiquant la présence d'un serveur web Debian actif. Plusieurs autres hôtes sont aussi dotés de ports filtrés ou fermés, suggérant des politiques de sécurité renforcées.

30. ALERTES SNORT GENEREES PAR LES SCANS NMAP

Les résultats montrent que les différents scans Nmap effectués sur le sous-réseau 192.168.10.0/24 ont déclenché plusieurs alertes Snort sur les autres instances pfSense du réseau, telles que celle de Dylan qui, auparavant, ne détectait pas de telles activités.

Dans la capture d'écran de l'interface Snort, nous pouvons voir que des alertes ont été générées pour des connexions suspectes vers le **pfSense de Dylan**. Par exemple :

The screenshot shows the 'Alert Log View Settings' interface for Snort. It includes settings for the interface to inspect (WAN (vmx1)), auto-refresh view (250 lines), and alert actions (Download, Clear). The 'Alert Log View Filter' section shows 49 entries in the active log. Two specific entries are highlighted:

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-26 13:12:56	⚠️	3	TCP	Unknown Traffic	208.115.231.22	80	192.168.10.109	12929	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2024-11-26 13:05:38	⚠️	3	TCP	Unknown Traffic	77.95.69.67	80	192.168.10.109	46701	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

- Une alerte enregistrée le **26 novembre 2024 à 13:12:56** provient de l'adresse IP **208.115.231.22** ciblant l'IP interne **192.168.10.109**, avec une classification de trafic inconnu, indiquant une réponse HTTP inattendue avant une demande client.
- Une autre alerte, quelques minutes plus tôt à **13:05:38**, indique une connexion TCP depuis **77.95.69.67** vers le même hôte sur le port **46701**, où aucune longueur de contenu ou encodage de transfert HTTP n'a été trouvée dans la réponse.

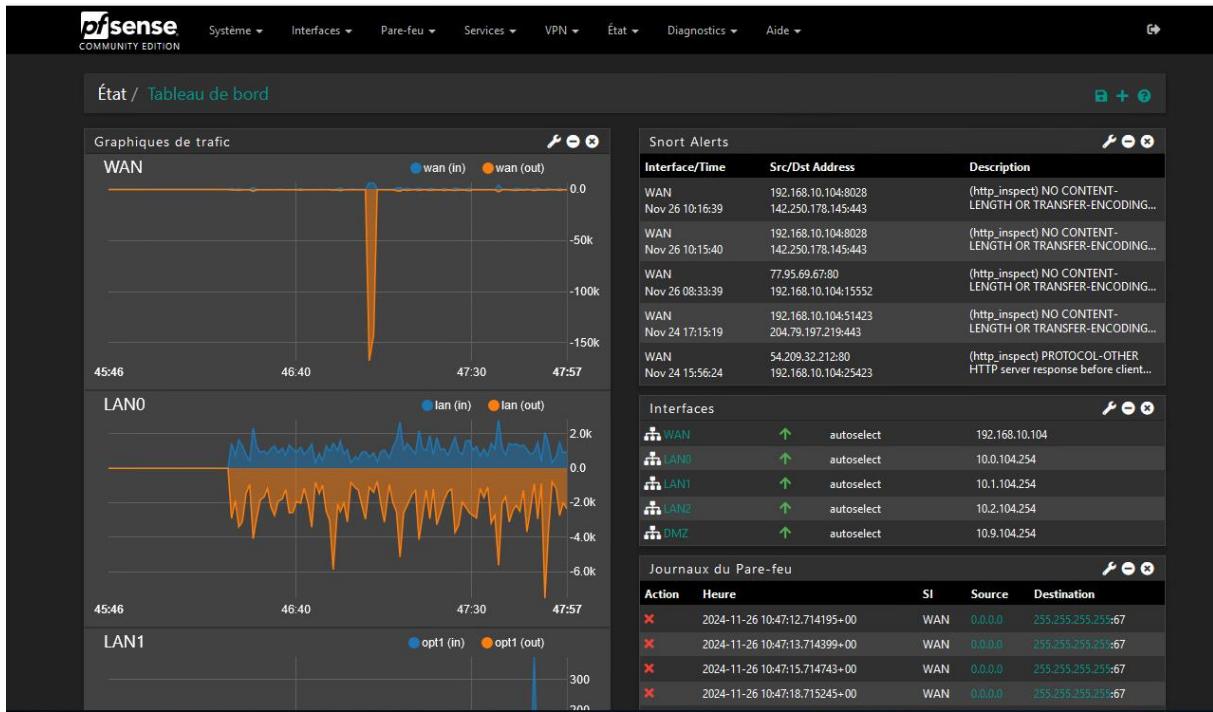
Ces alertes montrent que Snort a réagi aux activités de scan, détectant des signatures anormales associées aux requêtes faites par les outils de scan, comme Nmap, utilisés précédemment. Cela prouve que Snort fonctionne bien maintenant sur les instances comme celle de Dylan, qui n'arrivait pas à détecter ces types de scans auparavant.

Ces détections sont importantes, car elles indiquent que le réseau est capable de signaler les tentatives de découverte des services ou de reconnaissance réseau, ce qui améliore considérablement la sécurité globale de l'infrastructure.

31. TABLEAU DE BORD

Personnalisation du Tableau de Bord pfSense

Le tableau de bord pfSense que vous avez personnalisé offre une vue d'ensemble claire et détaillée sur plusieurs aspects critiques du réseau. Voici les éléments personnalisés et leur utilité :



1. Graphiques de Trafic pour les Interfaces WAN et LAN :

- Les graphiques de trafic sont affichés pour les interfaces **WAN** et **LAN** (LAN0, LAN1). Ils permettent de visualiser l'activité du trafic entrant et sortant. Par exemple, une baisse notable dans le trafic sortant sur l'interface WAN peut indiquer un problème temporaire ou une reconfiguration du réseau. Le graphique de **LAN0** montre un flux relativement constant, indiquant une activité régulière sur le réseau local.

2. Alertes Snort en Temps Réel :

- La section **Snort Alerts** montre les alertes de sécurité générées par le système IDS/IPS (Snort). Elle inclut des détails tels que l'interface, l'adresse source/destination, et une brève description de l'alerte. Par exemple, des alertes comme NO CONTENT-LENGTH OR TRANSFER-ENCODING sur le port HTTP montrent que des anomalies ont été détectées dans les réponses HTTP. Ces informations sont cruciales pour comprendre les incidents de sécurité en temps réel et prendre des mesures correctives.

3. Statut des Interfaces :

- Une autre section importante est la liste des **Interfaces**. Elle présente chaque interface réseau (WAN, LAN0, LAN1, DMZ), son statut (autosélectionné) et l'adresse IP attribuée. Cela offre une vue rapide pour vérifier l'état de chaque interface et s'assurer que toutes les connexions sont opérationnelles.

4. Journaux du Pare-feu :

- La section **Journaux du Pare-feu** présente les événements les plus récents, tels que les connexions bloquées. Par exemple, on voit des requêtes bloquées provenant d'adresses non routables (0.0.0.0). Cela est utile pour identifier rapidement les tentatives de connexion suspectes ou non autorisées et vérifier si les règles du pare-feu fonctionnent comme prévu.

Cette personnalisation du tableau de bord pfSense permet de centraliser et de visualiser en un seul endroit toutes les informations essentielles : trafic réseau, alertes de sécurité, état des interfaces, et événements de pare-feu. Cela rend la surveillance réseau plus efficace et vous permet de réagir rapidement en cas de problème.

32. CONCLUSION :

pfSense est une solution de pare-feu et de routeur open source qui se distingue par sa robustesse, sa flexibilité, et sa capacité à sécuriser et gérer des réseaux complexes de manière professionnelle. À travers l'installation, la configuration des interfaces réseau, et l'ajustement des paramètres DNS et NTP, pfSense permet un contrôle précis sur l'ensemble des éléments fondamentaux du réseau.

Les capacités de surveillance et d'analyse des journaux (qu'ils soient textuels ou graphiques via Syslog) offrent aux administrateurs une vision complète et détaillée des activités réseau, facilitant ainsi la détection des anomalies et le diagnostic des incidents. Cette surveillance est renforcée par des solutions comme Snort pour la détection des intrusions, et ClamAV pour la protection antivirus, garantissant une sécurité multi-niveaux.

pfSense intègre également des fonctionnalités avancées pour la gestion des services réseau, notamment le DHCP, la configuration d'alias et la protection contre le DNS rebinding, tout en assurant une gestion fine des règles de pare-feu sur chaque interface (WAN, LAN, DMZ). L'ajout d'un proxy et d'un reverse proxy via Squid et SquidGuard permet non seulement de réguler le trafic, mais également de filtrer le contenu et de garantir une utilisation sécurisée de la bande passante.

En termes de sécurité, pfSense propose la mise en œuvre de certificats HTTPS et la configuration de VPN (OpenVPN), permettant une communication sécurisée pour les utilisateurs distants. La flexibilité offerte par la configuration des alias IP, des certificats, et des règles NAT contribue à faire de pfSense une solution de choix pour les environnements professionnels.

Enfin, la possibilité de personnaliser le tableau de bord et d'automatiser les tâches via des outils comme Cron simplifie la gestion du réseau, tout en offrant une vue d'ensemble rapide et claire sur l'état du système, les alertes, et les performances des interfaces.

En résumé, pfSense est une solution complète et performante, idéale pour des infrastructures allant de petites à grandes entreprises. Il offre une sécurité solide, une grande flexibilité, et des outils de gestion de réseau puissants. Que ce soit pour la surveillance, la protection contre les intrusions, la gestion du trafic ou l'administration des services réseau, pfSense constitue une base fiable et sécurisée pour toutes les opérations critiques d'un réseau moderne.

33. SOURCES :

Table des Sources

1. Installation et configuration de Squid avec ClamAV sur pfSense

<https://www.ceos3c.com/pfsense/install-squid-clamav-pfsense>

2. Mise en place et configuration de Snort sous pfSense

<https://www.portfolio-hm.com/documents/MISE%20EN%20PLACE%20ET%20CONFIGURATION%20DE%20SNORT%20Sous%20PFSENSE.pdf>

3. Configuration du paquet Snort sur pfSense

<https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html>

4. Proxy transparent : mise en place de Squid sur pfSense

<https://www.it-connect.fr/proxy-transparent-mise-en-place-de-squid-sur-pfsense>

5. Tutoriel Snort et pfSense

<https://www.osnet.eu/fr/content/tutoriels/tutoriel-snort-et-pfsense>

6. Configuration du mode IPS en ligne avec Snort 4.0 sur pfSense

<https://forum.netgate.com/topic/143812/snort-package-4-0-inline-ips-mode-introduction-and-configuration-instructions>