Rapport de configuration du réseau Laboratoire

Sommaire :

I. Plan du réseau	2
II. Adressage réseau IP VLAN	
1. Adressage IP	3
2. VLAN	
III. Configuration des VSwitch	
1. VSwitch WAN	4
2. VSwitch LAN	5
IV. Configuration du Pfsense frontière	6
1. Création des cartes réseau/adressage	6
→ Carte WAN	6
→ Carte LAN	7
Affectation IP sur les cartes via la console	9
→ Création VLAN	11
V. Création des hôtes	14
1. Création des PC Clients	14
→ Adressage IP	14
→ Adressage VLAN	15
2. Création serveur NAS	16
→ Configuration réseau NAS	
Configurer un adressage IP TRUENAS	
ightarrow Configuration VLAN	23
3. Configuration de la banque de données	24
→ Modification ACL	
4. Création du partage SMB	
→ Activation SMBv1	
5. Création des utilisateurs/groupes	
ightarrow Créer un groupe d'utilisateur	
→ Créer un utilisateur	32
→ Test de connexion + transfert de données	
VI. Configuration du Pfsense Filtrage	
1. Création carte réseau	
→ Carte WAN	
ightarrow Carte LAN	
2. Adressage IP des cartes	
→ Carte WAN	
→ Interface LAN	
3. Création du proxy	
ightarrow Installation de Squid sur PfSense	
→ Configurer Squid (Proxy) sur PfSense	
→ Créer l'autorité de certification PfSense	
ightarrow SSL Inspection avec Squid	
ightarrow Installation de Squid Guard sur PfSense	51
ightarrow Configuration de Squid Guard sur PfSense	
→ Test du proxy	57



Le réseau sera entièrement virtualisé sur un hyperviseur en Windows Server

2022.

I. Plan du réseau

II. Adressage réseau IP | VLAN

1. Adressage IP

Nom Réseau	Adresse IP	Passerelle	Hôtes
Gestion	192.168.1.0/24	192.168.1.254	PC Gestion NASSRV-TRUENAS
Filtrage	192.168.2.0/24	192.168.2.254	- PC Filtrage
ХР	192.168.3.0/24	192.168.3.254	- PC XP
Corporate	192.168.4.0/24	192.168.4.254	- PC Corporate

2. VLAN

Réseau	VLAN
192.168.1.0/24	1
192.168.2.0/24	2
192.168.3.0/24	3
192.168.4.0/24	4

III. Configuration des VSwitch

1. VSwitch WAN

Eastionnaire de commutateur virtuel pour SRV-LAB-2025

– 🗆 X

Commutateurs virtuels	💤 Propriétés du commutateur virtuel	^
📲 Nouveau commutateur réseau virtuel	Non I	
🗄 🚣 LAN Pfsense		
Interne uniquement	WAN Pfsense	
 WAN Pfsense Broadcom NetXtreme Gigabit Ether 	Notes :	
Paramètres du réseau global	· · · · · · · · · · · · · · · · · · ·	
Plage d'adresses MAC 00-15-5D-00-96-00 à 00-15-5D-00	~	
	Type de connexion	
	À quoi voulez-vous connecter ce commutateur virtuel ?	
	Réseau externe :	
	Broadcom NetXtreme Gigabit Ethernet 🛛 🗸 🗸	
	Autoriser le système d'exploitation de gestion à partager cette carte réseau Activer la virtualisation d'E/S de racine unique (SR-IOV) Réseau interne Réseau privé	
	ID du réseau local virtuel	
	Activer l'dentification LAN virtuelle pour le système d'exploitation de gestion	
	L'1dentificateur VLAN spécifie le réseau local virtuel utilisé par le système d'exploitation de gestion pour toutes les communications réseau par le biais de cette carte réseau. Ce paramètre n'affecte pas la mise en réseau d'ordinateurs virtuels.	
	SP_TOV pa paut être confouré que lors de la création du computateur victual	
	SR-IOV ne peut être configuré que lors de la création du commutateur virtuel. OK Annuler Appliquer	~

Premièrement, le **VSwitch** côté **WAN** afin de posséder un accès à **internet**, accès par pont via une **carte réseau physique** du serveur sans configuration particulière.

2. VSwitch LAN

🚰 Gestionnaire de commutateur virtuel pour SRV-LAB-2025

– 🗆 X

*	Commutateurs virtuels	🚣 Propriétés du commutateur virtuel —————	1
	Nouveau commutateur réseau virtuel	Nom :	
+	Toterne uniquement		
+	- WAN Pfsense	LAN PISEISE	
	Broadcom NetXtreme Gigabit Ether	Notes :	
	Paramètres du réseau global	~	
	Plage d'adresses MAC 00-15-5D-00-96-00 à 00-15-5D-00	~	
		Type de connexion	
		À quoi voulez-vous connecter ce commutateur virtuel ?	
		○ Réseau externe :	
		Broadcom NetXtreme Gigabit Ethernet 🛛 🗸 🗸	
		Autoriser le système d'exploitation de gestion à partager cette carte réseau	
		Activer la virtualisation d'E/S de racine unique (SR-IOV)	
		Réseau interne	
		🔿 Réseau privé	
		ID du réseau local virtuel	
		Activer l'identification LAN virtuelle pour le système d'exploitation de gestion	
		L'îdentificateur VLAN spécifie le réseau local virtuel utilisé par le système d'exploitation de gestion pour toutes les communications réseau par le biais de cette carte réseau. Ce paramètre n'affecte pas la mise en réseau d'ordinateurs virtuels.	
		Supprimer	
		SR-IOV ne peut être configuré que lors de la création du commutateur virtuel.	

Un **VSwitch** afin de pouvoir y connecter nos **VMs**, en connexion **interne** afin d'isoler notre réseau de l'extérieur mais de pouvoir communiquer nos **VMs** entre elles.

IV. Configuration du Pfsense frontière

Création des cartes réseau/adressage
 → Carte WAN

Pour créer notre **Pfsense** frontière entre l'extérieur et l'intérieur de notre réseau, nous avons quelques configurations à réaliser.



Pour la carte **WAN**, on crée une **carte simple** sur notre hyperviseur sans configuration particulière en lui spécifiant le **commutateur WAN** que l'on a créé.

Paramètres pour SRV-Pfsense sur SRV-LAB	-2025 —	×
SRV-Pfsense \checkmark	◄ ► Ŭ	
Matériel Ajouter un matériel Microprogramme Démarrer à partir de Fichier Sécurité Démarrage sécurisé désactivé	Carte réseau Spécifiez la configuration de la carte réseau ou retirez la carte réseau. Commutateur virtuel : WAN Pfsense ID du réseau local virtuel	
Mormore 4096 Mo 2 processeur 2 processeurs virtuels Sontrôleur SCSI Disque dur SkV-Pfsense.vhdx	Activer l'identification LAN virtuelle L'identificateur VLAN spécifie le réseau local virtuel utilisé par cet ordinateur virt pour toutes les communications réseau par le biais de cette carte réseau. 2	tuel
© Lecteur de DVD Pfsense.iso ₽ 単 Carte réseau	Gestion de bande passante	
WAN Pfsense UAN Pfsense LAN Pfsense	Spécifiez le mode d'utilisation de la bande passante réseau par cette carte rése La bande passante maximale et la bande passante minimale sont mesurées en mégabits par seconde.	au.
Gestion Nom SRV-Pfsense Services dintégration Ourlance services effects	Bande passante minimae . Bande passante maximale : Pour n'appliquer aucune restriction à la valeur minimale ou maximale, province passante maximale autore au	
Points de contrôle Production Emplacement du fichier de paginati Dr.\	Pour retirer la carte réseau de cet ordinateur virtuel, cliquez sur Retirer.	rer
Action de démarrage automatique Redémarrer le service s'il était en c CAction d'arrêt automatique Enregistrer		
1	OK Annuler App	liquer

On affecte pas d'adresse IP fixe, on laisse la carte en mode DHCP.

WAN	(wan)	-> hn0	->	v4/DHCP4:	10.12.0.140/23

→ Carte LAN

La création de la carte du côté **LAN** de notre réseau requiert un peu plus de manipulation, il faut tout d'abord créer la **carte réseau** en précisant les **VLAN** auxquels elle va être affectée sur notre **VSwitch**, soit le **VLAN 1, 3 et 4**.

Pour pouvoir créer un **lien agréger** sur notre **carte réseau**, il faut la créer via **Powershell** :

Add-VMNetworkadapter -VMName "nomVM" -Name "nomAdaptateur"

Ce qui nous donne dans notre exemple :

Add-VMNetworkadapter -VMName "SRV-Pfsense" -Name "LAN Pfsense"

Et par la suite, on agrège les VLAN à notre carte :

set-VMNetworkAdapterVlan -VMName **"nomVM"** -VMNetworkAdapterName **"nomadaptateur" -**Trunk -AllowedVlanIdList **"numéroVLAN"** -NativeVlanId **numéroVLANnatif**

Ce qui nous donne dans notre exemple :

set-VMNetworkAdapterVlan -VMName "**SRV-Pfsense"** -VMNetworkAdapterName **"LAN Pfsense"** -Trunk -AllowedVlanIdList **"3,4"** -NativeVlanId **1**

On peut vérifier par la suite si notre commande à bien marché en exécutant la commande :

Get-VMNetworkAdapterVlan -VMName "SRV-TRUENAS"



On voit notre première carte (**WAN**) en mode **'Untagged'** (affectée à aucun **VLAN**).

Et on voit notre deuxième carte (LAN) en mode 'Trunk' sur les VLAN 1, 3 et 4.

Paramètres pour SRV-Pfsense sur SRV-LAB-2025

	×
--	---

* Matériel	📮 Carte réseau ————————————————————————————————————
Ajouter un matériel	Spécifiez la configuration de la carte réseau ou retirez la carte réseau
Microprogramme	Commutateur virtuel :
Démarrage sécurisé désactivé	
Mémoire	ID du reseau local virtuel
4096 Mo	Activer lidentification LAN virtuelle
+ Processeur	L'identificateur VLAN spécifie le réseau local virtuel utilisé par cet ordinateur virtuel
2 processeurs virtueis	pour toutes les communications réseau par le biais de cette carte réseau.
	2
SRV-Pfsense.vhdx	
Lecteur de DVD	Gestion de bande passante
Pfsense.iso	Activer la gestion de bande passante
🗄 📮 Carte réseau	
WAN Pfsense	La bande passante maximale et la bande passante reseau par cette carte reseau.
LAN Pfsense LAN Pfsense	mégabits par seconde.
Gestion	Bande passante minimale : 0 Mbits/s
T Nom	
SRV-Pfsense	Bande passante maximale : 0 Mbits/s
Services d'intégration	Pour n'appliquer aucune restriction à la valeur minimale ou maximale,
Quelques services offerts	spécifiez 0 comme valeur.
Points de contrôle	Pour retirer la carte réseau de cet ordinateur virtuel, cliquez sur Retirer.
Production	
D:\	Retirer
Action de démarrage automatique	
Redémarrer le service s'il était en c	
Action d'arrêt automatique	
Enregistrer	

On vérifie aussi qu'elle est bien créée et on affecte cette carte à notre VSwitch

LAN créé précédemment.

Par la suite, on y affecte une **adresse IP** via la **console**.

0) Logout (SSH only) 9) pfTop 10) Filter Logs 1) Assign Interfaces 2) Set interface(s) IP address 11) Restart webConfigurator 3) Reset webConfigurator password 12) PHP shell + pfSense tools 4) Reset to factory defaults 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 7) Ping host 16) Restart PHP-FPM 8) Shell Enter an option: 2 Available interfaces: 1 - WAN (hn0 - dhcp, dhcp6) 2 - LAN (hn1 - static) 3 – LAN_XP (hn1.3 – static) 4 - LAN_CORPORATE (hn1.4 - static) Enter the number of the interface you wish to configure: 2 Configure IPv4 address LAN interface via DHCP? (y/n) n Enter the new LAN IPv4 address. Press <ENTER> for none: > 192.168.1.254 Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 255.0.0.0 Enter the new LAN IPv4 subnet bit count (1 to 32): For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: Configure IPv6 address LAN interface via DHCP6? (y/n) n Enter the new LAN IPv6 address. Press <ENTER> for none: Enter the new LAN IPv6 address. Press <ENTER> for none: Do you want to enable the DHCP server on LAN? (y/n) n Disabling IPv6 DHCPD... Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n Please wait while the changes are saved to LAN... Reloading filter... Reloading routing configuration... DHCPD... The IPv4 LAN address has been set to 192.168.1.254/24 You can now access the webConfigurator by opening the following URL in your web brows https://192.168.1.254/ Press <ENTER> to continue.

Explication :

- On tape 2 pour choisir la troisième option du système 'Set interface(s) IP address'.
- 2. On tape sur **2** encore une fois pour sélectionner la deuxième **carte réseau**.
- À ce moment-là, Pfsense demande quelle est l'adresse que l'on veut affecter à notre carte réseau (cette adresse sera la passerelle de notre réseau), d'après notre schéma réseau on y affecte l'adresse '192.168.1.254'.
- Pfsense nous demande le masque de notre réseau en format CIDR, on choisit 24 dans notre cas pour un réseau local classe C.
- Ici, vu que l'on configure une interface LAN, on passe cette étape en appuyant sur 'Entrer'.
- Dans notre cas, on ne veut pas d'adresse en format IPV6, on appuie sur 'N' pour ne pas activer le serveur DHCP en IPV6.
- Par la suite, on nous demande si on veut activer le serveur DHCP en IPV4, dans notre cas, on ne veut tout simplement pas de DHCP dans le réseau donc on appuie encore une fois 'N'.
- La dernière question nous demande si l'on veut désactiver l'accès à
 l'interface web en HTTPS, bien sûr on répond non à des fins de sécurité.

On appuie sur la touche **'Entrer'** et voici notre **carte LAN** configurée et fonctionnelle.

_AN (lan) -> hn1 -> v4: 192,168,1,254/24

→ Création VLAN

Pour créer les VLAN, on va le faire via le terminal de Pfsense.

0) Logout (SSH only) 1) Assign Interfaces 9) pfTop 10) Filter Logs 2) Set interface(s) IP address 11) Restart webConfigurator 3) Reset webConfigurator password 12) PHP shell + pfSense tools 4) Reset to factory defaults 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 16) Restart PHP-FPM 7) Ping host 8) Shell Enter an option: 1 Valid interfaces are: 00:15:5d:00:96:1e (up) Hyper-V Network Interface 00:15:5d:00:96:1f (down) Hyper-V Network Interface hn1 Do VLANs need to be set up first? If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the webConfigurator to configure VLANs later, if required. Should VLANs be set up now [yln]? y VLAN Capable interfaces: 00:15:5d:00:96:1e 00:15:5d:00:96:1f hn1 Enter the VLAN tag (1-4094): 3 VLAN Capable interfaces: 00:15:5d:00:96:1e 00:15:5d:00:96:1f Enter the parent interface name for the new VLAN (or nothing if finished): hn1 Enter the VLAN tag (1-4094): 4 VLAN Capable interfaces: 00:15:5d:00:96:1e hn0 00:15:5d:00:96:1f Enter the parent interface name for the new VLAN (or nothing if finished):

Enter the parent interface name for the new VLAN (or nothing if finished): VLAN interfaces: VLAN tag 3, parent interface hn1 hn1.4 VLAN tag 4, parent interface hn1 If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process. Enter the WAN interface name or 'a' for auto-detection (hn0 hn1 hn1.3 hn1.4 or a): hn0 Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (hn1 hn1.3 hn1.4 a or nothing if finished): hn1 Enter the Optional 1 interface name or 'a' for auto-detection (hn1.3 hn1.4 a or nothing if finished): hn1.3 Enter the Optional 2 interface name or 'a' for auto-detection (hn1.4 a or nothing if finished): hn1.4 The interfaces will be assigned as follows: WAN -> hn0 LAN -> hn1 0PT1 -> hn1.3 OPT2 -> hn1.4 Do you want to proceed [yln]? Writing configuration...done. One moment while the settings are reloading... done! Hyper-V Virtual Machine - Netgate Device ID: 5f9d636c17f32dfd35c6 *** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense *** WAN (wan) -> hn0 -> v4/DHCP4: 10.12.0.150/23 LAN (lan) -> hn1 -> v4: 192.168.1.254/24
 OPT1 (opt1)
 -> hn1.3

 OPT2 (opt2)
 -> hn1.4
 0) Logout (SSH only) 9) pfTop 1) Assign Interfaces 10) Filter Logs 2) Set interface(s) IP address 11) Restart webConfigurator 3) Reset webConfigurator password 12) PHP shell + pfSense tools 4) Reset to factory defaults 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 16) Restart PHP-FPM 7) Ping host 8) Shell

Enter an option:

Explication :

- On tape I pour choisir l'option 'Assign Interfaces' afin d'assigner de nouvelles interfaces virtuelles pour nos VLAN.
- Pfsense nous demande si l'on veut déployer des VLAN maintenant, on tape 'y' pour yes.
- Par la suite, Pfsense veut savoir quelle est la carte réseau qui va être parente de nos interfaces virtuelles, on veut créer nos interfaces virtuelles sur le LAN, on sélectionne donc la carte LAN en tapant son identifiant (soit 'hn1' dans notre exemple).
- 4. À ce moment-là, on nous demande quel ID on veut donner à notre VLAN, d'après notre tableau et notre schéma, ce Pfsense doit avoir un trunk sur 3 VLAN (VLAN 1, 3, 4), la carte réseau physique de notre Pfsense est de base configurée sur le VLAN 1 (d'où l'adressage en 192.168.1.0 qu'on lui a donnée), il nous reste donc qu'à créer le VLAN 3 et VLAN 4.
- 5. À chaque fois, on a juste à sélectionner l'interface où l'on veut créer nos interfaces virtuelles et taper l'ID du VLAN que l'on veut créer sur cette interface. Quand c'est fini, appuyer sur 'Entrer'.
- 6. À cet instant, il faut que l'on **'catégorise'** nos interfaces, récapitulons :
 - a. HNO -> WAN
 - b. HNI -> LAN (VLAN 1)
 - c. HN1.3 -> LAN (VLAN 3)
 - d. HN1.4 -> LAN (VLAN 4)
 - → On procède donc dans cet ordre, en premier on nous demande l'interface WAN donc on tape HNO.
 - → En deuxième, notre interface LAN parente donc HNI.
 - → En troisième, notre interface LAN du VLAN 3 donc HN1.3.
 - → En quatrième, notre interface LAN du VLAN 4 donc HN1.4.
- Pour que nos VLAN soient assignés à une adresse IP, on suit la procédure d'assignation comme les autres cartes.

V. Création des hôtes

1. Création des PC Clients

→ Adressage IP

Les **PC clients** sont tous des clients **Windows 10 Pro**, cependant sur notre infrastructure chaque poste contient un **adressage IP** différent.

Nom d'hôte	Adresse IP	Passerelle	N°VLAN
PC Gestion NAS	192.168.1.10 /24	192.168.1.254	1
PC Filtrage	192.168.2.10 /24	192.168.2.254	2
PC XP	192.168.3.10 /24	192.168.3.254	3
PC Corporate	192.168.4.10 /24	192.168.4.254	4

Pour chaque **PC** :

Clic droit sur le logo internet -> Ouvrir paramètre et Internet -> Modifier les options d'adaptateur -> Clic droit sur la carte réseau -> Propriété -> double clic sur Protocole Internet Version 4 (TCP / IPv4).



On sélectionne **"utiliser l'adresse IP suivante"** et on rentre l'adresse pour chaque **hôte** comme convenu dans le tableau. Dû à l'absence de **serveur DNS** dans notre réseau, on préfèrera utiliser **8.8.8.8** pour assurer l'accès à internet (**DNS Google**).

→ Adressage VLAN

Pour pouvoir affecter chaque **carte réseau** à leurs **VLAN**, il faut pour chaque **hôte** :

°C	Gestion NAS 🗸 🗸	4 ► ७
	Matériel Microprogramme Démarrer à partir de Fichier Sécurité Démarrage sécurisé activé Mémoire 8192 Mo Processeur 4 processeurs virtuels Contrôleur SCSI Disque dur PC Gestion NAS.vhdx Carte réseau LAN Pfsense Carte réseau LAN Pfsense Services d'Intégration Quelques services offerts Points de contrôle Production Points de contrôle Production	Image: Carte réseau Spécifiez la configuration de la carte réseau ou retirez la carte réseau. Commutateur virtuel : LAN Pfsense ID du réseau local virtuel ID du réseau local virtuel Activer l'identification LAN virtuelle L'identificateur VLAN spécifie le réseau local virtuel utilisé par cet ordinateur virtuel pour toutes les communications réseau par le biais de cette carte réseau. I Gestion de bande passante Activer la gestion de bande passante Spécifiez le mode d'utilisation de la bande passante réseau par cette carte réseau. La bande passante maximale et la bande passante réseau par cette carte réseau. La bande passante maximale et la bande passante minimale sont mesurées en mégabits par seconde. Bande passante maximale : 0 Mbits/s Image: Pour n'appliquer aucune restriction à la valeur minimale ou maximale, spécifiez 0 comme valeur. Pour retirer la carte réseau de cet ordinateur virtuel, diquez sur Retirer.
	D:\ Action de démarrage automatique Redémarrer le service s'il était en c Action d'arrêt automatique Enregistrer	Pour retirer la carte réseau de cet ordinateur virtuel, diquez sur Retirer.

On affecte ici pour chaque poste son **VLAN**, dans mon exemple **PC Gestion NAS**

sur le **VLAN 1**.

2. Création serveur NAS



On clique sur 1 pour procéder à l'installation :

🕎 o sur SRV-LAB-2025 - Connexion à un ordinateur virtuel	 - 0	\times
Fichier Action Média Presse-papiers Affichage Aide		
TrueNAS 13.8-U6.7 Console Setup		
Install/Upgrade		
2 Shell 3 Reboot Sustem		
4 Shutdown System		
Cance 1>		
		(0) 0
Etat : Exécution		0 🚞



On sélectionne le **seul disque** que l'on a monté comme **disque d'OS**

On sélectionne **'Yes'** comme quoi on est bel et bien conscient que l'on va effacer toutes les **données** présentes sur le **disque dur** pour l'installation.



On rentre un **mot de passe** qui sera le mot de passe **administrateur** du serveur ainsi que le mot de passe servant à l'**authentification** sur la page web de management.

🖳 o sur SRV-LAB-2025 - Connexion à un ordinateur virtuel	_	\times
Fichier Action Média Presse-papiers Affichage Aide		
1		
Enter your root password; cancel for no root		
Paccused and a second s		
Confirm Password: *******		
< OK > <cancel></cancel>		
État Exécution		 M 🗛
Licit - EAELUIION		

Par la suite, on choisit le mode de boot UEFI qui est le plus récent.

🕎 o sur SRV-LAB-2025 - Connexion	à un ordinateur virtuel			- 🗆 🗙
Fichier Action Média Pres	se-papiers Affichage Aide			
🖿 🔘 🔳 🥘 🔘 11 🕩 🖥	5 2 壁			
	TrueNAS	Boot Mode	1	
	TrueNAS can be booted in either B	BIOS or UEFI mode.		
	BIOS mode is recommended for lega	cy and enterprise hardware,		
	whereas UEFI may be required for	newer consumer motherboards.		
	<pre>Soot via UEFI></pre>	<boot bios="" via=""></boot>		
	L			
st. Evénution				



L'installation est terminée !

On éteint le serveur, on enlève l'**ISO** du lecteur DVD et l'on ajoute le **disque dur** qui servira à stocker les données de notre partage, puis on démarre le serveur.

Paramètres pour SRV-TRUENAS sur SRV-L	AB-2025	- 🗆 X
SRV-TRUENAS ~	ق ♦ ♦	
Matériel Ajouter un matériel	👝 Disque dur	
Microprogramme Démarrer à partir de Fichier	Vous pouvez modifier la façon dont ce disque virtuel. Si un système d'exploitation est instal l'attachement peut empêcher l'ordinateur virt	: dur virtuel est attaché à l'ordinateur llé sur ce disque, la modification de tuel de démarrer.
Securite Démarrage sécurisé désactivé	Contrôleur :	Emplacement :
Mémoire	Contrôleur SCSI \checkmark	1 (en cours d'utilisation) $$
16384 Mo	Média	
Processeur 8 processeurs virtuels Contrôleur SCSI	Vous pouvez compacter, convertir, étendr disque dur virtuel en modifiant le fichier as complet au fichier.	re, fusionner, reconnecter ou réduire un socié. Spécifiez le chemin d'accès
	Disque dur virtuel :	
SRV-TROENAS-OS.VIIdX	D:\SRV-TRUENAS-1.vhdx	
SRV-TRUENAS-1.vhdx	Nouveau Mod	lifier Inspecter Parcourir
Lecteur de DVD Augun	Disque dur virtuel physique :	
Carte réseau LAN Pfsense	×	
Gestion Nom SRV-TRUENAS	 Si le disque dur physique que vou vérifiez que le disque est hors coi sur l'ordinateur physique pour gé 	us voulez utiliser n'est pas répertorié, nnexion. Utilisez la Gestion des disques rer les disques durs physiques.
Services d'intégration Quelques services offerts	Pour retirer le disque dur virtuel, diquez sur R disque, mais ne supprime pas le fichier associ	Retirer. Cette opération déconnecte le é.
Points de contrôle Production		Retirer
Emplacement du fichier de paginati		
Action de démarrage automatique Redémarrer le service s'il était en c		
C Action d'arrêt automatique Enregistrer		
	ОК	Annuler Appliquer

Après le redémarrage du serveur, on tombe sur cette page :



On constate que le serveur ne possède aucune adresse IP d'où le message "The

web interface could not be accessed, please check network configuration".

Pour y remédier, on va procéder comme ceci :

→ Configuration réseau NAS

Configurer un adressage IP TRUENAS

Console setup 1) Configure Network Interfaces 2) Configure Link Aggregation 3) Configure VLAN Interface 4) Configure Default Route 5) Configure Static Routes 6) Configure DNS 7) Reset Root Password 8) Reset Configuration to Defaults 9) Shell 10) Reboot 11) Shut Down Please check network configuration. Enter an option from 1–11: 1 Select an interface (q to quit): 1 Remove the current settings of this interface? (This causes a momentary disconnection Configure interface for DHCP? (y/n) n Configure IPv4? (y/n) y Interface name:hn0 Several input formats are supported Example 1 CIDR Notation: Example 2 IP and Netmask separate: IP: 192.168.1.1 Netmask: 255.255.255.0, /24 or 24 IPv4 Address:192.168.1.200/24 Saving interface configuration: Ok Configure IPv6? (y/n) n Restarting network: ok Console setup 1) Configure Network Interfaces 2) Configure Link Aggregation Configure VLAN Interface
 Configure Default Route
 Configure Static Routes
 Configure DNS 7) Reset Root Password 8) Reset Configuration to Defaults 10) Reboot 11) Shut Down The web user interface is at: http://192.168.1.200 https://192.168.1.200 Enter an option from 1–11: S

Explication :

- 1. On tape **'1'** pour choisir la fonction **"Configure Network Interfaces"** afin de pouvoir configurer nos interfaces réseaux.
- 2. Vu que nous avons qu'une seule carte réseau est présente sur notre serveur, on **tape '1'** encore une fois pour **sélectionner la carte réseau 'Hn0'**
- 3. On choisit l'option **'N'** car nous ne **voulons pas supprimer** les **paramètres réseaux** mais seulement les **remplacer**.
- 4. On ne veut **pas configurer l'interface** en mode **DHCP** vu que celui-ci est **désactiver** sur notre **LAN**
- 5. On veut **configurer** notre interface en **IPv4** donc on tape **'Y'**
- 6. On peut **renommer** le **nom de l'interface** sur notre système, ici, inutile de changer donc on retape **'hn0'**.
- A partir de ce moment la on renseigne l'adresse IP que nous voulons assigner à notre serveur soit '192.168.1.200/24' conformémant au <u>schéma</u> <u>réseau</u>
- 8. On ne veut **pas d'adressage IPv6,** donc on tappe **'N'** pour **refuser**
- 9. La configuration réseau est finie, on peut voir que nos interfaces redémarrent et que l'adressage est bien pris en compte

→ Configuration VLAN

Notre serveur **NAS** doit être accessible par le **VLAN 1** et le **VLAN 3** comme indiqué sur le plan. Actuellement, il est configuré seulement pour être accessible sur le **VLAN 1**, pour y remédier, on va configurer notre carte existante en mode **'TRUNK'**.

On va procéder quasiment de la même manière que pour le **TRUNK** du serveur **Pfsense**, cependant, notre carte réseau existe déjà, donc pas besoin de la créer. Il faut juste agréer les **VLAN 1** et **3** à la carte. :

set-VMNetworkAdapterVlan -VMName **SRV-TRUENAS** -VMNetworkAdapterName **"Carte réseau"** -Trunk -AllowedVlanIdList **"3"** -NativeVlanId <mark>1</mark>

On peut **vérifier** par la suite si **notre commande** a bien été prise en compte **avec** la commande :

Get-VMNetworkAdaptervlan -VMName **SRV-TRUENAS**

PS C:\Users	\Administrateur≻ Get-\	/MNetwo	orkAdaptervlan	-VMName	SRV-TRUENAS
VMName	VMNetworkAdapterName	Mode	VlanList		
SRV-TRUENAS	Carte réseau	Trunk	1,3		

Notre **TRUNK** est bien créé et fonctionnel !

3. Configuration de la banque de données

Pour pouvoir configurer un **partage** sur notre serveur, nous devons nous connecter sur l'**interface WEB** de **TRUENAS**.

Pour s'y faire, on se connecte à l'hôte **'PC Gestion NAS'** et on ouvre une page web en tapant l'adresse IP de notre **NAS** dans la barre de recherche.

Ici, le nom d'utilisateur par défaut est **'root'** et le mot de passe est celui que l'on a tapé pendant l'installation de **TRUENAS**.

✓ S TrueNAS - 192.168.1.200 × +		- 0 ×
← → C △ Non sécurizé 192.168.1.200/ui/sessions/signin		Bg 🛧 😩 i
i i i i i i i i i i i i i i i i i i i		
	TrueNAS	
	CORE	
	Nom duilisateur *	
	Mot de passe *	
	TrueNAS CORE © © 2025 JJJ Systems	
		Activer Windows
		Accedez dux parametres pour activer windows.

On se retrouve sur la **page d'administration** de notre serveur :



Tout d'abord, on va créer un **groupe de disques** (**Pool**), pour s'y faire il faut se rendre dans le menu **Storage -> Pools :**

•	٢	TrueNAS - 192.168.1.2	200	×	+				-	0	×
÷	÷	C 🛆 Non sé	curisé	192.16	1.200/ui/storage/pools			5 2	☆	٠	:
	<	TrueNAS		=		🗱 systems [.]	¢	ê (•	. (ს
		A					ueNAS CO)RE® © 21)25 - <mark>IX</mark> S		
		SRV-TRUENAS.local									
		ashboard			Pools				A	DD	
	, ,	ccounts									
	s	ystem			No pools						
		asks									
x	N	letwork									
	s	nanshots									
	-	Mwara-Snanehote									
	U	isks									
	Ir	nport Disk									
₿		irectory Services									
	s	haring									
輩	s	ervices									
*		lugins				Activer Window					
		ails									
		enation									

On clique sur **ADD** afin de **créer un pool** :

•	TrueNAS - 192.168.1.2	00	× +					-	0	×
←	→ C ▲ Non sé	curisé 19	2.168.1.200/ui/storage/pools/import					\$ 1	۲	:
	🛠 TrueNAS		≡ <			₫X systems [.]	۵ ۵	. .	ه (,
	A root						ueNAS CORE®	© 2025 - 🗙		
	SRV-TRUENAS.local									
	Dashboard		Create or import pool	Decrynt nool	Relect nool to import		a a			
-	Accounts									
	System		Create a pool: Create new pool ⑦ 							
	Tasks		O Import an existing pool ③							
x	Network									
			CANCEL CREATE POOL							
	Snapshots									
	VMware-Snapshots									
	Disks									
	Import Disk									
•	Directory Services									
	Sharing									
	Services									
*	Plugins					Activer Window				
	Jails									

On a le choix entre **créer ou importer** un **pool**, on choisit de **créer un pool**

Ľ	TrueNAS - 192.168.1.2	00 3	+				- 0 ×
÷	→ C ▲ Non sé	ourisé 192	168.1.200/ui/storage/pools/manager				💀 🕁 😩 E
	TrueNAS		≡ <				🚯 systems: 🕸 🖨 🌲 🌣 🙂
							TrueNAS CORE® @ 2025 - IXsystems, Inc.
	root SRV-TRUENAS.local						
	Dashboard		Pool Manager				
	Accounts		Name* NAS				
	System						
	Tasks						
x	Network		Available Disks		Data VDevs		
			✓ Disk Type Capacity		Disk Type Cap	acity	
			da1 UNKNO 300 GiB →	(\rightarrow)			
	Snapshots						
	VMware-Snapshots		T selected / T total		U SERCIEU / U IUIAI		
	Disks		Filter disks by name Filter disks by capacity		Stripe Estimated raw capacity: 0 B 🧿		
	Import Disk		Estimated total raw data capacity: 0 B				
			CREATE CANCEL				
•	Directory Services						
	Sharing						
副	Services						
*	Plugins						
ाङा	Jails						
- TEN	D						

On nomme notre partage **'NAS'** et on sélectionne le **disque dur** que l'on avait

ajouté à notre serveur précédemment

•	TrueNAS - 192.168.1.20	10 ×	+	-					-	ø ×
←	\rightarrow C \land Non set	urisé 192,	68.1.200/ui/storage/pools/manager						\$2 \$	a :
	STrue NAS		≡ <					(X) systems:	ê ê 🌲	ф ()
	🛱 root							Τιυ	eNAS CORE® © 2025 -	iXsystems, Inc.
	SRV-TRUENAS.local		Pool Manager							
-	Dashboard									
*	Accounts		Name* NAS Description (?)							
□	System									
	Tasks									
x	Network		Available Disks		Data VE	levs				
			Disk Type Capacity		Disk	Туре	Capacity			
					da1	UNKNOW	300 GiB			
	Snapshots		0 selected / 0 total	0 selecte	d / 1 total					
	VMware-Snapshots			Stripe						
	Disks		Filter disks by name Filter disks by capacity	Estimated ra	aw capacity: 298 GiB 🕅					
	Import Disk		Estimated total raw data capacity: 298 GiB							
•	Directory Services		Caulton: A shipe data vdev is highly discouraged and will result in data loss.							
	Sharing		CREATE CANCEL							
	Services									
*	Plugins							Activer Windows		
	Jails									NS.

Il faut cliquer sur la **flèche** afin que le disque soit catégorisé dans les disques **VDevs**. Dans notre cas, on doit aussi cliquer sur **"Force"** car nous n'avons qu'un seul disque, pratique qui n'est pas sécurisé car si le disque vient à être défectueux, toute la **pool** sera corrompue. On coche donc la case **"Force"** afin de forcer la création d'un **pool** contenant qu'un seul disque.

•	TrueNAS - 192.168.1.2	00	× +										-	0	×
←	→ C ▲ Non sé	turisé 19	92.168.1.200/ui/st	orage/pools									Be ta	-	:
	TrueNAS		≡ <								()>systems	۲	1	٠	
												rueNAS CO	RE® © 2025		ns, Inc.
	root SRV-TRUENAS.local														
5	Dashboard		Pools											ADD	
*	Accounts		NAS (S)	rstem Dataset Pool)			ONLINE 🤡 11.3 MiB	(0%) Used 286.8 GiB Free						\$ ^	
	System		Name 🗢	Type 🗢	Used 🗢	Available 🗢	Compression 🗢	Compression Ratio 🗢	Readonly 🗢	Dedup 🗢	Comments 🗢				
ē	Tasks		NAS	FILESYSTEM	11.3 MiB	286.8 GiB		12.67	faise	OFF					
1	Network														

Notre **pool** est bien créé, on va donc maintenant créer notre ensemble de

données en cliquant sur les 3 petits points à droite puis 'Add Dataset'.

Pools										ADD
NAS (System)	Dataset Pool)		ON	LINE 🥑 11.68 MiB (0%) Used 286.8 GiB Free					\$ ^
Name 🗢 NAS	Type ≑ FILESYSTEM	Used ≑ 11.68 MiB	Available 🗢 286.8 GiB	Compression 🗢 Iz4	Compression Ratio 🗢	Readonly \$ false	Dedup 🗢 OFF	Comments 🗢		
									Dataset Actions Add Dataset Add Zvol Edit Options Edit Permissions User Quotas Group Quotas Create Snapshot	
Name a	nd Options									
public									0	
Comments Partage p	ublic pour tous le	es utilisateurs							0	
_{Sync} Inherit (s	standard)								<u>•</u> 0	
Compression	z4)								<u>•</u> 0	
Enable Atime Inherit (c	off)								<u>•</u> 0	
Encrypti	ion Options	d) 🕜								
Other O	ptions									
ZFS Deduplic Inherit (c	off)								<u></u> Ø	
									~ @	
Share Type SMB									<u>•</u> 0	
SUBM	IIT CANC	EL AD		DNS						

Dans cette situation, on veut **créer** un espace de **partage public** pour nos **deux**

VLAN, on le nomme donc 'Public' et on définit 'Share Type' en mode 'SMB'.

NAS (System Data	aset Pool)		0	LINE 🤡 11.93 MIB (0%) Used 286.8 GIB Free					
Name 🗢	Туре 🗢	Used 🗢	Available 🗢	Compression 🗢	Compression Ratio 🗢	Readonly 🗢	Dedup 🗢	Comments 🗢	
✓ NAS	FILESYSTEM	11.93 MiB	286.8 GiB	lz4	12.31	false	OFF		
public	FILESYSTEM	112 KiB	286.8 GiB	Inherits (Iz4)	1.00	false	OFF	Partage public pour tous les utilisateurs	

→ Modification ACL

Une **ACL** ou **"Access Control List"** est un ensemble de règles qui définissent les autorisations d'accès à des ressources (comme des fichiers ou des réseaux), spécifiant qui peut y accéder et quelles actions peuvent être effectuées (lecture, écriture, exécution).

Dans notre cas, nous voulons que notre partage **"public"** soit accessible en **lecture, écriture, exécution** pour tous les utilisateurs.

Pools										ADD
NAS (System Datas	set Pool)		ONL	.INE 🤡 11.98 MiB (09	%) Used 286.8 GiB Free					۰ 🌣
Name 🗢	Туре 🗢	Used 🗢	Available 🗢	Compression 🗢	Compression Ratio 🗢	Readonly 🗢	Dedup 🗢	Comments 🗢		
✓ NAS	FILESYSTEM	11.98 MiB	286.8 GiB	lz4	12.28	false	OFF			:
public	FILESYSTEM	112 KiB	286.8 GiB	Inherits (Iz4)	1.00	false	OFF	Partage public pour tous les utili	sateurs	
									Dataset Actions	
									Add Zvol	
									Edit Options	
									Edit Permissions	
									User Quotas	
									Group Quotas	
									Delete Dataset	
									Create Snapshot	

Pour modifier les **ACL**, on se rend dans **Storage -> Pools**.

Puis on **clique** sur **"Edit Permissions" :**

File Information	Access Control List	
Path	Who *	
/mnt/NAS/public	everyone@	• 0
User	ACL Type *	
root	O Allow	- 0
Apply User 🕜	Permissions Type *	
Group	Basic	• 🔿
wheel	O Permissions *	
Apply Group ⊘	Full Control	• 0
	Flags Type *	
	Basic	• 🔿
	Flags *	
SELECT AN ACL PRESET	No Inherit	• 0
		DELETE

Dans notre cas, on veut que tous les utilisateurs aient toutes les permissions, on sélectionne donc **"Everyone"** dans **"Who"** et dans **"Permission"** on met **"Full Control"** et on clique sur **"Save"** pour sauvegarder.

4. Création du partage SMB

Nous allons donc **mettre à disposition** notre **banque de données** via un **partage SMB.**

Pour le créer on va se rendre dans Sharing -> Windows Shares (SMB).

•	S TrueNAS - 192.168.1.20	00	× +					-	ø ×
÷	→ C ▲ Non séc	urisé 19	92.168.1.200/ui/sharing/smb				٥	2 ☆	2 :
	TrueNAS		≡ <			(∭) systems	¢ 🕯	. ¢	ن ا
						-	rueNAS CORE® @	2025 - <mark>iXs</mark> j	rstems, Inc.
	root SRV-TRUENAS.local								
-	Dashboard		Samba			Q Filter Samba	COLUMNS	- AC	D
*	Accounts		Name	Path	Description	Enabled			
묘	System								
Ē	Tasks								
*	Network								—
	Storage								
•	Directory Services								
	Apple Shares (AFP)								
	Block Shares (ISCSI)								
	Unix Shares (NFS)								
	WebDAV Shares								
幸	Services								
*	Plugins								
ाल्ला	Jails					Activer Window Accédez aux paramè			
- 1650									

On clique sur ADD pour créer un nouveau partage :

Basic			
+ /mnt/NAS/public		0	
🔻 🛅 /mnt			
V NAS			
▶ Public ACL			
Name			
public			0
public Purpose Default share parameters			
public Purpose Default share parameters	→ ⑦ Description		0

On **parcourt l'arborescence** pour **trouver** notre **banque de données 'public'** et on **clique** sur **'Submit'** pour le **créer.**

→ Activation SMBv1

Attention, le protocole SMBv1 est obsolète et vulnérable à des attaques. Il manque de chiffrement et de protections modernes. L'utiliser expose donc les systèmes à des risques de sécurité élevés.

Un souci s'oppose à nous, **PC XP** ne peut pas accéder au partage car **Windows XP** ne prend pas en charge le protocole **SMB** au-dessus de la version **1**. Pour pallier ce problème, nous allons forcer l'activation **SMBv1** en allant dans l'onglet **'Service'**.

	TrueNAS	≡ <				🚺 systems 🛭 🕼	:₿ ♠ ‡	ሳ
	nort					TrueNA	S CORE® © 2025 - iXsyst	tems, Inc.
	SRV-TRUENAS.local							
8	Dashboard		Q Filter Service					
**	Accounts -		Name	Running	Start Automatically	Actions		
	System 🔫			•		1		
	Tasks 👻		NFS	•		1		
x	Network -		OpenVPN Client	•		1		
	Storage 🚽		OpenVPN Server	•		1		
ᢒ	Directory Services 👻		Rsync	•		1		
	Sharing 👻		S.M.A.R.T.	•		1		
醋				•		1		
*	Plugins		SMB	•		1		
Iği	Jails		SNMP	•		1		
16	Reporting		SSH	•		1		
	Virtual Machines			•		1		
4	Display System Processes		UPS	•		1		
>_	Shell		17 total			Activer Windews 1 Accédez aux paramètres po	2 > M our activer Windows.	

Ensuite, cliquez sur le crayon à la ligne SMB

NetBIOS	
NetBIOS Name * truenas	
NetBIOS Alias	
Workgroup * WORKGROUP	
Description TrueNAS Server	0
✓ Enable SMB1 support ⑦	
VILMVI Auth	
SAVE CANCEL ADVANCED OPTIONS	

Cochez la case "Enable SMB1 support" et "NTLMv1 Auth" et cliquez sur "Save"

5. Création des utilisateurs/groupes

→ Créer un groupe d'utilisateur

Pour **tester notre NAS** nous allons **créer deux utilisateurs**, ces **deux utilisateurs doivent faire partie d'un groupe**. Pour **créer un groupe** on se rend dans la catégorie **Account -> Groups**

	TrueNAS		≡ <			₫≯ syster	ns: 🕼 🖹 🐥	ф ()				
	ft root			counts / Groups TrueNAS CORE® @ 2025 - XXystems, in								
	SRV-TRUENAS.local											
	Dashboard		Groups			Q Filter Groups	COLUMNS - ADD	•				
*			Group	GID	Builtin	Permit Sudo						
	Users											
□	System											
Ē	Tasks											
x	Network											
	Storage											
•	Directory Services											
	Sharing											
	Services											
*	Plugins							j ,				
	Jails											
16	Reporting											
□	Virtual Machines					Activer Win						
4	Display System Proce	sses										

On clique sur ADD en haut à droite afin de créer un nouveau groupe :



Dans notre cas, on nomme le groupe "Public" et on clique sur "Submit".

→ Créer un utilisateur

TrueNAS ≡ < 💔 systems: 🕼 🖨 🌲 🗢 U TrueNAS CORE® @ 2025 eroot SRV-TRUENAS.local Dashboard COLUMNS - ADD 🔅 Users Accounts Userna Full Name Builtir Groups 💻 System Storage 🕄 Directory Services 👻 Sharing 🚖 Plugins Jails II. Reporting Uirtual Machines 4

Pour créer nos utilisateurs, on se rend dans l'onglet Account -> Users :

On clique sur ADD pour créer un nouvel utilisateur :

Identifi	cation	1				
Full Name*					e	৯
Usemame *						-
test						2
Email					G	3
Password *					`	-
••••					🖉 🖉	
Confirm Pa:	ssword *			ø		
User ID) and (Groups				
User ID *						
1000					0	?)
New	Primar	y Group	0			
Primary Gro public	чp				• 6	?)
Auxiliary	Groups					2
Directo	ries a	nd Per	missions		Authentication	
	Home Di	rectory			SSH Public Key	
+	/none:	astent		0		
	/mnt					2)
Home Di	rectory	Permiss	iions?		No • (?
	Read	Write	Execute		Shell	
User	\checkmark	\checkmark	 Image: A set of the set of the		sh <u></u> ⊂(2
Group	\checkmark		✓		Lock User 🧿	
Other	\checkmark		\checkmark		Permit Sudo 🧿	
					Microsoft Account ?	
					✓ Samba Authentication (?)	

Pour tester nos droits on va créer deux utilisateurs avec les mêmes configuration :

- Nos utilisateurs "test" et "test" doivent appartenir au groupe "public"
 comme groupe primaire
- Nous ne voulons pas que nos utilisateurs possèdent de répertoire nominatif, donc dans la section "Directories and Permissions" et dans le champ "Home Directory", on tape "/nonexistent".
- → Test de connexion + transfert de données

On va tout d'abord essayer de se connecter du **"PC XP"** sur le **NAS** :

de la ser	Connecter un lect	eur réseau			X	194	-	
	Connecter un lec	teur réseau 🚺	ecter à un dossier	réseau partagé et		1200	The	-
	Tentative de conne×	ion à \\192.168.1.200\public en cours	afin d'accéder à ce	dossier depuis le				
		Annuler	r et le dossier aux				X	
1. Sec. 1.		Dossier : \\192.168.1.200\pub Exemple : \\serveur\pa	lic artage	Parcourir				
1000		Se reconnecter à l'a Se connecter sous un p	ouverture de session nom d'utilisateur différ	ent.	BUF		💌 🄁 ок	
		Ouvrir une session de : serveur réseau.	stockage en ligne ou s	e connecter à un	Documents of	de Administrateur		-
		•	: Précédent Term i	Connecter à srv-t	ruenas.local	? 🗙		
		Modifier un paramètre Autres emplacements	Lecteurs de	R	G			
-		Favoris réseau		Connexion à 192.168	3.1.200			· · ·
A CONTRACTOR OF THE	S. ARK	Mes documents Documents partagés	Peripheriqu	Nom d'utilisateur :	🖸 test	~		
		Panneau de configuration		Mot de passe :	••••	лр (D:)		-
		Détails 🎗			Memoriser mon mot de pass	se		
		Poste de travail Dossier système			OK Ar	nuler		
								355
The state of the s	Rear A							
								An In
	THE OWNER				Sector Mark			A STER
🛃 démarrer	ste de travail		as Balter At A			100 F 100 F 10	FR 🕰 👔	08:43

📽 public sur 'TrueNAS Server (192.168.1.200)' (N:)	
Fichier Edition Affichage Favoris Outils ?	1
🕞 Précédente 👻 🌍 👻 🏂 Rechercher 🔊 Dossiers 📰 -	
Adresse 😹 N:1	🖌 🄁 ок
Gestion des fichiers	
Créer un nouveau dossier	
Autres emplacements 🛞	
Poste de travail Image: Imag	
Détails	

On est bien connecté, notre **utilisateur** a bien accès au **partage**, on va tester nos **droits** en essayant un **transfert de fichier** :

1000	all is	9			1		4 ···
	📽 public sur 'Tru	eNAS Server (192.	168.1.200)' (N:)				Ent of h
	Fichier Edition Af	fichage Favoris Ou	itils ?			🥂	
	Précédente •	🕥 - 🎓 🔎	Rechercher 😥 Dossie	rs 🛄 -		-	
	Adresse 🌋 N:\				✓ →	ок	1
PC-XP-32, vhdx	Gestion des fich Créer un nouv Publier ce dos	iers 🔊	PC-XP-32.vhc Fichier VHDX 1 937 408 Ko	х Соріе	X		Эок
	Autres emplaces	ments (*) ail ts rtagés u		PC-XP-32.vhdx De Bureau' vers 'N:\' 50 secondes restantes	Annuler		
	Decails	Ŭ					
🦺 démarrer 🔰 😨 P	oste de travail	🗝 public sur 'TrueN	AS S			FR	😤 💓 💙 08:57

On fait pareil pour le "PC Gestion NAS" :

Image: Construction Image: Construction Image: Constredon Image: Constredon	C Affichane Connecter un le Tentative de co Lecteur : Dossier :	cteur réseau × nnexion à \\192.168.1.200\public en cours Annuler N: ✓ (\\192.168.1.200\public Exemple : \\serveur\partage ☑ Se reconnecter lors de la connexion ☐ Se connecter à l'aide d'informations d'identificat	r ? souhaitez vous connecte	Sécurité Windows × Entrer les informations d'identification réseau > Entrez vos informations d'identification pour vous connecter à : 192.168.1.200 test1 • • • Mémoriser mes informations d'identification • Mémoriser mes informations d'identification • Le nom d'utilisateur ou le mot de passe est incorrect. •	
9 élément(s)		Se connecter à un site Web permettant de stocker o	des documents et des im Terminer	Nuclei Crow Insérer une carte à puce Insérer un autre compte OK Annuler	

On récupère le fichier que l'on a posé avec le PC-XP :



On voit que nos **droits** fonctionnent correctement malgré qu'on ne les ait pas tous **testés**.

VI. Configuration du Pfsense Filtrage

Dans notre schéma, on a un PfSense qui sert de serveur proxy sur le VLAN 2.

Pour le créer, on procède comme ceci :

1. Création carte réseau

→ Carte WAN



On crée notre première carte côté **WAN**, celle-ci doit être sur le **VLAN 1** conformément à notre schéma.

→ Carte LAN

/-Pfsense-Filtrage	✓ ▲ ▶ ②	
Matériel	Carte réseau	
Ajouter un matériel		
Microprogramme	Spécifiez la configuration de la carte	e réseau ou retirez la carte réseau.
Démarrer à partir de Fichier	Commutateur virtuel :	
Securite Démarrage ségurisé désactivé	LAN Ptsense	~
Mémoire	ID du réseau local virtuel	
2048 Mo	Activer l'identification LAN vir	rtuelle
Processeur	L'identificateur VI AN spécifie le r	éseau local virtuel utilisé par cet ordinateur virtuel
2 processeurs virtuels	pour toutes les communications r	éseau par le biais de cette carte réseau.
Contrôleur SCSI	2	
Disque dur SPV-Pfsense-Filtrage vbdv		
Lecteur de DVD	Gestion de bande passante	
Pfsense.iso	Activer la gestion de bande p	passante
Carte réseau		
LAN Pfsense	Spécifiez le mode d'utilisation de La bande passante maximale et l	la bande passante réseau par cette carte réseau. a bande passante minimale sont mesurées en
Carte réseau	mégabits par seconde.	
Gestion	Bande passante minimale :	0 Mbits/s
Nom		0
SRV-Pfsense-Filtrage	Bande passante maximale :	0 MDITS/S
Services d'intégration	Pour n'appliquer aucune res	striction à la valeur minimale ou maximale,
Queiques services offerts	specifiez o confine valeur.	
Production	Pour retirer la carte réseau de cet o	ordinateur virtuel, diquez sur Retirer.
Emplacement du fichier de paginati	.	Retirer
D:\		
Action de démarrage automatique		
Redemarrer le service s'il etait en c.	•	
 Action d'arret automatique Enregistrer 		
Aust in full generation for		
	1	

Comme pour la carte **WAN**, il faut mettre la carte **LAN** dans son **VLAN** respectif, donc le **n°2** dans ce cas-ci.

2. Adressage IP des cartes

→ Carte WAN 0) Logout (SSH only) 9) pfTop 1) Assign Interfaces 10) Filter Logs 2) Set interface(s) IP address 11) Restart webConfigurator 3) Reset webConfigurator password 12) PHP shell + pfSense tools 13) Update from console 4) Reset to factory defaults 14) Enable Secure Shell (sshd) 5) Reboot system 6) Halt system 15) Restore recent configuration 7) Ping host 16) Restart PHP-FPM 8) Shell Enter an option: 2 Available interfaces: 1 - WAN (hn0 - static) 2 – LAN (hn1 – static) Enter the number of the interface you wish to configure: 1 Configure IPv4 address WAN interface via DHCP? (y/n) n Enter the new WAN IPv4 address. Press <ENTER> for none: > 192.168.1.253 Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 Enter the new WAN IPv4 subnet bit count (1 to 32): > 24 For a WAN, enter the new WAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: > 192,168,1,254 Should this gateway be set as the default gateway? (y/n) y Configure IPv6 address WAN interface via DHCP6? (y/n) n Enter the new WAN IPv6 address. Press <ENTER> for none: Do you want to enable the DHCP server on WAN? (y/n) n Disabling IPv4 DHCPD... Disabling IPv6 DHCPD... Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n Please wait while the changes are saved to WAN... Reloading filter... Reloading routing configuration... DHCPD... The IPv4 WAN address has been set to 192,168,1,253/24 Press <ENTER> to continue.

Explication :

- On tape 2 pour choisir la troisième option du système 'Set interface(s) IP address'.
- 2. On tape sur **1** pour sélectionner la première carte réseau.
- À ce moment-là, PfSense demande quelle est l'adresse que l'on veut affecter à notre carte réseau, d'après notre schéma réseau, on y affecte l'adresse '192.168.1.253'.
- PfSense nous demande le masque de notre réseau en format CIDR, on choisit 24 dans notre cas pour un réseau local classe C.
- Ici, vu que l'on configure une interface WAN dans un réseau existant, on doit définir la passerelle en amont, on tape donc l'adresse IP de notre passerelle soit 192.168.1.254.
- Dans notre cas, on ne veut pas d'adresse en format IPV6, on appuie sur 'N' pour ne pas activer le serveur DHCP en IPV6.
- Par la suite, on nous demande si on veut activer le serveur DHCP en IPV4, dans notre cas, on veut tout simplement pas de DHCP dans le réseau, donc on appuie encore une fois 'N'.
- La dernière question nous demande si l'on veut désactiver l'accès à l'interface web en HTTPS, bien sûr, on répond non à des fins de sécurité.

→ Interface LAN

0) Logout (SSH only) 9) pfTop 1) Assign Interfaces 10) Filter Logs 2) Set interface(s) IP address 11) Restart webConfigurator 3) Reset webConfigurator password 12) PHP shell + pfSense tools 4) Reset to factory defaults 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 7) Ping host 16) Restart PHP-FPM 8) Shell Enter an option: 2 Available interfaces: 1 - WAN (hn0 - static) 2 - LAN (hn1 - static) Enter the number of the interface you wish to configure: 2 Configure IPv4 address LAN interface via DHCP? (y/n) n Enter the new LAN IPv4 address. Press (ENTER) for none: > 192.168.2.254 Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 Enter the new LAN IPv4 subnet bit count (1 to 32): > 24 For a WAN, enter the new LAN IPv4 upstream gateway address. For a LAN, press <ENTER> for none: Configure IPv6 address LAN interface via DHCP6? (y/n) n Enter the new LAN IPv6 address. Press <ENTER> for none: Do you want to enable the DHCP server on LAN? (y/n) n Disabling IPv4 DHCPD... Disabling IPv6 DHCPD... Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n Please wait while the changes are saved to LAN... Reloading routing configuration... DHCPD... The IPv4 LAN address has been set to 192.168.2.254/24 You can now access the webConfigurator by opening the following URL in your web brows https://192.168.2.254/ Press <ENTER> to continue.

Explications

- On tape 2 pour choisir la troisième option du système 'Set interface(s) IP address'.
- 2. On tape sur **2** encore une fois pour sélectionner la deuxième carte réseau.
- À ce moment-là, PfSense demande quelle est l'adresse que l'on veut affecter à notre carte réseau (cette adresse sera la passerelle de notre réseau), d'après notre schéma réseau, on y affecte l'adresse '192.168.2.254'.
- 4. **PfSense** nous demande le masque de notre réseau en format **CIDR**, on choisit **24** dans notre cas pour un réseau local classe C.
- 5. Ici, vu que l'on configure une interface **LAN**, on passe cette étape en appuyant sur **'Entrer'**.
- Dans notre cas, on ne veut pas d'adresse en format IPV6, on appuie sur 'N' pour ne pas activer le serveur DHCP en IPV6.
- Par la suite, on nous demande si on veut activer le serveur DHCP en IPV4, dans notre cas, on ne veut tout simplement pas de DHCP dans le réseau, donc on appuie encore une fois 'N'.
- La dernière question nous demande si l'on veut désactiver l'accès à l'interface web en HTTPS, bien sûr, on répond non à des fins de sécurité.

3. Création du proxy

→ Installation de Squid sur PfSense

Connectez-vous sur l'interface d'administration de **PfSense** afin d'installer le paquet **"squid"**. Pour cela, sous **"System"**, cliquez sur **"Package Manager"** et ensuite sur l'onglet **"Available Packages"**.

System > Package Manager > Available Packages

Recherchez **"squid"** et cliquez sur le bouton **"Install"** à droite, au niveau de la ligne correspondante.

	B, System	n • Interfaces • Firewall • Services • VPN • Status • Diagnostics • Help •	6
System	/ Packa	age Manager / Available Packages	0
Installed Pa	ickages	Available Packages	
Search Search terr	n	squid Both Q Search Clear Enter a search string or *nix regular expression to search package names and descriptions.	Θ
Packages	;		
Name	Version	Description	
Lightsquid	3.0.6_8	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: Ø lighttpd-1.4.59 Ø lightsquid-1.8_5	+ Install
biupa	0.4.45_5	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies:	+ Install
squidGuard	1.16.18_20	High performance web proxy URL filter. Package Dependencies:	+ Install

À la fin de l'installation, le message **"pfSense-pkg-squid installation successfully completed"** doit s'afficher.

System 👻	Interfaces 🕶	Firewall 🗸	Services -	VPN 🗸	Status 🗸	Diagnostic				
System / Package Manager / Package Installer										
uid installation	successfully com	pleted.								
ges Availa	able Packages	Package Insta	ller							
	System - Package N uid installation ges Availa	System - Interfaces - Package Manager / F uid installation successfully com ges Available Packages	System • Interfaces • Firewall • Package Manager / Package Ins uid installation successfully completed. ges Available Packages Package Insta	System • Interfaces • Firewall • Services • Package Manager / Package Installer uid installation successfully completed. ges Available Packages Package Installer	System • Interfaces • Firewall • Services • VPN • Package Manager / Package Installer uid installation successfully completed. ges Available Packages Package Installer	System • Interfaces • Firewall • Services • VPN • Status • Package Manager / Package Installer uid installation successfully completed. ges Available Packages Package Installer				

Le paquet étant installé, on peut passer à la **configuration**.

→ Configurer Squid (Proxy) sur PfSense

La configuration de **Squid** s'effectue via le menu "Services" :

Services > Squid Proxy Server

La configuration est découpée en plusieurs onglets. Afin de pouvoir activer **Squid**, il faut configurer le **cache local** sinon le démarrage du processus **Squid** échouera. Cliquez sur l'onglet **"Local Cache"**. Comme pour chaque section, nous retrouvons de nombreux paramètres... Pour le cache, j'attire votre attention sur ces options :

- Hard Disk Cache Size : par défaut sur "100" pour 100 Mo, cette valeur correspond à la taille maximale du cache sur l'espace disque. Vous pouvez augmenter cette valeur à 1024 Mo pour avoir 1 Go de cache.
- Hard Disk Cache Location : l'emplacement du cache, à savoir par défaut "/var/squid/cache".

Que vous décidiez de modifier ou non l'un des paramètres de la section **"Local Cache"**, vous devez cliquer sur le bouton **"Save"** en bas de la page.

Package /	Proxy S	Server: Cache M	anageme	ent / Lo	cal Cache		
General Re	emote Cach	e Local Cache	Antivirus	ACLs	Traffic Mgmt	Authentication	U
Squid Cache	General	Settings					
Disable	Caching	Disable caching con This may be required if	mpletely. Squid is only	used as a pr	roxy to audit websit	e access.	
Cache Repla	acement Policy	Heap LFUDA The cache replacemen heap LFUDA	t policy decide	s which obj	ects will remain in c	✓ ache and which obje	cts ar
Low-Water M	lark in %	90 The low-water mark for	AUFS/UFS/di	skd cache o	bject eviction by th	e cache_replacement	_polic

Ensuite, cliquez sur l'onglet **"General"**. Là encore, il y a de nombreuses options. Voici ce qu'il faut configurer à minima :

- Enable Squid Proxy : cochez la case pour activer Squid sur le pare-feu, ce qui signifie qu'il va démarrer.
- [facultatif] Listen IP Version : écouter en IPv4, en IPv6 ou les deux.
- Proxy interface(s) : sur quelle interface souhaitez-vous activer le proxy ?
 Ici, ce sera seulement sur l'interface "LAN" donc je la sélectionne. Vous pouvez en sélectionner plusieurs si besoin, mais dans tous les cas le
 "WAN" ne sera pas sélectionné.
- Proxy Port : on laisse le port par défaut, à savoir 3128, mais il ne devra pas être déclaré sur les postes clients puisque l'on va configurer Squid en mode proxy transparent.
- Allow Users on interface : cochez cette case pour autoriser implicitement les utilisateurs connectés sur le réseau "LAN" à utiliser le proxy. Cela évite de déclarer le réseau dans un second temps.

Squid General Setting	gs	
Enable Squid Proxy	Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.	
Keep Settings/Data	If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.	
Listen IP Version	IPv4 v Select the IP version Squid will use to select addresses for accepting client connections.	
CARP Status VIP	none Income	GTER status.
Proxy Interface(s)	WAN LAN loopback The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.	
Outgoing Network Interface	Default (auto)	
Proxy Port	3128 This is the port the proxy server will listen on. Default: 3128	
ICP Port	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	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.	Activer W
Patch Captive Portal	This feature was removed - see Bug #5594 for details!	Accedez aux

Descendez dans la page... et cochez l'option **"Transparent HTTP Proxy"** pour activer le mode **proxy transparent** pour le protocole **HTTP**. Pour l'activer pour le protocole **HTTPS**, il faudra cocher une autre option (nous en parlerons par la suite).

Dans le même esprit qu'au début de la configuration, sélectionnez **"LAN"** pour l'option **"Transparent Proxy Interface(s)"**.

En configurant l'option **"Bypass Proxy for these Source IPs"**, vous avez la possibilité de déclarer des **adresses IP sources** (ou un **sous-réseau source**) qui peuvent passer outre le proxy et accéder en direct à Internet. Dans le même esprit, l'option **"Bypass Proxy for these Destination IPs"** permet d'outrepasser le proxy pour certaines destinations.

Transparent Proxy Se	ettings
Transparent HTTP Proxy	 Enable transparent mode to forward all requests for destination port 80 to the proxy server.
	Transparent proxy mode works without any additional configuration being necessary on cients. Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below. Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections, configure WPAD/PAC options on your DNS/DHCP servers.
Transparent Proxy Interface(s)	WAN LAN The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.
Bypass Proxy for Private Address Destination	Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.
Bypass Proxy for These Source IPs	Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)
Bypass Proxy for These Destination IPs	Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)

Pour le moment, laissez l'option **"Enable SSL filtering"** décochée.

HTTPS/SSL Interception	Enable SSL filtering.	
SSL/MITM Mode	Splice Whitelist, Bump Otherwise	×
	The SSL/MITM mode determines how SSL intercept	tion is treated when 'SSL Man In the Middl
	Default: Splice Whitelist, Bump Otherwise. Click Info	o for details. 🕕
SSL Intercept Interface(s)	WAN	^
	LAN	

Continuez de descendre dans la page... Activez les **journaux** comme ceci :

- Enable Access Logging : cochez l'option pour activer les journaux, ce qui va permettre de savoir qui fait quoi sur Internet.
- Rotate Logs : pendant combien de jours souhaitez-vous conserver les logs ? Pour les établissements scolaires, c'est pendant 365 jours qu'il faut conserver les logs (sauf erreur de ma part).

Logging Settings	
Enable Access Logging	 This will enable the access log. Warning: Do NOT enable if available disk space is low.
Log Store Directory	/var/squid/logs The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs Important: Do NOT include the trailing / when setting a custom location.
Rotate Logs	365 Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Ensuite, la section **"Headers Handling, Language and Other Customizations"** permet de configurer les messages **Squid**. Le champ **"Visible Hostname"** correspond au **nom d'hôte** qui peut s'afficher côté client, notamment sur les pages de blocage **Squid**, tout comme l'**e-mail** spécifié pour l'option **"Administrator's Email"**. Pour les messages d'erreurs justement, précisez la **langue française** au niveau de l'option **"Error Language"**.

Pour des raisons de sécurité, on va masquer les informations sur **Squid**, notamment la **version**, en cochant l'option **"Suppress Squid Version"**. Ce qui donne :

Visible Hostname	Proxy IT-Connect
	This is the hostname to be displayed in proxy server error messages.
Administrator's Email	admin@it-connect.fr
	This is the email address displayed in error messages to the users.
Error Language	fr
	Select the language in which the proxy server will display error messages to users.
X-Forwarded Header	(on) ~
Mode	Choose how to handle X-Forwarded-For headers. Default: on 🔋
Disable VIA Header	☐ If not set, Squid will include a Via header in requests and replies as required by RFC2610
URI Whitespace	strip v
Characters Handling	Choose how to handle whitespace characters in URL. Default: strip (
uppress Squid Version	Suppresses Squid version string info in HTTP headers and HTML error pages if enabled

Voilà, on est arrivé au bout de la page de configuration ! Cliquez sur **"Save"** pour appliquer cette nouvelle configuration.

→ Créer l'autorité de certification PfSense

Pour commencer, il faut créer une **autorité de certification** sur notre pare-feu **PfSense**. Rendez-vous dans le menu **"System"** puis **"Cert. Manager"** et dans l'onglet **"CAs"**. Cliquez sur **"Add"** et renseignez les différents champs : c'est tout simple.

Note : si vous avez une **autorité de certification Active Directory**, il doit être possible d'ajouter un **certificat existant** directement.

Vous obtenez une **autorité de certification**, comme la mienne nommée **"CA-ITCONNECT"** et qui existait déjà sur mon pare-feu, car je l'utilise pour le **VPN client-to-site**.

CAs Certifi	cates C	ertificate Revoca	tion			
Search						(
Search term				Both V Q Se	arch 🕤 Clear	
Search term		Enter a search s	tring or *nix regul	ar expression to search certificate names and distinguished names.	arch D Clear	
Search term Certificate Au	uthorities	Enter a search s	tring or *nix regul	ar expression to search certificate names and distinguished names.	arch 🕤 Clear	
Search term Certificate Au	uthorities Internal	Enter a search s	tring or *nix regul Certificates	ar expression to search certificate names and distinguished names.	In Use	Actions
Search term Certificate At lame CA-ITCONNECT	uthorities Internal	Enter a search s Issuer self-signed	tring or *nix regul Certificates 2	Both Q Se ar expression to search certificate names and distinguished names. Distinguished Name ST=Normandie, 0=IT-Connect, L=Caen, CN=it-connect, C=FR ()	In Use	Actions

→ SSL Inspection avec Squid

Retournez dans la configuration de **Squid**, via le menu **"Services"**. Cochez l'option **"Resolve DNS IPv4 First"** pour activer la **résolution DNS en amont du filtrage**, ce qui est recommandé lorsque l'on filtre le **HTTPS** (ce que l'on s'apprête à faire).



Ensuite, activez l'option **"Enable SSL filtering"**. Pour le mode **"SSL/MITM Mode"**, choisissez le mode **"Splice All"** : c'est le mode le moins contraignant à mettre en œuvre, car il ne nécessite pas de déployer le **certificat de l'autorité de certification** sur l'ensemble des postes clients. C'est aussi le mode recommandé lorsque l'on prévoit de déployer **Squid Guard**, ce qui sera le cas dans la seconde partie de ce tutoriel.

Remarque : si vous prenez l'autre mode, il faut exporter le certificat de la **CA créée précédemment** et le déployer sur toutes les machines qui vont passer par le **proxy transparent**.

Sélectionnez l'**autorité de certification** créée précédemment au niveau de l'option **"CA"**.

SSL Man In the Midd	le Filtering
HTTPS/SSL Interception	Enable SSL filtering.
SSL/MITM Mode	Splice All
SSL intercept interface(s)	WAN LAN The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.
SSL Proxy Port	3129 This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129
SSL Proxy Compatibility Mode	Modern
DHParams Key Size	2048 (default) v DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.
CA	CA-ITCONNECT Select Certificate Authority to use when SSL interception is enabled.
SSL Certificate Deamon Children	This is the number of SSL certificate deamon children to start. May need to be increased in busy environments. Default: 5
Remote Cert Checks	Accept remote server certificate with errors Do not verify remote certificate Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.
Certificate Adapt	Sets the "Not After" (setValidAfter) Sets the "Not Before" (setValidBefore) Sets CN property (setCommonName) See sslproxy_cert_adapt directive documentation and Mimic original SSL server certificate wiki article for details.

Sauvegardez via le bouton en bas de page.

→ Installation de Squid Guard sur PfSense

L'installation de ce paquet sur **PfSense** passe par le menu habituel sous "System", puis "Package manager". Dans la section "Available Packages", recherchez "squid" et vous devriez voir le paquet Squid Guard apparaître. Il ne reste plus qu'à cliquer sur le bouton "Install".

	System 🗸	Interfaces 🛨	Firewall 🗕	Services -	VPN •	Status 🕶	Diagnostics				
System /	System / Package Manager / Package Installer										
pfSense-pkg-sq	uidGuard instal	lation successfull	y completed.								
Installed Packa	ges Availa	able Packages	Package Insta	ller							

Une fois que c'est fait, nous pouvons passer à la configuration via le menu "Services" où se trouve une entrée "SquidGuard Proxy Filter".

→ Configuration de Squid Guard sur PfSense

Pour le moment, on va s'intéresser à l'onglet **"General Settings"**. N'allez pas trop vite : ne cochez pas l'option **"Check this option to enable SquidGuard"** pour le moment, car il faut le **préconfigurer** avant de l'activer.

Sys	stem +	Interfaces +	Firewall +	Services +	VPN +	Status +	Diagnostics +	Help	•	¢
Package / Pro	oxy filter	SquidGua	rd: Genera	al settings ,	/ Genera	al settings	5			Θ
General settings	Common A	ACL Groups	ACL Tar	get categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync	
General Options										
Ena	ble Imp The To a	Check this option to enable squidGuard. mportant: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details. The Save button at the bottom of this page must be clicked to save configuration changes. To activate squidGuard configuration changes, the Apply button must be clicked. Apply								
	Squ	idGuard servi	ce state: STC	PPED						
LDAP Options										
Enable LDAP Fil	iter 🗆 E	nable options fo	r setup Idap cor	nnection to creat	e filters with	ldap search				
LDAP	DN Cont	figure your LDAP	DN (ex: cn=Adr	ninistrator,cn=Us	sers,dc=dom	ain)				

Cochez les deux options suivantes pour activer les **logs** : **"Enable GUI Log"** et **"Enable log"**.

Service options	
Rewrite process children	16 Maximum number of SquidGuard redirector processes that Squid may spawn. Using too few of these helper processes (a.k.a. "helpers") creates request queues. Using too many helpers wastes your system resources. (Default: 16)
Rewrite process children startup	8 Sets a minimum of how many SquidGuard processes are to be spawned when Squid starts or reconfigures. (Default: 8)
Rewrite process children idle	4 Sets a minimum of how many SquidGuard processes Squid is to try and keep available at all times. (Default: 4)
Logging options	
Enable GUI log	Check this option to log the access to the Proxy Filter GUI.
Enable log	Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.
Enable log rotation	Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.
Miscellaneous	
Clean Advertising	Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

Au sein de la section **"Blacklist"**, cochez l'option **"Check this option to enable blacklist"** afin d'activer l'utilisation d'une **blacklist**, c'est-à-dire une liste noire. Nous allons utiliser la **liste noire de L'Université Toulouse Capitole**, car elle est **française**, **fiable** et existe depuis plusieurs années. Elle contient de nombreuses **catégories** afin de répartir les sites et permettre un **blocage ciblé** selon certaines catégories.

Ensuite, renseignez l'option "Blacklist URL" avec l'URL suivante :

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Enfin, cliquez sur le bouton "Save".

Miscellaneous	
Clean Advertising	□ Check this option to display a blank gif image instead of the default block page. With this option the user ge
Blacklist options	
Blacklist	Check this option to enable blacklist
Blacklist proxy	
	Blacklist upload proxy - enter here, or leave blank. Format: host:[port login:pass] . Default proxy port 1080. Example: '192.168.0.1:8080 user:pass'
Blacklist URL	http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.
	Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or l your pfsense (/tmp/blacklist.tar.gz).
	Save

Maintenant, basculez sur l'onglet **"Blacklist"** de **SquidGuard**. Cliquez sur le bouton **"Download"** pour télécharger la dernière version de la **liste noire** que nous avons renseignée dans les **paramètres de SquidGuard**.

Package / S	quidGuard /	Blacklists						
General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	×
Blacklist Updat	t e progress							
<u>1 % http://dsi.ut-cap</u>	bitole.fr/blacklists/do	wnload/blacklists_	_for_pfsense.tar.gz					
Enter FTP or HTTP p	path to the blacklist a	rchive here.						
😣 Blacklist u	pdate Log							
Begin blacklist Start download.	update	anitole fr/blac	klists/download					
/blacklists_for	pfsense.tar.gz	ap10010.11, 5140						
Unpack archive								
Scan blacklist of Found 63 items	categories.							
Start rebuild DE	3.							
Completed 1 %								
				111.				

Afin d'exploiter la **liste noire**, nous devons créer des règles sous la forme d'ACL. Cliquez sur **"Common ACL"** afin de créer une règle de base et commune au sein de **Squid**, tandis que la section **"Groups ACL"** permet de créer des **ACL ciblées** avec plusieurs critères (par exemple : **"bloquer une catégorie selon une plage horaire spécifique"** ou **"bloquer une catégorie à tous les membres d'un groupe Active Directory"**).

Au sein du champ **"Target Rules List"**, vous avez la liste de toutes les **catégories récupérées** à partir de la **blacklist toulousaine**.

Package / Proxy	ckage / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL									
General settings	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	XMLRPC Sync			
General Options										
Target Rules	!blk_blacklists_adult !blk_black	klists_sexual_educatio	n all							
	ACCESS: 'whitelist' - always pa	ss; 'deny' - block; 'allow' 1	' - pass, if not	blocked.				access access	deny 	× ×
	[bik_blacklists_associa [bik_blacklists_associa [bik_blacklists_astrolo [bik_blacklists_audio-v [bik_blacklists_bank] [bik_blacklists_bitcon]	tions_religieuses] gy] ideo]						access access access access access access		× × × ×
	[blk_blacklists_blog] [blk_blacklists_celebrit [blk_blacklists_chat] [blk_blacklists_chat] [blk_blacklists_cleanin	y] g]						access access access access access	 	× × × ×
	[blk_blacklists_cooking [blk_blacklists_cryptoji [blk_blacklists_publicit [blk_blacklists_radio] [blk_blacklists_reaffec	u acking] e] ted]						access access access access access	 	× × × ×
	[bik_blacklists_remote [bik_blacklists_remote [bik_blacklists_residen [bik_blacklists_sect] [bik_blacklists_sexual_	control] tial-proxies] education]						access access access access access	 deny	× × × ×
	[bik_blacklists_shopp] [blk_blacklists_shorter [blk_blacklists_social [blk_blacklists_special [blk_blacklists_special	igi ier] networks]						access access access access access	 	~ ~ ~
	[blk_blacklists_stalker [blk_blacklists_strict_r [blk_blacklists_strong_ [blk_blacklists_transla [blk_blacklists_trichen]	vare] edirector] redirector] ion]						access access access access access		~ ~ ~
	[blk_blacklists_tricheu [blk_blacklists_update [blk_blacklists_update [blk_blacklists_warez]	pix]						access access access access access		* * *
	[blk_blacklists_webma Default access [all]	il]						access access	allow 🗸	~

Dans notre cas, nous devons bloquer la catégorie **"Pornographie"** correspondante à **"[blk_blacklists_adult]"** et

"[blk_blacklists_sexual_education]", il faut donc modifier la valeur du champ "access" pour préciser "deny".

En complément, pensez à configurer la valeur du champ **"Default access** [all]" sur **"allow"** pour autoriser toutes les autres catégories (par défaut).

Afin d'éviter qu'un petit malin contourne la restriction en précisant l'adresse **IP du serveur distant** à la place du nom de domaine, cochez l'option **"Do not allow IP-Addresses in URL"**.

En complément, si vous souhaitez utiliser la fonction **SafeSearch** des moteurs de recherche, cochez la case **"Use SafeSearch Engine"**, tout en sachant que cela permet d'utiliser **Google, Bing, DuckDuckGo, Qwant**, etc.

Do not allow IP- Addresses in URL	To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.
Proxy Denied Error	
	The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by \$g['product_name'] proxy"
Redirect mode	int error page (enter error message)
	Select redirect mode here. Note: If you use 'transparent proxy', then 'int' redirect mode will not accessible. Options:ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'.
Redirect info	
	Enter external redirection URL, error message or size (bytes) here.
Use SafeSearch engine	C Enable the protected mode of search engines to limit access to mature content.
	At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. Note: This option overrides 'Rewrite' setting.
Rewrite	none (rewrite not defined)
	Enter the rewrite condition name for this rule or leave it blank.

Enfin, activez les **logs** pour cette règle en cochant l'option **"Log"** tout en bas, puis cliquez sur **"Save"**.

Log	Check this option to enable logging for this ACL.
	Save

La configuration étant prête, retournez dans "General Settings", cochez l'option "Check this option to enable SquidGuard" et cliquez sur "Apply".

Package / Pr	roxy filter Squ	uidGuard: Ge	eneral settings	Genera	al settings	;		
General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	x
General Options								
En	The Save	his option to enab Please set up at le button at the b te squidGuard o	east one category on the pottom of this page i configuration chang	e 'Target Cate must be cli es, the App	gories' tab befo cked to save Iy button mu	ore enabling. Se configuratio Ist be clicke e	ee this link n change d.	for d
	SquidGu	ard service stat	e: STOPPED					

Le statut du service SquidGuard doit changer et passer sur "STARTED". Si ce n'est pas le cas, vérifiez que Squid a bien démarré de son côté.

Remarque importante : à chaque fois que vous modifiez la configuration de **SquidGuard** (exemple : bloquer une catégorie supplémentaire), il faut impérativement venir dans l'onglet **"General Settings"** pour cliquer sur le bouton **"Apply"** sinon les modifications ne sont pas prises en compte !

Package / Pro	oxy filter Squ	idGuard: Ge	eneral settings ,	Genera	al settings	;		
General settings	Common ACL	Groups ACL	Target categories	Times	Rewrites	Blacklist	Log	X
General Options	Ible Check t Important: The Save To activa	his option to enab Please set up at lo button at the b te squidGuard o	le squidGuard. east one category on the pottom of this page i configuration chang	e 'Target Cate must be cli es, the App	egories' tab befo cked to save bly button mu	ore enabling. Se configuratio ist be clicke e	ee this link n change 1.	for de



Pour tester si notre filtrage fonctionne correctement, on va devoir consulter des **sites pornographiques** pour voir si le **proxy bloque bien** le site :



Après avoir testé deux sites pornographiques différents, on voit que les sites se sont bien fait bloquer et sont inaccessibles.