

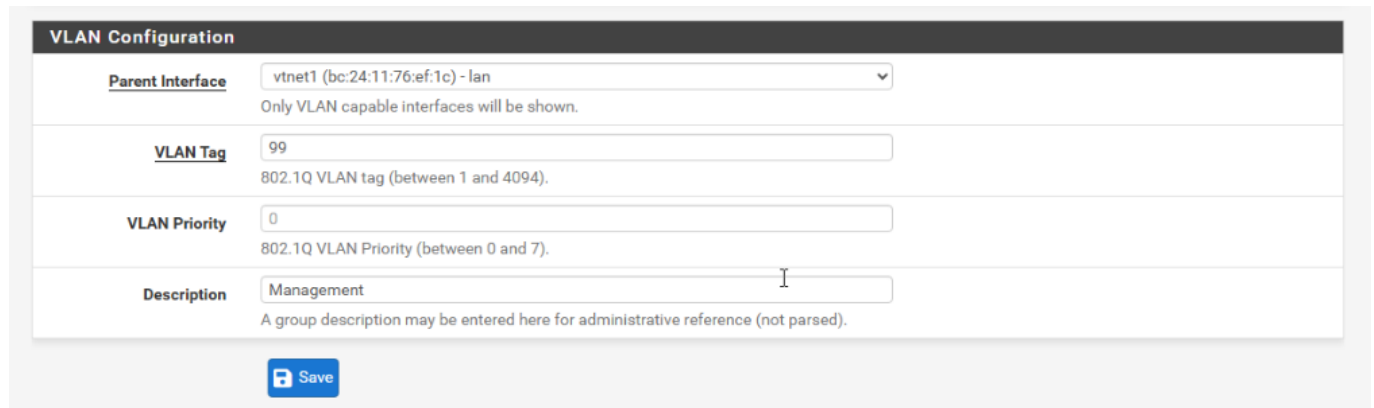
Sécurisation, supervision et services réseau - Proxmox

I - Cloisonnement et durcissement du réseau

I/I - VLAN Management

I/I/I - Création du VLAN Management

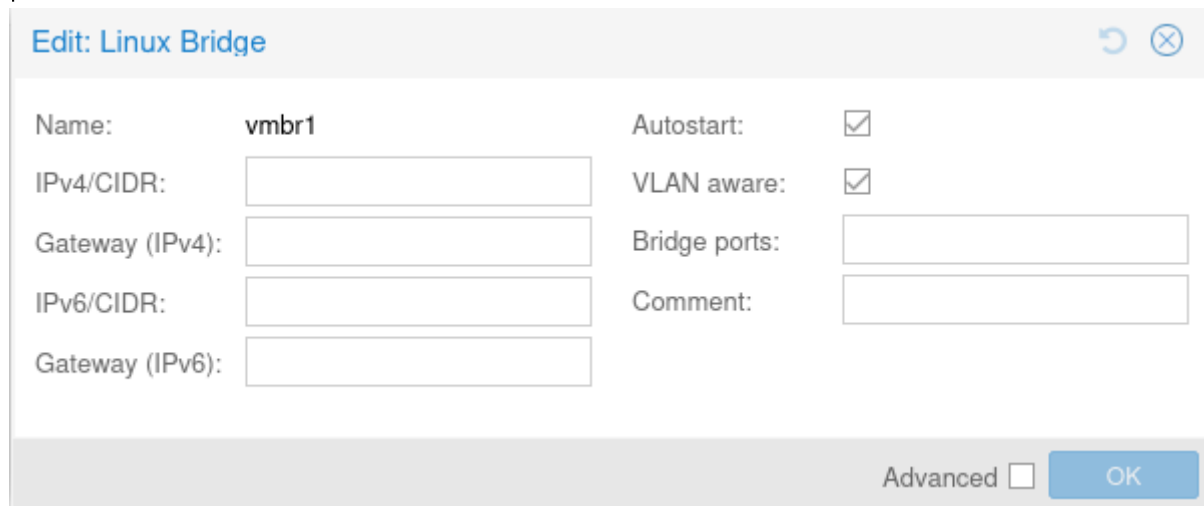
Tout d'abord, il va falloir créer une interface VLAN 99 qui va correspondre au VLAN Management, pour cela il va falloir aller sur: **Interfaces -> Assignements -> VLANs** puis cliquer sur **Add**.



The screenshot shows the 'VLAN Configuration' form in Proxmox. It has a dark header bar with the title 'VLAN Configuration'. Below it, there are four main sections, each with a label and a text input field. The first section is 'Parent interface' with a dropdown menu showing 'vtnet1 (bc:24:11:76:ef:1c) - lan'. Below this is a note: 'Only VLAN capable interfaces will be shown.' The second section is 'VLAN Tag' with a text input field containing '99'. Below this is a note: '802.1Q VLAN tag (between 1 and 4094)'. The third section is 'VLAN Priority' with a text input field containing '0'. Below this is a note: '802.1Q VLAN Priority (between 0 and 7)'. The fourth section is 'Description' with a text input field containing 'Management'. Below this is a note: 'A group description may be entered here for administrative reference (not parsed)'. At the bottom of the form is a blue 'Save' button with a floppy disk icon.

Après l'avoir configuré, clique sur **Save**.

Il ne faut pas oublier d'activer le support de VLANs sur l'interface *vmbr1* qui correspond à l'interface LAN. Pour cela il va falloir se rendre sur: **Datacenter -> pve -> System -> Network**. On clique sur l'interface *vmbr1*, puis sur le bouton **Edit** et on coche la case **VLAN aware**.



The screenshot shows the 'Edit: Linux Bridge' form in Proxmox. It has a light gray header bar with the title 'Edit: Linux Bridge' and two icons (refresh and close). Below it, there are two columns of fields. The first column contains: 'Name:' with the value 'vmbr1', 'IPv4/CIDR:', 'Gateway (IPv4):', 'IPv6/CIDR:', and 'Gateway (IPv6):'. The second column contains: 'Autostart:' with a checked checkbox, 'VLAN aware:' with a checked checkbox, 'Bridge ports:', and 'Comment:'. At the bottom right of the form is an 'Advanced' checkbox (unchecked) and an 'OK' button.

I/I/II - Configuration du VLAN Management sur pfSense

On se rend sur le pfSense puis on introduit l'option *1) Assign Interfaces* en tapant le chiffre 1. Le rendu final doit être le suivant:

```
The interfaces will be assigned as follows:

WAN   -> vtnet0
LAN   -> vtnet1
OPT1  -> vtnet2
OPT2  -> vtnet1.99

Do you want to proceed [yIn]? y
```

Ensuite il va falloir configurer l'adresse IP du VLAN Management. Pour cela il faut choisir l'option 2) *Set interface(s) IP address* en tapant le chiffre 2. Le rendu final doit être le suivant:

```
MANAGEMENT (opt2) -> vtnet1.99 -> v4: 192.168.99.1/24
```

I/I/III - Ajout d'une VM Windows Admin

On va créer une VM Windows 11 avec la configuration de la carte réseau suivante:

Edit: Network Device

Bridge:

vmbr1

Model:

Intel E1000

VLAN Tag:

99

MAC address:

BC:24:11:7D:52:AE

Firewall:

☒

Help

Advanced

☐

OK

Et la configuration IP suivante:

Attribution d'adresse IP :	Manuel
Adresse IPv4 :	192.168.99.10
Masque IPv4:	255.255.255.0
Passerelle IPv4 :	192.168.99.1

Pour communiquer avec notre passerelle, il va falloir créer la règle pare-feu suivante:

☐

5/12.08 MiB

IPv4 *

MANAGEMENT subnets

*

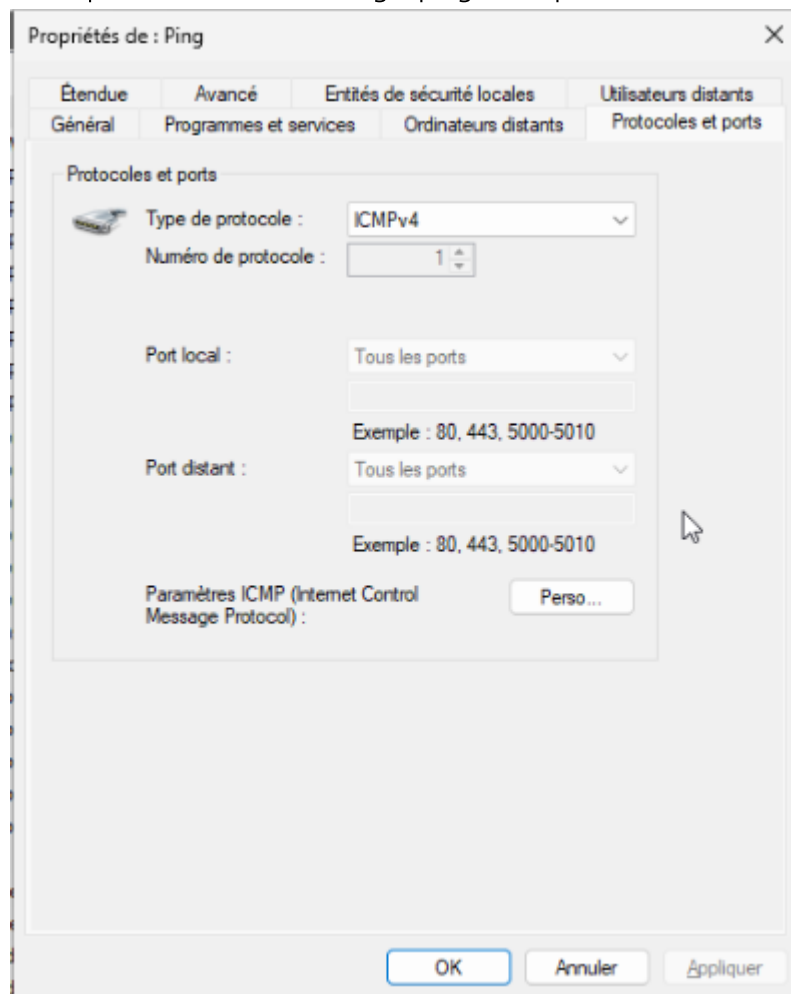
This Firewall (self)

*

*

none

Ainsi que la création d'une règle ping sur le pare-feu de la VM Admin:



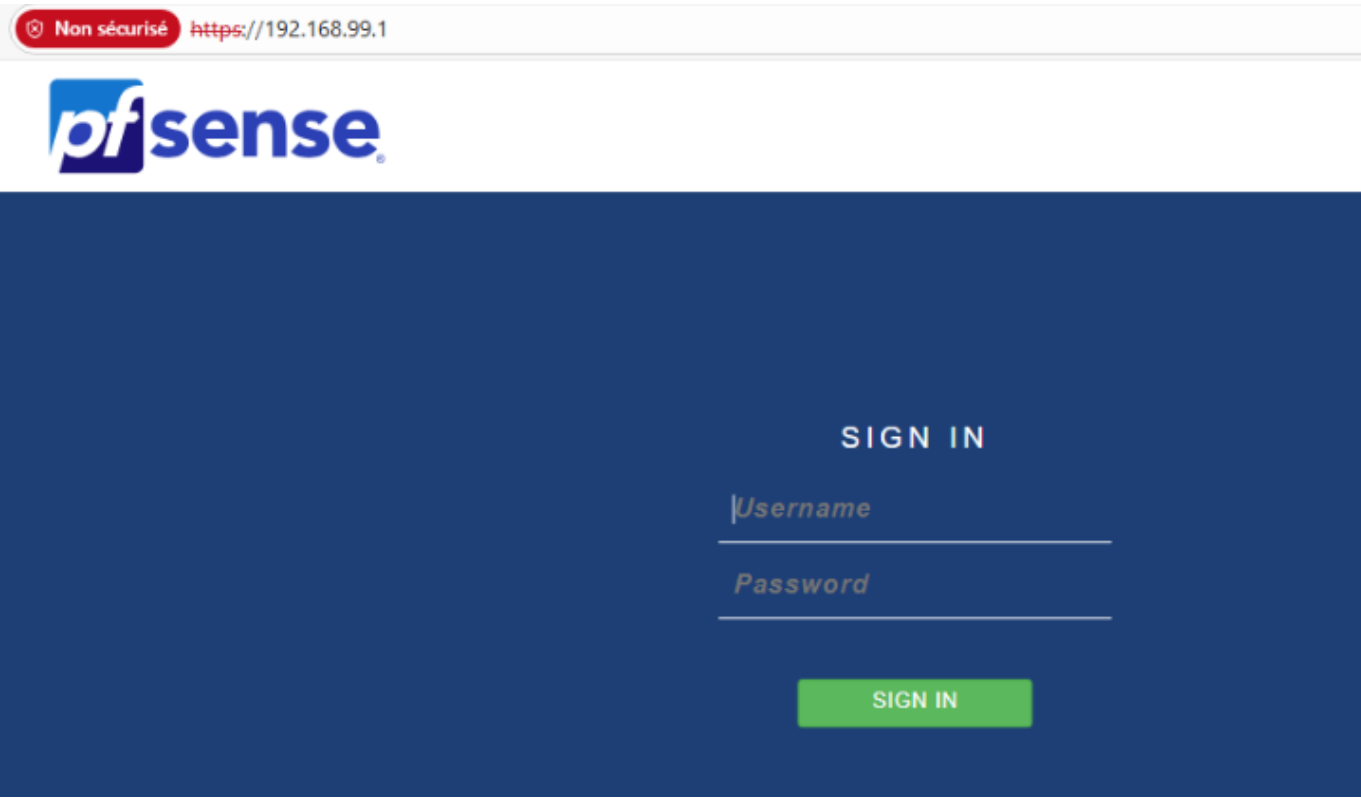
Test de Ping de la VM Admin vers sa passerelle par défaut:

```
C:\Users\Windows11-client>ping 192.168.99.1

Envoi d'une requête 'Ping' 192.168.99.1 avec 32 octets de données :
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.99.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Connexion à l'interface de configuration du pfSense:



I/I/IV - Configuration du pfSense pour limiter l'accès à lui-même

Sur pfSense :

- **System -> Advanced -> Admin Access**
- Activer uniquement HTTPS
- Limiter l'écoute à Management. Pour cela il va falloir créer des règles pare-feu sur toutes les interfaces sauf Management:

☐		0/0 B	IPv4 TCP	LAN subnets	*	This Firewall (self)	*	*	none
--------------------------	--	-------	----------	-------------	---	----------------------	---	---	------

- Désactiver HTTP et SSH pour les autres interfaces. Tout d'abord on crée l'Alias suivant. Pour cela il faut se rendre sur **Firewall -> Aliases -> Ports**:

Firewall Aliases Ports					
Name	Type	Values	Description		Actions
WEB_PORTS	Port(s)	80, 443			

Puis sur chaque interface, on crée les règles suivantes:

☐		0/0 B	IPv4 TCP	*	*	This Firewall (self)	WEB_PORTS	*	none	
☐		0/0 B	IPv4 TCP	*	*	This Firewall (self)	22 (SSH)	*	none	

Normalement, les autres appareils peuvent encore se connecter sur l'interface de configuration du pfSense. Pour régler ce problème il va falloir se rendre sur **System -> Advanced -> Admin Access**. Et on coche l'option suivante:

Anti-lockout

☒ Disable webConfigurator anti-lockout rule

When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

II - Mise en place d'un DNS local et d'un proxy

II/I - DNS local sur pfSense

Tout d'abord il va falloir activer le DNS Resolver (Unbound) depuis l'interface de configuration du pfSense. Puis on se rend sur **Services -> DNS Resolver** et on coche *Enable DNS Resolver*.

Ensuite, sur *Network Interfaces*, on va selectionner les interfaces LAN, MAnagement et Localhost.

Enfin, il faut cocher *Register DHCP leases in the DNS Resolver* et *Register DHCP static mappings in the DNS Resolver*.

Pour ajouter les enregistrements manuels, on se rend sur: **Services -> DNS Resolver -> onglet Hosts Overrides** et on ajoute les lignes suivantes:

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
pfsense	local	192.168.99.1		 
webdmz	local	192.168.2.100		 

II/II - Proxy Squid + filtrage SquidGuard

II/II/I - Installation de Proxy Squid

Pour installer Proxy Squid, il faut se rendre sur: **System -> Package Manager -> Available Packages** et on installe *squid* et *squidGuard*.

Installed Packages

Available Packages

Installed Packages

Name	Category	Version	Description	Actions
✓ squid	www	0.4.46	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:  squidclamav-7.2  squid_radius_auth-1.10  squid-6.3  c-icap-modules-0.5.5_1	  
✓ squidGuard	www	1.16.19	High performance web proxy URL filter. Package Dependencies:  squidguard-1.4_15  pfSense-pkg-squid-0.4.46	 

II/II/II - Configuration de Proxy Squid

Tout d'abord on se rend sur: **Services -> Squid Proxy Server** et on le configure de la façon suivante:

- Cocher *Enable Squid Proxy*.
- Cocher *Allow Users on interface*.
- Cocher *Transparent HTTP Proxy*.

- *Transparent Proxy Interface(s)* : LAN.

II/II/III - Configuration de SquidGuard

Tout d'abord on se rend sur: **Services -> SquidGUard Proxy Filter** et on le configure de la façon suivante:

- Cocher *Enable*.
- Cocher *Enable GUI log*.
- Cocher *Enable log*.
- Cocher *Blacklist* et renseigner l'url `http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz` dans la zone de texte *Blacklist URL*.
- Cliquer sur *Save*.
- Aller dans l'onglet **Services -> SquidGUard Proxy Filter -> Blacklist** et télécharger la blacklist `http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz` en appuyant sur *Download*.

Blocage de certains sites

Pour bloquer certaines catégories de sites Web, il va falloir se rendre sur **Services -> SquidGUard Proxy Filter -> Common ACL**. Puis on clique sur le +:



On va *deny* les catégories *social_networks*, *adult* et *malware*.

- Cocher *Do not allow IP-Addresses in URL* ainsi que *Log* puis *Save*.
- Redémarrer le service squid et squidGuard en allant dans **Status -> Services**.

Sur la VM client du LAN, on peut encore accéder à `http://facebook.com` même après avoir vidé le cache avec la commande `ipconfig /flushdns`. Pour le bloquer, il va falloir se rendre sur **Services -> DNS Resolver -> onglet Hosts Overrides** et on ajoute un nouveau avec la configuration suivante:

www	facebook.com	127.0.0.1	 
-----	--------------	-----------	---

Si on essaie d'accéder au site, cela ne fonctionnera pas.

III - Supervision et journalisation centralisée

III/I - Création d'une VM Debian

Tout d'abord, il faut créer une VM Debian sur le LAN avec la configuration suivante:

- Nom : Serveur-Logs
- Bridge : vmbr1
- Adresse IP : 192.168.1.20/24
- Passerelle : 192.168.1.1
- DNS : 192.168.1.1

III/II - Installation et configuration de rsyslog

Pour installer *rsyslog*, il faut utiliser la commande suivante `apt install rsyslog`.

Ensuite, on utilise la commande `nano /etc/rsyslog.conf` pour décommenter les lignes suivantes:

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

Et on redémarre `rsyslog` avec la commande `systemctl restart rsyslog` et `systemctl enable rsyslog`.

Il va falloir ensuite ouvrir le port 514 TCP et UDP sur le pfSense:



Configuration de pfSense pour envoyer ses logs

Tout d'abord il faut se rendre sur **Status -> System Logs -> Settings** et faire la configuration suivante:

- Cocher *Enable Remote Logging*.
- *Remote log servers* : 192.168.1.20/24.
- Sélectionner System Events, Firewall Events, VPN Events sur *Remote Syslog Contents*.
- *Save*.

On peut vérifier la réception sur la Debian avec la commande suivante `sudo tail -f /var/log/syslog`.

III/III - ntopng (supervision graphique)

Pour avoir une supervision graphique, on va utiliser le logiciel *ntopng*. Pour cela, il faut taper les commandes suivantes sur le serveur de logs:

```
get https://packages.ntop.org/apt/bullseye/all/apt-ntop.deb
apt install ./apt-ntop.deb
apt-get clean all
apt-get update
apt-get install ntopng
```

Pour accéder à cette interface, j'utilise l'URL `192.168.1.20:3000` sur la VM client sur le LAN.

IV - Sauvegarde, restauration et automatisation

IV/I - Activation du service SSH

Sur l'interface de configuration du pfSense, on se rend sur **System -> Advanced -> Admin Access** et on coche *Secure Shell Server*. Ensuite sur le pfSense, on choisit l'option `8) Shell` et on tape la commande suivante:

```
Enter an option: 8

[2.7.2-RELEASE][root@pfSense.hone.arpa]/root: pfSh.php playback svc restqrt ssh
d
```

Ensuite, on va créer une clé SSH et la copier sur l'entrée admin de 192.168.1.1, pour cela on va taper les commandes suivantes sur le serveur de logs:

```
ssh-keygen  
ssh-copy-id admin@192.168.1.1
```

On peut maintenant se connecter via SSH au pfSense:

```
root@debian12:~# ssh admin@192.168.1.1  
(admin@192.168.1.1) Password for admin@pfSense.home.arpa:  
QEMU Guest - Netgate Device ID: 2548397f117e269cb31d  
  
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.50.0.54/8  
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24  
DMZ (opt1)     -> vtnet2      -> v4: 192.168.2.1/24  
MANAGEMENT (opt2) -> vtnet1.99 -> v4: 192.168.99.1/24  
  
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) Disable Secure Shell (sshd)  
6) Halt system                15) Restore recent configuration  
7) Ping host                  16) Restart PHP-FPM  
8) Shell  
  
Enter an option: _
```

IV/II - Sauvegarde automatisée

Tout d'abord on crée le répertoire sur le serveur de logs avec la commande `mkdir /backup`. Puis la commande `crontab -e` et on tape la ligne suivante:

```
0 20 * * * scp admin@192.168.1.1:/cf/conf/config.xml /backup/pfsense-$(date +%F) .xml
```