

DynFi 3.0

Gérer les VLANs

MODULE 4

VLANs



DynFi[®]

DYNAMIC FIREWALLS

SOMMAIRE

- AJOUTER UNE INTERFACE RESEAU DANS DYNFI POUR LA GESTION DE VLAN :**
 - Ajout d'un nouveau VMBR dans Proxmox
 - Ajout de la nouvelle interface réseau dans DynFi
 - Création de "Linux VLAN" dans Proxmox
- CREATION ET PARAMETRAGE DE VLANS DANS DYNFI**
- PARAMETRAGE DES SERVICES DHCP DANS DYNFI**
- CONNEXION D'UNE MACHINE A UN VLAN PROXMOX ET GESTION DES REGLES DE PARE-FEU DANS LE VLAN**

© tutos-info.fr - 07/2024



DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

Note importante :

Pour réaliser ce tutoriel, vous devez avoir suivi les 3 premiers modules (voir sur <https://tutos-info.fr>), à savoir :

- création d'un routeur DynFi avec 2 interfaces réseau WAN + LAN
- un accès au routeur (soit depuis une machine du réseau LAN, soit depuis l'interface WAN)

Notre environnement de travail, ici, est Proxmox mais ce tutoriel est transposable à d'autres logiciels de virtualisation (Virtualbox, vmWare Player).

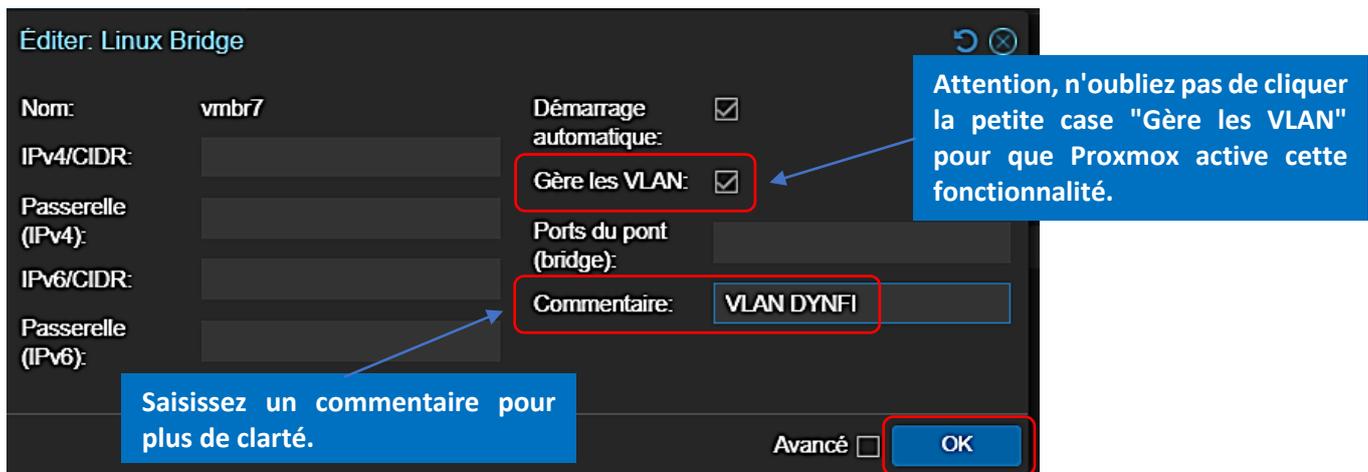
1 – AJOUTER UNE INTERFACE RESEAU A DYNFI 3.0 POUR LA GESTION DE VLANS

Dans ce tutoriel nous allons voir comment gérer des VLANs dans DynFi. Pour cela, on commence par **ajouter une nouvelle interface réseau à la machine virtuelle DynFi (depuis l'interface de Proxmox)** en effectuant les manipulations suivantes :

A – AJOUT D'UN NOUVEAU "VMBR" DANS PROXMOX POUR LA GESTION DU VLAN

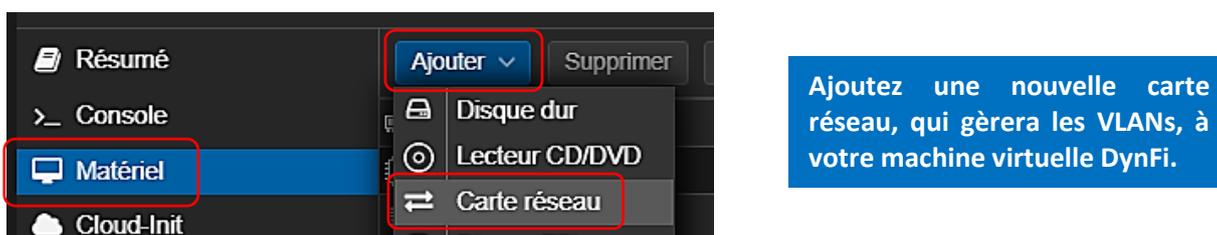
Depuis la console d'administration de Proxmox, effectuez les manipulations suivantes :

- Cliquez sur le **nom du nœud Proxmox**
- Cliquez, dans le volet de droite, sur **"Réseau"**
- Cliquez le bouton **"Créer"** - **"Linux Bridge"** ; complétez la fenêtre **en n'oubliant pas de cliquer la case "Gère les VLAN"** puis cliquez **"OK"** :



Une fois votre "vmbr" créé (repérez-le avec son numéro, ici nous avons "vmbr7"), ajoutez-le à votre machine virtuelle DynFi :

- Cliquez **sur le nom de votre machine virtuelle DynFi**
- Cliquez, dans le volet de droite, sur **"Matériel"** et cliquez le bouton **"Ajouter"**
- Cliquez **"Carte réseau"** :



- Sélectionnez le "vibr" (le "7" chez nous) que vous venez de créer et qui servira pour la gestion des VLANs
- Cliquez le bouton "Ajouter" :

Ajouter: Carte réseau

Pont (bridge): **vibr7** Modèle: VirtIO (paravirtualisé)

Étiquette de VLAN: aucun VLAN Adresse MAC: auto

Pare-feu:

Aide Avancé **Ajouter**

Votre machine virtuelle Dynfi comporte, désormais, 3 cartes réseau :

⇄ Carte réseau (net0)	virtio=52:54:00:01:14:03,bridge=vibr0	WAN
⇄ Carte réseau (net1)	virtio=BC:24:11:20:44:E9,bridge=vibr6	LAN
⇄ Carte réseau (net2)	virtio=BC:24:11:9F:A8:DE,bridge=vibr7	VLAN

Le "vibr0" est affecté à l'interface **WAN**

Le "vibr6" est affecté à l'interface **LAN**

Le "vibr7" est affecté à la gestion des **VLANs**

B – AJOUT DE LA NOUVELLE INTERFACE DANS DYNFI

- Connectez-vous à l'interface de gestion de DynFi
- Cliquez "Interfaces" – "Attribution" ; une fenêtre affiche la nouvelle interface réseau :

Interfaces: Attribution

Interface (ID)	Port réseau	
LAN (lan)	vtnet1 (bc:24:11:20:44:e9)	🗑️
WAN (wan)	vtnet0 (52:54:00:01:14:03)	🗑️
Nouvelle interface :	vtnet2 (bc:24:11:9fa8:de)	+
Description	<input type="text"/>	
		Sauvegarde

- Ici, la nouvelle interface réseau est reconnue sous le nom "vtnet2"
- Cliquez le bouton "+" sur fond bleu et le bouton "Sauvegarde" ; la fenêtre affiche les interfaces actives :

Interface (ID)	Port réseau	
LAN (lan)	vtnet1 (bc:24:11:20:44:e9)	🗑️
OPT1 (opt1)	vtnet2 (bc:24:11:9fa8:de)	🗑️
WAN (wan)	vtnet0 (52:54:00:01:14:03)	🗑️

- Modifiez le nom de la nouvelle interface qui est repérée, actuellement, sous le nom "**OPT1(opt1)**" **en cliquant sur "OPT1"** ; une fenêtre s'affiche :
 - Cliquez la case "**Activer l'interface**" (**important !**)
 - Saisissez un nom pour l'interface (par exemple "**VLAN1**") :

Interfaces: [OPT1]

Configuration de base aide complète

Activer Activer l'interface

Verrouiller Empêcher le retrait de l'interface

Équipement vtnet2

Description

- Cliquez le bouton "**Sauvegarde**" ; une nouvelle fenêtre s'affiche :

La configuration VLAN1 a été modifiée.
Vous devez appliquer les modifications pour qu'elles prennent effet.
Ne pas oublier d'ajuster la plage DHCP si besoin après application.

Appliquer les changements

- Cliquez le bouton "**Appliquer les changements**" ; votre interface destinée à la gestion d'un VLAN est maintenant assignée dans DynFi (en cliquant "**Interfaces**", vous verrez apparaître l'ensemble) :



Une interface supplémentaire "VLAN1" est maintenant attribuée dans DynFi. Elle gèrera les futurs VLANs.

A ce stade, nous devons éteindre notre routeur DynFi en cliquant, dans le menu "**Alimentation**" l'option "**Mise hors tension**" :



- Cliquez le bouton "**Oui**" pour valider l'extinction et patientez :

Alimentation: Mise hors tension

Are you sure you want to power off the system?

Oui Non

Stoppez le routeur DynFi afin qu'il puisse prendre en compte la configuration des VLANs Proxmox (voir pages suivantes).

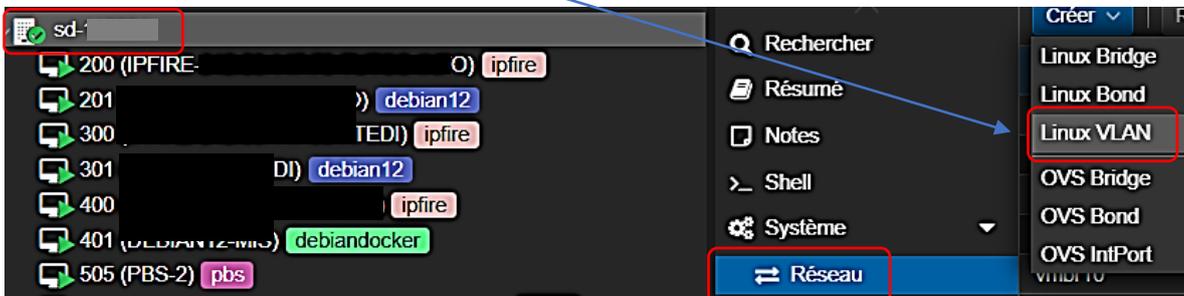
Votre appareil est en cours d'extinction

The system is powering off now.

C – CREATION DES "LINUX VLAN" DANS PROXMOX

Une fois le routeur DynFi éteint, il faut paramétrer, dans Proxmox, le "vmbr" qui servira pour les VLANs. Comme précédemment, nous allons ajouter une interface à notre Proxmox, mais il s'agit, cette fois, d'une interface de type « **Linux VLAN** ». Pour cela, depuis la console d'administration de Proxmox, procédez ainsi :

- Cliquez **sur le nom du nœud Proxmox**
- Cliquez, dans le volet de droite, "**Réseau**" et cliquez "**Créer**"
- Cliquez "**Linux VLAN**" :



- Saisissez les paramètres réseau souhaité pour votre VLAN et cliquez le bouton "**Créer**" :

- Cliquez le bouton "**Appliquer la configuration**"; le "**Linux VLAN**" apparaît dans la liste des réseaux :

vlan10	Linux VLAN	Oui	Oui
--------	------------	-----	-----

Assurez-vous que le VLAN est bien démarré et activé (sinon regardez si la petite case "Gère les VLAN a bien été cochée dans le vmbr).

- Créez un autre VLAN comme celui-ci par exemple :

- Cliquez le bouton "**Appliquer la configuration**" pour activer ce nouveau "**Linux VLAN**". Notre hyperviseur Proxmox présente maintenant nos 2 VLANs activés :

vlan10	Linux VLAN	Oui	Oui
vlan20	Linux VLAN	Oui	Oui

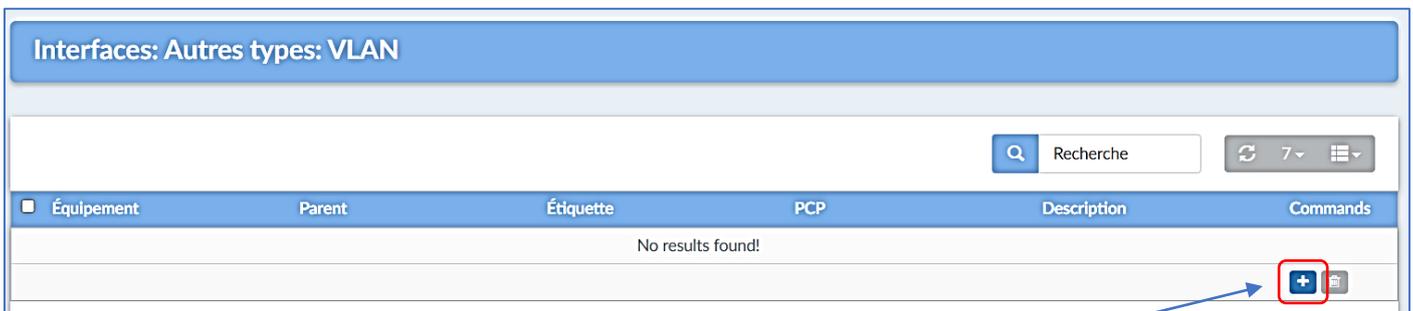
Assurez-vous que les VLANs soient bien démarrés et activés (sinon regardez si la petite case "Gère les VLAN a bien été cochée dans le vmbr).

Note : dans cette version de Proxmox (8.2), il n'est plus nécessaire de redémarrer l'hyperviseur pour que la gestion des VLANs soit prise en compte. En cochant la petite case "Gère les VLAN" lors de la création des "vmbr", Proxmox initialise la fonction après avoir cliqué l'option "Appliquer la configuration".

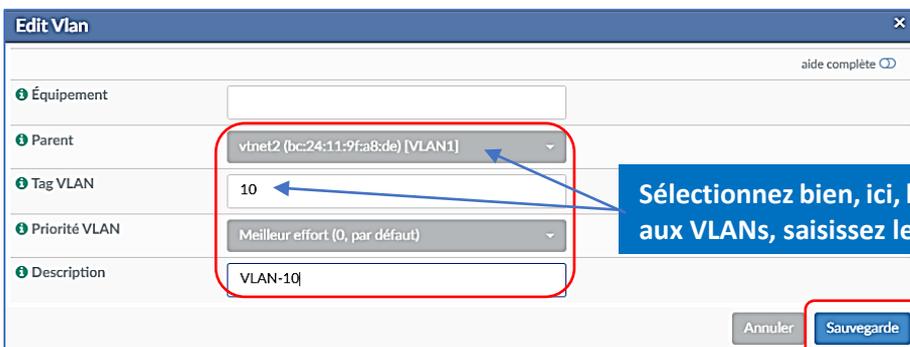
2 – CREATION DE VLANS DANS LE ROUTEUR DYNFI 3.0

Après avoir créé vos "**Linux VLAN**" dans Proxmox, effectuez les manipulations suivantes :

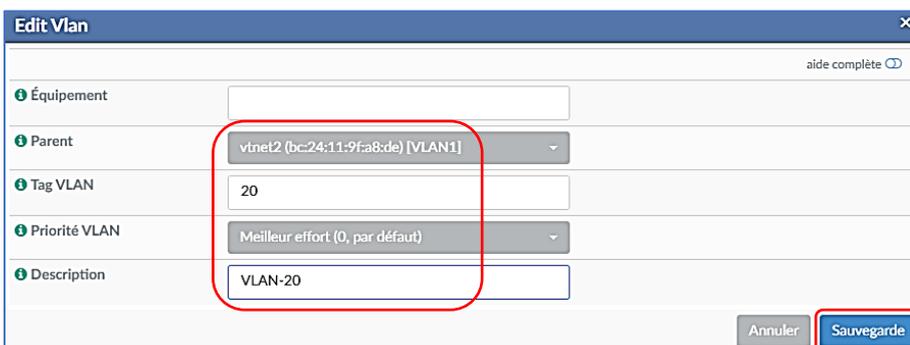
- Rallumez votre routeur DynFi
- Connectez-vous à l'interface de gestion de DynFi
- Cliquez "**Interfaces**" – "**Autres types**" et "**VLAN**"; une fenêtre s'affiche :



- Cliquez le petit "+" sur fond bleu en haut à droite de la fenêtre
- Configurez votre 1^{er} VLAN (ne vous trompez pas d'interface réseau !) et cliquez "**Sauvegarde**" :



- Créez le second VLAN de la même manière qu'avec le 1^{er} :



Les VLANS créés s'affichent ; cliquez le bouton "**Apply**" pour valider la création de vos VLANS :

Équipement	Parent	Étiquette	PCP	Description	Commands
<input type="checkbox"/> vlan01	vtnet2 (bc:24:11:9fa8:de) [VLAN1]	10	Meilleur effort (0, par défaut)	VLAN-10	
<input type="checkbox"/> vlan02	vtnet2 (bc:24:11:9fa8:de) [VLAN1]	20	Meilleur effort (0, par défaut)	VLAN-20	

Showing 1 to 2 of 2 entries

Apply

- Cliquez sur "**Interfaces**" – "**Attribution**"; une nouvelle interface apparaît :

Interface (ID)	Port réseau	
LAN (lan)	vtnet1 (bc:24:11:20:44:e9)	
VLAN1 (opt1)	vtnet2 (bc:24:11:9fa8:de)	
WAN (wan)	vtnet0 (52:54:00:01:14:03)	
Nouvelle interface :	vlan01 VLAN-10 (Parent : vtnet2, Tag : 10)	
	Description	

+

Sauvegarde

- Sélectionnez le 1^{er} VLAN avec l'étiquette "**vlan01 VLAN-10**" et cliquez le "+" sur fond bleu
- **Répétez l'opération avec le second VLAN** ; les VLANS sont maintenant identifiés :

Interface (ID)	Port réseau	
LAN (lan)	vtnet1 (bc:24:11:20:44:e9)	
OPT2 (opt2)	vlan01 VLAN-10 (Parent : vtnet2, Tag : 10)	
OPT3 (opt3)	vlan02 VLAN-20 (Parent : vtnet2, Tag : 20)	
VLAN1 (opt1)	vtnet2 (bc:24:11:9fa8:de)	
WAN (wan)	vtnet0 (52:54:00:01:14:03)	

Les 2 VLANS apparaissent sous le nom "OPT2" et "OPT3" ici.

Sauvegarde

- Cliquez le bouton "**Sauvegarde**"

Maintenant que les 2 VLANS sont attribués, nous allons les renommer afin qu'ils soient plus "lisibles" dans le routeur DynFi (voir pages suivantes).

- Cliquez sur "**OPT2**" afin de rendre le VLAN plus "visible" dans DynFi ; une fenêtre s'ouvre, complétez-la :

Interfaces: [OPT2]

Configuration de base aide complète

Activer	<input checked="" type="checkbox"/> Activer l'interface
Verrouiller	<input type="checkbox"/> Empêcher le retrait de l'interface
Équipement	vlan01
Description	VLAN-10

Activez l'interface et saisissez une description au VLAN.

Configuration générique

Bloquer les réseaux privés	<input type="checkbox"/>
Bloquer les réseaux factices	<input type="checkbox"/>
Type de configuration IPv4	Adresse IPv4 statique
Type de configuration IPv6	Aucun
Adresse MAC	
MTU	
MSS	
Mode promiscuité	<input type="checkbox"/>
Politique de passerelle dynamique	<input type="checkbox"/> Cette interface ne nécessite pas de système intermédiaire servant de passerelle

Activez "Adresse IPv4" statique ici.

Configuration adresse IPv4 statique

Adresse IPv4	192.168.10.254	24
Passerelle IPv4	Auto-détection	

Saisissez l'adresse IPv4 du VLAN avec le masque de sous-réseau souhaité.

Sauvegarde Annuler

- Cliquez le bouton "**Sauvegarde**" ; une fenêtre s'affiche ; cliquez "**Appliquer les changements**" :

Interfaces: [VLAN100]

La configuration VLAN100 a été modifiée.
Vous devez appliquer les modifications pour qu'elles prennent effet.
Ne pas oublier d'ajuster la plage DHCP si besoin après application.

Appliquer les changements

- Répétez l'opération avec l'autre VLAN ("**OPT3**") :

Interfaces: [OPT3]

Configuration de base aide complète

Activer	<input checked="" type="checkbox"/> Activer l'interface
Verrouiller	<input type="checkbox"/> Empêcher le retrait de l'interface
Équipement	vlan02
Description	VLAN-20

Activez l'interface et saisissez une description au VLAN.

Configuration générale

Bloquer les réseaux privés

Bloquer les réseaux factices

Type de configuration IPv4: Adresse IPv4 statique

Type de configuration IPv6: Aucun

Adresse MAC:

MTU:

MSS:

Mode promiscuité:

Politique de passerelle dynamique: Cette interface ne nécessite pas de système intermédiaire servant de passerelle

Configuration adresse IPv4 statique

Adresse IPv4: 192.168.20.254

Passerelle IPv4: Auto-détection

Saisissez l'adresse IPv4 du VLAN avec le masque de sous-réseau souhaité.

Sauvegarde Annuler

- Cliquez le bouton "Appliquer les changements" :

La configuration VLAN20 a été modifiée.
 Vous devez appliquer les modifications pour qu'elles prennent effet.
 Ne pas oublier d'ajuster la plage DHCP si besoin après application.

Appliquer les changements

Vous devez avoir, maintenant, dans le menu "Interfaces" ceci :

Interfaces

[LAN]

[VLAN1]

[VLAN10]

[VLAN20]

[WAN]

Nos deux VLANs sont maintenant assignés et s'affichent dans les interfaces DynFi.

3 – PARAMETRAGES DES SERVICES DHCP POUR CHAQUE VLAN

Maintenant que nos 2 VLANs sont créés dans DynFi, nous allons mettre en place un serveur DHCP pour chaque VLAN. Ce dernier distribuera des adresses dynamiques aux machines qui se connecteront à l'un ou l'autre des VLANs. Pour cela, depuis l'interface de gestion de DynFi, effectuez les manipulations suivantes :

- Cliquez "Services" – "DHCPv4"
- Cliquez sur le nom de votre 1^{er} VLAN (VLAN10) ; une fenêtre s'ouvre, complétez-la :

Activer: Activer le serveur DHCP sur l'interface VLAN10

Refuser les clients inconnus:

Ignorer les UID des clients:

Sous-réseau: 192.168.10.0

Masque de sous-réseau: 255.255.255.0

Plage disponible: 192.168.10.1 - 192.168.10.254

Plage: 192.168.10.10 192.168.10.100

Saisissez l'adresse IPv4 du VLAN avec le masque de sous-réseau souhaité.

Étendues supplémentaires	Groupes d'adresses	Paramètres
Si vous avez besoin de groupes d'adresses supplémentaires à l'intérieur de ce sous-réseau en dehors de la plage ci-dessus, ils peuvent être spécifiés ici.		
1 Serveurs WINS	<input type="text"/> <input type="text"/>	Laissez ces options par défaut pour le moment.
2 Serveurs DNS	<input type="text"/> <input type="text"/>	
3 Passerelle	<input type="text"/>	Laissez un blanc pour utiliser les serveurs DNS par défaut du système : Cette adresse IP d'interface si un service DNS est activé ou les serveurs DNS globaux configurés.
4 Nom de domaine	<input type="text"/>	Par défaut, l'IP de cette interface du pare-feu est utilisée comme passerelle, si une passerelle (en ligne) valide a été configurée sous Système->Passerelles. Indiquez ici une autre passerelle si ce n'est pas la bonne passerelle pour votre réseau. Tapez "none" pour aucune attribution de passerelle.
5 Liste de domaine de recherche	<input type="text"/>	La valeur par défaut consiste à utiliser le nom de domaine de ce système comme nom de domaine par défaut fourni par DHCP. Vous pouvez spécifier un autre nom de domaine ici.
6 Durée par défaut du bail (secondes)	<input type="text"/>	Le serveur DHCP peut fournir en option une liste de domaines de recherche (séparateur de liste est le caractère point-virgule)
7 Durée maximum du bail (secondes)	<input type="text"/>	Ceci est utilisé pour les clients qui ne demandent pas une limite d'expiration spécifique. La valeur par défaut est de 7200 secondes.
8 Délai de réponse (secondes)	<input type="text"/>	Ceci est la durée maximale du bail pour les clients qui demandent une heure d'expiration spécifique. La valeur par défaut est 86400 secondes.
9 MTU de l'interface	<input type="text"/>	Il s'agit du nombre minimum de secondes depuis qu'un client a essayé d'acquiescer un nouveau bail avant que le serveur DHCP ne réponde à sa demande. La valeur par défaut est 0 seconde (pas de délai).
10 IP de redondance :	<input type="text"/>	Cette option spécifie le MTU à utiliser sur cette interface. La valeur légale minimale pour le MTU est de 68.
11 Répartition du basculement :	<input type="text"/>	Laissez un blanc pour désactiver. Entrez l'adresse IP de l'interface de l'autre machine. Les machines doivent utiliser CARP. L'adskew de l'interface détermine si le processus DHCPd est primaire ou secondaire. Assurez-vous que l'adresse IP d'une machine est inférieure à 20 (et que l'autre est supérieure à 20). Notez que changer cette valeur effacera la base de données des baux en cours !
12 ARP Statique	<input type="checkbox"/> Activer les entrées ARP statique	Avertissement : Cette option persiste même si le serveur DHCP est désactivé. Seules les machines énumérées ci-dessous seront en mesure de communiquer avec le pare-feu sur cette carte réseau.
13 Format de la date et l'heure	<input type="checkbox"/> Modifier l'heure de bail d'affichage DHCP de l'heure UTC à l'heure locale.	Avertissement : Par défaut, les baux DHCP sont affichés en heure UTC. En cochant ce cas, l'heure du bail DHCP sera affichée en heure locale et définie sur le fuseau horaire sélectionné. Ceci sera utilisé pour toutes les durées de bail des interfaces DHCP.

Attention, il n'est pas possible de tout expliquer dans ce 1^e tutoriel. Laissez les options complémentaires vides pour le moment.

- Cliquez le bouton "**Sauvegarde**" (en bas de la fenêtre de configuration)
- Vérifiez que le statut de votre serveur DHCP est bien actif (**flèche verte**) :



Activez les services DHCP pour le VLAN20 en répétant l'opération. Il est temps de passer aux tests qui permettront de voir si une machine, connectée à un VLAN reçoit bien une adresse IP dynamique.

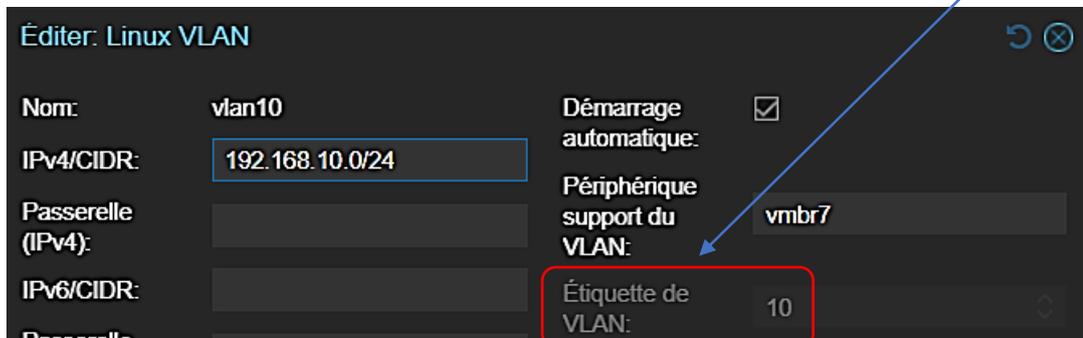
4 – CONNEXION D'UNE MACHINE A UN VLAN PROXMOX ET GESTION DES REGLES DANS LE VLAN

Pour effectuer nos tests, nous allons nous servir d'une machine virtuelle Debian que nous connecterons au VLAN adéquat depuis Proxmox.

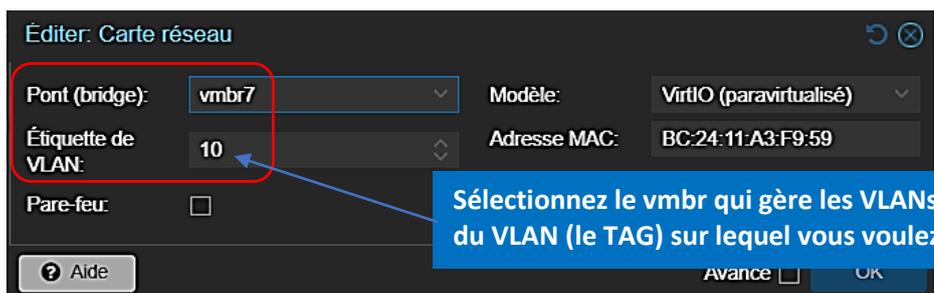
Pour cela, vous devez soit créer une nouvelle machine virtuelle Debian ou vous servir d'une machine existante (ce sera notre cas ici).

- Connectez-vous à l'interface de gestion de Proxmox
- Arrêtez la machine Debian si nécessaire

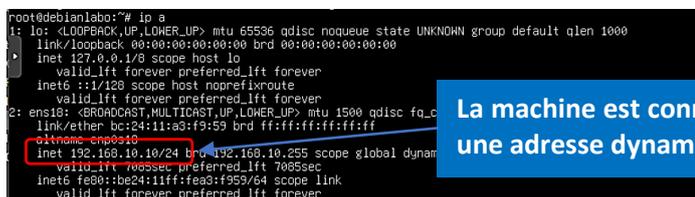
Attention, notez le bon "tag" du VLAN avant de procéder ! Si vous ne voulez pas vous tromper, double-cliquez sur le "vibrX" gérant les VLANs dans Proxmox (le "7" chez nous) et notez le "tag" :



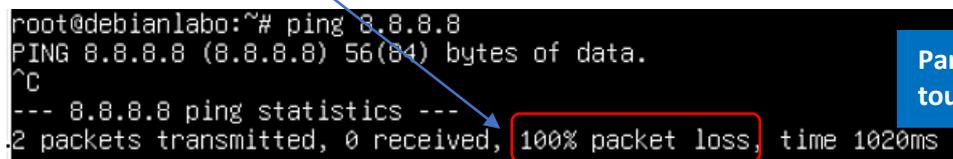
- Cliquez sur le nom de votre machine virtuelle Debian
- Cliquez "Matériel" et sélectionnez le **VMBR** qui gère vos VLANs en faisant bien attention de lui affecter le bon "tag" VLAN comme ceci :



- Faites démarrer la machine Debian et loguez-vous en "root" ou avec un utilisateur
- Saisissez la commande suivante "ip a" pour vérifier l'adresse dynamique reçue par la machine ; on constate, ici, que la machine a bien reçu une adresse IP dynamique dans le réseau "VLAN-10", à savoir 192.168.10.10/24 (1^{ère} adresse dynamique de l'étendue DHCP) :



- Faites un test de "ping" vers "8.8.8.8" avec la commande "ping 8.8.8.8" ; un problème est détecté puisqu'il y n'a pas de connexion vers Internet :



Ce problème est logique puisqu'aucune règle de pare-feu n'a été définie sur le VLAN-10. Pour vous en convaincre, faites ceci :

- Cliquez "Pare-feu" – "VLAN10" ; vous constatez qu'il n'y a aucune règle :

Pare-feu: Règles: VLAN10

Par défaut, DynFi bloque tous les flux sur le VLAN.

Sélectionnez une catégorie

Inspecteur

Log

Aucune règle de VLAN10 n'est actuellement définie. Toutes les connexions entrantes sur cette interface seront bloquées jusqu'à ce que vous ajoutiez une règle de passage. Des exceptions pour les règles générées automatiquement peuvent s'appliquer.

Protocole	Source	Port	Destination	Port	Passerelle	Planificateur	Description
autorisateur	bloquer	rejetter	rejetter	tracur	Entran		première correspondance
passer (désactivé)	bloquer (désactivé)	rejetter (désactivé)	rejetter (désactivé)	tracur (désactivé)	Sortant		dernière correspondance

- Créez la règle basique suivante pour le "VLAN10" (surtout pas en production !):

Éditer la règle du pare-feu

Nous créons, ici, une règle basique afin de vous faire comprendre pourquoi les flux ne passaient pas jusqu'à présent. Cette règle n'est pas à reproduire en production !

Action: Accepter

Désactivé: Désactiver cette règle

Rapide: Appliquer l'action immédiatement sur la correspondance.

Interface: VLAN10

Direction: in

Version TCP/IP: IPv4

Protocole: any

Source / Inverseur:

Source: tous

Source: Avancés

Destination / Inverseur:

Destination: tous

i Plage de ports de destination de :
 tous

i Log Enregistrer les paquets concernés par cette règle

i Catégorie

i Description

Fonctionnalités avancées

i Source OS Tous

i Pas de Sync XMLRPC

i Planificateur aucun(e)

i Passerelle défaut

Options avancées

Afficher/Masquer

Sauvegarde Annuler

- Cliquez le bouton "**Sauvegarde**" ; vous obtenez la règle suivante :

Pare-feu: Règles: VLAN10

Sélectionnez une catégorie

Inspecteur Log

	Protocole	Source	Port	Destination	Port	Passerelle	Planificateur	Description	
								Règles auto-générées	3
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	*		
<input type="checkbox"/>	autorisateur	bloquer	rejeter	tracur	→	Entran	première correspondance		
<input type="checkbox"/>	passer (désactivé)	bloquer (désactivé)	rejeter (désactivé)	tracur (désactivé)	←	Sortant	dernière correspondance		

- Cliquez le bouton "**Appliquer les modifications**" pour que la règle soit activée
- Faites, à nouveau, un test de ping ; vous constaterez que les flux sont autorisés sur le VLAN-10 et que le test de ping est valide :

```
root@debianlabo:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=1.55 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=1.61 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=1.77 ms
```

La règle s'est appliquée et les flux sont maintenant autorisés dans le VLAN.

Attention, il s'agit ici d'un test de laboratoire. Bien entendu, ne laissez pas cette règle "portes ouvertes" en production ! Il sera nécessaire d'appliquer des règles de sécurité plus strictes par la suite !

- Arrêtez la machine Debian avec la commande "init 0". Depuis l'interface de gestion de Proxmox, connectez la machine au VLAN portant le tag "20" comme ci-dessous :



- Redémarrez la machine Debian et vérifiez que l'adresse dynamique obtenue est bien celle allouée par le serveur DHCP du vlan-20, c'est-à-dire de type 192.168.20.xx/24 :

```
root@debianlabo:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether bc:24:11:a3:f9:59 brd ff:ff:ff:ff:ff:ff
  altname enp0s18
  inet 192.168.20.10/24 brd 192.168.20.255 scope global dynamic noprefixroute
    valid_lft 7068sec preferred_lft 7068sec
  inet6 fe80::be24:11ff:fea3:f959/64 scope link
    valid_lft forever preferred_lft forever
```

La machine est connectée au VLAN 20 et a bien reçu une adresse dynamique du serveur DHCP VLAN 20.

- Faites un test de ping de 8.8.8.8 ; vous constaterez que le ping n'aboutit pas étant donné qu'aucune règle de pare-feu n'a été créée au niveau du VLAN-20 :

```
root@debianlabo:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

Par défaut, DynFi bloque tous les flux sur le VLAN.

Par défaut, DynFi bloque tout le trafic au niveau du VLAN-20 :

Protocole	Source	Port	Destination	Port	Passerelle	Planificateur	Description
Règles auto-générées							
autorisateur	bloquer		rejeter		traceur		Entran
passer (désactivé)	bloquer (désactivé)		rejeter (désactivé)		tracer (désactivé)		Sortant

Pour que le test de ping fonctionne, il faudra autoriser les flux au niveau du VLAN-20 comme nous l'avons fait précédemment avec le VLAN-10 :

```
root@debianlabo:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4102ms

root@debianlabo:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=1.72 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=1.50 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=1.66 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=1.50 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
```

La règle s'est appliquée et les flux sont maintenant autorisés dans le VLAN.

Attention, il s'agit ici d'un test de laboratoire. Bien entendu, ne laissez pas cette règle "portes ouvertes" en production ! Il sera nécessaire d'appliquer des règles de sécurité plus strictes par la suite !