



# CONFIGURATION DE PFSENSE POUR LA SÉCURISATION ET LE FILTRAGE RÉSEAU

Encadrer par Touihri Ayoub





# PLAN

## de la présentation

01 *Contexte et Objectifs du Projet*

02 *Présentation de NTS Info*

03 *Problématique et objectifs du projet*

04 *Configuration des Aliases pour Gérer le Réseau*

05 *Routage inter-VLAN*

06 *Limitation de Bande Passante pour le VLAN Guest*

07 *Configuration d'un VLAN*

08 *Les méthodes de blocage des sites web*

09 *Conclusion et questions.*



01

## *Contexte du projet*

L'objectif était de concevoir et configurer un réseau sécurisé avec pfSense, en implémentant une segmentation via des VLANs et un filtrage des sites web non professionnels pour optimiser la sécurité et la productivité.





02

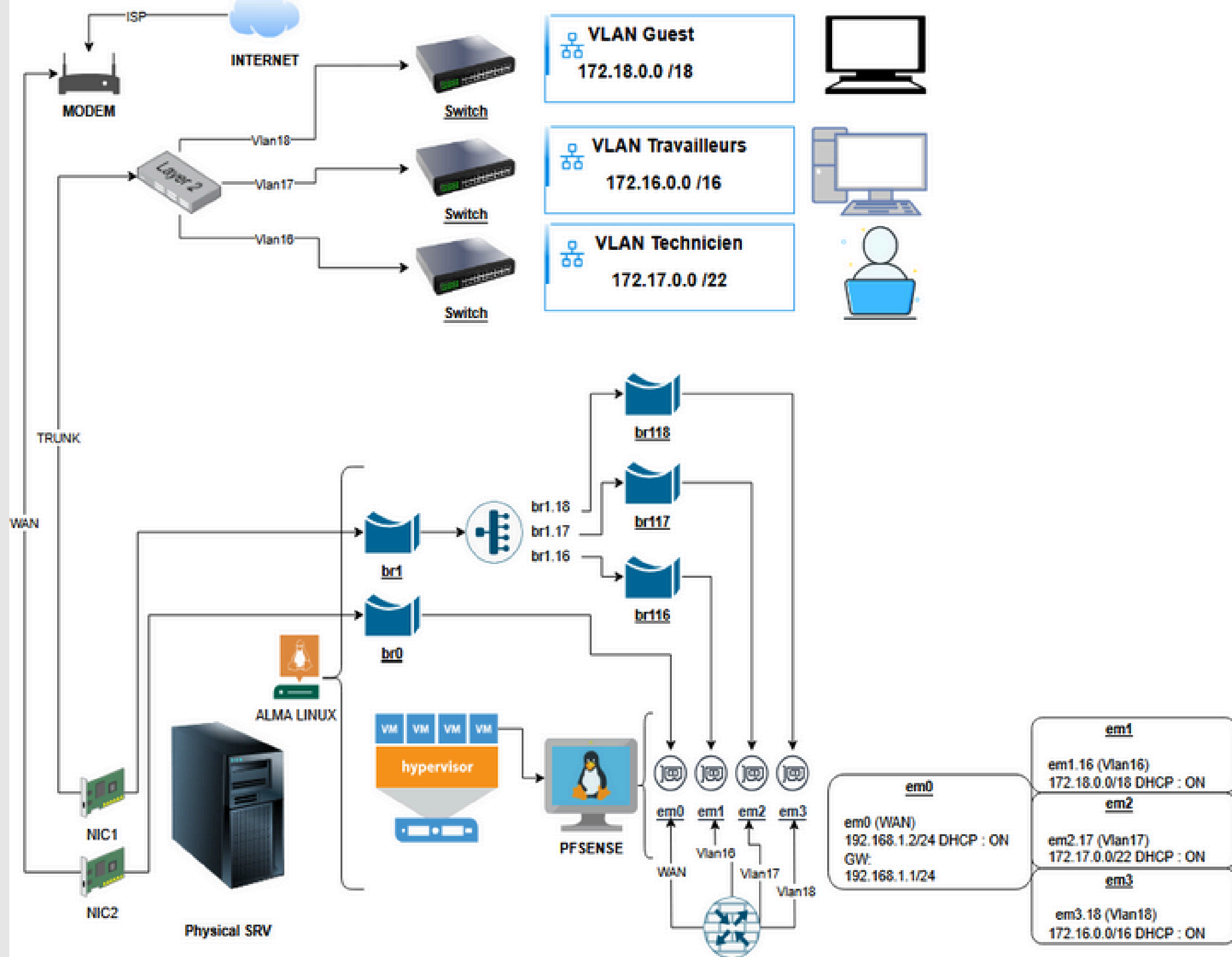
## *Présentation de NTS info*

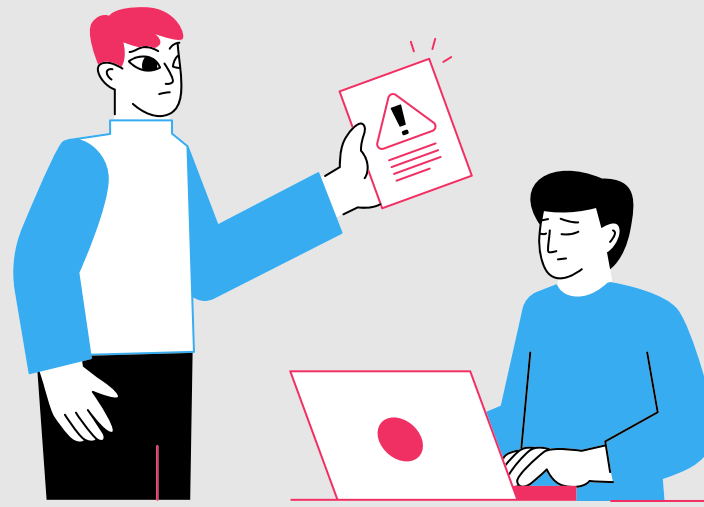
New Technology Services Info (NTS), fondée en 2018 et basée à Ezzahra, est une entreprise spécialisée dans les solutions réseau, la sécurité informatique et le support technique. Elle mise sur des outils open-source comme pfSense pour offrir des solutions performantes et économiques à ses clients.



*Architecture  
cibler*

La première version du réseau a été conçue avec trois blocs distincts, chacun représentant un groupe d'utilisateurs ou de services (ex. : Administrateurs, Techniciens, Travailleurs).





## Problématique

Mise en place d'un réseau initialement composé de trois blocs (puis étendu à quatre), avec des besoins spécifiques :











- \* Isolation ou communication contrôlée entre les blocs.
- \* Centralisation de la sécurité via un pare-feu robuste.
- \* Restriction d'accès à des sites web non professionnels pour limiter les distractions et protéger le réseau.



## Objectifs

- \* Concevoir une architecture réseau sécurisée et segmentée.
- \* Configurer pfSense pour gérer le trafic et appliquer des règles de filtrage.
- \* Tester et valider l'efficacité des solutions mises en œuvre.



IP Ports URLs All				
Firewall Aliases IP				
Name	Type	Values	Description	Actions
VLAN_Guest	Network(s)	172.18.0.0/18	VLAN des Guests	  
VLAN_Technicien	Network(s)	172.17.0.0/22	VLAN des Technicien	  
VLAN_Travailleurs	Network(s)	172.16.0.0/16	VLAN des Travailleurs	  
				 Add  Import

## 04

# Configuration des Aliases pour Gérer le Réseau

Les alias dans pfSense regroupent des adresses IP, ports ou réseaux sous un nom unique, simplifiant la gestion du filtrage et du routage. J'ai associé chaque VLAN à un alias (ex. VLAN\_Technicien), permettant de définir des règles de pare-feu et des routes de manière centralisée. Cette approche a amélioré la clarté des configurations et réduit les erreurs lors des ajustements.



\* Le routage inter-VLAN est géré via des règles de pare-feu dans pfSense. Les alias (ex. VLAN\_Technicien) ciblent des sous-réseaux pour autoriser/bloquer le trafic. Exemple : L'image montre une règle permissive pour le VLAN Guest (any destination), illustrant la flexibilité du routage.

\* L'ordre des règles et les alias simplifient la maintenance.

Firewall / Rules / Edit

### Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	Any Choose which IP protocol this rule should match.

### Source

Source	<input type="checkbox"/> Invert match	Address or Alias	VLAN_Guest	/	
--------	---------------------------------------	------------------	------------	---	--

### Destination

Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	
-------------	---------------------------------------	-----	---------------------	---	--



## Limitation de Bande Passante pour le VLAN Guest

Pour maintenir la stabilité du réseau, j'ai configuré un limiteur de bande passante dans pfSense via le module Traffic Shaper. Ce limiteur restreint le VLAN Guest à 10 Mbps, empêchant la saturation du réseau par des usages non prioritaires. Tout en allouant équitablement les ressources restantes. Cette approche garantit des performances optimales pour les services critiques, même lors des pics d'utilisation.

Firewall / Traffic Shaper / Limiters

By Interface By Queue **Limiters** Wizards

**+ New Limiter**

**Limiters**

**Enable** ☒ Enable limiter and its children

**Name** Limiteur VLAN Guest

**Bandwidth**

Bandwidth	Bw type	Schedule
10	Mbit/s	none

**+ Add Schedule**

**Mask** None

If 'source' or 'destination' slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet.

32 128

IPv4 mask bits IPv6 mask bits

255.255.255.255/? ::::: ::::: ::::: ::::: ::::: ::::: ::::: :::::/?

**Description** Limiteur Download/Upload pour le VLAN Guest

A description may be entered here for administrative reference (not parsed).

**In / Out pipe** Limiteur\_VLAN\_Guest Limiteur\_VLAN\_Guest\_

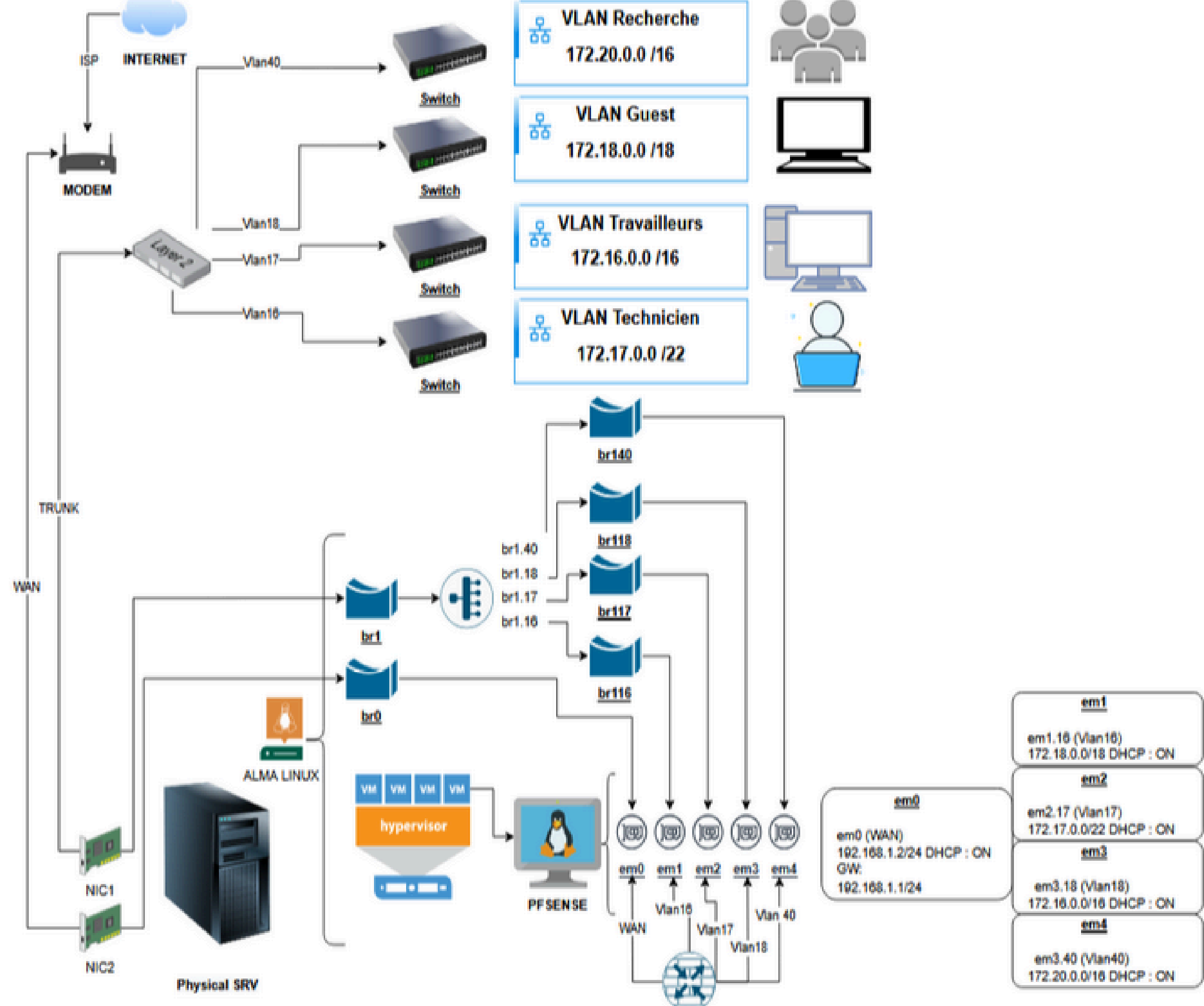
Choose the Out queue/Virtual interface only if In is also selected. The Out selection is applied to traffic leaving the interface where the rule is created, the In selection is applied to traffic coming into the chosen interface.  
If creating a floating rule, if the direction is In then the same rules apply, if the direction is Out the selections are reversed, Out is for incoming and In is for outgoing.

**Ackqueue / Queue** none none

Choose the Acknowledge Queue only if there is a selected Queue.

*Architecture  
Finale*

L'ajout du VLAN Recherche nécessite une isolation des activités sensibles via des règles de pare-feu strictes bloquant tout accès non autorisé depuis les autres VLANs. La segmentation réseau a été renforcée par un routage contrôlé via pfSense, limitant les communications inter-VLANs aux flux essentiels.





## 07

# Configuration d'un VLAN

### Réalisation




Le VLAN Recherche isole le trafic sensible de l'équipe de recherche des autres segments réseau, offrant une sécurité renforcée.

J'ai principalement configuré ce VLAN dans pfSense ,les autres VLANs (Administrateurs, etc.) étaient supposés déjà mis en place ou repris tels quels.

Sur pfSense, j'ai ensuite assigné une plage d'adresses IP, activé le DHCP et défini des règles de filtrage spécifiques pour le VLAN Recherche.

Interfaces / VLANs / Edit

### VLAN Configuration

<u>Parent Interface</u>	em2 (00:0c:29:4a:d7:78)  <b>L'interface a utiliser</b>
	Only VLAN capable interfaces will be shown.
<u>VLAN Tag</u>	40  <b>Tag / trunk</b>
	802.1Q VLAN tag (between 1 and 4094).
<u>VLAN Priority</u>	7  <b>Priorité QoS</b>
	802.1Q VLAN Priority (between 0 and 7).
<u>Description</u>	VLAN des Recherches
	A group description may be entered here for administrative reference (not parsed).

- Parent Interface : Port physique (em2) utilisé pour le VLAN.
- VLAN Tag : Identifiant unique (40) pour séparer le trafic.
- Priorité QoS : Niveau maximal (7) pour prioriser le trafic critique.
- Description : Étiquette administrative (VLAN des Recherches).

# Bloquer

Une règle de pare-feu pour bloquer l'accès depuis tous les VLAN Internes vers VLAN Recherche.

Action

Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

RECH

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

RECH subnets

Source Address

Destination

Destination

☐ Invert match

Address or Alias

VLAN\_

VLAN\_Technicien

VLAN\_Travailleurs

VLAN\_Guest

VLAN\_Internes

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, you may run out of space.

Action

Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Address or Alias

VLAN\_Internes

Destination

Destination

☒ Invert match

RECH subnets

Destination Address

# Passer

Une règle de pare-feu pour le VLAN Recherche pour permettre l'accès à tous les VLAN internes.



## *DNS et DHCP*



### **DNS Resolver**

Le DNS Resolver (Unbound) a été préféré pour sa sécurité : DNSSEC valide l'authenticité des réponses DNS, tandis que SSL/TLS chiffre les requêtes pour éviter les interceptions. Le blocage des serveurs DNS externes force les utilisateurs à utiliser le DNS interne, empêchant le contournement des règles de filtrage.



### **DHCP**

Le service DHCP intégré à pfSense a été configuré pour attribuer automatiquement des adresses IP aux appareils des VLANs (plage : 172.20.0.50 - 172.20.255.254). Cette automatisation simplifie la gestion des connexions et évite les conflits d'adresses, tout en centralisant la configuration réseau.



## 08

# Les méthodes de blocage des sites web

### Blocage par règles et alias

**Princ:** Créer un alias regroupant les domaines ou IP à bloquer, puis appliquer une règle de pare-feu qui interdit le trafic vers ces alias.

**Avn:** Facile à mettre en place, interface intégrée à pfSense.

**Lim:** Moins efficace pour les sites qui changent souvent d'IP ou utilisent des sous-domaines multiples (ex. Facebook).

### Filtrage DNS par Domain Override

Rediriger les requêtes DNS pour certains noms de domaine vers une IP non routable ou locale, empêchant l'accès réel au site.

Simple à configurer via l'onglet « DNS Resolver » ou « Forwarder » de pfSense.

Les utilisateurs peuvent contourner ce filtrage en modifiant leur serveur DNS

### Filtrage avancé via pfBlockerNG

S'appuyer sur des listes externes ou personnalisées pour bloquer automatiquement des domaines, IP, voire des ASN entiers.

Mise à jour automatique, gestion fine par catégories, possibilité de planifier le blocage (Schedules).

Configuration plus complexe, peut nécessiter des réglages (listes, journaux) pour éviter les blocages indésirables.





# *PfBlockerNG*

## C'est quoi ?

pfBlockerNG est un module puissant intégré à pfSense qui bloque automatiquement les sites indésirables via des listes noires régulièrement mises à jour.

## Utilisation

J'ai configuré pfBlockerNG pour importer des listes de blocage incluant des ASN.

ASN (Autonomous System Number) : J'ai utilisé les numéros de système autonome pour bloquer des plages d'adresses IP associées à certains fournisseurs ou plateformes.

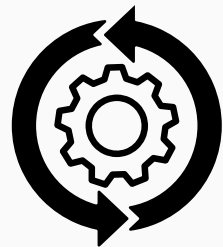
Cette méthode s'est révélée efficace, même pour bloquer des sites réputés difficiles à filtrer comme Facebook.

J'ai également mis en place des règles programmées (schedules) pour ajuster les paramètres et éviter les blocages indésirables.

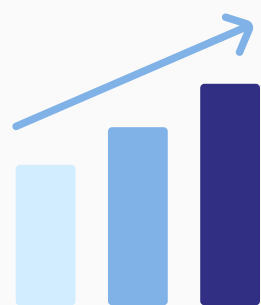




Ce projet a permis de concevoir et de sécuriser une infrastructure réseau en appliquant des méthodes avancées de segmentation, de filtrage et de gestion du trafic.



L'utilisation de pfSense a offert une solution flexible et performante pour le contrôle du réseau, l'optimisation des ressources et la mise en place de politiques de sécurité adaptées.



L'approche méthodique adoptée a permis d'expérimenter plusieurs solutions, d'analyser leurs performances et d'optimiser la configuration pour répondre aux besoins spécifiques du projet.





Citrix – Configuring Link Aggregation

<https://docs.netScaler.com/en-us/citrix-adc/current-release/networking/interfaces/configuring-link-aggregation.html>

TechTarget – OSPF (Open Shortest Path First)

<https://www.techtarget.com/searchnetworking/definition/OSPF-Open-Shortest-Path-First>

Netgate – Documentation pfBlockerNG

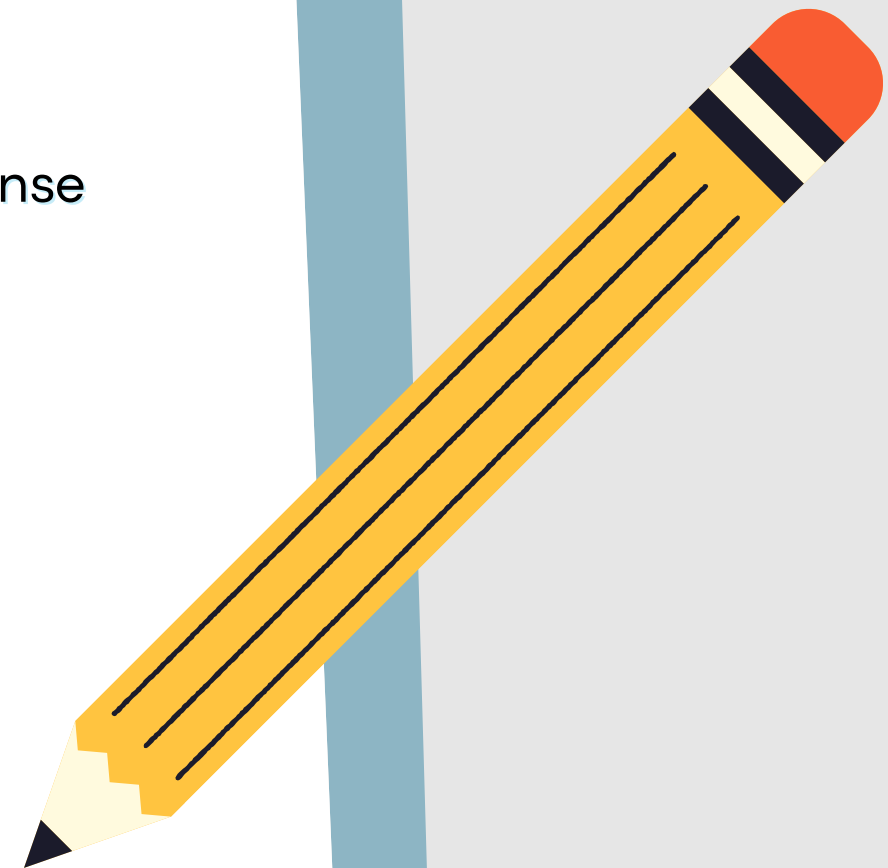
<https://www.netgate.com/docs/pfblockerng/en/latest/>

Tutoriels et guides YouTube sur pfSense – Configuration VLAN dans pfSense

<https://www.youtube.com/watch?v=mJrvvC-eHAE>

Dépôt GitHub du projet – Configurations et schémas

<https://github.com/21Yeet21/StageL2RSI.git>





***Merci Pour  
votre attention !***

