ROYAUME DU MAROC
Direction Régionale Rabat – Salé – Kénitra
OFPPT / INSTITUT SPÉCIALISÉ DE TECHNOLOGIE APPLIQUÉE

RAPPORT DE TRAVAUX PRATIQUES

CONFIGURATION ET SÉCURISATION D’UN PARE-FEU

DURCISSEMENT DES SYSTÈMES ET RÉSEAUX

Réalisé par :

Youness Boussedari

Filière :

Infrastructure Digitale - Option Cyber Security

Module :

Durcissement des Systèmes

Année Académique :

2025 – 2026

Table des Matières

1. Introduction
2. Objectifs du TP
3. Présentation de l'Environnement
4. Architecture Réseau
5. Installation et Configuration Initiale
6. Configuration des Interfaces Réseau
7. Configuration des Règles de Pare-feu
8. Sécurisation des Accès (SSH)
9. Mise en Place du Portail Captif
10. Tests et Validation
11. Analyse de Sécurité Approfondie
12. Conclusion

• DESIGN STRUCTURE – RAPPORT TP

Nom : Youness Boussedari
Spécialité : Cyber Security
Module : Durcissement des Systèmes
Année : 2025–2026

• PAGE DE GARDE (Design Proposé)

ROYAUME DU MAROC
Direction Régionale Rabat – Salé – Kénitra

RAPPORT DE TRAVAUX PRATIQUES

MODULE : DURCISSEMENT DES SYSTÈMES

🔐 Configuration et Sécurisation d’un Pare-feu

👤 Réalisé par :
Youness Boussedari

🎓 Filière : Infracructure Digitale-option Cyber Security

📅 Année académique : 2025–2026

👨‍🏫 Encadrant : …………………

📌 Design Conseils :

- **Titre centré**
- **Nom en gras**
- **Taille 16–18 pour titre principal**
- **Bordure simple ou ligne horizontale élégante**
- **Logo établissement en haut**

- # STRUCTURE PROFESSIONNELLE INTERNE

Utilise cette organisation claire et académique 👇

1. Introduction

✓ **Contexte général**
✓ **Importance du durcissement**
✓ **Objectif du TP**

2. Présentation de l’Environnement

2.1 Matériel utilisé

2.2 Logiciels utilisés

2.3 Architecture réseau

(Insérer schéma réseau ici)

3. Installation et Configuration Initiale

3.1 Installation

3.2 Attribution des interfaces

3.3 Paramétrage initial

(Screenshots propres avec légende)

4. Configuration des Interfaces Réseau

4.1 Interface LAN

4.2 Interface WAN

4.3 Interface DMZ

📝 **Toujours ajouter :**

- **Adresse IP**
- **Masque**

- **Rôle de l’interface**

5. Sécurisation des Accès

5.1 Activation SSH

5.2 Configuration clé RSA

5.3 Désactivation authentification par mot de passe

⚠ **Ajouter justification sécurité (analyse technique)**

6. Mise en Place du Portail Captif

6.1 Activation

6.2 Configuration authentification

6.3 Création utilisateurs

6.4 Test fonctionnel

(Insérer capture page login)

8. Analyse de Sécurité

✓ Segmentation réseau
✓ Réduction surface d'attaque
✓ Protection accès administrateur
✓ Contrôle des utilisateurs

(Partie très importante pour avoir bonne note)

9. Conclusion

✓ Résumé technique
✓ Compétences acquises
✓ Importance du durcissement

10. Annexes

- Plan d'adressage IP
- Commandes utilisées
- Screenshots supplémentaires
- # DESIGN CONSEILS POUR WORD

✓ Police recommandée :

- Titres → Arial 14/16 Bold
- Texte → Times New Roman 12

✓ Marges : 2.5 cm
✓ Interligne : 1.5
✓ Numérotation automatique des sections
✓ Légendes sous chaque image

📌 Structure Finale Résumée

1. Page de garde
2. Introduction
3. Environnement
4. Installation
5. Configuration Réseau
6. Sécurisation SSH
7. Portail Captif
8. Tests
9. Analyse Sécurité
10. Conclusion

1. Introduction

Dans un contexte où les cybermenaces évoluent rapidement et où les infrastructures informatiques sont exposées à des risques constants (intrusions, attaques par force brute, accès non autorisés), le durcissement des systèmes constitue une mesure essentielle pour garantir la sécurité des réseaux. La mise en place d’un pare-feu robuste permet de contrôler les flux de données, segmenter le réseau et réduire la surface d’attaque.

Le présent travail pratique a pour objectif l’installation et la configuration du pare-feu open source pfSense, afin d’assurer la protection d’un réseau interne. Les travaux réalisés incluent la configuration des interfaces réseau (LAN, WAN, DMZ), la sécurisation de l’accès distant via SSH à l’aide d’une authentification par clé RSA, ainsi que la mise en place d’un portail captif permettant de contrôler l’accès des utilisateurs aux ressources réseau.

Ce TP vise ainsi à appliquer des mécanismes fondamentaux de sécurité tels que la segmentation réseau, le contrôle d’accès et le renforcement des services d’administration. L’ensemble des configurations réalisées s’inscrit dans une démarche de durcissement visant à améliorer la résilience et la maîtrise des accès au sein d’une architecture réseau sécurisée.

2. Objectifs du TP

L’objectif principal de ce travail pratique est de mettre en œuvre une solution de sécurité réseau basée sur le pare-feu pfSense afin d’assurer le durcissement d’une infrastructure informatique.

Les objectifs spécifiques sont les suivants :

- Installer et configurer pfSense dans un environnement virtuel.
- Paramétrer les interfaces réseau (LAN, WAN et éventuellement DMZ) afin d’assurer la connectivité et la segmentation du réseau.
- Configurer l’administration via l’interface Web sécurisée.
- Activer et sécuriser l’accès distant SSH en imposant une authentification par clé RSA.
- Mettre en place un portail captif pour contrôler l’accès des utilisateurs au réseau.
- Créer et gérer des comptes utilisateurs pour l’authentification.
- Tester et valider le bon fonctionnement de l’architecture mise en place.

Ce TP vise à appliquer des techniques fondamentales de durcissement, notamment la segmentation réseau, la sécurisation des accès administratifs et le contrôle d’authentification des utilisateurs.

4. Configuration des Interfaces Réseau

Cette étape consiste à configurer les différentes interfaces du pare-feu pfSense afin d'assurer la connectivité, la segmentation du réseau et le contrôle des flux entre les différentes zones.

4.1 Configuration de l'interface LAN

L'interface LAN représente le réseau interne de l'organisation.

- **Attribution d'une adresse IP statique :**
  192.168.10.1/24
- **Activation du serveur DHCP pour distribuer automatiquement les adresses IP aux postes clients.**
- **Vérification de l'accès à l'interface Web via :**
  https://192.168.10.1

Objectif sécurité :
Garantir un point d'administration stable et assurer la gestion contrôlée des équipements internes.

4.2 Configuration de l'interface WAN

L'interface WAN assure la connexion vers le réseau externe (Internet).

- **Configuration en mode DHCP (dans un environnement NAT).**
- **Vérification de l'obtention automatique d'une adresse IP.**
- **Test de connectivité Internet.**

Objectif sécurité :
Permettre l'accès aux ressources externes tout en maintenant le filtrage via le pare-feu.

4.3 Configuration de l'interface DMZ

L'interface DMZ permet d'isoler les services accessibles publiquement du réseau interne.

- **Attribution d'une adresse IP statique :**
  192.168.20.1/24
- **Création d'un sous-réseau distinct du LAN.**
- **Séparation logique entre LAN et DMZ.**

Installation et configuration initiale de pfSense

🎯 Objectif

Déployer un pare-feu opérationnel servant de passerelle sécurisée entre le réseau interne et Internet.

⚙️ Étapes techniques

A. Installation

- **Télécharger l'image ISO officielle depuis le site de pfSense.**
- **Installer sur :**
  - **Machine physique dédiée**
  - **ou machine virtuelle (VMware / VirtualBox)**

B. Configuration initiale via console

Après installation :

- **Attribution des interfaces réseau :**
  - **WAN → interface connectée à Internet**
  - **LAN → réseau interne**
- **Configuration IP du LAN (192.168.1.1/24)**
- **Activation serveur DHCP**

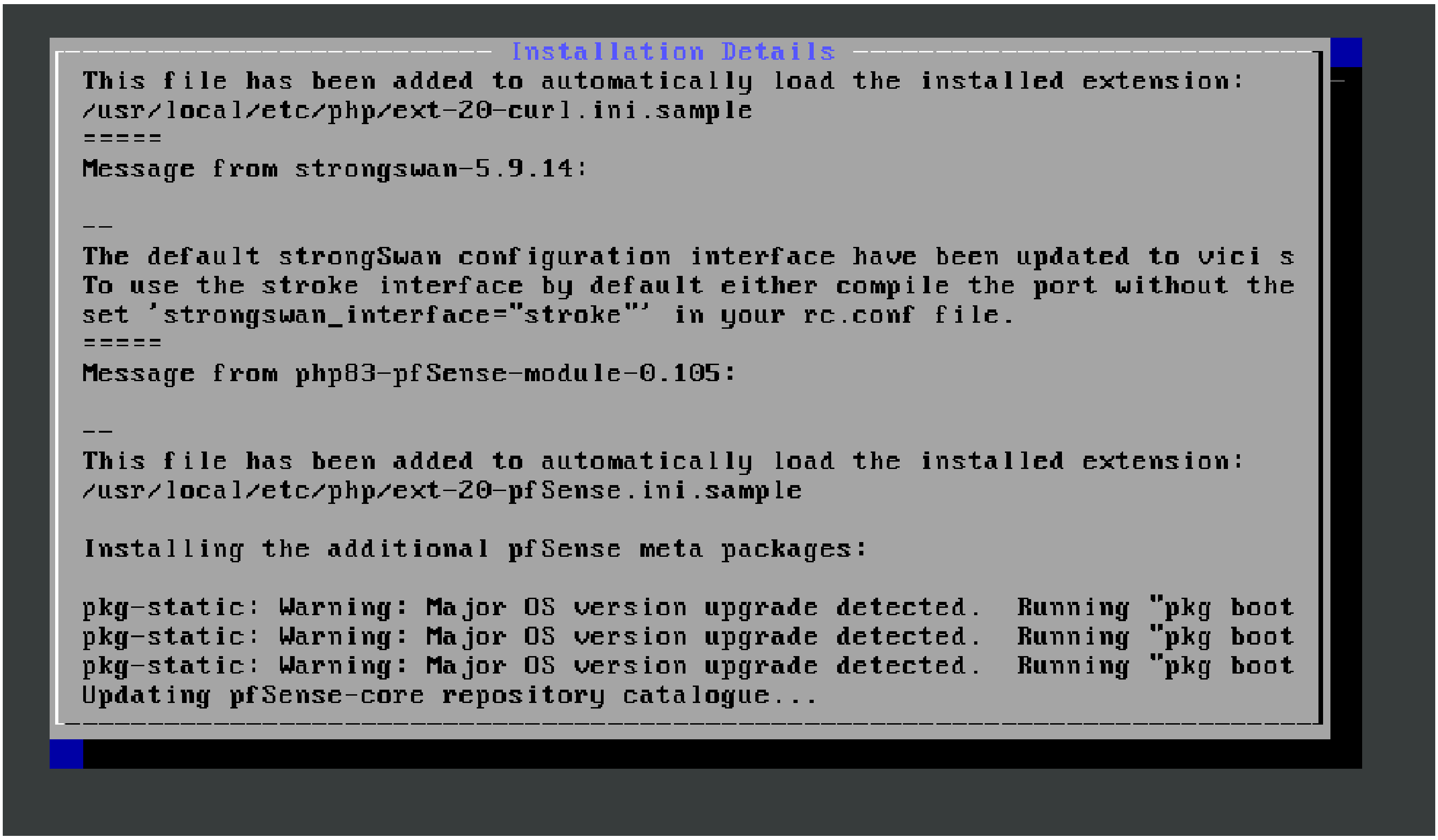
Résultat attendu

- **Accès à l'interface Web via :**

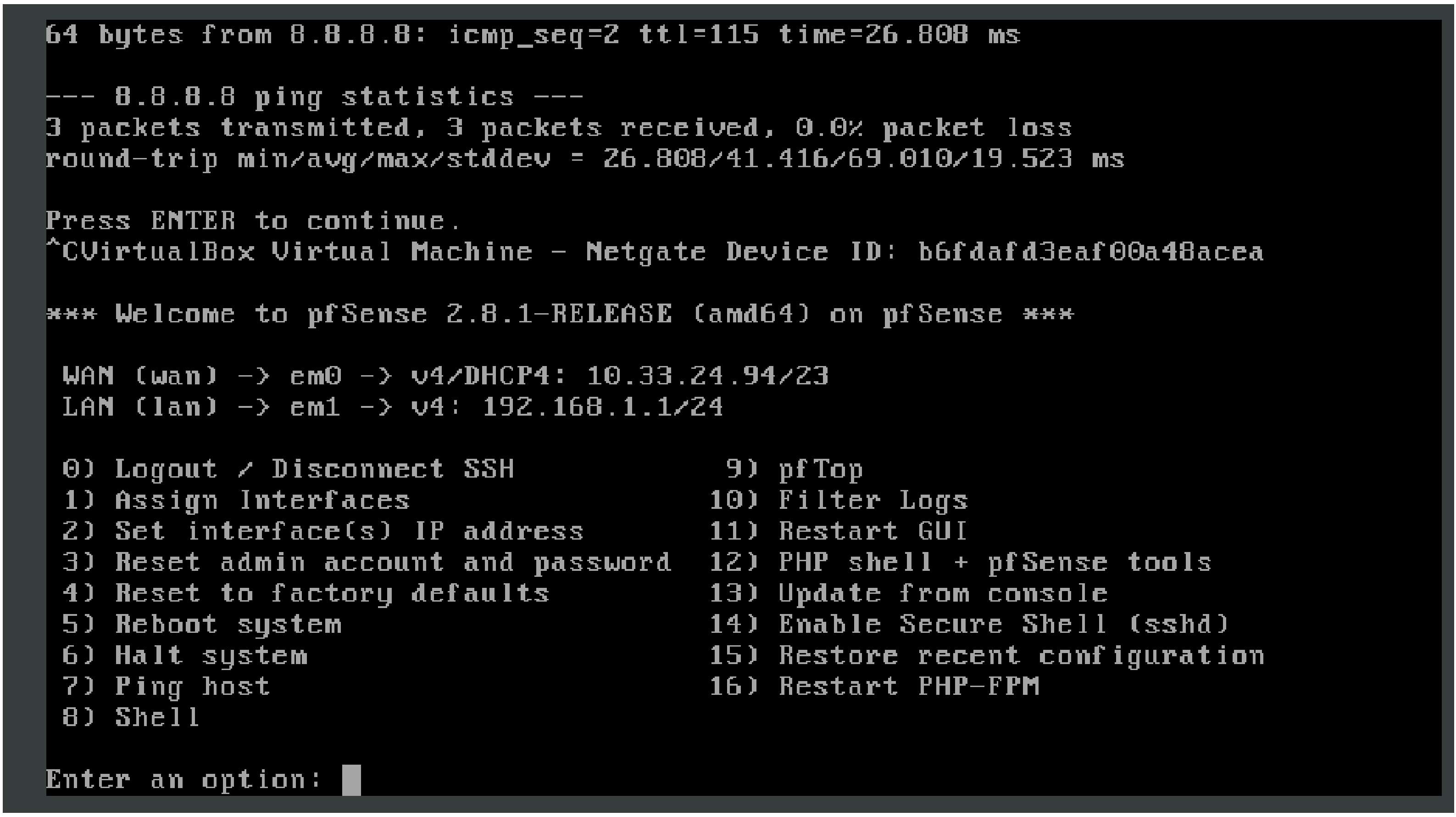
https://192.168.1.1

L'objectif de ce lab est de configurer un pare-feu PfSense pour assurer la sécurité du réseau de votre organisation. Les principales tâches incluent :

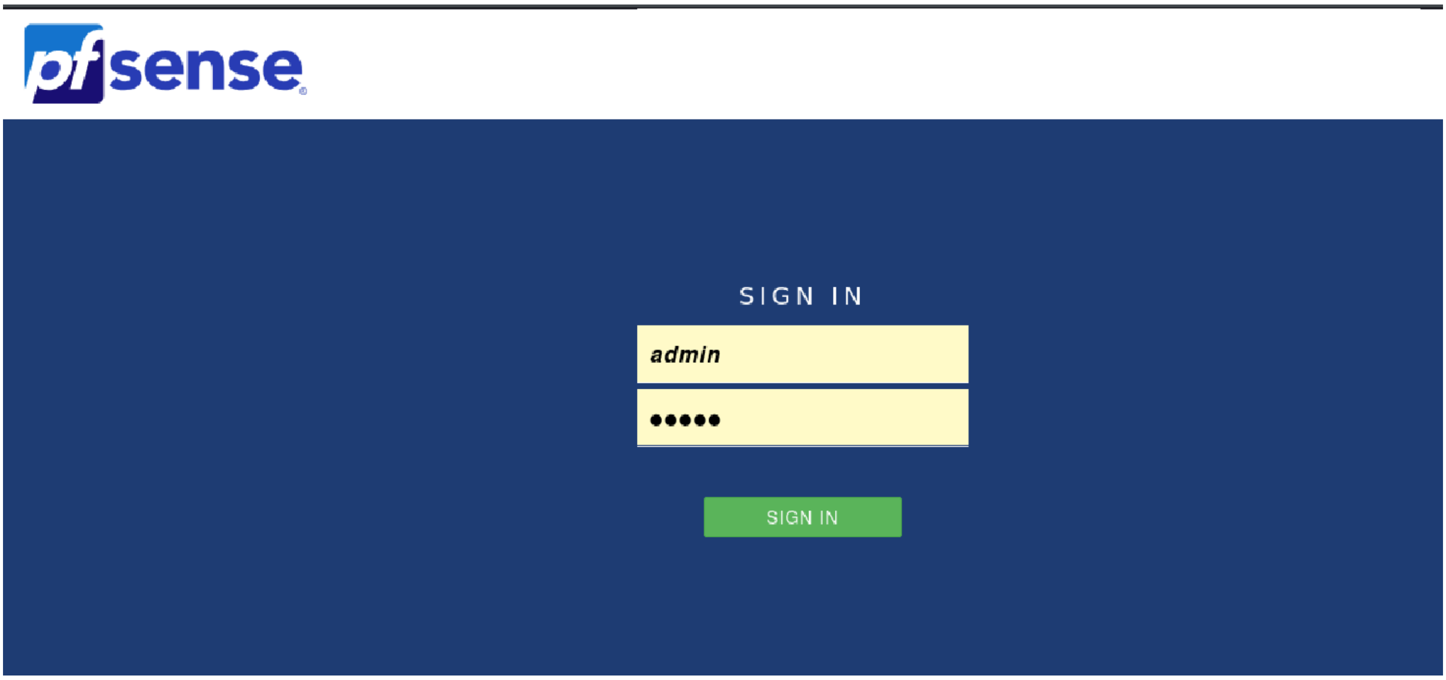
- **L'installation et la configuration initiale de PfSense.**



```
This file has been added to automatically load the installed extension:
/usr/local/etc/php/ext-20-curl.ini.sample
=====
Message from strongswan-5.9.14:

--
The default strongSwan configuration interface have been updated to vici s
To use the stroke interface by default either compile the port without the
set 'strongswan_interface="stroke"' in your rc.conf file.
=====
Message from php83-pfSense-module-0.105:

--
This file has been added to automatically load the installed extension:
/usr/local/etc/php/ext-20-pfSense.ini.sample

Installing the additional pfSense meta packages:

pkg-static: Warning: Major OS version upgrade detected.  Running "pkg boot
pkg-static: Warning: Major OS version upgrade detected.  Running "pkg boot
pkg-static: Warning: Major OS version upgrade detected.  Running "pkg boot
Updating pfSense-core repository catalogue...
```



```
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=26.808 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 26.808/41.416/69.010/19.523 ms

Press ENTER to continue.
^CVirtualBox Virtual Machine - Netgate Device ID: b6fdafd3eaf00a48acea

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

 WAN (wan) -> em0 -> v4/DHCP4: 10.33.24.94/23
 LAN (lan) -> em1 -> v4: 192.168.1.1/24

 0) Logout / Disconnect SSH              9) pfTop
 1) Assign Interfaces                   10) Filter Logs
 2) Set interface(s) IP address         11) Restart GUI
 3) Reset admin account and 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:
```

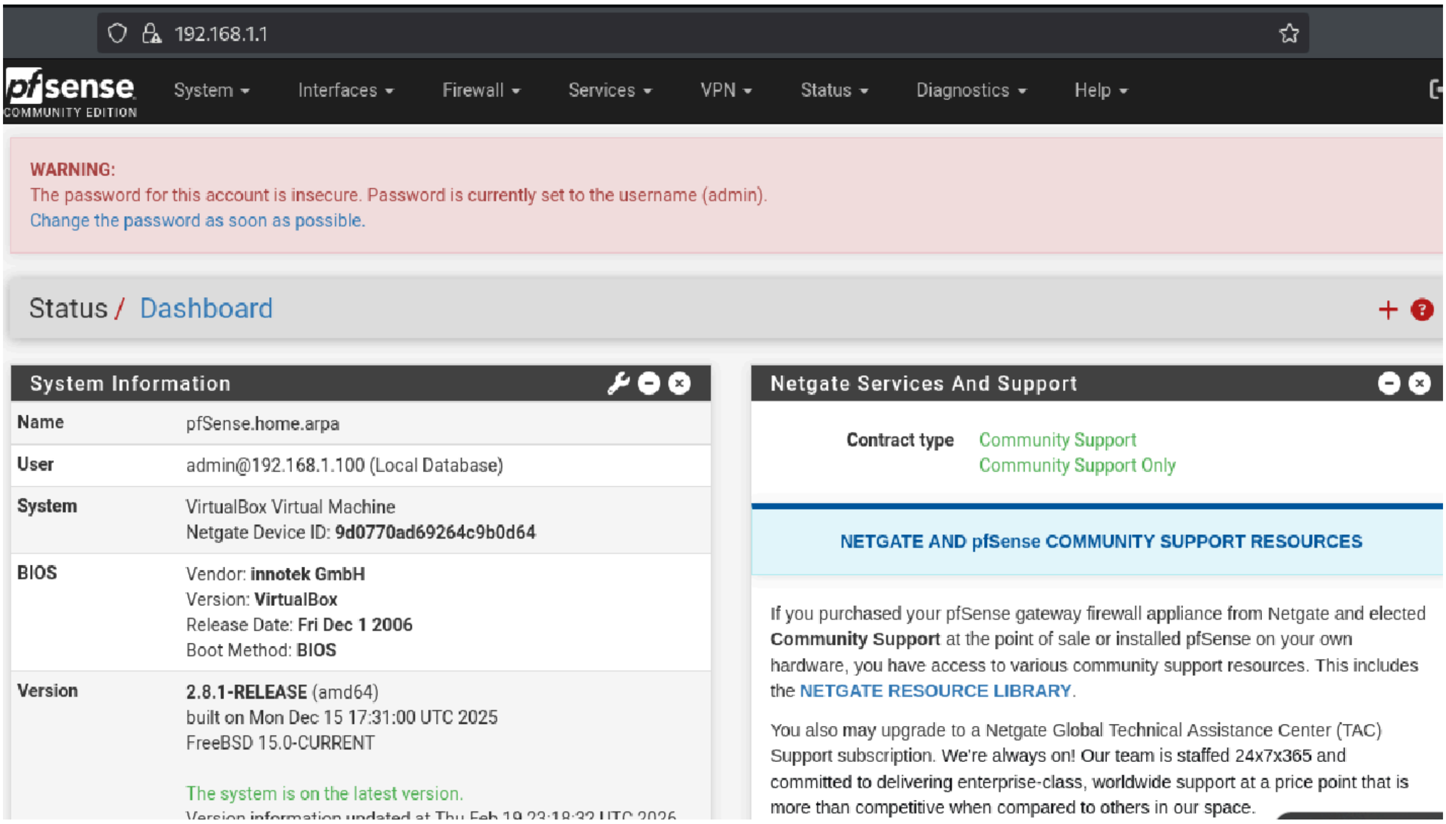


SIGN IN

admin

●●●●●

SIGN IN



192.168.1.1
sense COMMUNITY EDITION
System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING:
The password for this account is insecure. Password is currently set to the username (admin).
Change the password as soon as possible.

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.1.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: **9d0770ad69264c9b0d64**
BIOS	Vendor: **innotek GmbH** Version: **VirtualBox** Release Date: **Fri Dec 1 2006** Boot Method: **BIOS**
Version	**2.8.1-RELEASE** (amd64) built on Mon Dec 15 17:31:00 UTC 2025 FreeBSD 15.0-CURRENT The system is on the latest version. Version information updated at Thu Feb 19 23:18:32 UTC 2026

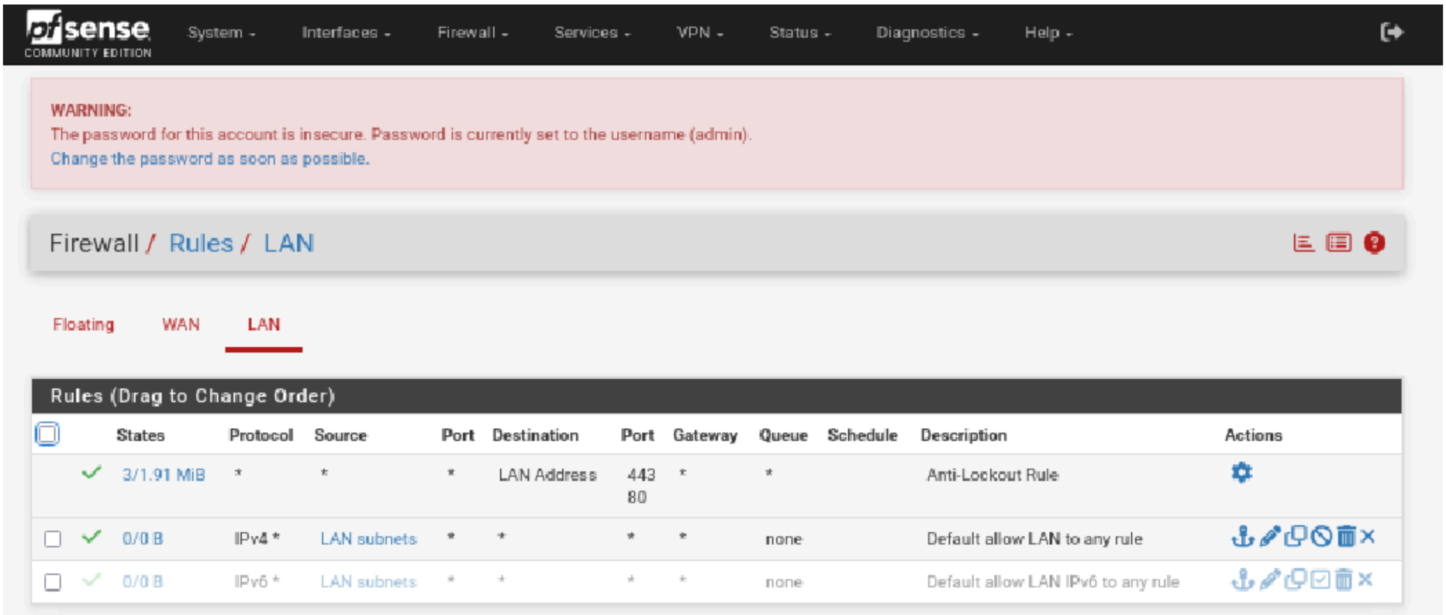
Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.



WARNING:
The password for this account is insecure. Password is currently set to the username (admin).
Change the password as soon as possible.

Firewall / Rules / LAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	3/1.91 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
□	✓	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ⧉ ⊘ 🗑 ✕
□	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ⧉ ☑ 🗑 ✕

Configuration des interfaces réseau (LAN / WAN / DMZ)

🌍 WAN (Internet)

Rôle

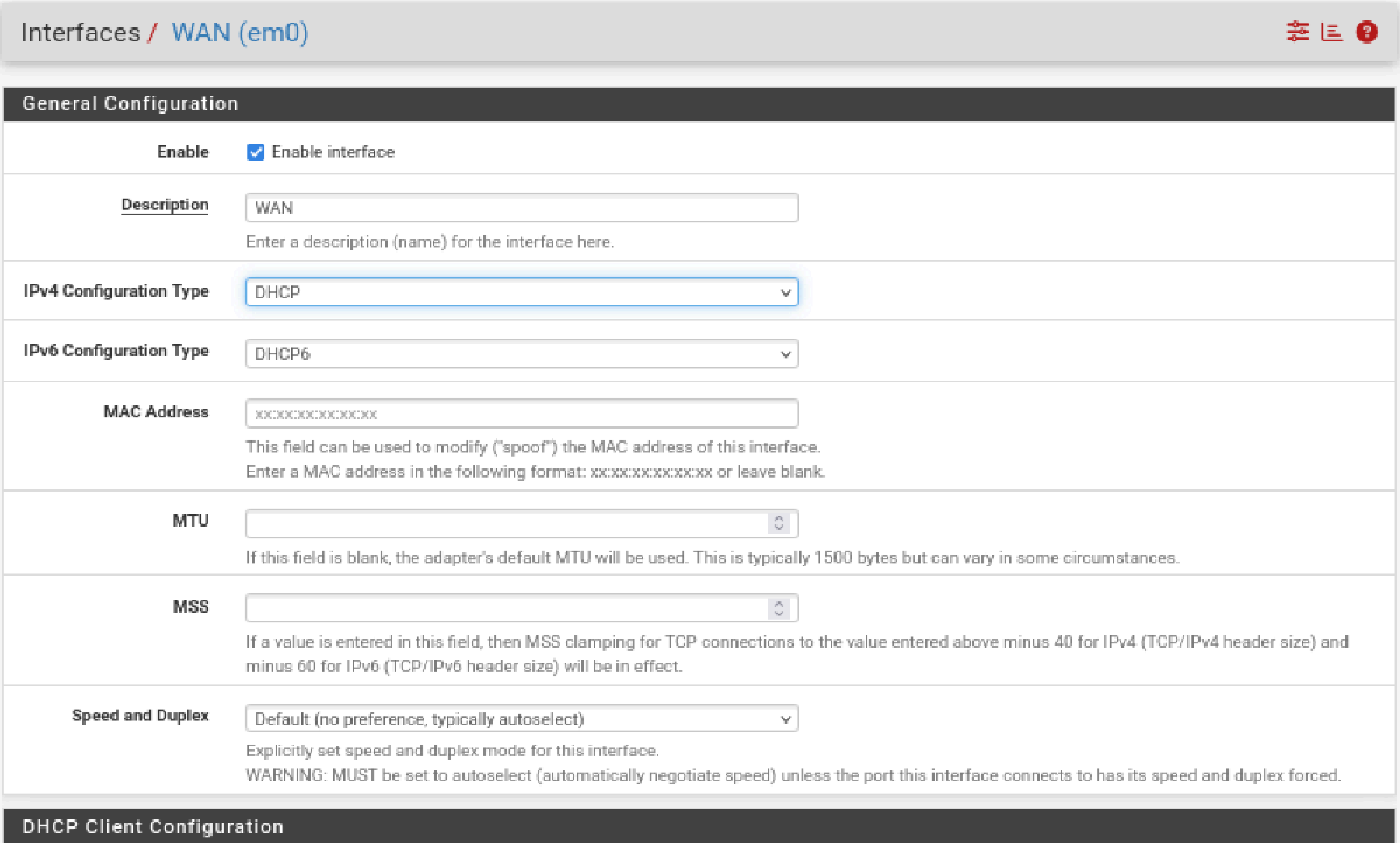
Interface exposée vers l’extérieur.

Configuration

- **Type IP : DHCP ou IP statique**
- **Gateway configurée automatiquement ou manuellement**
- **Bloquer accès privé (Block private networks)**

Sécurité

- **Aucune règle entrante ouverte par défaut**
- **NAT automatique activé**



Interfaces / WAN (em0)

General Configuration

Enable ☑ Enable interface

Description: WAN

Enter a description (name) for the interface here.

IPv4 Configuration Type: DHCP

IPv6 Configuration Type: DHCP6

MAC Address: xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.

Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:

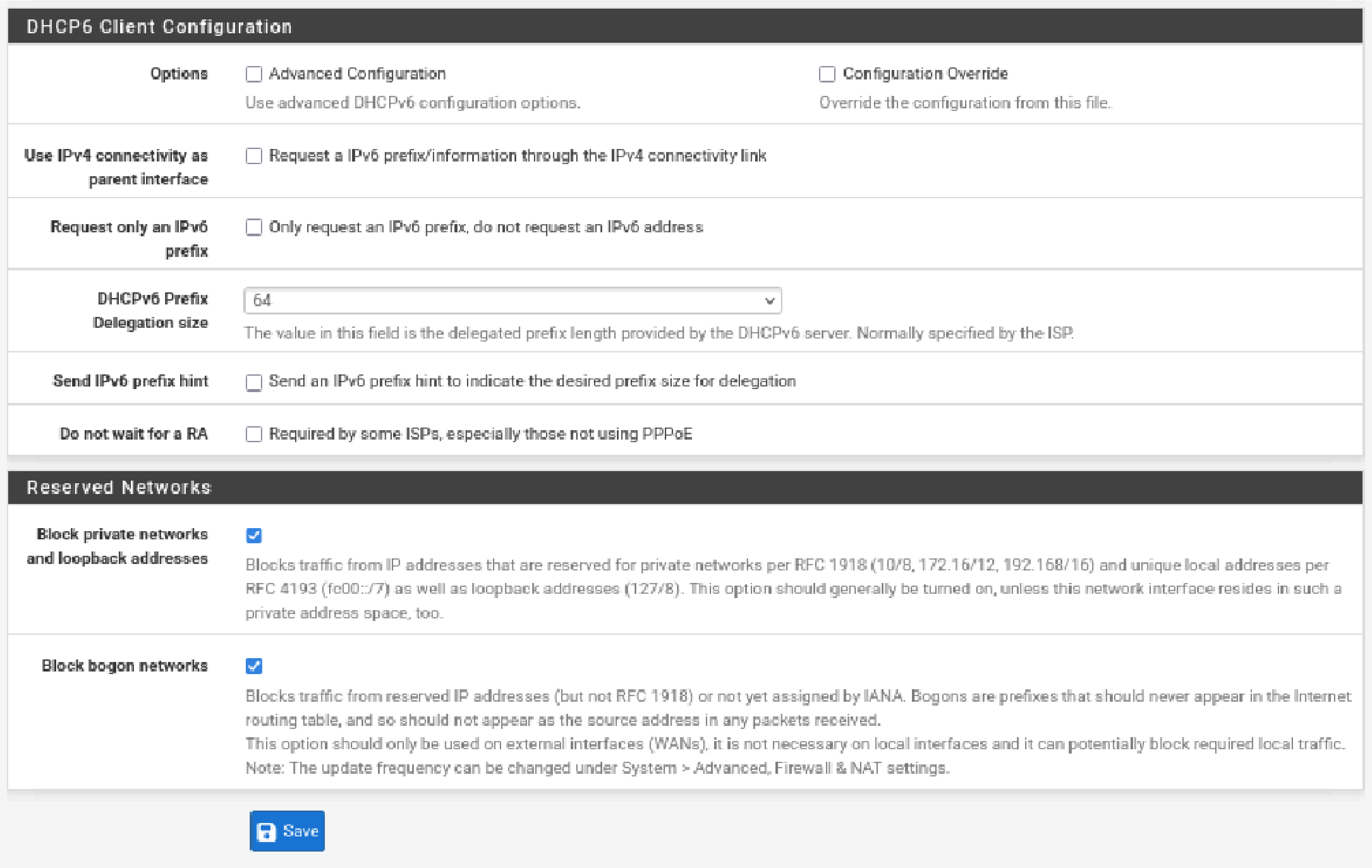
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.

WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

DHCP Client Configuration



DHCP6 Client Configuration

Options: □ Advanced Configuration — Use advanced DHCPv6 configuration options.
□ Configuration Override — Override the configuration from this file.

Use IPv4 connectivity as parent interface: □ Request a IPv6 prefix/information through the IPv4 connectivity link

Request only an IPv6 prefix: □ Only request an IPv6 prefix, do not request an IPv6 address

DHCPv6 Prefix Delegation size: 64
The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.

Send IPv6 prefix hint: □ Send an IPv6 prefix hint to indicate the desired prefix size for delegation

Do not wait for a RA: □ Required by some ISPs, especially those not using PPPoE

Reserved Networks

Block private networks and loopback addresses: ☑
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks: ☑
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Configuration LAN

🎯 Objectif

Créer réseau interne sécurisé.

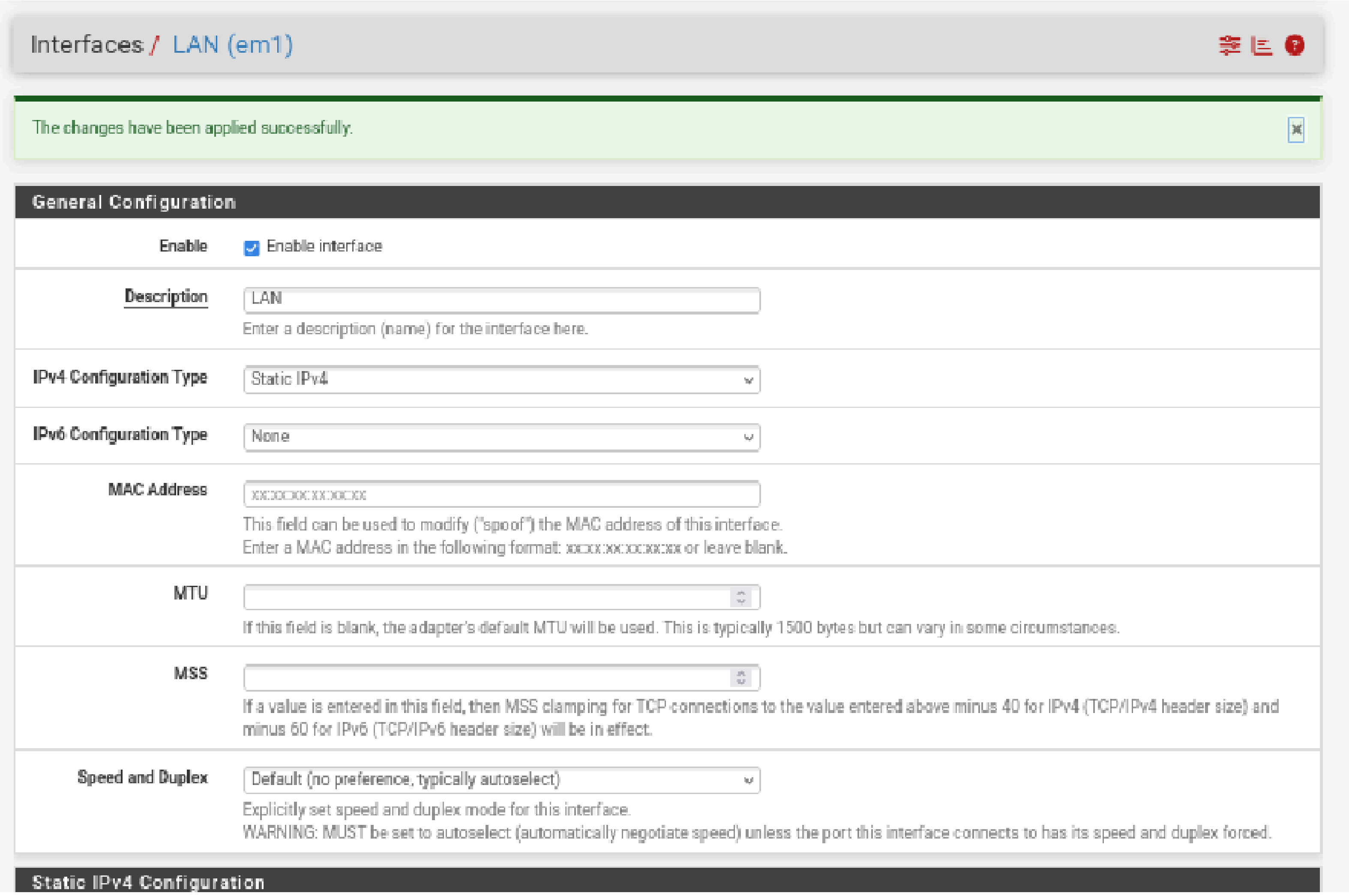
Étapes

1. **Aller dans :**
   Interfaces → LAN
2. **Configurer :**
   - **IPv4 : Static**
   - **Exemple IP : 192.168.10.1 /24**
3. **Activer DHCP :**
   - **Services → DHCP Server → LAN**
   - **Enable DHCP**

   - **Range : 192.168.10.10 → 192.168.10.100**
4. **Save → Apply**

Vérification

Connecter un PC au LAN
 Il doit recevoir une IP automatiquement.



Interfaces / LAN (em1)

The changes have been applied successfully.

General Configuration

Enable	☑ Enable interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

Configuration DMZ

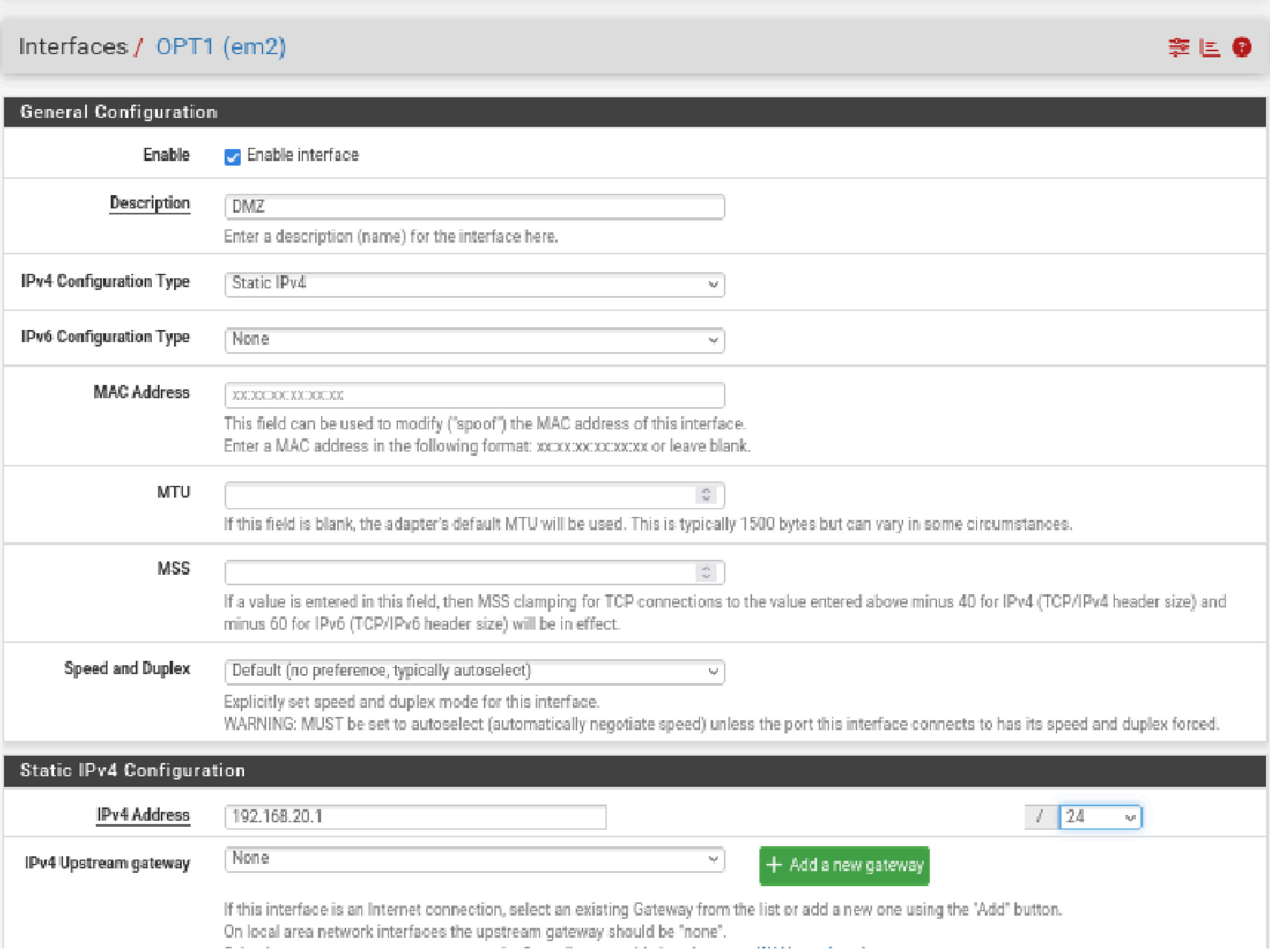
🎯 Objectif

Isoler les serveurs publics.

Étapes

1. **Interfaces → Assignments**
2. **Ajouter nouvelle interface (OPT1)**
3. **Renommer en : DMZ**
4. **Activer interface**
5. **Configurer IP :**
    - **Exemple : 192.168.20.1 /24**

6. **Save → Apply**



Interfaces / OPT1 (em2)

General Configuration

Enable ☑ Enable interface

Description: DMZ
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: 192.168.20.1 / 24

IPv4 Upstream gateway: None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".

Configuration des règles Firewall

C’est la partie la plus importante 🔥

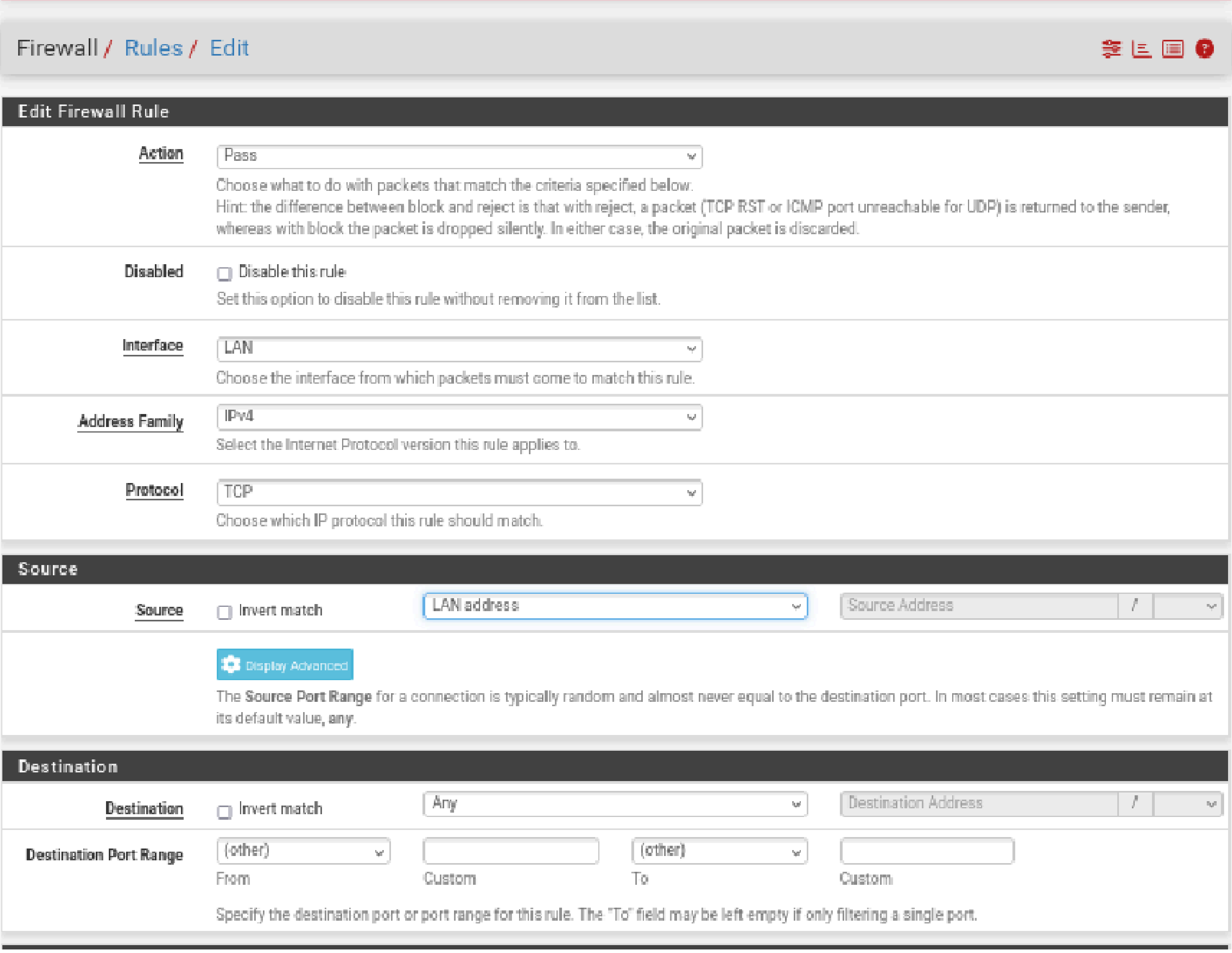
Règles LAN

Firewall → Rules → LAN

Ajouter règle :

- **Action : Pass**
- **Source : LAN net**
- **Destination : any**

👉 **Autorise LAN → Internet**



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: □ 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: TCP
Choose which IP protocol this rule should match.

Source

Source: □ Invert match — LAN address — Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match — Any — Destination Address /

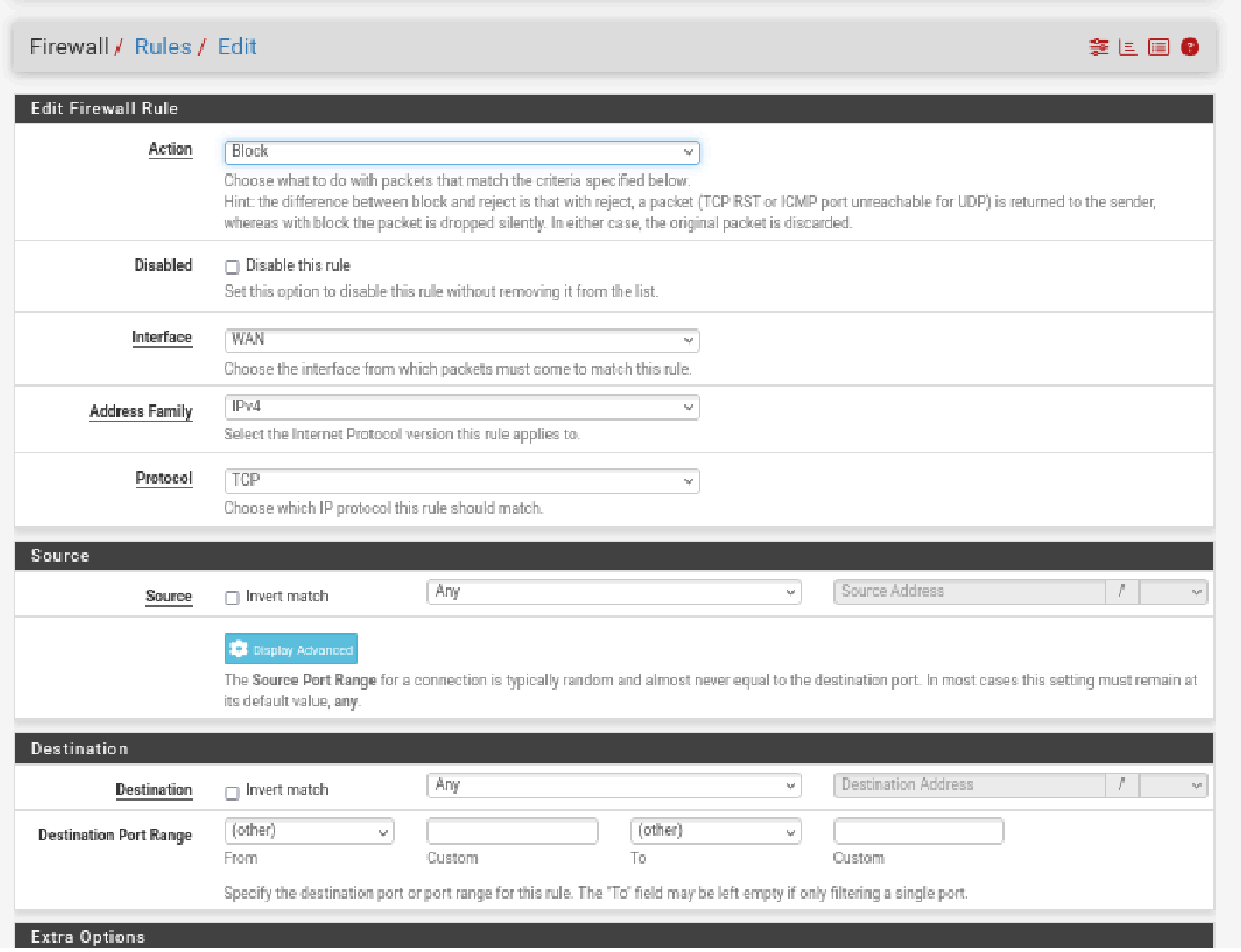
Destination Port Range: (other) From — Custom — (other) To — Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Règles WAN

Par défaut : tout est bloqué

Ne rien ouvrir sauf besoin spécifique.



Firewall / Rules / Edit

Edit Firewall Rule

Action: Block

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: WAN

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: TCP

Choose which IP protocol this rule should match.

Source

Source: □ Invert match | Any | Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match | Any | Destination Address /

Destination Port Range: (other) | | (other) |

From | Custom | To | Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Règles DMZ

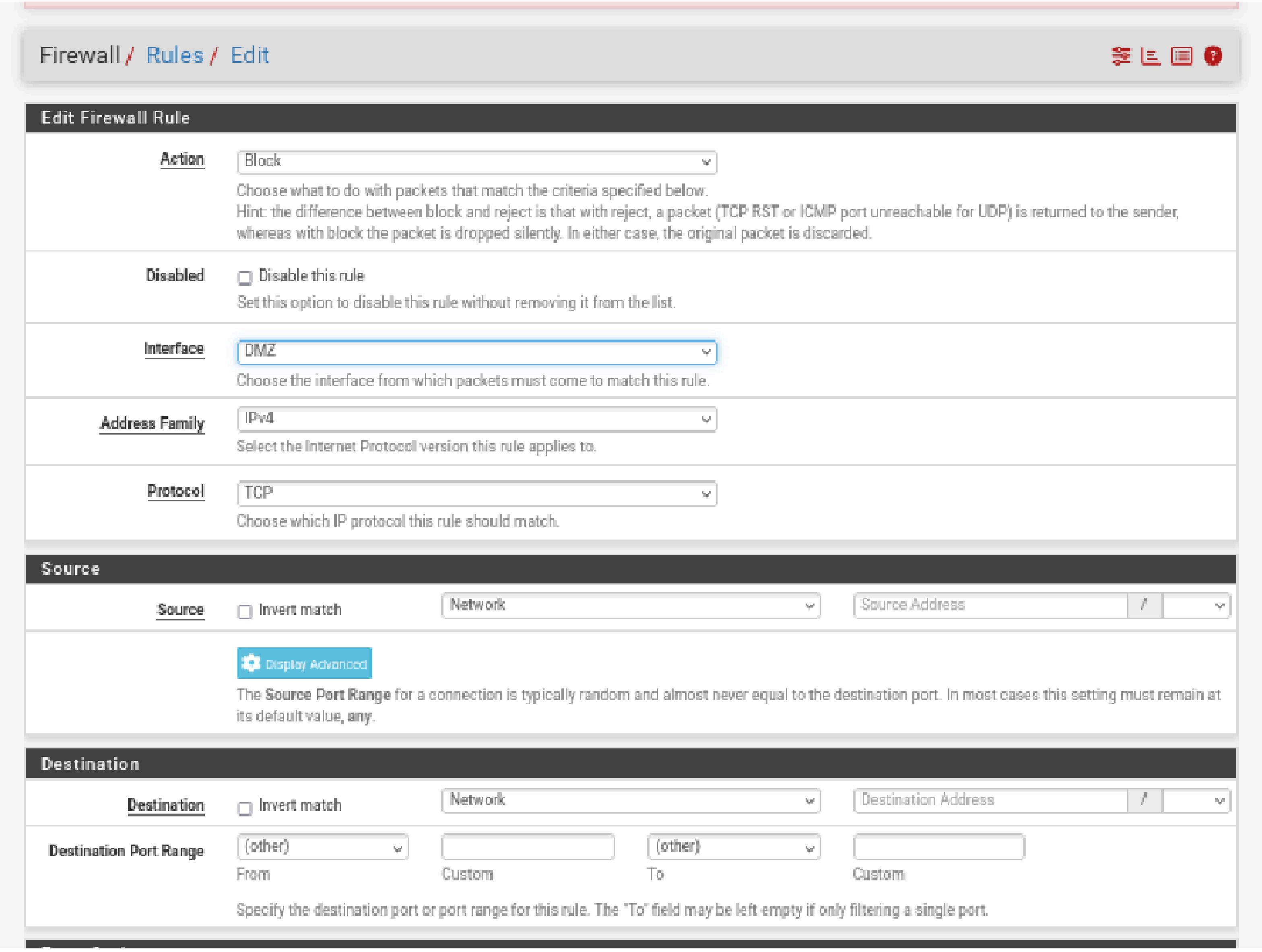
Firewall → Rules → DMZ

Exemple sécurisé :

- **Autoriser DMZ → WAN (HTTP/HTTPS)**
- **Bloquer DMZ → LAN**

Ajouter règle :

- **Action : Block**
- **Source : DMZ net**
- **Destination : LAN net.**



Firewall / Rules / Edit

Edit Firewall Rule

Action	Block 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	DMZ 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	TCP Choose which IP protocol this rule should match.

Source

Source	□ Invert match — Network — Source Address /
	Display Advanced The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

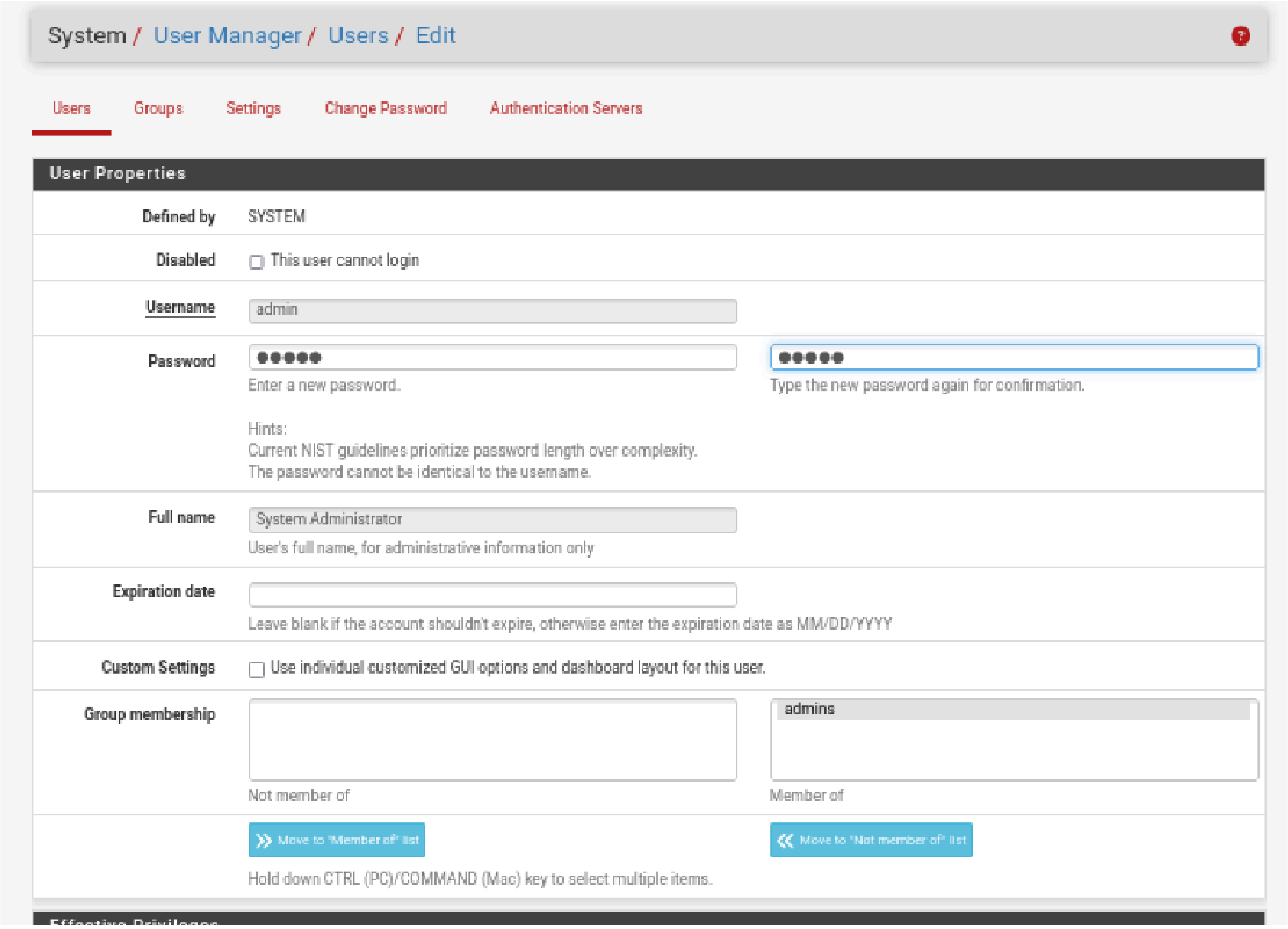
Destination	□ Invert match — Network — Destination Address /
Destination Port Range	(other) From — Custom — (other) To — Custom Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Administration via l’interface WEB

L’interface web permet de gérer et sécuriser PfSense facilement. Étapes :

1. **Accès à l’interface web**
   - Ouvrir un navigateur → entrer l’IP LAN (https://192.168.1.1).
   - Identifiant par défaut : admin
   - Mot de passe par défaut : pfsense
2. **Changer le mot de passe par défaut**
   - Menu : **System → User Manager → Admin → Edit**
   - Choisir un mot de passe complexe.

-



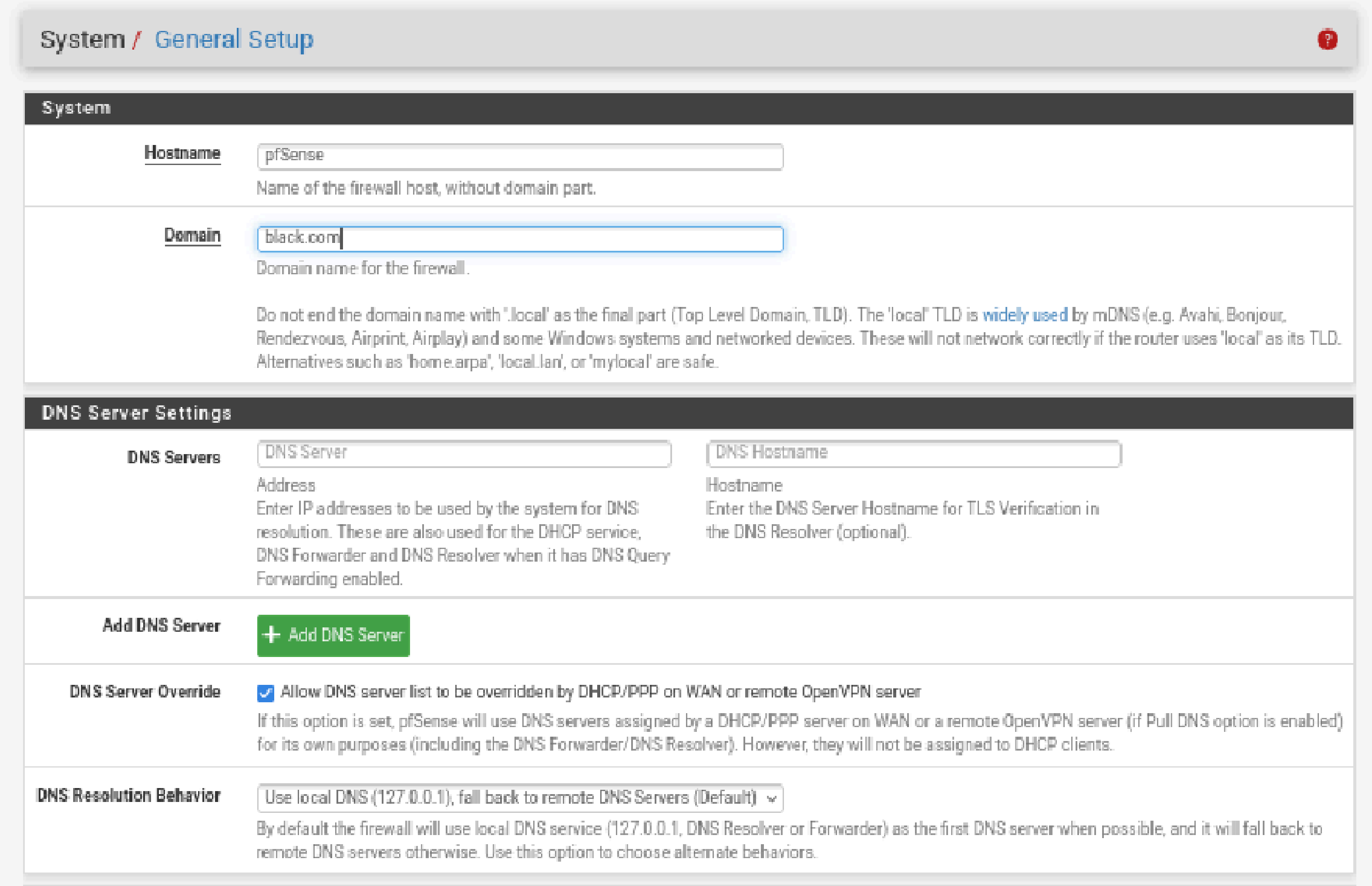
System / User Manager / Users / Edit

User Properties

Defined by	SYSTEM	
Disabled	□ This user cannot login	
Username	admin	
Password	●●●●● Enter a new password. Hints: Current NIST guidelines prioritize password length over complexity. The password cannot be identical to the username.	●●●●● Type the new password again for confirmation.
Full name	System Administrator User's full name, for administrative information only	
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY	
Custom Settings	□ Use individual customized GUI options and dashboard layout for this user.	
Group membership	Not member of	admins Member of
	» Move to "Member of" list	« Move to "Not member of" list
	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	

Effective Privileges

1. **Configurer les paramètres système principaux**
   - **System → General Setup** :
     - Définir le nom du système et le domaine.
     - Configurer les serveurs DNS.
   - **System → Advanced** :
     - Activer HTTPS pour l’accès web.
     - Restreindre l’accès non sécurisé.
2. **Mettre à jour PfSense**
   - **System → Update** → vérifier et installer les dernières mises à jour.
3. **Créer une sauvegarde de configuration**
   - **Diagnostics → Backup & Restore** : sauvegarder la configuration avant modifications majeures.



System / General Setup

System

Hostname: pfSense
Name of the firewall host, without domain part.

Domain: black.com
Domain name for the firewall.

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

DNS Server Settings

DNS Servers: DNS Server | DNS Hostname
Address
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.
Hostname
Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).

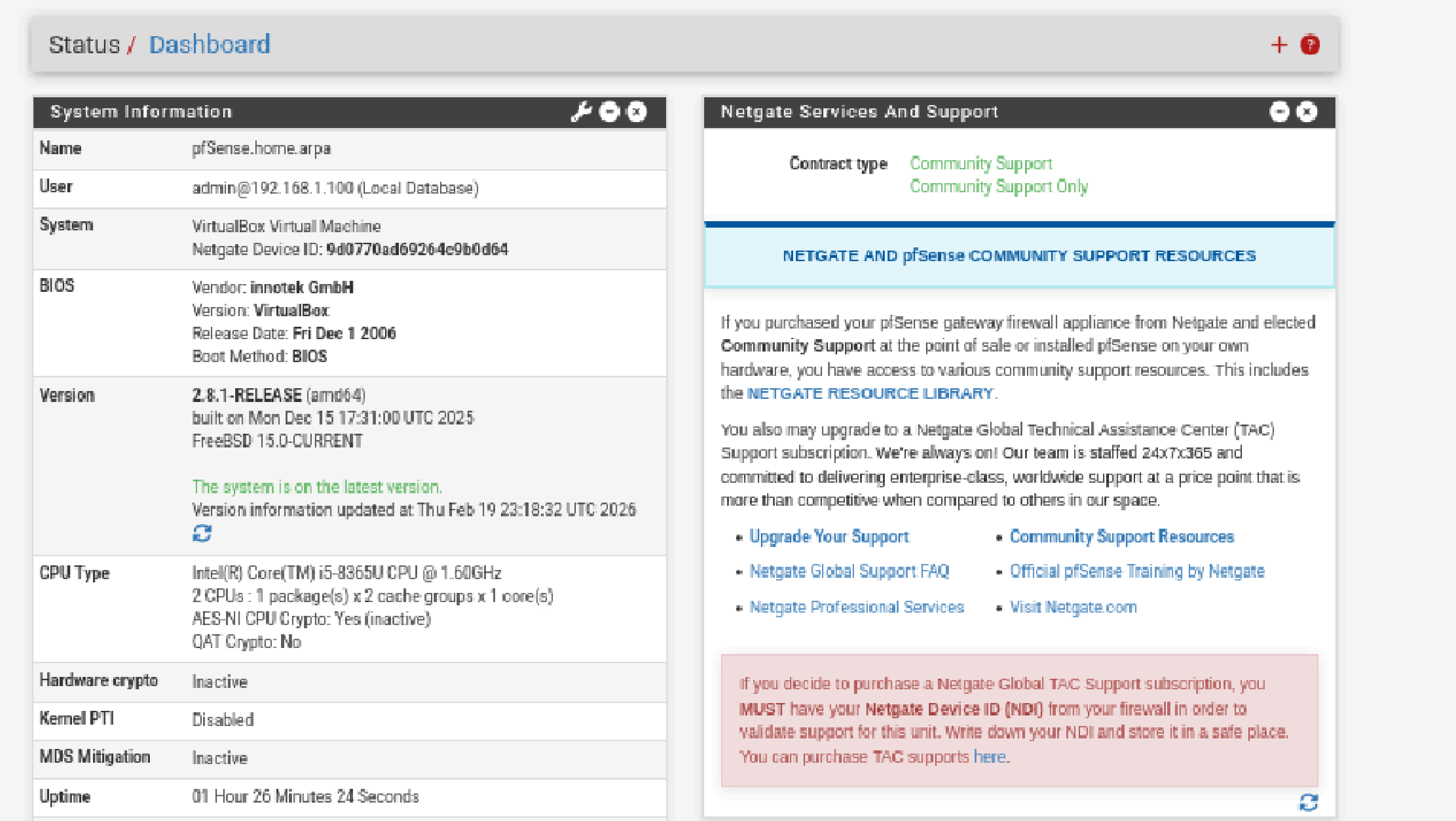
Add DNS Server: + Add DNS Server

DNS Server Override: ☑ Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

DNS Resolution Behavior: Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)
By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

○

1. **Surveiller le système**
   - **Status → Dashboard** : consulter l'état des interfaces, CPU, RAM et logs.



Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.1.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: **9d0770ad69264c9b0d64**
BIOS	Vendor: **innotek GmbH** Version: **VirtualBox** Release Date: **Fri Dec 1 2006** Boot Method: **BIOS**
Version	**2.8.1-RELEASE** (amd64) built on Mon Dec 15 17:31:00 UTC 2025 FreeBSD 15.0-CURRENT The system is on the latest version. Version information updated at Thu Feb 19 23:18:32 UTC 2026
CPU Type	Intel(R) Core(TM) i5-8365U CPU @ 1.60GHz 2 CPUs : 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	01 Hour 26 Minutes 24 Seconds

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

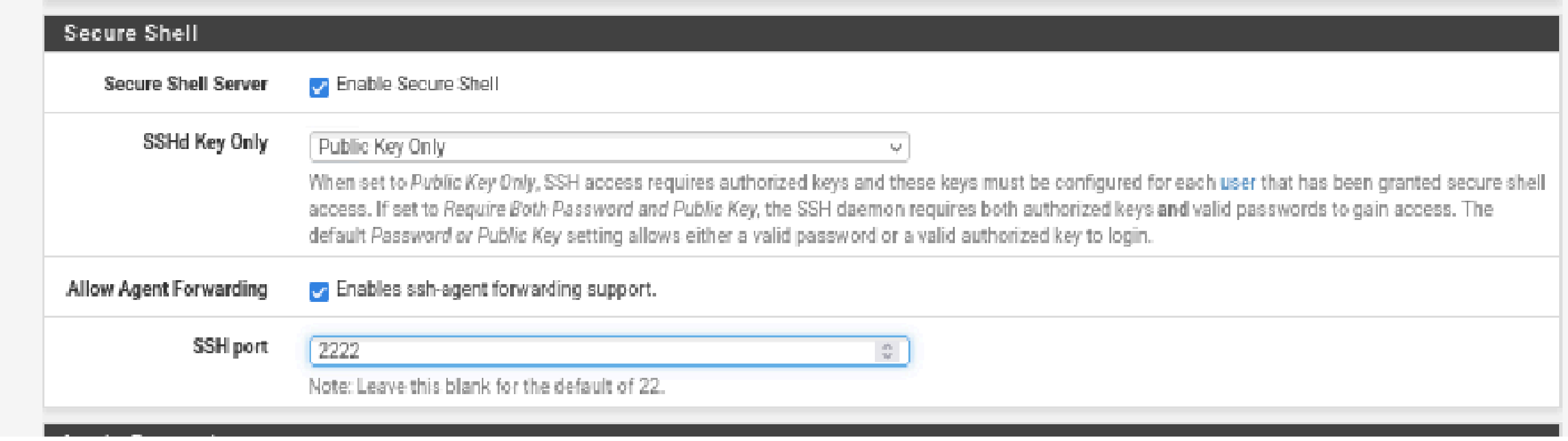
If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.

Sécurisation de l'accès SSH 😃

System → Advanced → Admin Access → Enable SSH

Préférer l'authentification par clés SSH.

Changer le port par défaut (22) pour plus de sécurité.



Secure Shell

Secure Shell Server ☑ Enable Secure Shell

SSHd Key Only Public Key Only

When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys and valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

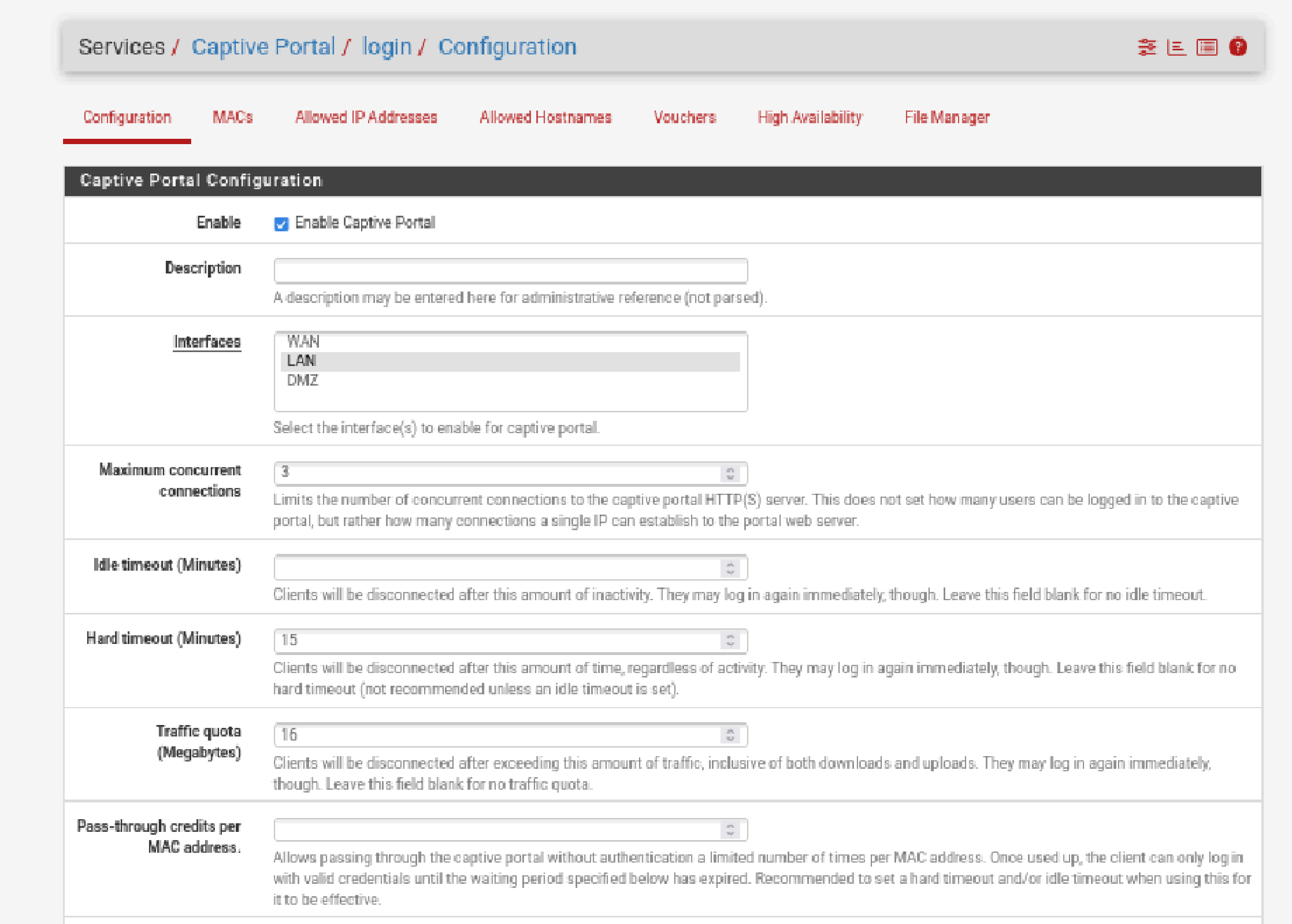
Allow Agent Forwarding ☑ Enables ssh-agent forwarding support.

SSH port 2222

Note: Leave this blank for the default of 22.

Mise en place du portail captif

- **Services → Captive Portal**
- Créer une zone, l’assigner à LAN ou Wi-Fi.
- Configurer la page de connexion et les règles d’accès (durée de session, type d’authentification).



Captive Portal Configuration

Enable ☑ Enable Captive Portal

Description

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

Interfaces
WAN
LAN
DMZ

Select the interface(s) to enable for captive portal.

Maximum concurrent connections 3

Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

Idle timeout (Minutes)

Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout (Minutes) 15

Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Traffic quota (Megabytes) 16

Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.

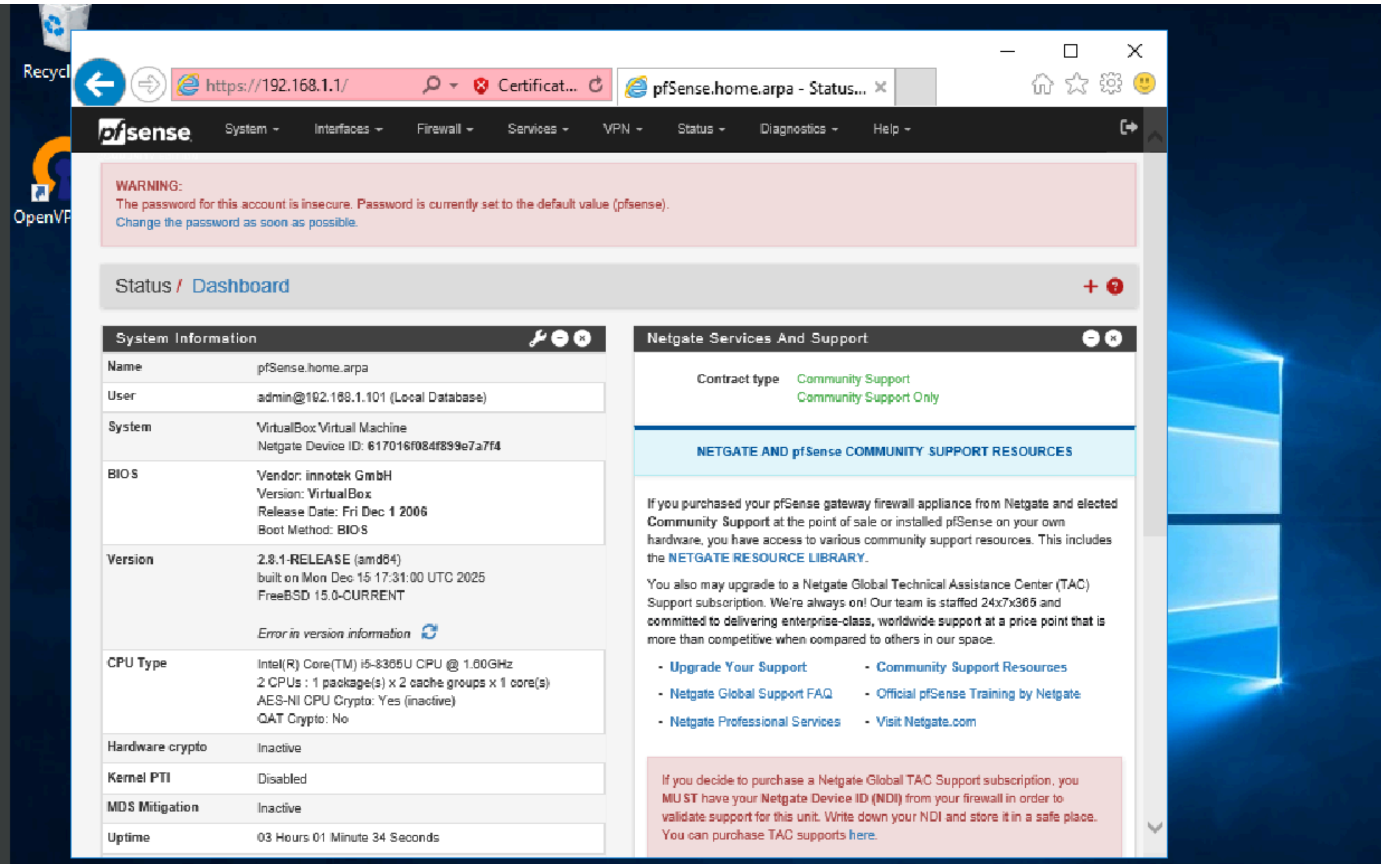
Pass-through credits per MAC address.

Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.

4. Les Travaux demandés

4.1. Configuration des Interfaces Réseau

1. Accédez à l'interface Web de PfSense.



WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.1.101 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 617016f084f899e7a7f4
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006 Boot Method: BIOS
Version	2.8.1-RELEASE (amd64) built on Mon Dec 15 17:31:00 UTC 2025 FreeBSD 15.0-CURRENT *Error in version information*
CPU Type	Intel(R) Core(TM) i5-8365U CPU @ 1.60GHz 2 CPUs : 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	03 Hours 01 Minute 34 Seconds

Netgate Services And Support

Contract type Community Support
Community Support Only

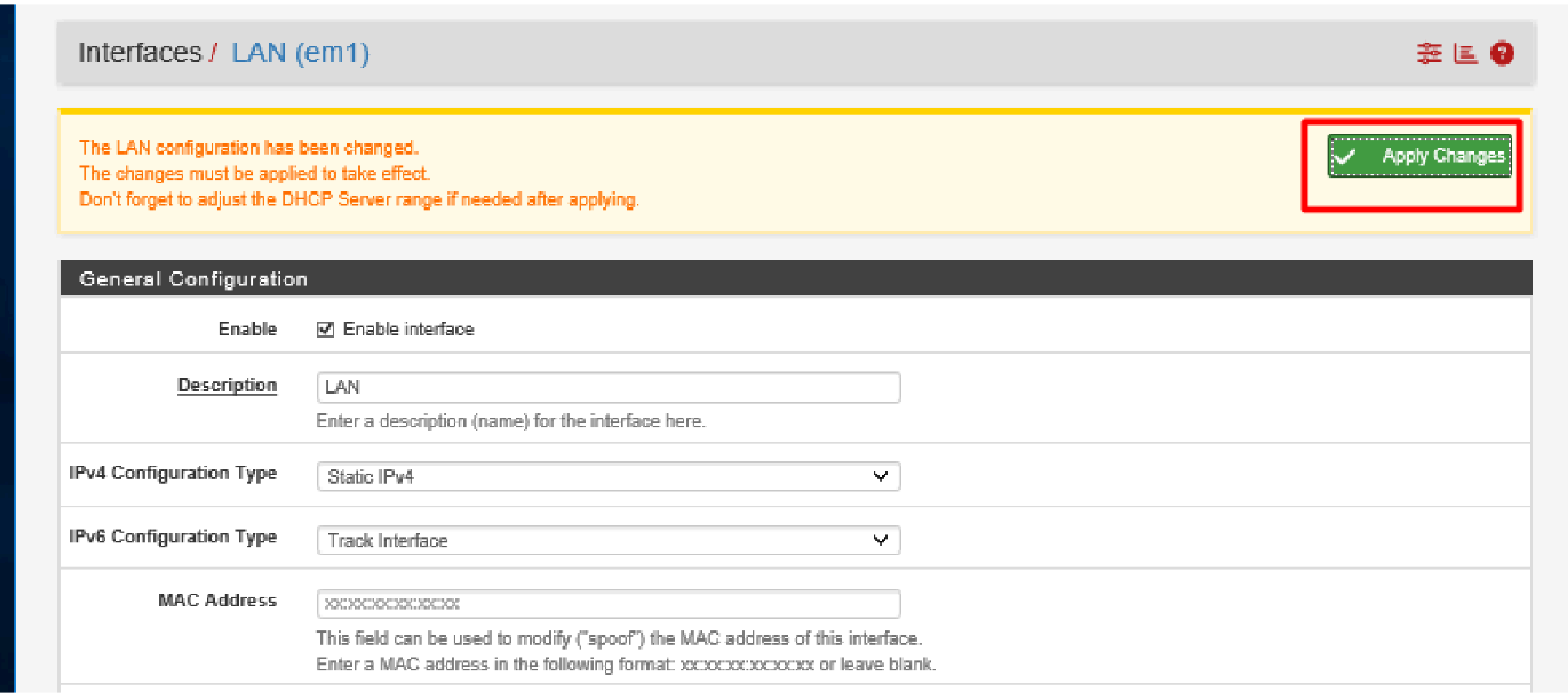
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.



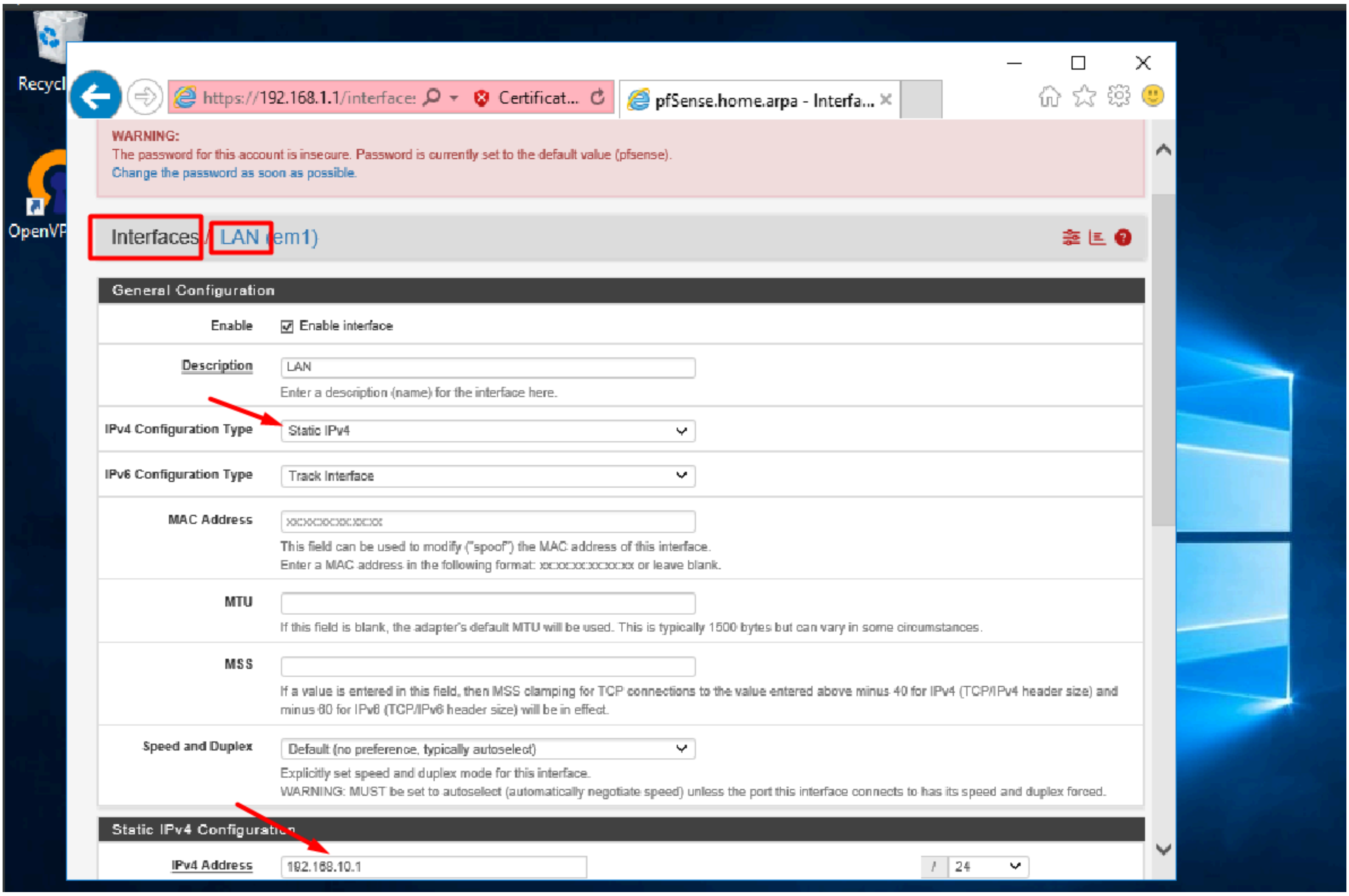
Interfaces / LAN (em1)

The LAN configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

General Configuration

Enable	☑ Enable interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	Track Interface
MAC Address	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

2. Configurez l'interface LAN avec une adresse IP statique



https://192.168.1.1/interface:
Certificat...
pfSense.home.arpa - Interfa...
Recycl
OpenVP

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Interfaces / LAN (em1)

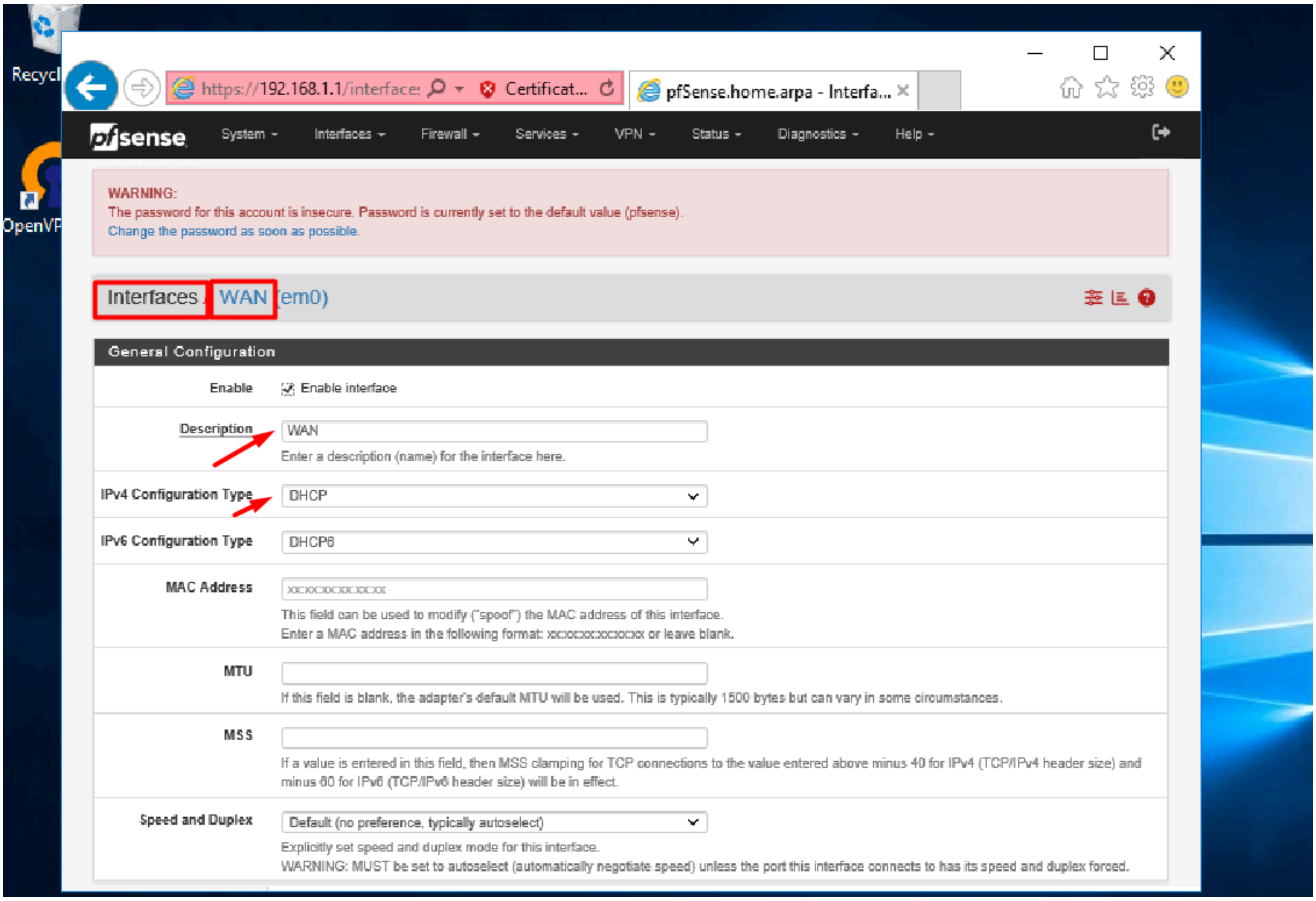
General Configuration

Enable	☑ Enable interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	Track Interface
MAC Address	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	192.168.10.1 / 24

3. Configurez l'interface WAN pour la connexion Internet.



WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

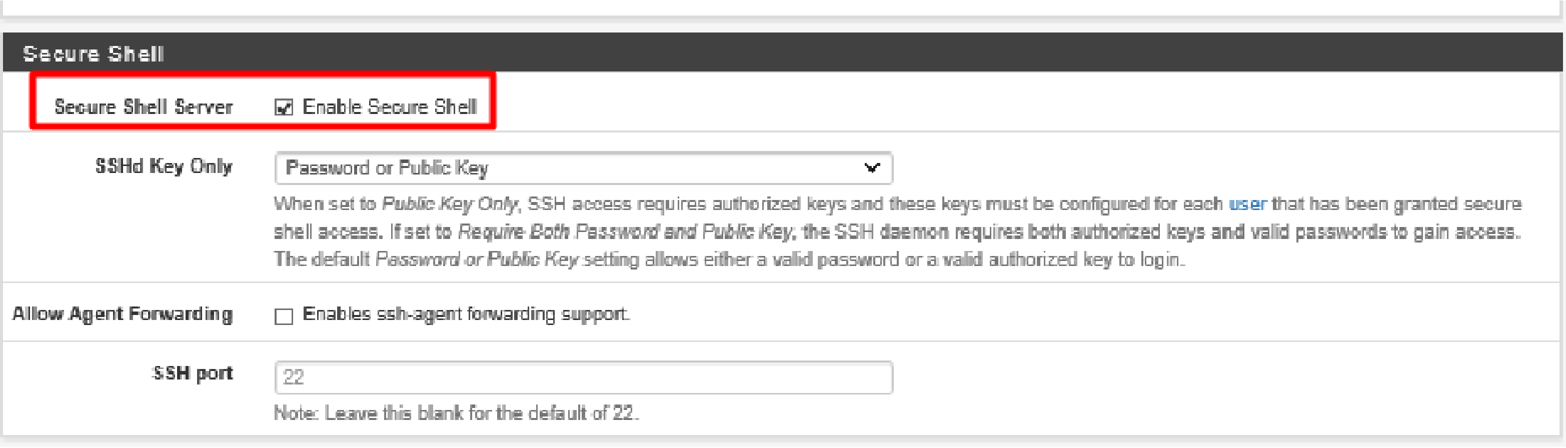
Interfaces / WAN (em0)

General Configuration

Enable	☑ Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	DHCP6
MAC Address	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

4.2. Configuration de l'Accès SSH

1. Activez le service SSH via l'interface Web.



Secure Shell

Secure Shell Server ☑ Enable Secure Shell

SSHd Key Only: Password or Public Key

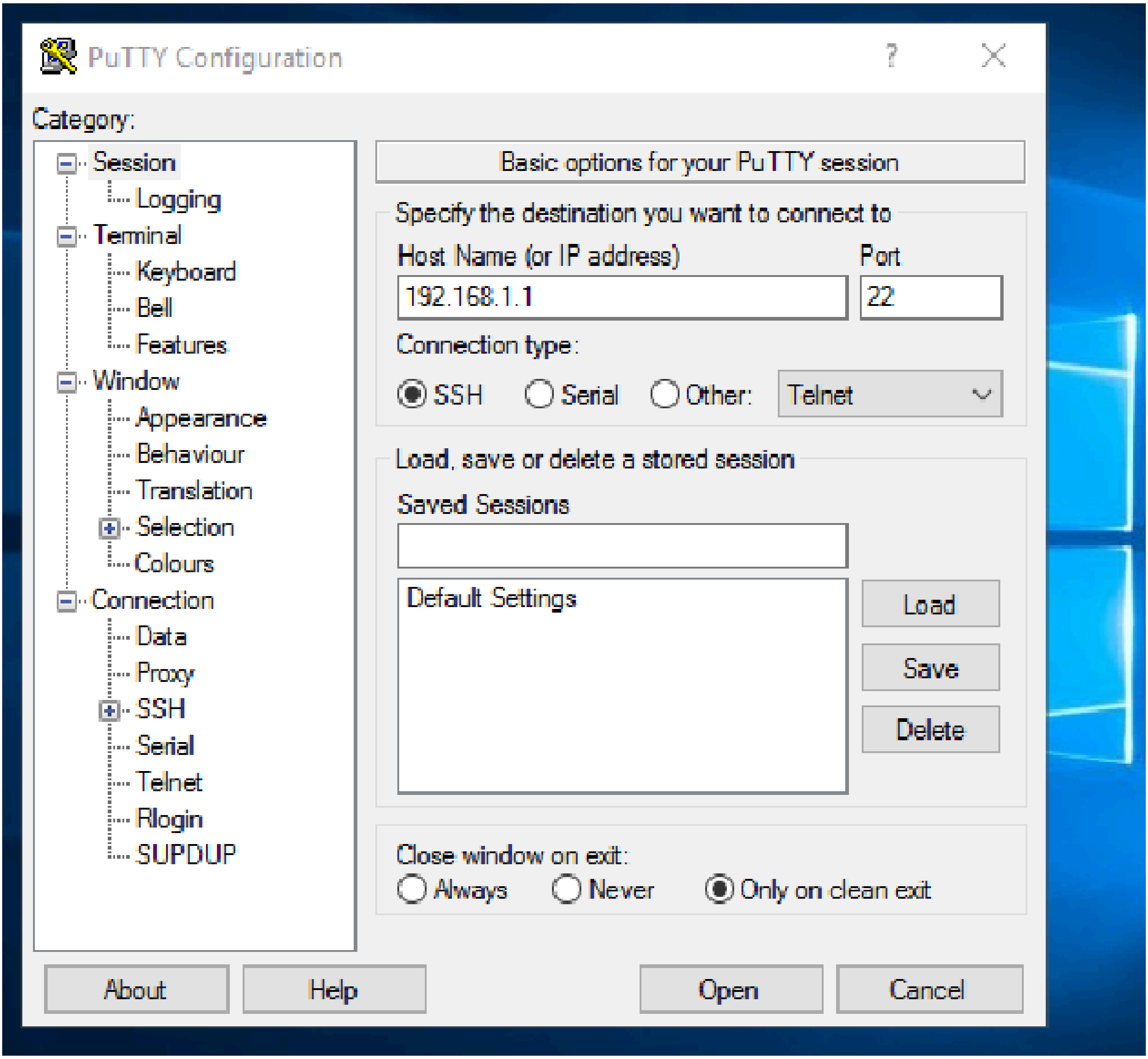
When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys and valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

Allow Agent Forwarding ☐ Enables ssh-agent forwarding support.

SSH port: 22

Note: Leave this blank for the default of 22.

2. Testez la connexion SSH en utilisant Putty.



Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.1

Port: 22

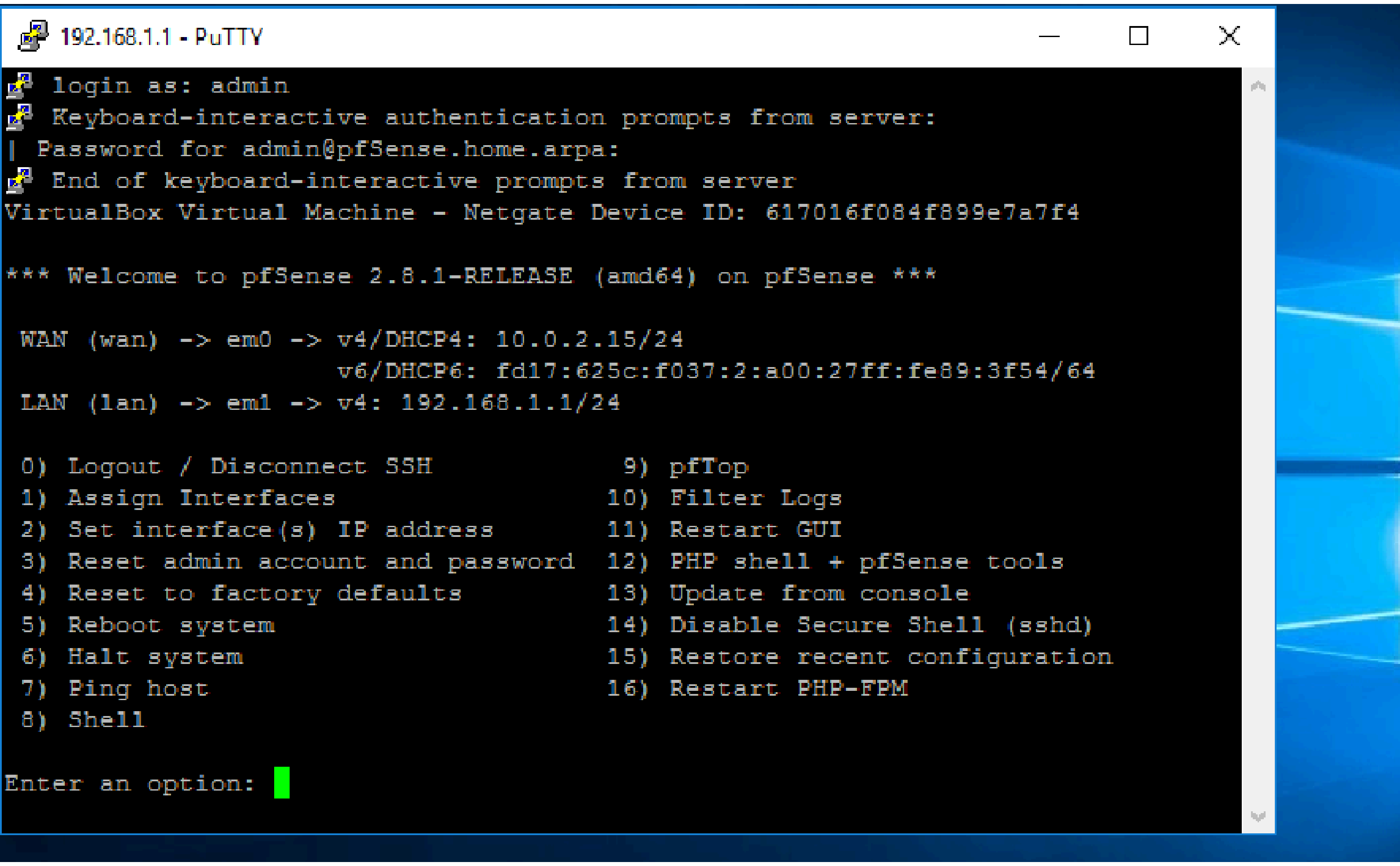
Connection type:
● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

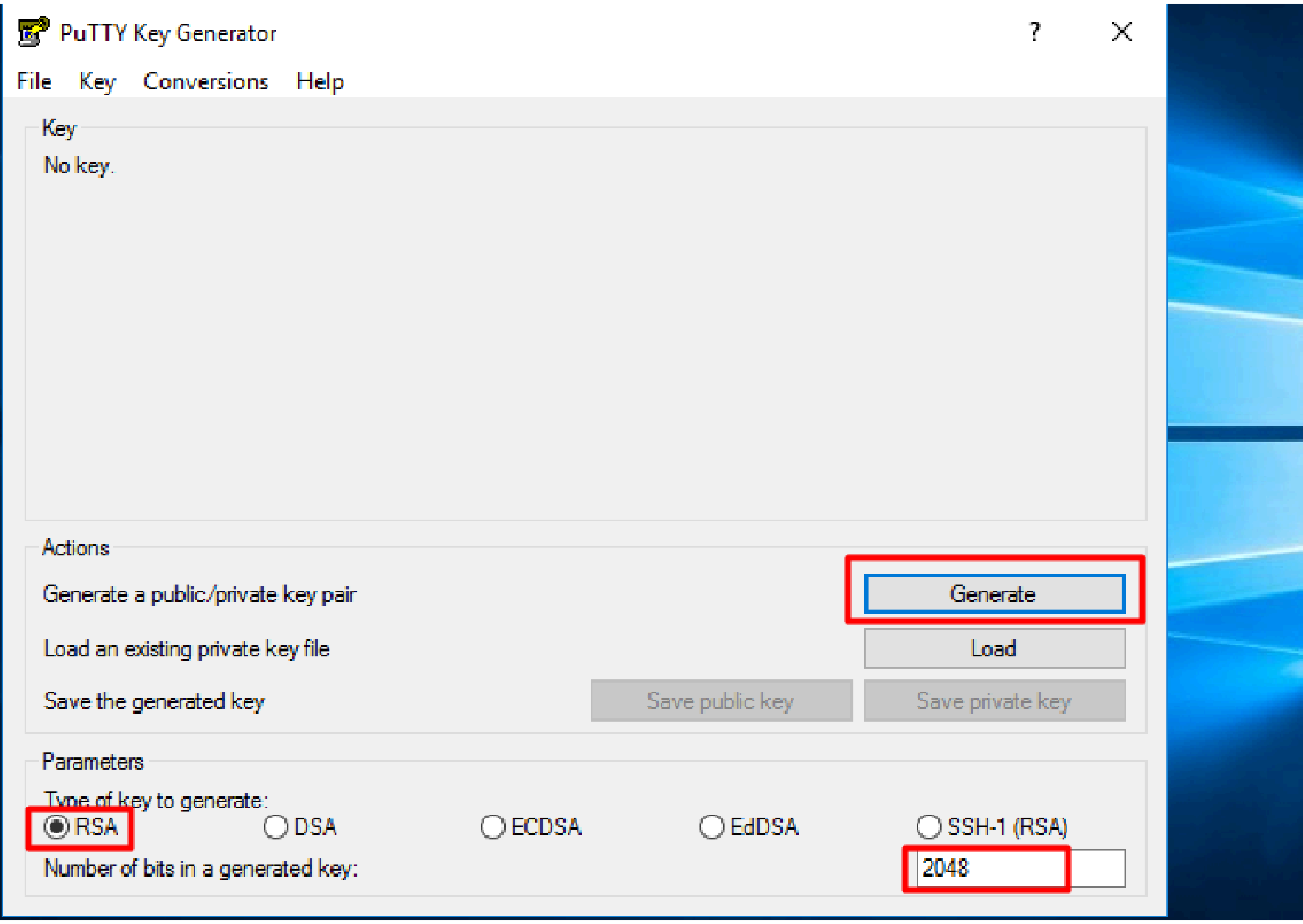
Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit



```
login as: admin
Keyboard-interactive authentication prompts from server:
| Password for admin@pfSense.home.arpa:
End of keyboard-interactive prompts from server
VirtualBox Virtual Machine - Netgate Device ID: 617016f084f899e7a7f4

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

 WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
                     v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe89:3f54/64
 LAN (lan) -> em1 -> v4: 192.168.1.1/24

 0) Logout / Disconnect SSH            9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart GUI
 3) Reset admin account and 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: 
```

3.Désactivez l'authentification par mot de passe et configurez l'authentification par clé RSA avec PuttyKeygen.



Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

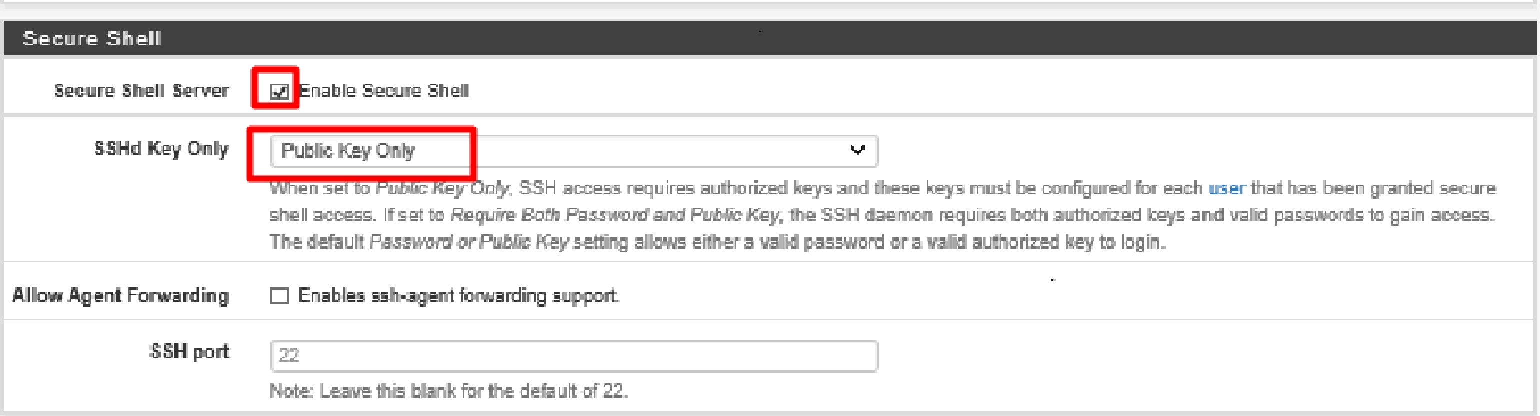
Save the generated key

Parameters

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048



Secure Shell

Secure Shell Server ☑ Enable Secure Shell

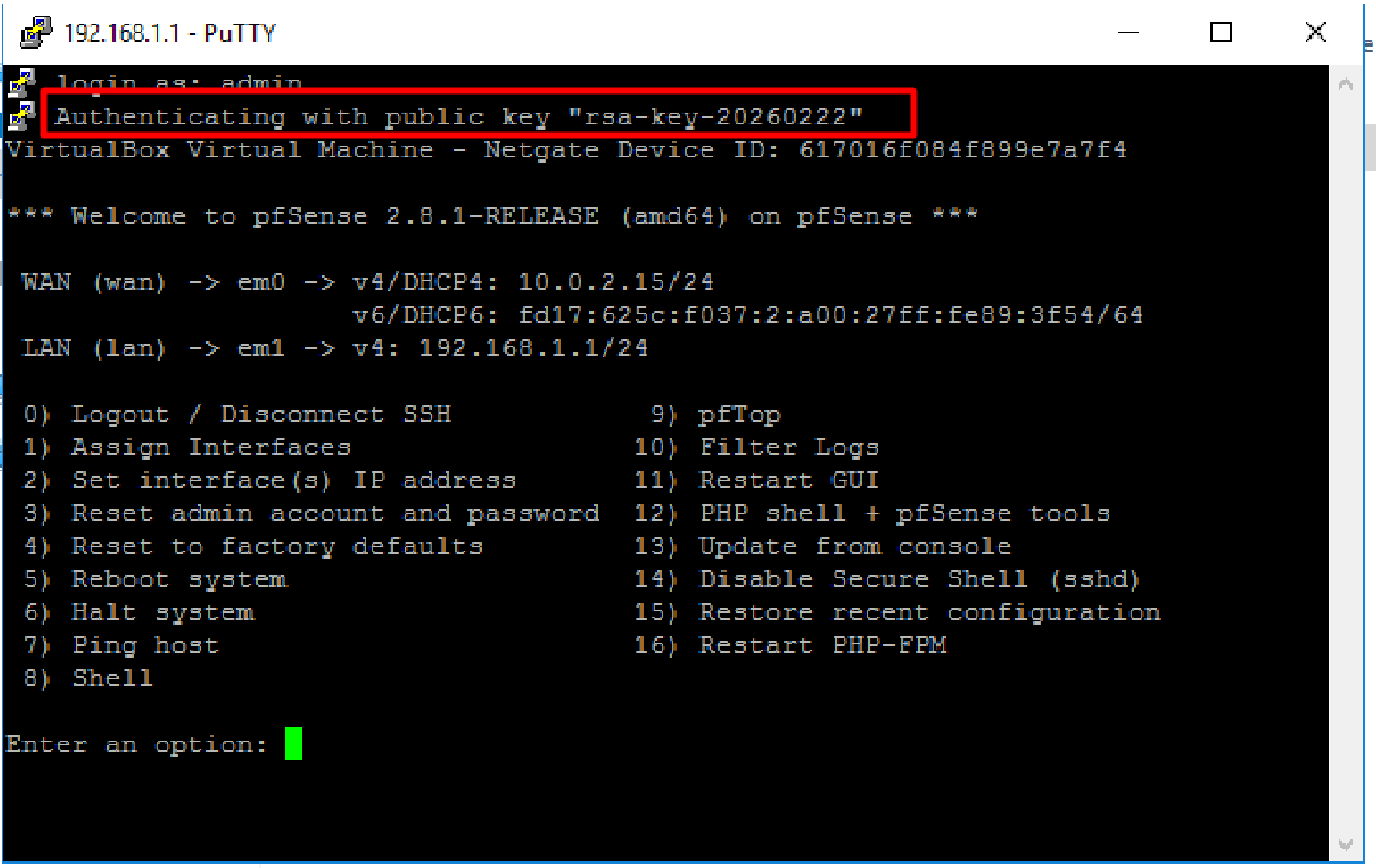
SSHd Key Only: Public Key Only

When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys and valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

Allow Agent Forwarding ☐ Enables ssh-agent forwarding support.

SSH port: 22

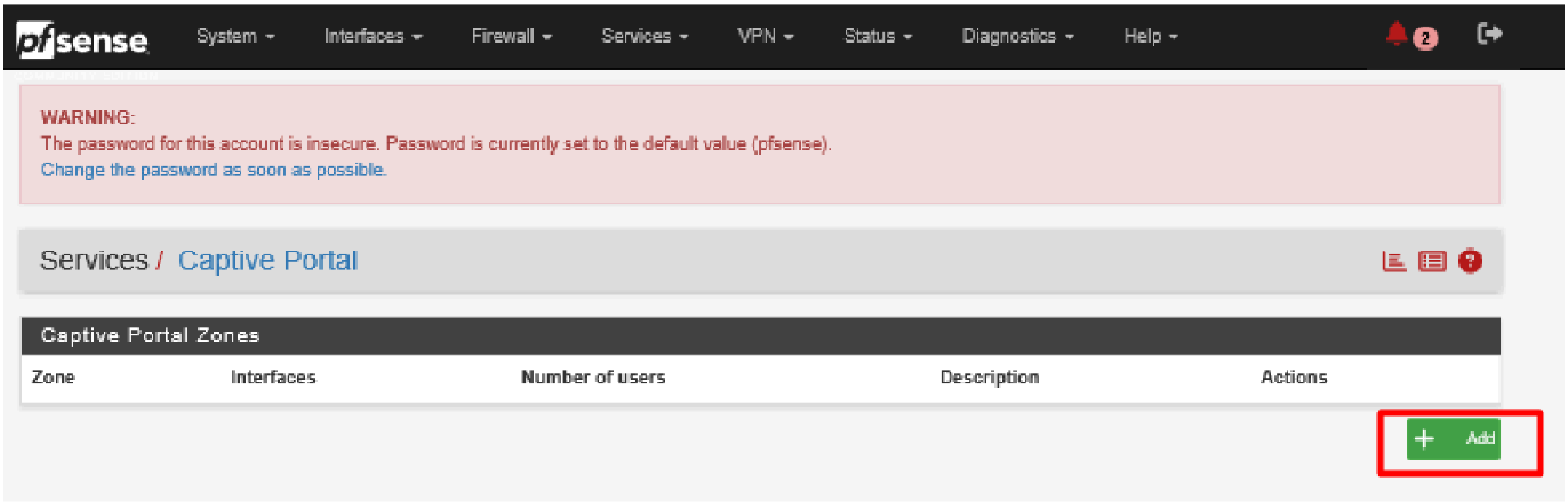
Note: Leave this blank for the default of 22.



```
login as: admin
Authenticating with public key "rsa-key-20260222"
VirtualBox Virtual Machine - Netgate Device ID: 617016f084f899e7a7f4

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

 WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
                     v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe89:3f54/64
 LAN (lan) -> em1 -> v4: 192.168.1.1/24

 0) Logout / Disconnect SSH             9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart GUI
 3) Reset admin account and 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:
```

4.3. Configuration du Portail Captif

1. Activez la fonction de portail captif sur l'interface LAN

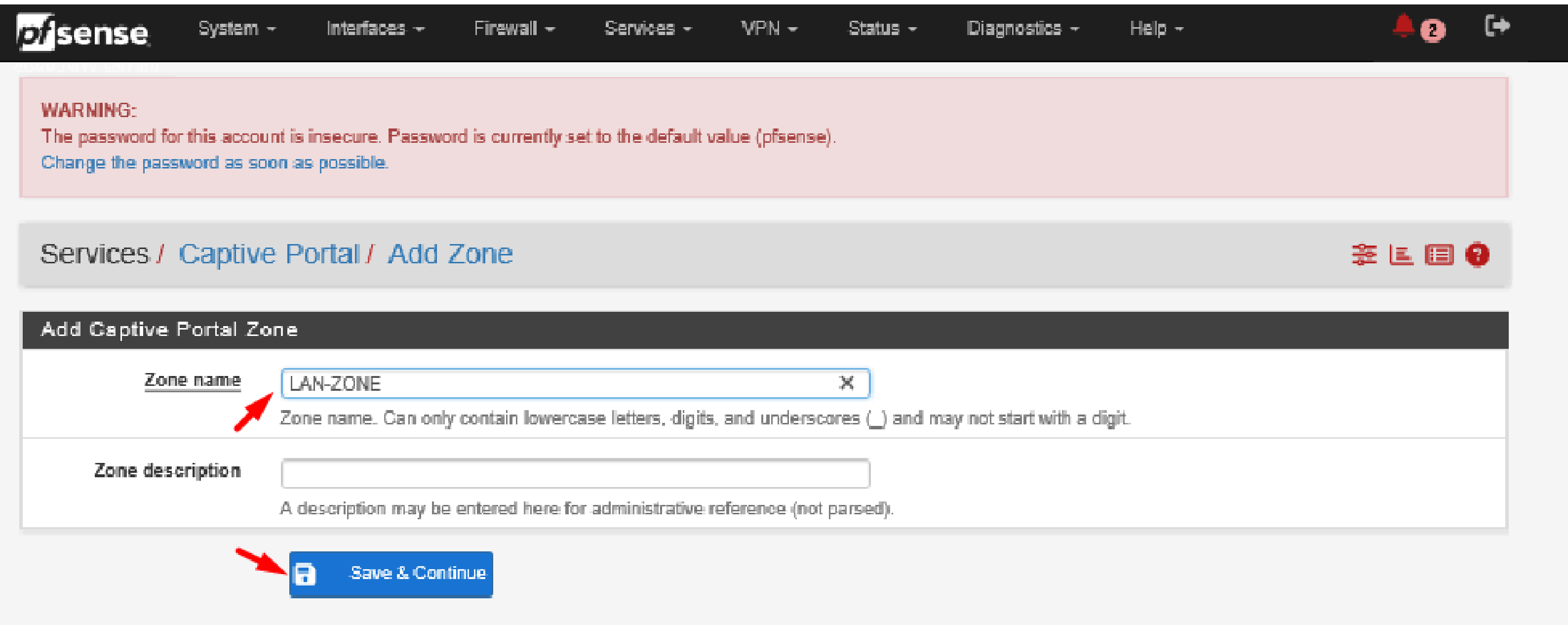


WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions



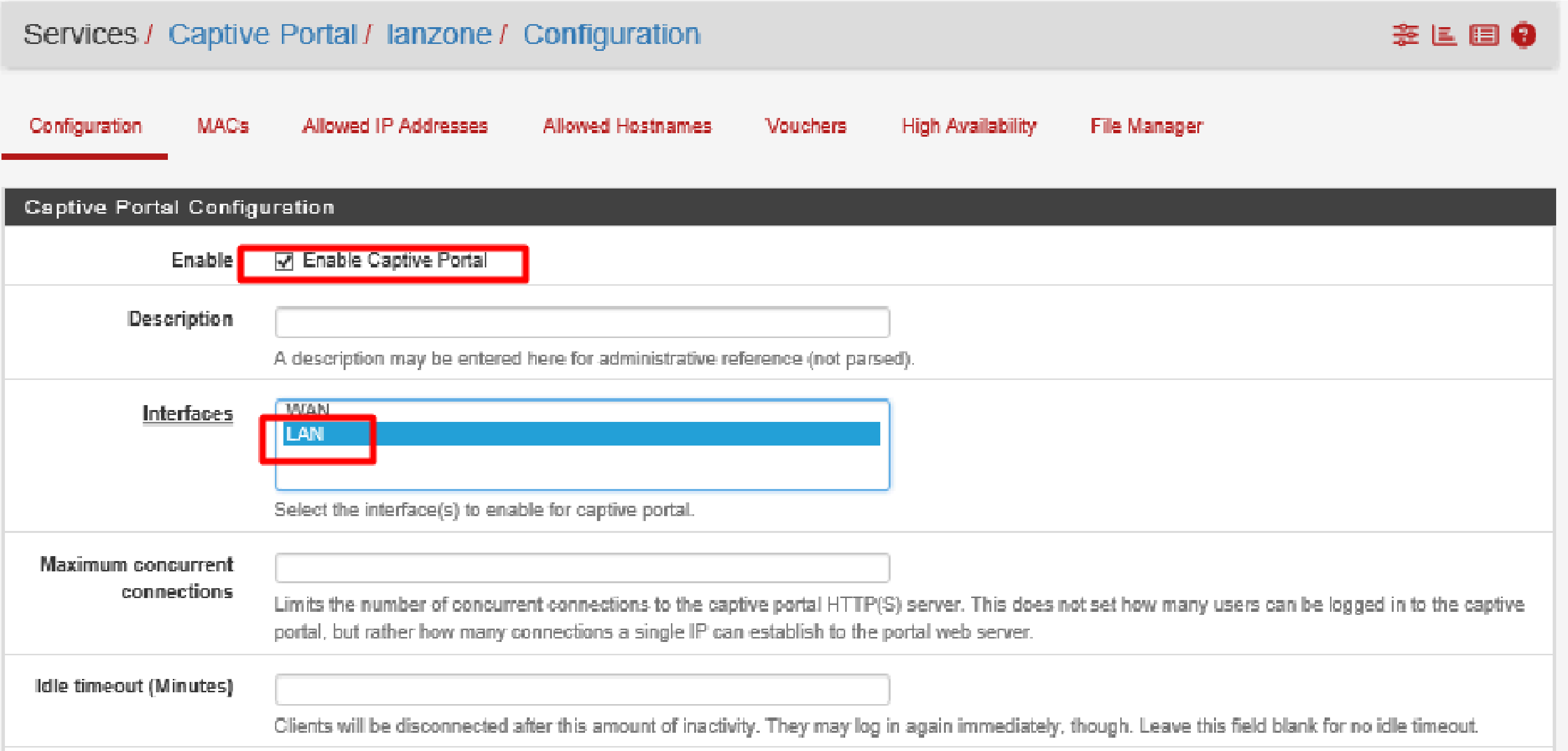
WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name: LAN-ZONE
Zone name. Can only contain lowercase letters, digits, and underscores (_) and may not start with a digit.

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


Services / Captive Portal / lanzone / Configuration

Captive Portal Configuration

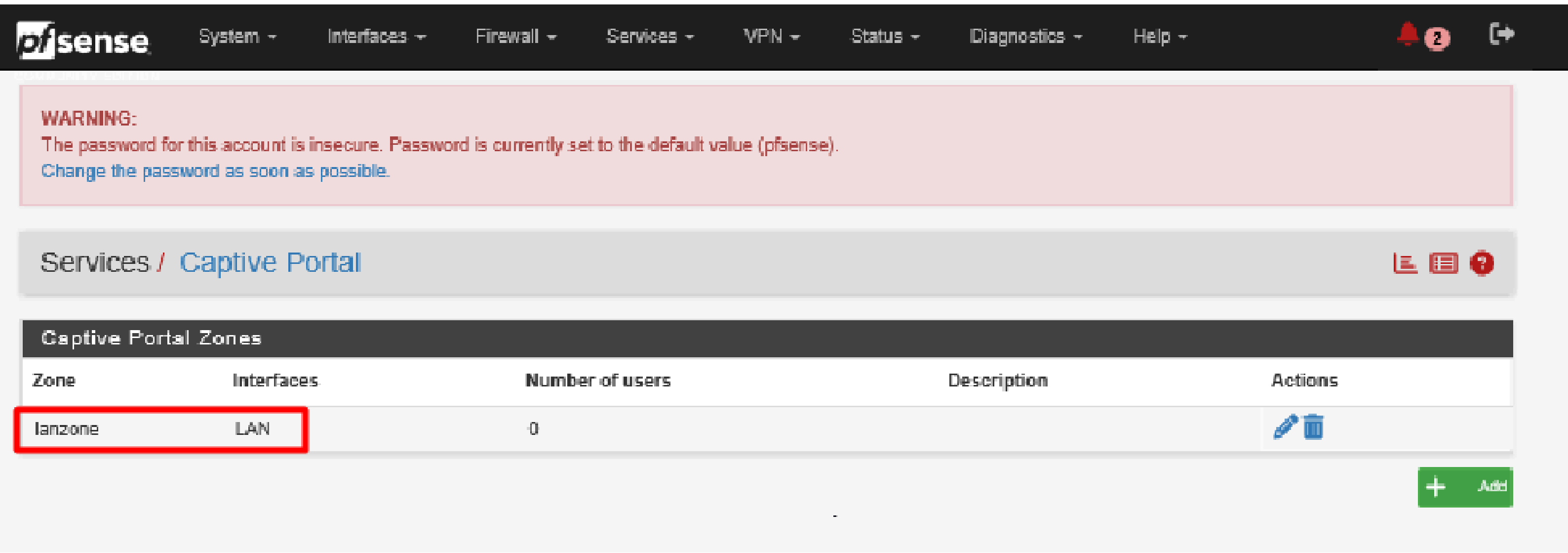
Enable: ☑ Enable Captive Portal

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

Interfaces: WAN / LAN
Select the interface(s) to enable for captive portal.

Maximum concurrent connections:
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

Idle timeout (Minutes):
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

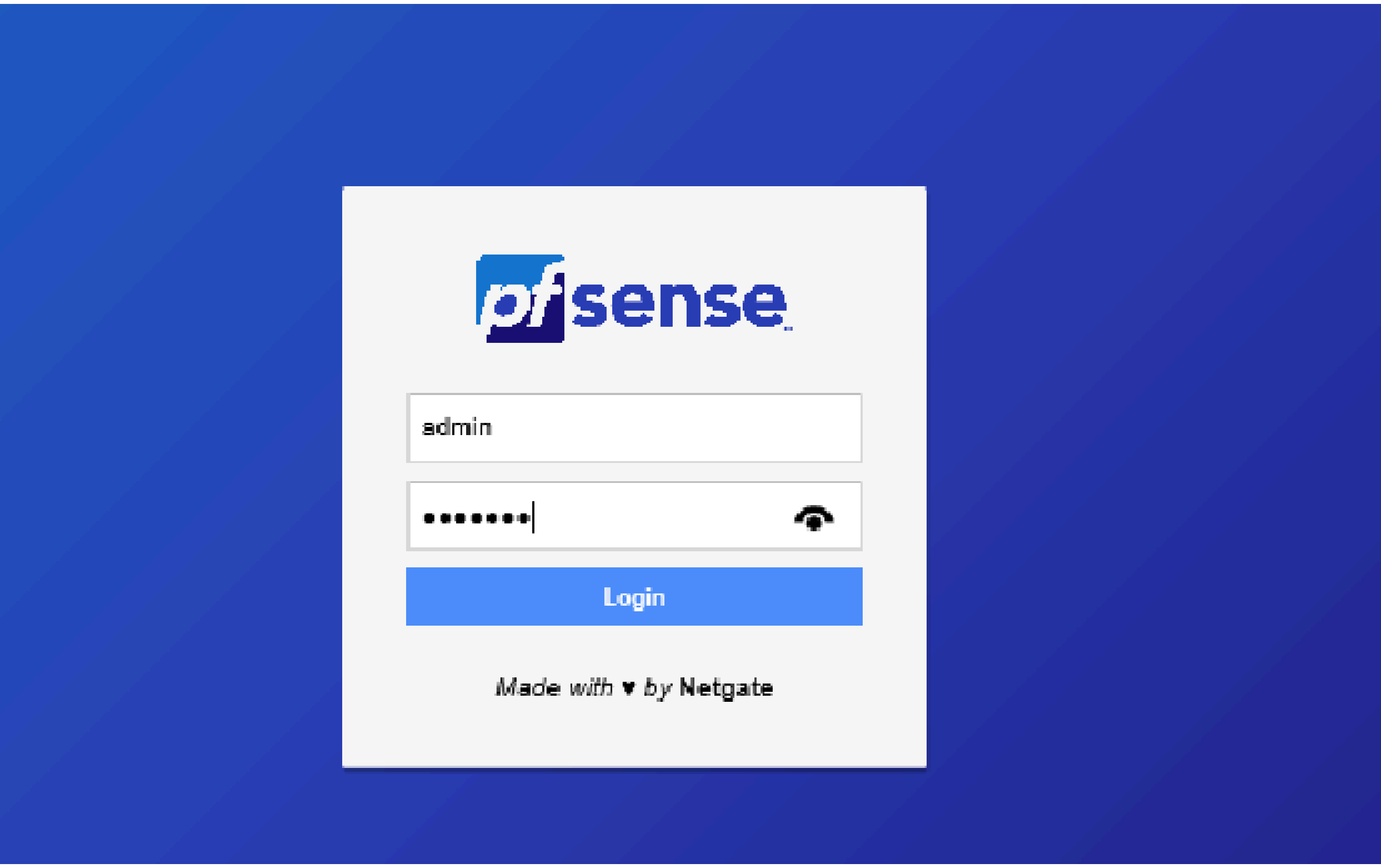


WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

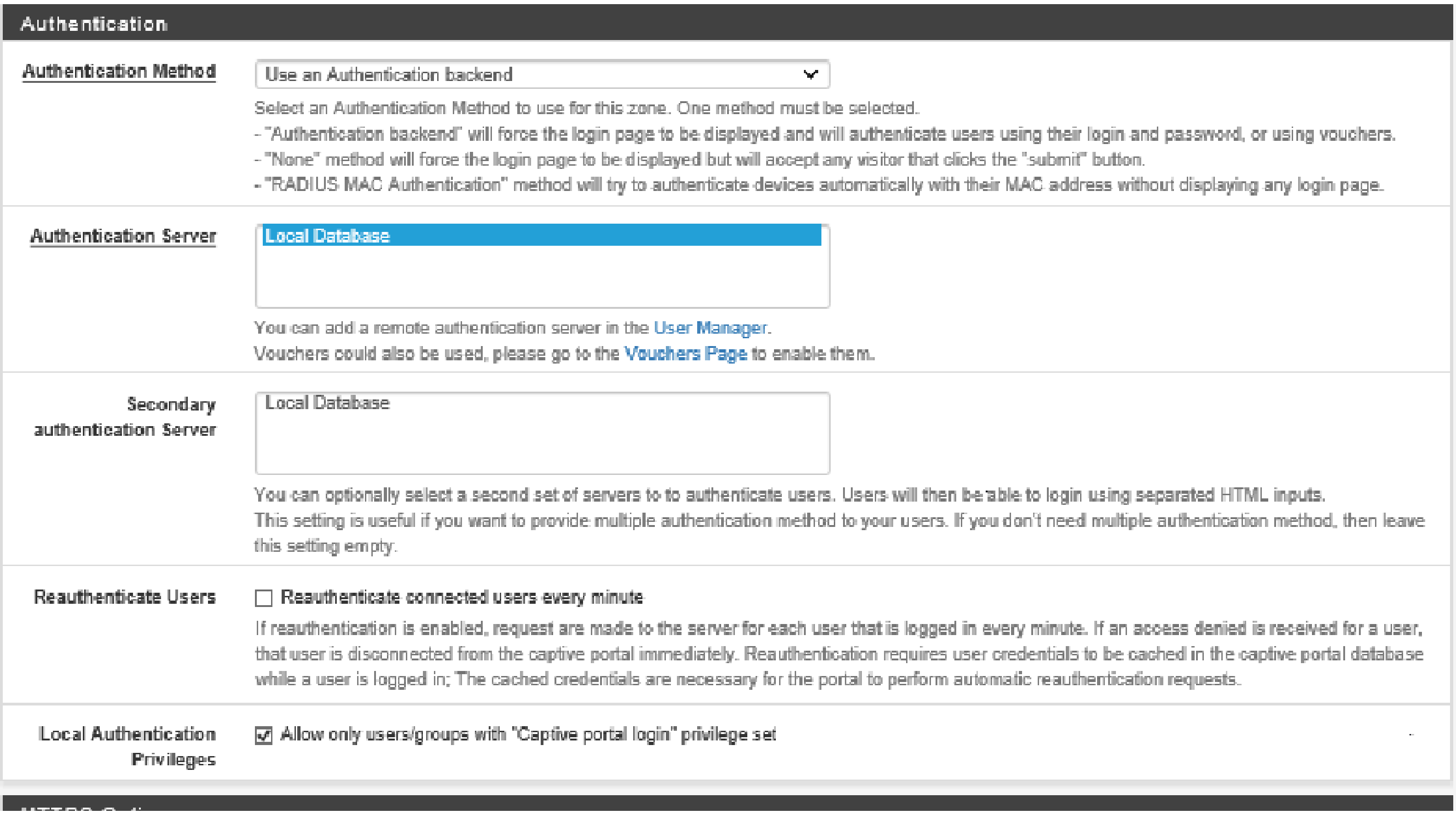
Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
lanzone	LAN	0		



2. Créez un portail captif avec authentification.



Authentication

Authentication Method: Use an Authentication backend

Select an Authentication Method to use for this zone. One method must be selected.
- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server: Local Database

You can add a remote authentication server in the User Manager.
Vouchers could also be used, please go to the Vouchers Page to enable them.

Secondary authentication Server: Local Database

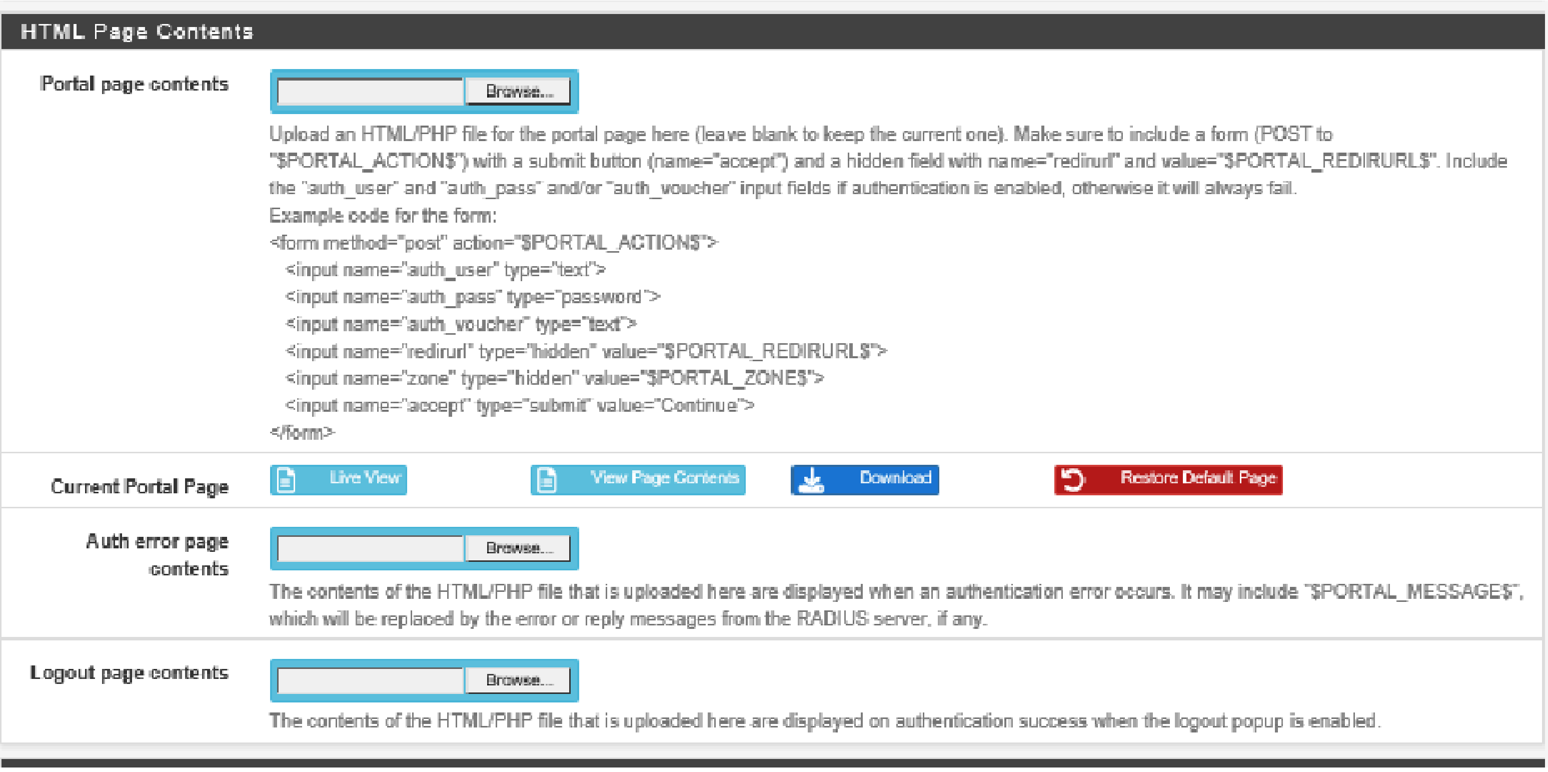
You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs.
This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

Reauthenticate Users: □ Reauthenticate connected users every minute

If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

Local Authentication Privileges: ☑ Allow only users/groups with "Captive portal login" privilege set

3. Ajoutez une page de connexion personnalisée.



HTML Page Contents

Portal page contents

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "$PORTAL_ACTION$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="$PORTAL_REDIRURL$". Include the "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail.

Example code for the form:

```
<form method="post" action="$PORTAL_ACTION$">
   <input name="auth_user" type="text">
   <input name="auth_pass" type="password">
   <input name="auth_voucher" type="text">
   <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
   <input name="zone" type="hidden" value="$PORTAL_ZONE$">
   <input name="accept" type="submit" value="Continue">
</form>
```

Current Portal Page

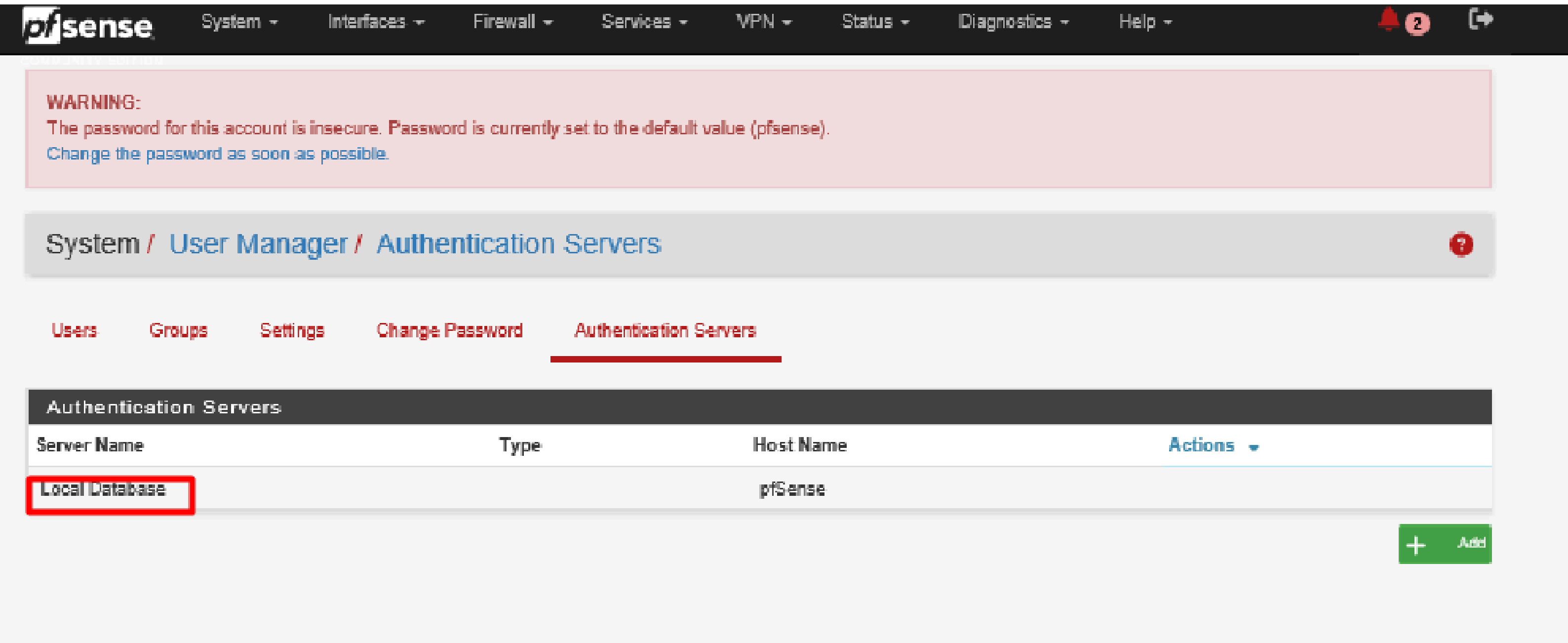
Auth error page contents

The contents of the HTML/PHP file that is uploaded here are displayed when an authentication error occurs. It may include "$PORTAL_MESSAGE$", which will be replaced by the error or reply messages from the RADIUS server, if any.

Logout page contents

The contents of the HTML/PHP file that is uploaded here are displayed on authentication success when the logout popup is enabled.

4. Configurez un backend d'authentification (local ou externe).



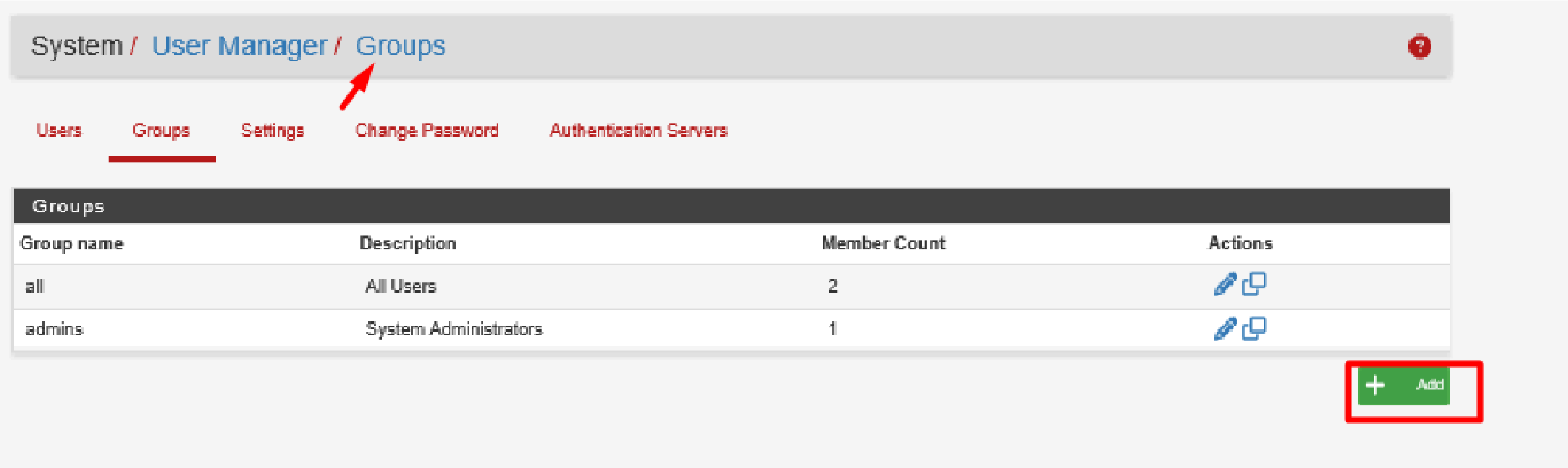
WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

System / User Manager / Authentication Servers

Authentication Servers

Server Name	Type	Host Name	Actions
Local Database		pfSense	

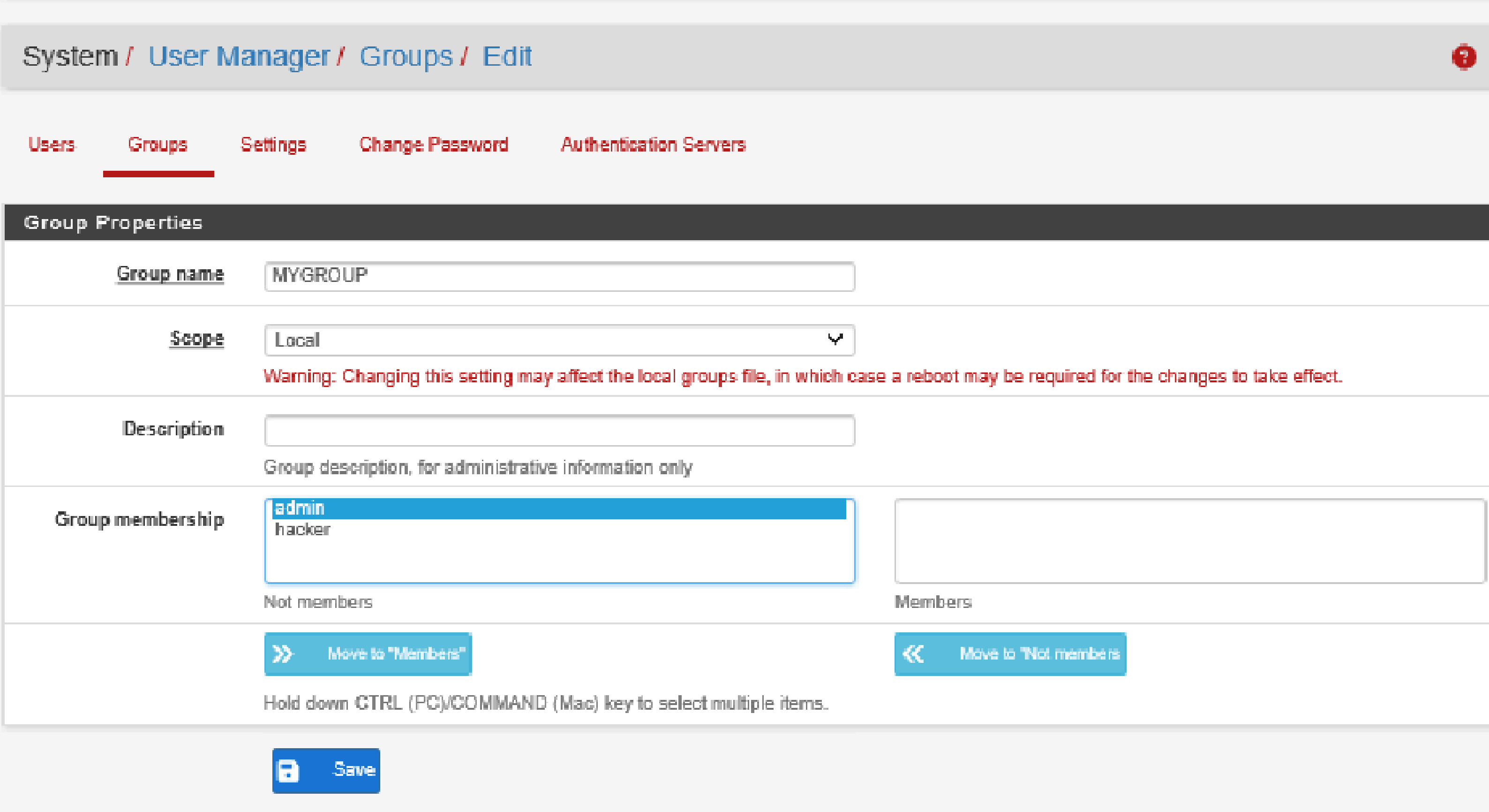
5. Créez un groupe et des utilisateurs pour la gestion des accès.



System / User Manager / Groups

Groups

Group name	Description	Member Count	Actions
all	All Users	2	✎ ⧉
admins	System Administrators	1	✎ ⧉

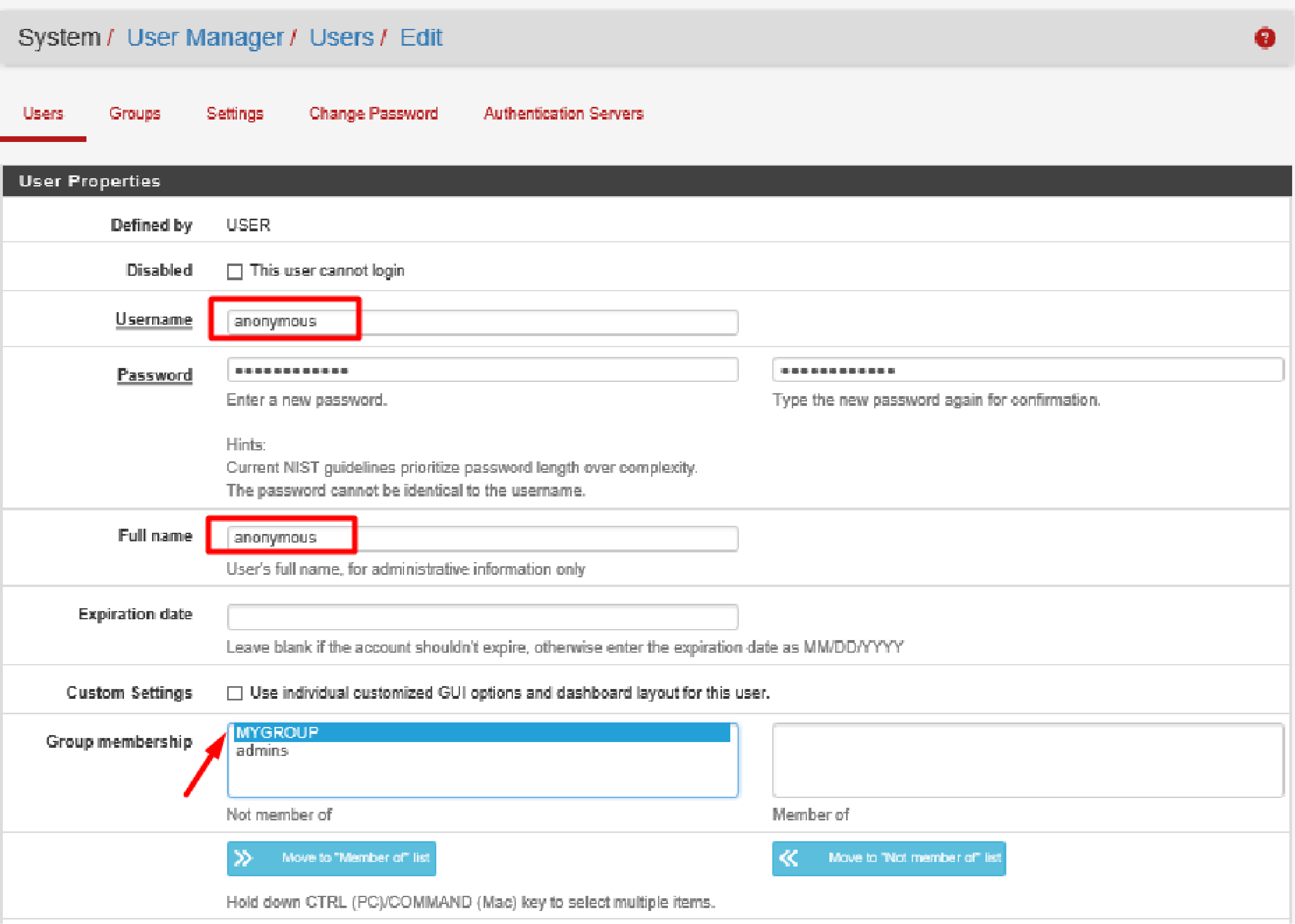


System / User Manager / Groups / Edit

Group Properties

Group name	MYGROUP
Scope	Local Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.
Description	Group description, for administrative information only
Group membership	Not members: admin, hacker Members:

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

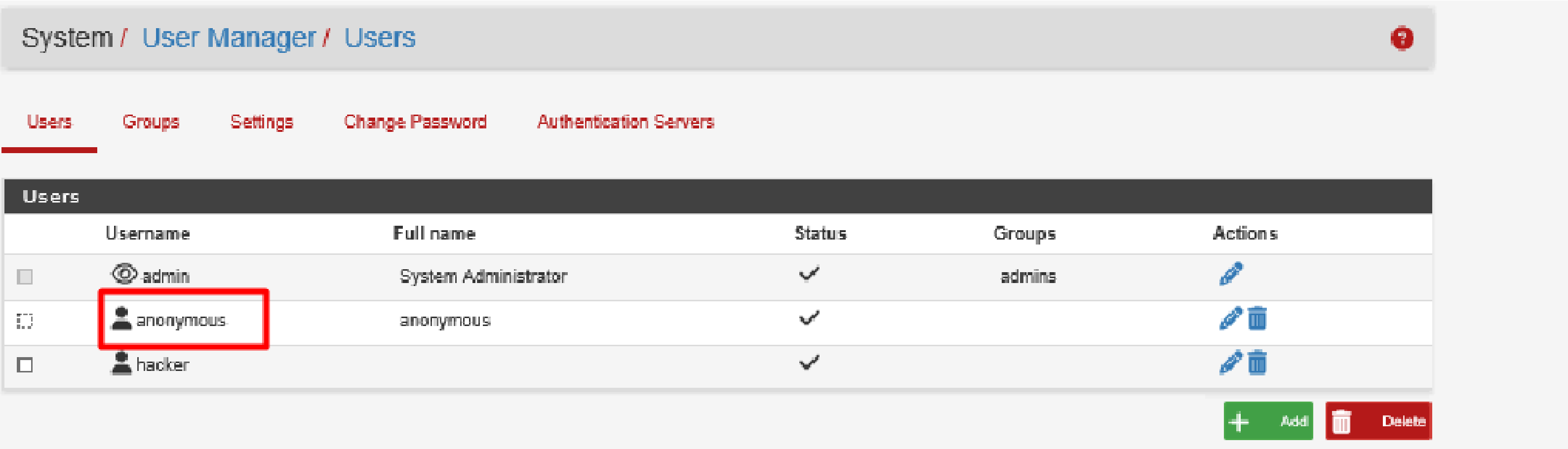


System / User Manager / Users / Edit

User Properties

Defined by	USER
Disabled	□ This user cannot login
Username	anonymous
Password	●●●●●●●●●●●● / ●●●●●●●●●●●●
	Enter a new password. / Type the new password again for confirmation.
	Hints: Current NIST guidelines prioritize password length over complexity. The password cannot be identical to the username.
Full name	anonymous
	User's full name, for administrative information only
Expiration date	
	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	□ Use individual customized GUI options and dashboard layout for this user.
Group membership	MYGROUP admins
	Not member of / Member of

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

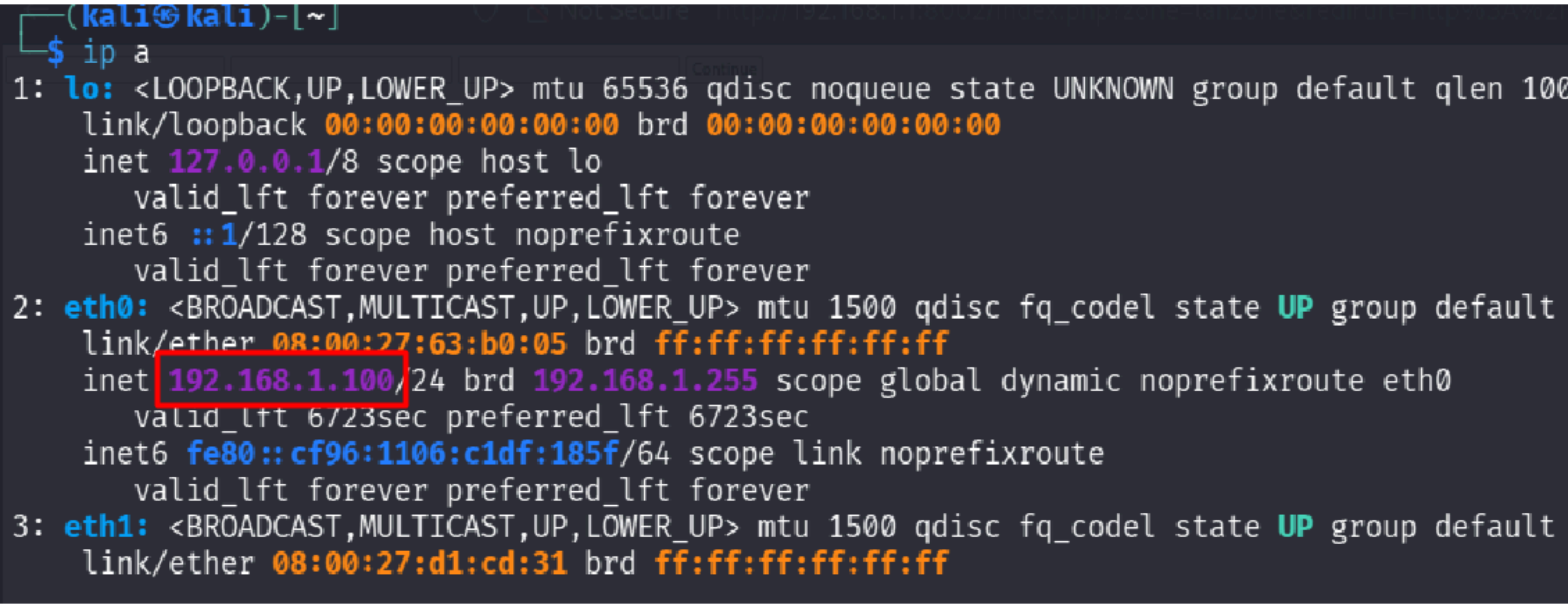


System / User Manager / Users

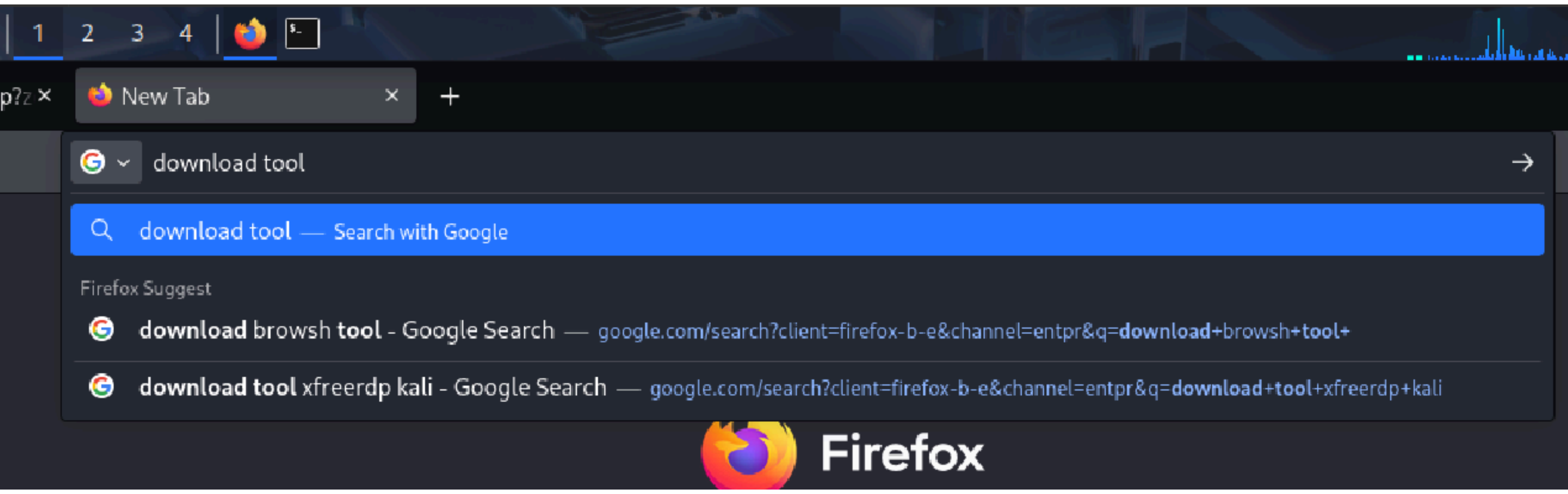
Users

	Username	Full name	Status	Groups	Actions
□	admin	System Administrator	✓	admins	✎
□	anonymous	anonymous	✓		✎ 🗑
□	hacker		✓		✎ 🗑

6. Testez la configuration à partir d'un poste client.



```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 100
    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
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:63:b0:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 6723sec preferred_lft 6723sec
    inet6 fe80::cf96:1106:c1df:185f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:d1:cd:31 brd ff:ff:ff:ff:ff:ff
```



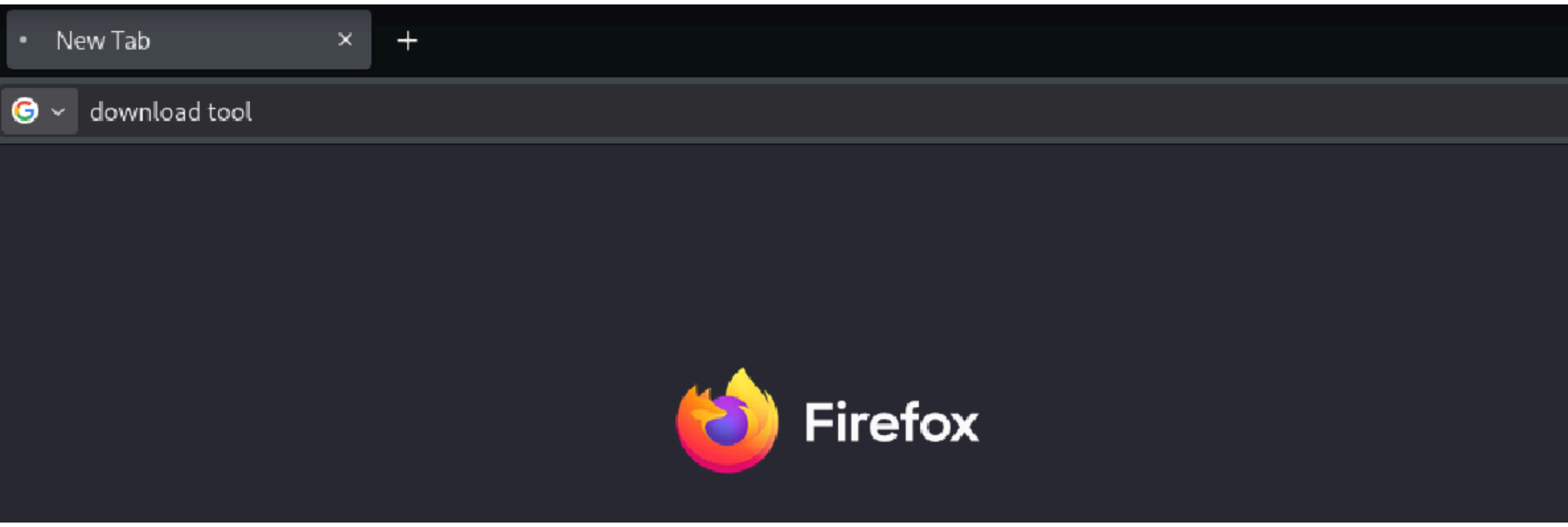
download tool

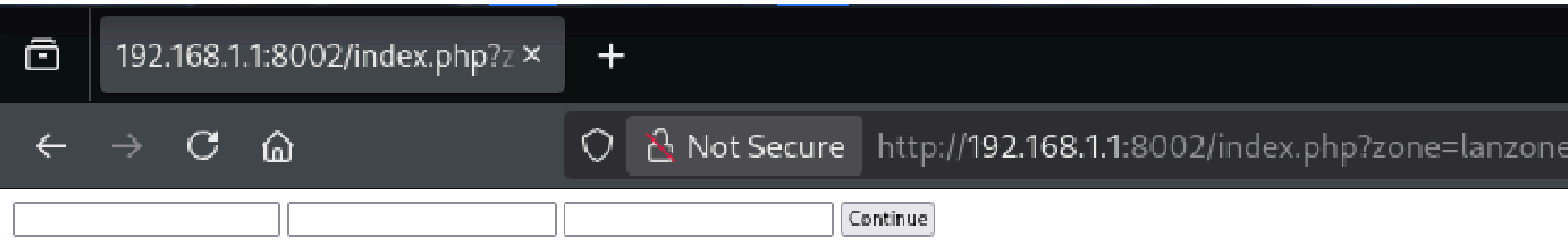
download tool — Search with Google

Firefox Suggest

download browsh tool - Google Search — google.com/search?client=firefox-b-e&channel=entpr&q=download+browsh+tool+

download tool xfreerdp kali - Google Search — google.com/search?client=firefox-b-e&channel=entpr&q=download+tool+xfreerdp+kali




192.168.1.1:8002/index.php?z
Not Secure
http://192.168.1.1:8002/index.php?zone=lanzone
Continue

5. Conclusion

Ce lab vous permettra d'acquérir les compétences pour configurer un pare-feu PfSense, gérer les accès réseau via un portail captif et sécuriser les connexions distantes avec SSH. En suivant ces étapes, vous serez en mesure de déployer une architecture réseau sécurisée, tout en contrôlant l'accès des utilisateurs aux ressources internes.