PROCÉDURE TECHNIQUE · BTS SIO SISR

Administrer un pare-feu pfSense depuis le menu console

Assigner les interfaces, configurer le LAN et le DHCP, réinitialiser le mot de passe admin, redémarrer, tester le réseau et restaurer une configuration, en SSH ou sur la console physique.

Auteur	Plot 1
Contexte	TP réalisé en équipe — Plot 1, domaine ngrange.local
Version	2.0 — novembre 2026
Environnement	pfSense « 2.9.0-RELEASE (amd64) » selon le TP d'origine · client SSH (PuTTY) · menu console à 16 options
Durée estimée	45 min

Identifiants d'accès — Plot 1

Machine / service	Adresse	Identifiant	Mot de passe
pfSense (web + console)	https://192.168.21.254	`admin`	`pfsense (par défaut, à remplacer)`
PC-CLIENT	192.168.21.10	`sio2`	`Azerty13.`

À savoir

Les captures proviennent du TP réalisé en équipe : les adresses et noms visibles peuvent différer ; les valeurs à utiliser sont celles du texte (Plot 1).

Sommaire

1. Objectif
2. Architecture et prérequis
3. Connexion et menu principal
4. Assigner les interfaces (option 1)
5. Configurer le LAN et le DHCP (option 2)
6. Réinitialiser le mot de passe admin (option 3)
7. Retour aux paramètres d'usine (option 4)
8. Redémarrer, arrêter (options 5 et 6)
9. Tester avec un ping (option 7)
10. Restaurer une configuration (option 15)
11. Vérification, dépannage, sécurité
12. Aide-mémoire et glossaire
13. Aide-mémoire : utiliser pfSense au quotidien

1. Objectif

Le menu console de pfSense permet d'agir sur le pare-feu quand l'interface web (webConfigurator) est inaccessible : adresse IP erronée, mot de passe perdu, interface mal assignée, configuration défectueuse. Cette procédure sert de support de dépannage et d'aide-mémoire. Elle détaille les options 1 à 7 et l'option 15, avec pour chacune son impact et son niveau de risque.

2. Architecture et prérequis

Élément	Valeur
Produit	pfSense 2.9.0-RELEASE (amd64), version indiquée par le TP d'origine
Accès	SSH (PuTTY) ou console physique (écran et clavier) ; compte `admin`
Nom de l'hôte	pfSense.home.arpa
Interface WAN	em0, <IP_WAN>/<masque> (non fournie ; côté box ou Internet)
Interface LAN	ue0 (adaptateur USB Ethernet), 192.168.21.254/24 (VLAN 21, passerelle des clients)
Plage DHCP du LAN	192.168.21.100 à 192.168.21.199 (les adresses .1 à .10 sont réservées aux serveurs en IP fixe ; DNS fournis aux clients : 192.168.21.1 et 192.168.21.2)
Interfaces détectées	em0 (MAC f8:b4:6a:bc:6d:50) et ue0 (MAC 3c:18:a0:50:0e:4c), toutes deux « up »
Prérequis	Mot de passe du compte admin ; au moins deux interfaces réseau ; SSH activé ou accès console

> **Attention**
> Le WAN (<IP_WAN>) et le LAN (192.168.21.0/24) doivent appartenir à deux sous-réseaux distincts : pfSense ne peut pas router correctement entre deux interfaces d'un même réseau. L'adresse WAN fournie par la box ou le réseau amont ne doit donc pas être dans 192.168.21.0/24.

3. Connexion et menu principal

1 Ouvrir la session SSH

Lancer le client SSH vers pfSense.home.arpa (ou son adresse IP). À l'invite `login as:`, saisir `admin` puis le mot de passe : l'authentification se fait en mode « keyboard-interactive ». Le menu console s'affiche ensuite. Sur la console physique, le même menu apparaît directement après le démarrage.

```
ssh admin@pfSense.home.arpa
```

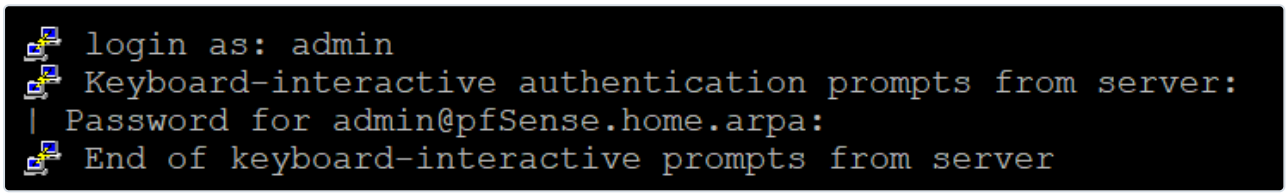

Figure 1 – Connexion SSH : identifiant et mot de passe du compte admin

2 Lire le menu principal

Le haut du menu rappelle l'état des interfaces et leurs adresses IPv4. Choisir une option en tapant son numéro puis Entrée ; la plupart demandent une confirmation `y/n`. Contrôler dès l'ouverture que WAN et LAN portent les adresses attendues.

```
WAN (wan)  -> em0 -> v4: 192.168.1.248/24
LAN (lan)  -> ue0 -> v4: 192.168.1.200/24

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
```

Figure 2 – Menu principal de la console pfSense

N°	Option	Fonction	Risque
0	Logout / Disconnect SSH	Fermer la session	Faible
1	Assign Interfaces	Associer ports physiques et rôles WAN / LAN	Moyen
2	Set interface(s) IP address	Adresse IP d'une interface et DHCP	Moyen
3	Reset admin account and password	Nouveau mot de passe admin	Moyen
4	Reset to factory defaults	Retour aux paramètres d'usine	Élevé
5	Reboot system	Redémarrer	Faible
6	Halt system	Arrêter proprement	Moyen
7	Ping host	Tester la connectivité depuis pfSense	Faible
8, 9, 10	Shell, pfTop, Filter Logs	Shell système, connexions en temps réel, journaux du pare-feu	Non détaillé
11, 16	Restart GUI, Restart PHP-FPM	Relancer l'interface web / PHP-FPM	Non détaillé
12, 13, 14	PHP shell, Update from console, Disable sshd	Outils PHP, mise à jour, désactivation du SSH	Non détaillé
15	Restore recent configuration	Revenir à une configuration de l'historique	Moyen

4. Assigner les interfaces (option 1)

> **Fiche**
> Option 1 · Objectif : associer em0 et ue0 aux rôles WAN et LAN · Impact : l'accès peut être perdu en cas d'erreur · Risque : moyen.

3 Lancer l'assignation et répondre à la question VLAN

Taper `1`. pfSense liste les interfaces valides avec leur adresse MAC et leur état : les MAC permettent d'identifier une carte quand la correspondance entre nom (em0, ue0) et port physique n'est pas évidente. À la question `Should VLANs be set up now [y|n]?`, répondre `n` : sans VLAN sur l'interface de base, ils se créent plus tard dans le webConfigurator.

```
Enter an option: 1


Valid interfaces are:

em0     f8:b4:6a:bc:6d:50   (up) AHCI enclosure management bridge
ue0     3c:18:a0:50:0e:4c   (up) USB Ethernet

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n
```

Figure 3 – Option 1 : interfaces valides et question sur les VLAN

4 Désigner le WAN puis le LAN

À `Enter the WAN interface name or 'a' for auto-detection`, saisir `em0`. À la question suivante, saisir `ue0` pour le LAN : cette étape active le mode complet Firewalling/NAT. Avec une troisième interface (OPT1, etc.), la saisir ensuite ; ici, Entrée sans rien taper termine la saisie. L'option `a` (auto-détection) exige de débrancher d'abord tous les câbles : à réserver au cas où l'on ignore quelle carte porte quel nom.

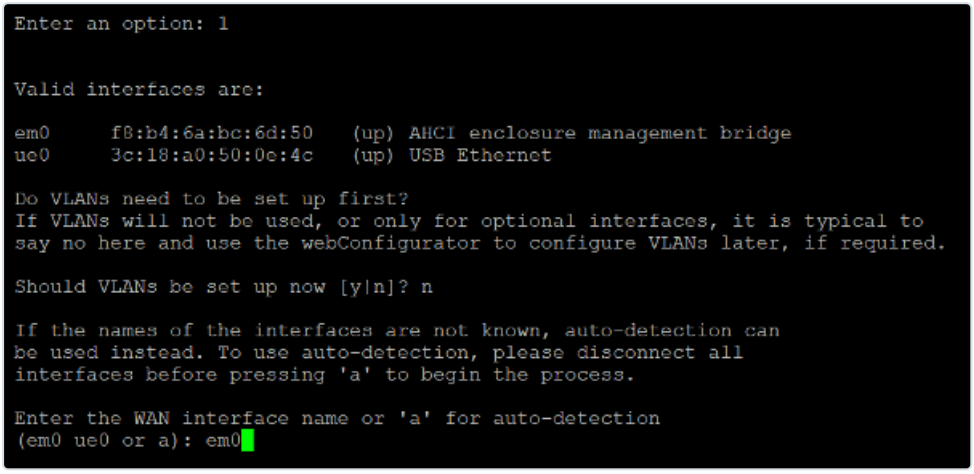

Figure 4 – Saisie de l'interface WAN (em0)

5 Valider l'assignation

pfSense récapitule `WAN -> em0` et `LAN -> ue0`, puis demande `Do you want to proceed [y|n]?`. Taper `y`. Le menu se réaffiche avec WAN (wan) -> em0 et LAN (lan) -> ue0 : vérifier que les adresses IP sont cohérentes avec le réseau.

```
Enter an option: 1
Should VLANs be set up now [y|n]? n
Enter the WAN interface name or 'a' for auto-detection: em0
Enter the LAN interface name or 'a' for auto-detection: ue0
Do you want to proceed [y|n]? y
```

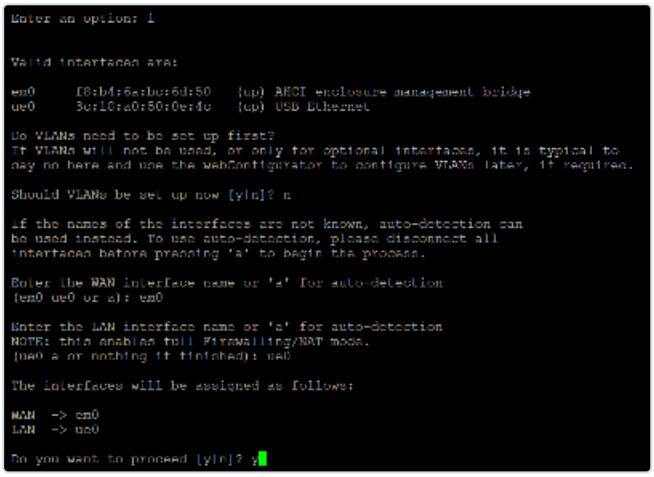

Figure 5 – Récapitulatif et confirmation de l'assignation (y)

> **Attention**
>
> Ne pas inverser WAN et LAN : l'accès à l'administration serait perdu. Modifier l'interface qui porte la session SSH coupe aussi cette session. Un adaptateur USB Ethernet (ue0) convient aux essais mais reste moins fiable qu'une carte PCI ou intégrée en usage permanent.

5. Configurer le LAN et le DHCP (option 2)

> **Fiche**
>
> Option 2 · Objectif : adresse, masque et serveur DHCP du LAN · Impact : la session SSH est coupée si elle passe par cette interface · Risque : moyen.

6 Choisir l'interface et saisir l'adresse

Taper `2`, puis le numéro `2` (LAN, ue0). À `Configure IPv4 address LAN interface via DHCP?`, répondre `n` pour une adresse statique. Saisir `192.168.21.254`, puis le masque en notation CIDR (nombre de bits de 1 à 32) : `24`.

Masque	Bits à saisir
255.255.255.0	24
255.255.0.0	16
255.0.0.0	8

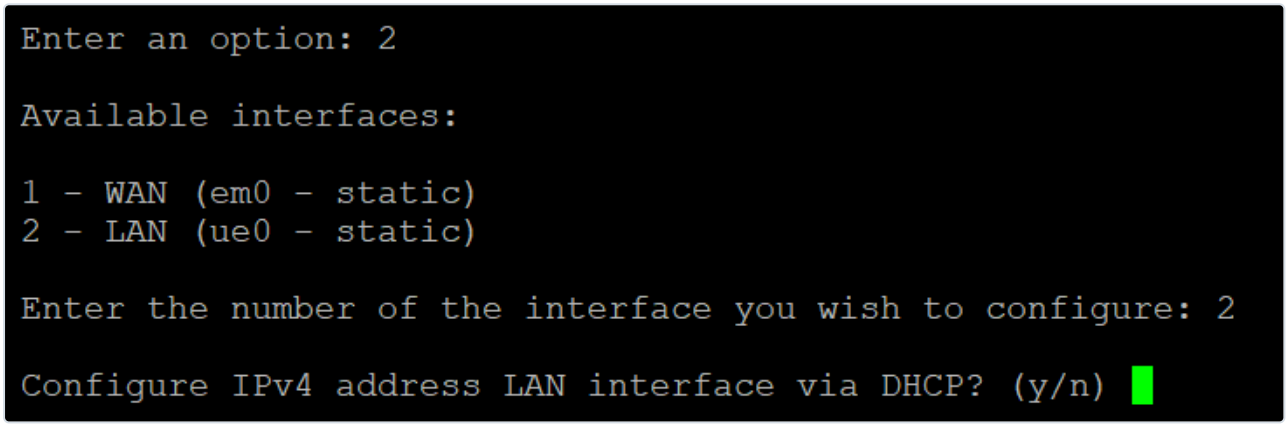

Figure 6 – Option 2 : choix de l'interface LAN et refus du DHCP client

7 Passerelle, IPv6, DHCP et protocole web

Laisser la passerelle vide (Entrée) : seul le WAN en possède une. Répondre `n` au DHCP6, Entrée pour l'adresse IPv6, puis `y` à `Do you want to enable the DHCP server on LAN?`. Saisir la plage : début `192.168.21.100`, fin `192.168.21.199` ; elle doit rester dans le sous-réseau du LAN, exclure l'adresse du pfSense (.254) et les adresses fixes des serveurs (.1 à .10). Enfin, pfSense affiche `Disabling IPv6 DHCPD...` et demande s'il faut revenir à HTTP pour le webConfigurator. Le TP d'origine a répondu `y` (HTTP) ; répondre `n` conserve HTTPS, recommandé. Les serveurs DNS remis aux clients (SRV-AD1EX 192.168.21.1 et SRV-AD2 192.168.21.2) se renseignent ensuite dans le webConfigurator (*Services › DHCP Server › LAN › DNS servers*) ; la passerelle distribuée est l'IP du LAN, 192.168.21.254.

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address: 192.168.21.254
Enter the new LAN IPv4 subnet bit count (1 to 32): 24
Upstream gateway address (LAN): [Entrée]
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address: [Entrée]
Do you want to enable the DHCP server on LAN? (y/n) y
Start address: 192.168.21.100    End address: 192.168.21.199
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

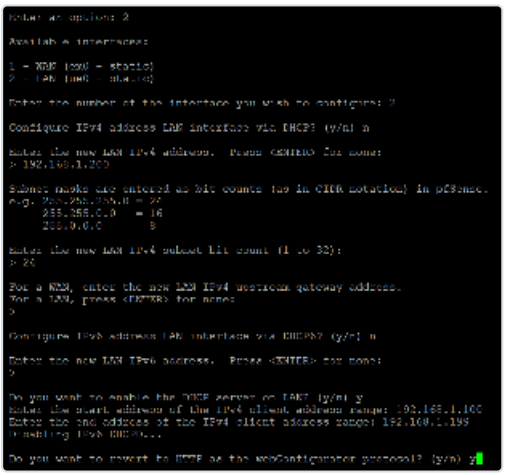

Figure 7 – Séquence complète de l'option 2 (le TP répond y à la dernière question)

Attention

HTTP n'est pas chiffré : mot de passe et configuration circulent en clair. Réserver la réponse y à un problème d'accès à l'interface web, et repasser en HTTPS ensuite. Si la session SSH utilise le LAN, se reconnecter à la nouvelle adresse après le changement.

6. Réinitialiser le mot de passe admin (option 3)

> **Fiche**
> Option 3 · Objectif : rétablir le compte admin (mot de passe oublié ou compte bloqué) · Impact : privilèges personnalisés de ce compte remis par défaut, autres comptes inchangés · Risque : moyen.

8 Confirmer et définir le nouveau mot de passe

Taper `3`. pfSense annonce que l'authentification et les privilèges du compte admin seront remis par défaut, puis demande `Proceed? (y|n)` : répondre `y`. Saisir le nouveau mot de passe à `New Password:` (saisie invisible), le ressaisir à `Confirm New Password:`. Le message `User Manager password changed for user 'admin' from console.` valide l'opération. Le mot de passe ne peut pas être identique à l'identifiant ; une phrase de passe longue vaut mieux qu'un mot de passe court et complexe (recommandation NIST rappelée par pfSense).

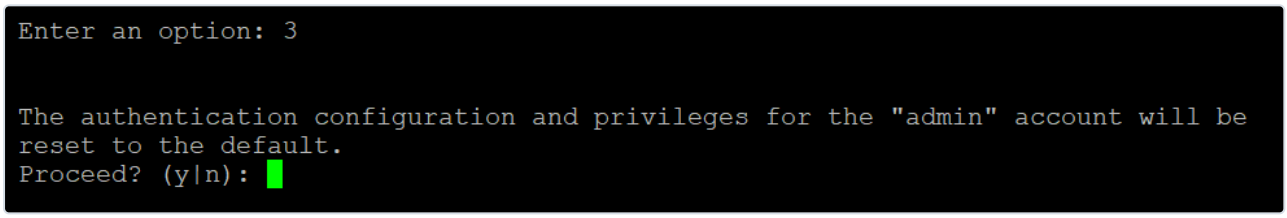

Figure 8 – Option 3 : avertissement et demande de confirmation

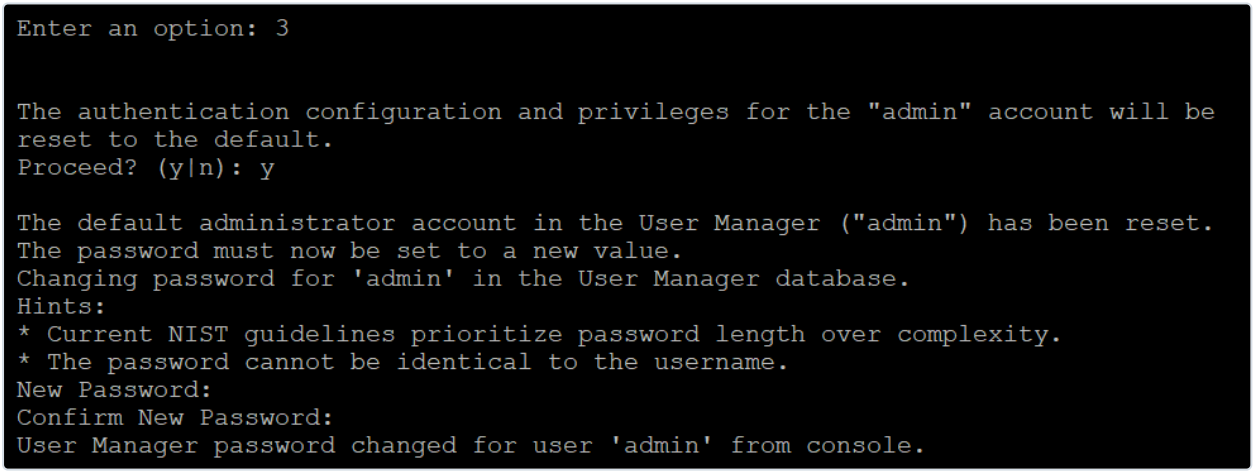

Figure 9 – Saisie et confirmation du nouveau mot de passe, message de réussite

7. Retour aux paramètres d'usine (option 4)

> **Fiche**
> Option 4 · Objectif : remettre pfSense à l'état initial · Impact : configuration effacée, paquets supplémentaires supprimés, redémarrage automatique · Risque : élevé.

Danger

Règles de pare-feu, DHCP, VPN, utilisateurs : tout est effacé et aucune seconde confirmation n'est demandée après le `y`. Exporter la configuration avant de continuer (webConfigurator : Diagnostics > Backup & Restore).

9 Réinitialiser, puis reconfigurer

Taper `4` : pfSense affiche trois avertissements (retour aux valeurs d'usine, redémarrage, suppression des paquets) puis `Do you want to proceed [y|n]?`. Répondre `y` pour confirmer ou `n` pour annuler. Après le redémarrage, la session SSH est perdue : réassigner les interfaces (section 4) puis reconfigurer l'IP du LAN (section 5).

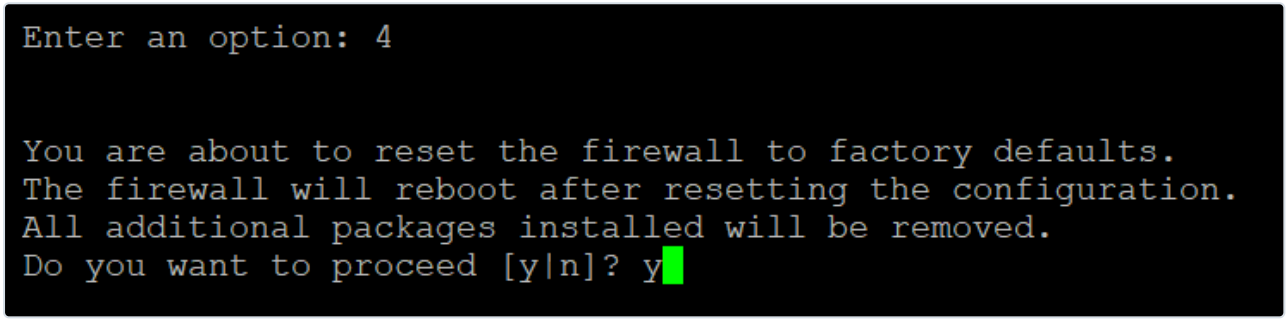

Figure 10 – Option 4 : avertissement et confirmation (y)

8. Redémarrer et arrêter (options 5 et 6)

10 Redémarrer (option 5, risque faible)

Taper `5` : pfSense prévient que le redémarrage peut durer plusieurs minutes. La configuration est conservée, mais le service est interrompu et la session SSH se ferme dès la validation ; attendre la fin du démarrage avant de se reconnecter. Trois modes sont proposés :

Touche	Mode	Usage
y	Reboot normally	Cas général : redémarrage complet
r	Reroot	Arrêt des processus, remontage des disques, nouvelle séquence de démarrage : plus rapide, sans redémarrage matériel
s	Single User Mode	Dépannage uniquement, accès console obligatoire

```
Enter an option: 5


pfSense will reboot. This may take a few minutes, depending on your hardware.
Do you want to proceed?

    Y/y: Reboot normally
    R/r: Reroot (Stop processes, remount disks, re-run startup sequence)
    S: Reboot into Single User Mode (requires console access!)
Enter an option: y
```

Figure 11 – Option 5 : choix du mode de redémarrage (y)

Attention

Ne jamais choisir le mode S à distance : sans écran ni clavier, la main ne peut pas être reprise.

11 Arrêter (option 6, risque moyen)

Taper `6`, puis `y` à `Do you want to proceed [y|n]?`. À utiliser avant de débrancher la machine, pour éviter de corrompre le système de fichiers. Contrairement à l'option 5, la machine ne redémarre pas seule : il faut la rallumer physiquement. Ne jamais l'utiliser sur un équipement inaccessible.

```
Enter an option: 6


pfSense will shutdown and halt system. This may take a few minutes, depending on your hardware.
Do you want to proceed [y|n]? y
```

Figure 12 – Option 6 : arrêt du système (y)

9. Tester la connectivité avec un ping (option 7)

12 Envoyer un ping depuis pfSense

Taper `7`, saisir une adresse IP ou un nom d'hôte (ici `192.168.21.10`, PC-CLIENT), puis Entrée à la fin pour revenir au menu. pfSense envoie 3 paquets de 56 octets. Cette option ne modifie rien. Le ping part du pare-feu lui-même : il teste la liaison pfSense-équipement, pas celle entre deux postes du réseau.

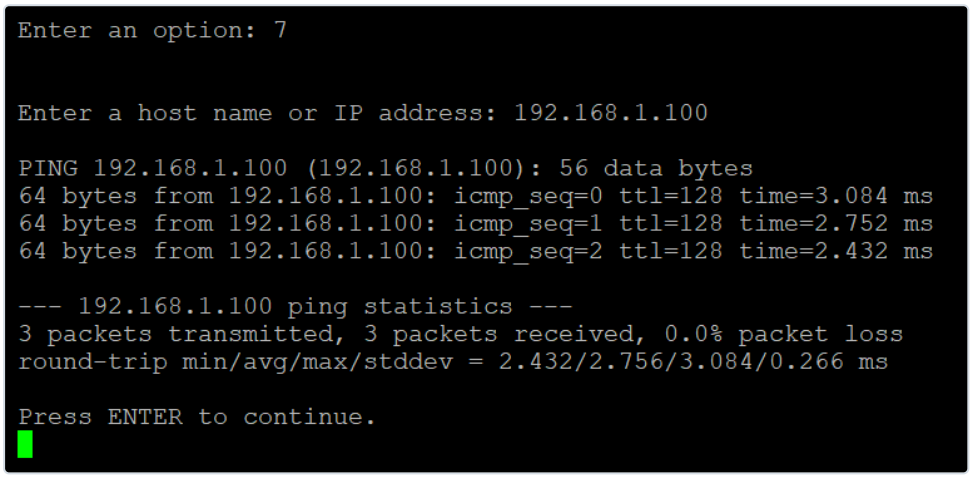

Figure 13 – Option 7 : ping de 192.168.21.10, 3 paquets reçus sur 3

Ligne affichée	Interprétation
64 bytes from … icmp_seq=0 ttl=128 time=3.084 ms	Une réponse par paquet ; le temps est le délai aller-retour. TTL 128 : valeur typique d'un poste Windows (simple indice)
3 packets transmitted, 3 packets received, 0.0% packet loss	0 % de perte : l'équipement répond
round-trip min/avg/max/stddev = 2.432/2.756/3.084/0.266 ms	Environ 2,4 à 3,1 ms : réseau local sain

10. Restaurer une configuration (option 15)

> **Fiche**
> Option 15 · Objectif : revenir à une configuration de l'historique · Impact : remplace la configuration actuelle, redémarrage ou relance des services possible · Risque : moyen.

13 Lister l'historique

Taper `15` : le sous-menu propose 1) List Backups, 2) Restore Backup, Q) Quit. Taper `1` pour afficher l'historique, numéroté de 01 (la plus récente) à 13 dans l'exemple. Chaque entrée indique le numéro, la date, la version du format de configuration (v24.6), l'auteur et la description.

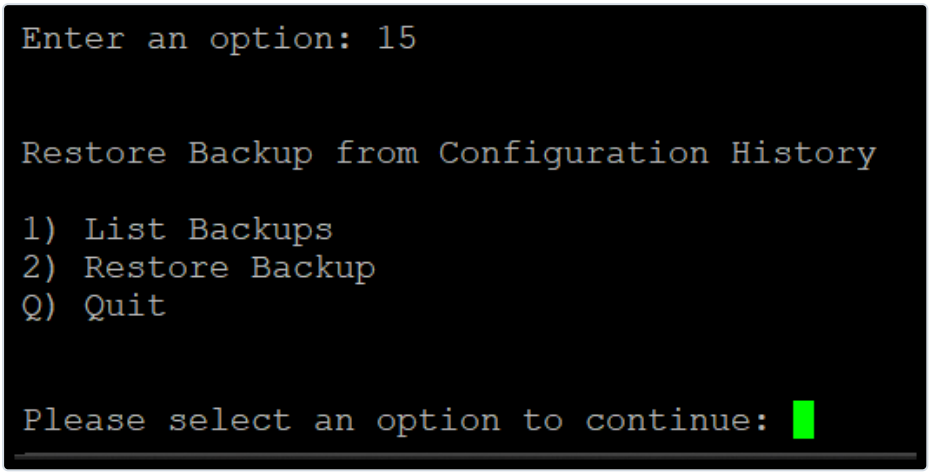

Figure 14 – Option 15 : sous-menu Restore Backup from Configuration History

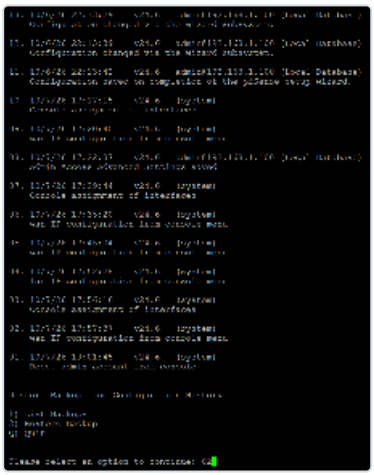

Figure 15 – Historique des configurations (13 sauvegardes dans l'exemple)

Élément	Exemple	Signification
Numéro	01.	Position dans l'historique (01 = la plus récente)
Date et heure	10/7/26 18:01:45	Moment de l'enregistrement
Version	v24.6	Version du format de configuration
Auteur	(system) ou admin@192.168.21.10 (Local Database)	(system) : modification faite depuis la console ; admin@adresse : faite par l'interface web
Description	Reset admin account from console	Action à l'origine de la sauvegarde

14 Restaurer la sauvegarde choisie

Taper `2` (Restore Backup), saisir le numéro de la sauvegarde (ici `2` : « wan IP configuration from console menu », 10/7/26 17:57:37), puis `Y` à `Is this the backup you wish to restore?`. Un message confirme la restauration ; redémarrer le pare-feu ou relancer les services pour qu'elle soit pleinement active.

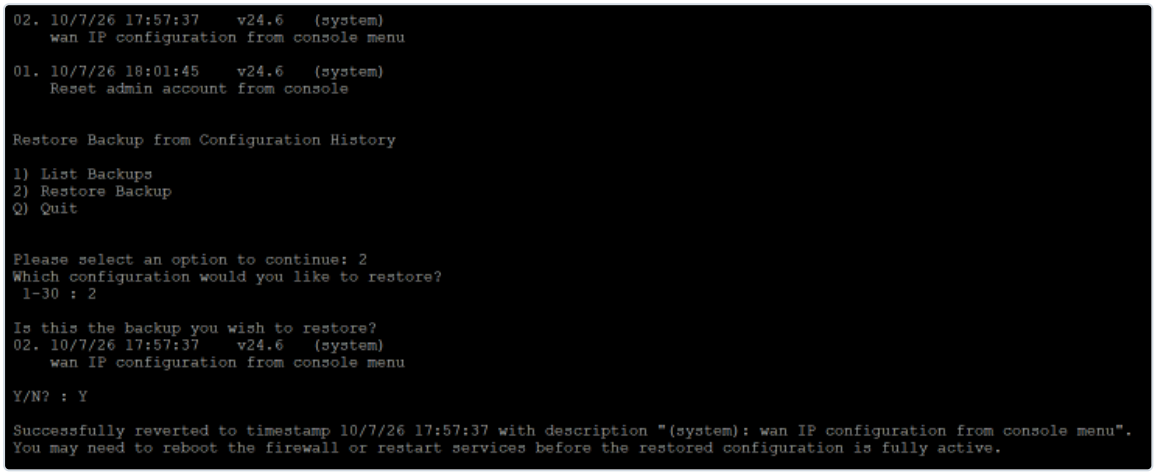

Figure 16 – Choix de la sauvegarde 02, confirmation et message de réussite

Attention

La restauration remplace la configuration actuelle : les modifications postérieures à la sauvegarde choisie sont perdues. Elle est utile après une erreur de configuration ou une réinitialisation. L'historique ne remplace pas un export de sauvegarde conservé hors du pare-feu.

11. Vérification, dépannage et sécurité

Vérification

Test	Commande / action	Résultat attendu
Assignation	Menu principal (en-tête)	WAN (wan) -> em0 ; LAN (lan) -> ue0, chacun avec son IPv4
Adresse du LAN	En-tête du menu après l'option 2	LAN (lan) -> ue0 -> v4: 192.168.21.254/24
Liaison	Option 7 vers un poste du LAN	0.0 % packet loss
DHCP	Poste client en DHCP, `ipconfig /renew` puis `ipconfig`	Adresse comprise entre 192.168.21.100 et 192.168.21.199, passerelle 192.168.21.254, DNS 192.168.21.1 et 192.168.21.2
Interface web	Navigateur vers https://192.168.21.254 (ou http:// si l'option a été choisie)	Page de connexion pfSense
Mot de passe admin	Connexion web ou SSH avec le nouveau mot de passe	Accès accepté

> **Résultat attendu**
> Le menu affiche les bonnes interfaces et adresses, l'option 7 répond sans perte, un poste du LAN reçoit une adresse de la plage DHCP et l'interface web s'ouvre avec le compte admin.

Dépannage

Symptôme	Cause probable	Solution
Interface web inaccessible	Mauvais protocole (HTTP / HTTPS) ou mauvaise adresse LAN	Lire l'IP du LAN dans le menu, tester http:// puis https://, option 11 (Restart GUI)
Session SSH coupée après l'option 1 ou 2	L'interface de connexion a changé d'adresse ou de rôle	Se reconnecter à la nouvelle adresse ; en dernier recours, passer par la console physique
Accès perdu après une assignation	WAN et LAN inversés	Refaire l'option 1 avec les bons noms, vérifier avec les adresses MAC
Aucun client ne reçoit d'adresse	DHCP non activé sur le LAN ou plage hors sous-réseau	Refaire l'option 2 : réponse y au DHCP, plage dans le LAN et sans l'IP du pfSense
Ping à 100 % de perte	Câble, mauvaise adresse, équipement éteint ou ICMP filtré	Contrôler le câble et l'adresse ; un pare-feu local peut bloquer le ping alors que l'équipement fonctionne. Tester aussi avec un nom d'hôte pour valider le DNS
Routage WAN-LAN inopérant	WAN et LAN dans le même sous-réseau	Choisir un LAN distinct (voir section 2)
Mot de passe admin perdu	—	Option 3
Erreur de configuration	Modification récente incorrecte	Option 15 vers une sauvegarde antérieure

Sécurité et bonnes pratiques

- Exporter la configuration avant toute opération sensible (Diagnostics > Backup & Restore) et conserver l'export hors du pare-feu.
- Garder un accès console (écran et clavier) avant de modifier interfaces ou adresses IP.
- Choisir des mots de passe longs, uniques, différents de l'identifiant.
- Préférer HTTPS pour le webConfigurator ; limiter l'accès SSH au réseau d'administration et le désactiver (option 14) quand il n'est plus utile.
- Vérifier la connectivité avec l'option 7 après chaque changement réseau.
- Utiliser un adaptateur USB uniquement pour les essais.

12. Aide-mémoire et glossaire

Tâche	Option	Saisies principales
Assigner les interfaces	1	1, n, em0, ue0, y
IP du LAN et DHCP	2	2, 2, n, 192.168.21.254, 24, Entrée, n, Entrée, y, 192.168.21.100, 192.168.21.199, n (HTTPS) ou y (HTTP)
Mot de passe admin	3	3, y, mot de passe, confirmation
Paramètres d'usine	4	4, y
Redémarrer / arrêter	5 / 6	5, y / 6, y
Ping	7	7, adresse ou nom d'hôte, Entrée
Restaurer	15	15, 1 (lister), 2, numéro de sauvegarde, Y

Terme	Définition
WAN / LAN	Interface côté Internet ou box / réseau local protégé
DHCP	Distribution automatique d'adresses IP aux postes
CIDR	Masque exprimé en nombre de bits (24 = 255.255.255.0)
VLAN	Réseau local virtuel : séparation logique sur un même support
NAT	Traduction d'adresses ; le mode Firewalling/NAT s'active en assignant le LAN
SSH / ICMP	Accès distant sécurisé en ligne de commande / protocole du ping
webConfigurator	Interface web d'administration de pfSense

13. Aide-mémoire : utiliser pfSense au quotidien

Gestes courants du webConfigurator, pour ne plus chercher sur Internet. Les chemins correspondent à l'interface pfSense CE récente ; l'intitulé exact peut varier légèrement d'une version à l'autre. Règle générale : après chaque modification, cliquer sur **Save** puis sur **Apply Changes**, faute de quoi rien n'est actif.

Interfaces et assignation

A **Interfaces › Assignments**

Choisir une carte dans « Available network ports », cliquer sur **Add** : elle devient OPTn. Cliquer sur son nom pour la configurer : cocher **Enable**, donner une description, choisir **IPv4 Configuration Type = Static IPv4**, saisir l'adresse et le masque, **Save**, **Apply Changes**. Le WAN a une passerelle (Gateway) ; un LAN n'en a pas. En console : option 1 (assignation) et option 2 (adresse).

VLAN, interface et DHCP par VLAN

B **Interfaces › Assignments › VLANs, puis Services › DHCP Server**

1) Onglet **VLANs** › Add : choisir la **Parent Interface**, saisir le **VLAN Tag** (1 à 4094), une description, Save. 2) Onglet **Interface Assignments** : ajouter le VLAN comme nouvelle interface, l'activer et lui donner une IP statique (un sous-réseau par VLAN). 3) *Services › DHCP Server*, onglet du VLAN : cocher **Enable**, définir la plage, éventuellement DNS et passerelle, Save. 4) Créer les règles de pare-feu de l'interface (sans règle, tout est bloqué). Côté switch, le port relié au pfSense doit porter le VLAN en Tagged.

Règles de pare-feu

C **Firewall › Rules (onglet de l'interface) et Firewall › Aliases**

Principes : les règles se lisent **de haut en bas**, la première qui correspond s'applique ; sur une interface, tout ce qui n'est pas autorisé est bloqué (refus implicite) ; les règles s'appliquent au trafic **entrant** sur l'interface. Pour ajouter : **Add** (en haut ou en bas), choisir Action (Pass, Block, Reject), Interface, Protocol, Source, Destination, **Destination Port Range**, une description, Save, Apply Changes. **Aliases** (Firewall › Aliases) : regrouper des hôtes, réseaux ou ports sous un nom réutilisable dans les règles.

Besoin	Règle (sur l'interface source)
Bloquer un VLAN vers un autre	Block, Source = réseau du VLAN A (« VLAN_A subnets »), Destination = réseau du VLAN B, placée au-dessus de la règle « Pass any »
Autoriser un port précis	Pass, Protocol TCP, Source = réseau concerné, Destination = hôte cible, Destination Port = port voulu (443 par exemple)
Autoriser Internet seulement	Règle 1 : Block vers « RFC1918 » (alias de réseaux privés) ; règle 2 : Pass vers any

NAT : redirection de port et sortant

D **Firewall › NAT › Port Forward / Outbound**

Port Forward : Add, Interface = WAN, Protocol, Destination = WAN address, Destination port range = port exposé, **Redirect target IP** = serveur interne, Redirect target port, **Filter rule association = Add associated filter rule** (crée la règle WAN qui autorise le flux), Save, Apply. **Outbound** : mode **Automatic** par défaut (le NAT des réseaux internes est géré automatiquement) ; passer en **Hybrid** ou **Manual** seulement pour des cas particuliers (plusieurs WAN, IP publique dédiée).

> **Attention**
> Exposer un port sur Internet reste un risque : limiter la source (alias) quand c'est possible et tenir le serveur à jour.

DHCP statique (réservation) et DNS Resolver

E **Services › DHCP Server › [interface] › DHCP Static Mappings ; Services › DNS Resolver**

Réservation : en bas de la page de l'interface, **Add** sous « DHCP Static Mappings » : MAC address, IP address (hors de la plage dynamique), hostname, description, Save, Apply. **DNS Resolver** (Unbound) : activer, cocher les interfaces d'écoute, ajouter des enregistrements locaux dans **Host Overrides** (hôte, domaine, IP) ou des redirections vers un DNS précis dans **Domain Overrides**. Le DNS public à utiliser se règle dans System › General Setup.

VPN : OpenVPN et WireGuard (grandes étapes)

F **VPN › OpenVPN (assistant) ; VPN › WireGuard**

OpenVPN accès distant : *VPN › OpenVPN › Wizards*, serveur « Local User Access » : 1) créer une autorité de certification (CA) ; 2) créer le certificat du serveur ; 3) choisir interface (WAN), protocole (UDP 1194), réseau du tunnel (exemple : 10.8.0.0/24), réseau local à joindre ; 4) cocher la création automatique des règles pare-feu ; 5) créer l'utilisateur et son certificat (System › User Manager) ; 6) installer le paquet *openvpn-client-export* pour générer le fichier client. **WireGuard** : activer le tunnel dans *VPN › WireGuard › Tunnels* (clé générée par pfSense, port UDP 51820 par défaut, adresse du tunnel), ajouter les pairs (clé publique, **Allowed IPs**) dans *Peers*, assigner l'interface du tunnel dans Interfaces › Assignments, puis créer la règle d'autorisation sur WAN (UDP 51820) et sur l'interface du tunnel. Selon la version, WireGuard est intégré ou fourni par un paquet.

Utilisateurs et groupes

G **System › User Manager**

Onglet **Users** › Add : nom, mot de passe, groupe, éventuellement certificat. Onglet **Groups** : définir les privilèges (page Assigned Privileges) : par exemple WebCfg - All pages, ou des droits restreints. Utiliser un compte nominatif plutôt que de partager `admin`. En cas de perte d'accès : console, option 3.

Sauvegarde et restauration de config.xml

H **Diagnostics › Backup & Restore**

Sauvegarder : section « Backup Configuration », choisir la zone (All), cocher *Encrypt this configuration file* avec un mot de passe, puis **Download configuration as XML**. **Restaurer** : section « Restore Configuration », choisir le fichier, **Restore Configuration** ; un redémarrage peut être nécessaire. Historique automatique : onglet **Config History** (restauration d'une révision précédente). En console : option 15.

```
# Le fichier de configuration actif
cat /conf/config.xml | head
# Copie manuelle avant une opération risquée
cp /conf/config.xml /root/config-avant-modif.xml
```

Journaux et diagnostic

I **Status › System Logs ; Diagnostics › Ping / Packet Capture / States**

Journaux : *Status › System Logs › Firewall* montre les paquets bloqués (cliquer sur l'icône de la règle pour l'identifier), onglet System pour le reste. **Ping** : *Diagnostics › Ping*, choisir l'interface source. **Packet Capture** : choisir interface, protocole, hôte, port, démarrer, arrêter, télécharger le fichier .pcap pour Wireshark. **States** : *Diagnostics › States* liste les connexions suivies (filtrable ; Reset States les vide). Contrôle global : *Status › Dashboard*.

```
pfctl -sr | head -n 20        # règles actives
pfctl -ss | grep 192.168.21.10  # connexions suivies d'un hôte
tcpdump -ni em0 host 192.168.21.10   # capture en direct (Ctrl+C pour arrêter)
```

Menu console : options utiles

Option	Usage courant
1 / 2	Assigner les interfaces / régler l'adresse IP d'une interface
3	Réinitialiser le compte admin
4	Retour aux paramètres d'usine (destructif)
5 / 6	Redémarrer / arrêter
7	Ping depuis le pare-feu
8	Shell système (commandes pfctl, tcpdump, etc.)
10	Journaux du filtre en direct
11	Relancer l'interface web si elle ne répond plus
13	Mise à jour depuis la console
14	Désactiver SSH
15	Restaurer une configuration récente
16	Redémarrer PHP-FPM (interface web figée)

Mises à jour

J **System › Update (ou console, option 13)**

Consulter la branche et la version disponibles, exporter la configuration (étape H), puis lancer la mise à jour : le pare-feu redémarre et le service est interrompu quelques minutes. Les paquets se gèrent dans *System › Package Manager* (Installed Packages / Available Packages). Lire les notes de version de Netgate avant une mise à jour majeure et la planifier hors période d'activité.

```
pfSense-upgrade -d    # vérifier les mises à jour disponibles (depuis le shell)
```

Raccourcis et emplacements utiles

Besoin	Emplacement
Assigner une interface, créer un VLAN	Interfaces › Assignments (onglets Interface Assignments, VLANs)
Serveur DHCP et réservations	Services › DHCP Server
Résolution DNS locale	Services › DNS Resolver
Règles et alias	Firewall › Rules, Firewall › Aliases
Redirections de port, NAT sortant	Firewall › NAT
VPN	VPN › OpenVPN, VPN › WireGuard
Comptes et privilèges	System › User Manager
Certificats	System › Certificates
Sauvegarde, restauration, historique	Diagnostics › Backup & Restore
Journaux du pare-feu	Status › System Logs › Firewall
Ping, capture, connexions	Diagnostics › Ping, Packet Capture, States
Accès SSH, HTTPS, port web	System › Advanced › Admin Access
Mises à jour et paquets	System › Update, System › Package Manager

Sources : documentation officielle Netgate pfSense (docs.netgate.com), chapitres « Console Menu », « Backup and Recovery » et « Configuration » · Procédure rédigée à partir d'un TP réalisé en équipe.