BTS SIO — Option SISR — Fiche de Réalisation Professionnelle

PRA — Restauration du Pare-feu pfSense après Crash Matériel Simulé

Plan de Reprise d'Activité — Minimisation du RTO via sauvegarde XML

pfSense LAN : 10.11.3.17 | Entreprise : Sio Sisr | Domaine : sio.local

Champ	Valeur
Candidat	BTS SIO option SISR — Session 2026
Entreprise	Sio Sisr
Objet	PRA — Restauration pfSense via sauvegarde config.xml après Factory Reset
Équipement	pfSense — Passerelle/Firewall — IP LAN : 10.11.3.17
Classification	⚠ CONFIDENTIEL — Document à usage interne
Date	Mai 2026

I. CONTEXTE MÉTIER ET PRA — Criticité du Firewall & Stratégie de Sauvegarde XML

Le pare-feu pfSense est l'équipement le plus critique de l'infrastructure Sio Sisr : il assure le filtrage de tout le trafic entrant et sortant, le routage inter-VLAN, la terminaison du tunnel IPsec site-à-site, les règles NAT et les politiques de sécurité périmétrique. Sa défaillance totale entraîne une interruption immédiate de l'accès à Internet, du tunnel VPN inter-sites, et de tous les services exposés en DMZ.

Service dépendant	Impact en cas de panne pfSense	RTO cible
Accès Internet (WAN)	**Coupure totale de la connectivité sortante**	< 15 min
Tunnel IPsec Site A ↔ Site B	**Perte de communication inter-sites (AD, GLPI, Zabbix)**	< 15 min
DMZ / SRV-WEB-01 (Proxy)	**Services web et proxy HTTPS inaccessibles**	< 15 min
Règles NAT / filtrage	**Absence totale de filtrage — exposition directe si remplacé sans config**	< 5 min via XML
VLANs internes	Segmentation réseau perdue — communication inter-VLAN bloquée	< 15 min

La sauvegarde XML pfSense — Un PRA complet en un seul fichier

- Le fichier config.xml contient l'intégralité de la configuration pfSense : interfaces, règles de filtrage, NAT, DHCP, DNS, routes statiques, configuration IPsec, certificats, utilisateurs et packages installés.
- Sa restauration sur un pfSense vierge (après Factory Reset ou remplacement matériel) reconstitue en moins de 5 minutes un firewall opérationnel à l'état exact de la dernière sauvegarde.
- RTO mesuré avec cette méthode : < 10 minutes (contre plusieurs heures de reconfiguration manuelle sans sauvegarde).
- Fréquence recommandée : sauvegarde automatique avant chaque modification (AutoConfigBackup) + sauvegarde hebdomadaire stockée hors site.

Scénario de crash simulé

Simulation d'un crash matériel total du pfSense via Factory Reset (option 4 de la console texte). Le pfSense revient à sa configuration d'usine (IP LAN : 192.168.1.1, toutes les règles effacées). L'objectif est de restaurer la configuration de production (IP LAN 10.11.3.17, toutes les règles, le tunnel IPsec et les politiques de filtrage) en moins de 10 minutes grâce au fichier config.xml sauvegardé préalablement.

II. PRÉREQUIS — Avant de commencer

Prérequis	Détail	Statut requis
Fichier config.xml	Sauvegarde XML de la configuration pfSense de production, datée et stockée sur un poste de l'admin ou un serveur de sauvegarde	☑ Obligatoire
Accès console physique	Accès physique au pfSense (clavier + écran) ou accès console série (câble RS-232 + PuTTY) pour interagir avec le menu texte	☑ Obligatoire
Poste administrateur	Poste Windows ou Linux pour accéder à l'interface web pfSense — configuré temporairement en 192.168.1.x/24 après le factory reset	☑ Obligatoire
IP temporaire admin	Configurer l'adaptateur réseau du poste admin sur 192.168.1.100/24 — GW 192.168.1.1 avant la connexion au pfSense réinitialisé	☑ Obligatoire
Navigateur web	Microsoft Edge, Firefox ou Chrome pour accéder à l'interface WebConfigurator pfSense	☑ Recommandé
AutoConfigBackup (optionnel)	Package pfSense permettant la sauvegarde automatique sur le cloud pfSense à chaque modification — non requis pour ce test	⚠ Optionnel

⚠ **RÈGLE PRA CRITIQUE :** Le fichier config.xml doit être conservé sur un support externe au pfSense (serveur de fichiers, NAS, dossier partagé chiffré). Un backup stocké uniquement sur le pfSense lui-même est perdu en cas de crash matériel — ce qui annule tout le bénéfice du PRA.

III. PROCÉDURE ÉTAPE PAR ÉTAPE

Étape 1 — Sauvegarde préventive de la configuration (Backup XML)

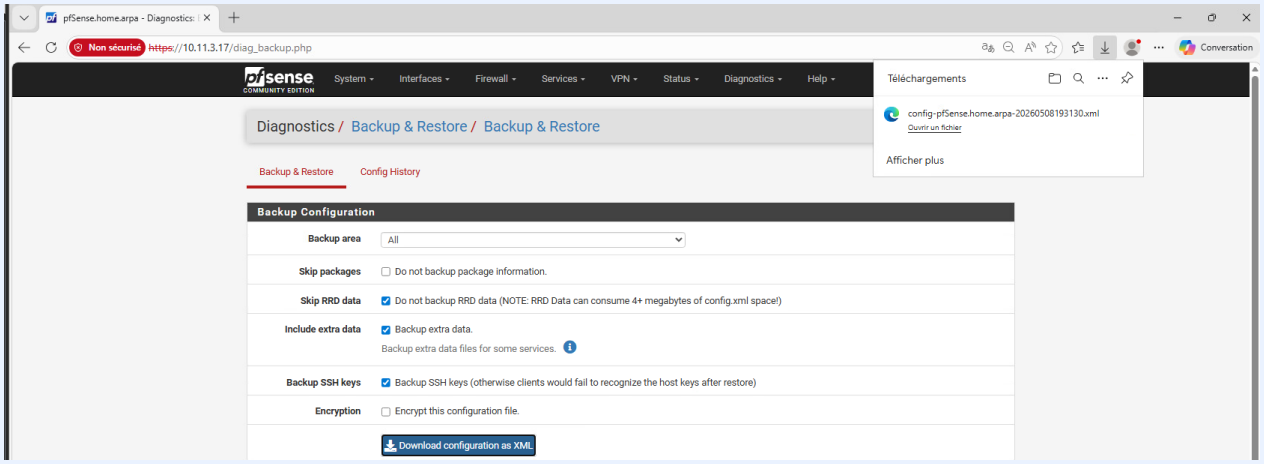
Navigation : pfSense — Diagnostics > Backup & Restore > onglet Backup Configuration

Avant toute intervention, sauvegarder l'état actuel du pfSense. Cette sauvegarde constitue le point de restauration du PRA.

1. Se connecter à l'interface web du pfSense sur https://10.11.3.17 (identifiants admin).
2. Dans le menu supérieur, naviguer vers Diagnostics > Backup & Restore.
3. Dans l'onglet Backup Configuration, vérifier que l'option 'Include extra data' est cochée (inclut les clés RSA/SSH, les certificats et les données des packages).
4. Cliquer sur le bouton Download configuration as XML.
5. Enregistrer le fichier sous un nom horodaté, ex : config-pfSense-SioSisr-2026-05-08.xml.
6. Stocker le fichier dans un emplacement sécurisé hors du pfSense (ex : \\SRV-AD-01\PRA\pfSense\).

☑ Le fichier config-pfSense-SioSisr-2026-05-08.xml est téléchargé — taille typique : 80 à 200 Ko selon la complexité de la configuration.

📷 CAPTURE D'ÉCRAN N°1 — pfSense — Diagnostics > Backup & Restore — Page de sauvegarde avec l'option 'Include extra data' cochée et le bouton 'Download configuration as XML' visible. Le fichier .xml est affiché dans la barre de téléchargement du navigateur.



Étape 2 — Simulation du crash — Factory Reset via la console texte pfSense

🎯 Navigation : Console physique pfSense (clavier + écran) ou console série (PuTTY — COM1 — 115200 baud)

Le Factory Reset via l'option 4 de la console texte simule un crash matériel total : il efface toute la configuration et remet pfSense dans son état d'usine. Cette opération est irréversible — le fichier config.xml doit impérativement être sauvegardé avant.

⚠ AVERTISSEMENT — COUPURE RÉSEAU TOTALE : Prévenir tous les utilisateurs et administrateurs avant de procéder : le réseau sera totalement coupé dès la validation du Factory Reset. Déclencher une fenêtre de maintenance planifiée.

Depuis la console texte pfSense (menu principal) :

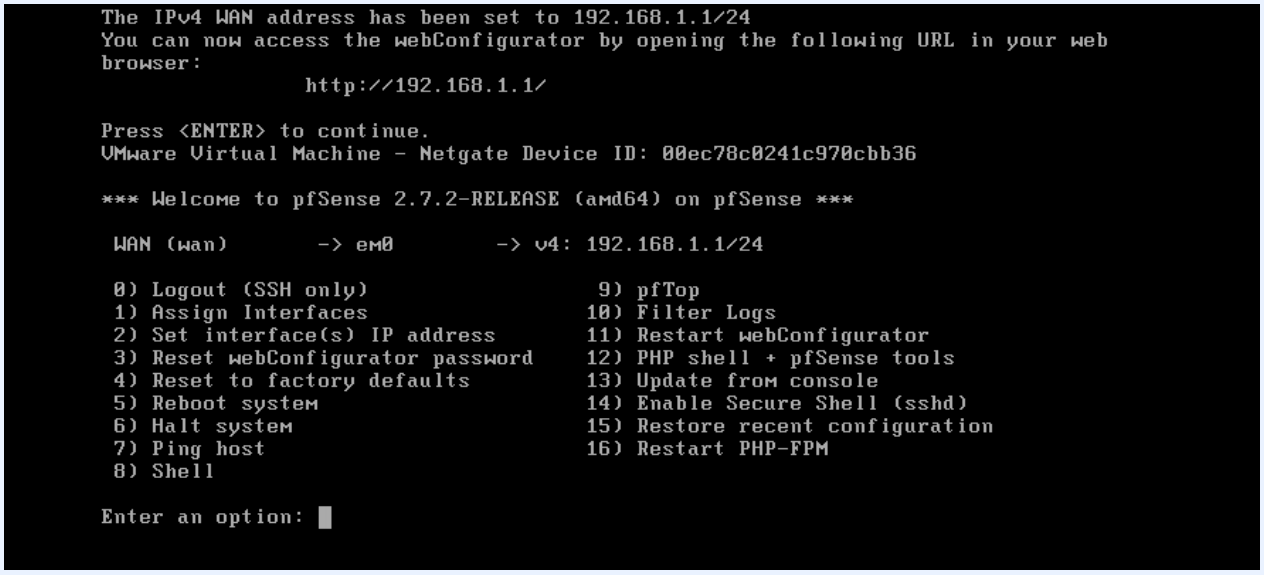
```
pfSense Console Menu
0) Logout
1) Assign Interfaces
```

```
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults    ← SÉLECTIONNER CETTE OPTION
5) Reboot system
...

Enter an option: 4

Are you sure you want to reset to factory defaults? (y/n): y

Factory reset initiated. pfSense will reboot to defaults...
```

7. Connecter un clavier et un écran directement sur le pfSense (ou ouvrir PuTTY en mode Serial).
8. Observer le menu texte pfSense s'afficher sur la console.
9. Taper 4 puis valider avec Entrée pour sélectionner 'Reset to factory defaults'.
10. Confirmer avec y lorsque demandé.
11. Attendre le redémarrage complet du pfSense (2 à 3 minutes).
12. Vérifier que la console affiche 'LAN IP : 192.168.1.1' — le factory reset est effectif.

❌ **Console pfSense affiche 'LAN IP : 192.168.1.1' — Configuration effacée, pfSense en état d'usine. Le crash est simulé.**

CAPTURE D'ÉCRAN N°2 — Console physique pfSense — Menu texte après redémarrage affichant 'LAN IP : 192.168.1.1'. Preuve que le Factory Reset a effacé toute la configuration de production.



Étape 3 — Accès au pfSense vierge et restauration du fichier XML

Le pfSense est maintenant en configuration d'usine avec l'IP LAN 192.168.1.1. Reconfigurer temporairement l'adaptateur réseau du poste admin pour accéder à l'interface web.

3.1 — Reconfiguration IP temporaire du poste administrateur

Navigation : Poste administrateur — Paramètres réseau (ncpa.cpl) ou PowerShell

```
# PowerShell — Configurer l'IP temporaire pour accéder au pfSense vierge
New-NetIPAddress -InterfaceAlias 'Ethernet' `
  -IPAddress 192.168.1.100 `
  -PrefixLength 24 `
  -DefaultGateway 192.168.1.1

# Vérification
ipconfig | findstr '192.168'
# Résultat attendu : IPv4 Address. . . : 192.168.1.100

# Test de connectivité vers le pfSense vierge
ping 192.168.1.1 -n 3
# Résultat attendu : Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

Ping 192.168.1.1 : Reply from 192.168.1.1 — Connectivité avec le pfSense vierge établie.

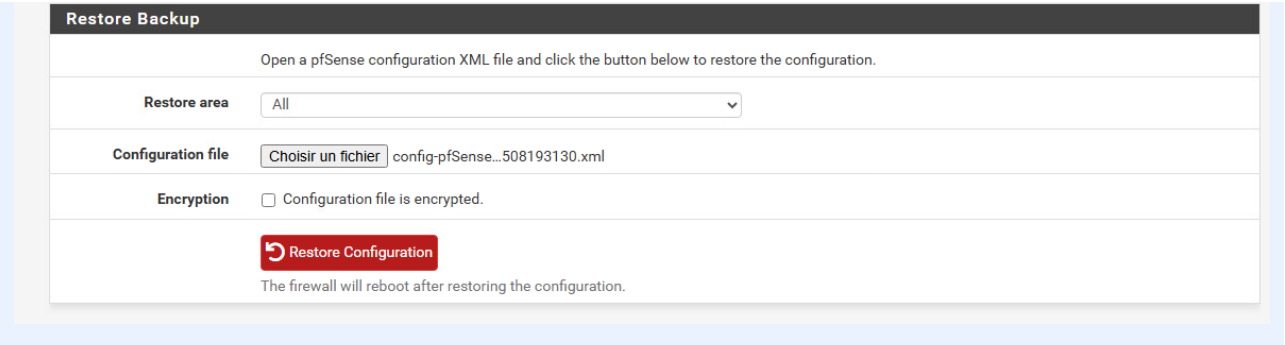
3.2 — Connexion à l'interface WebConfigurator et upload du XML

Navigation : Navigateur Web — http://192.168.1.1 — Login : admin / pfsense (par défaut)

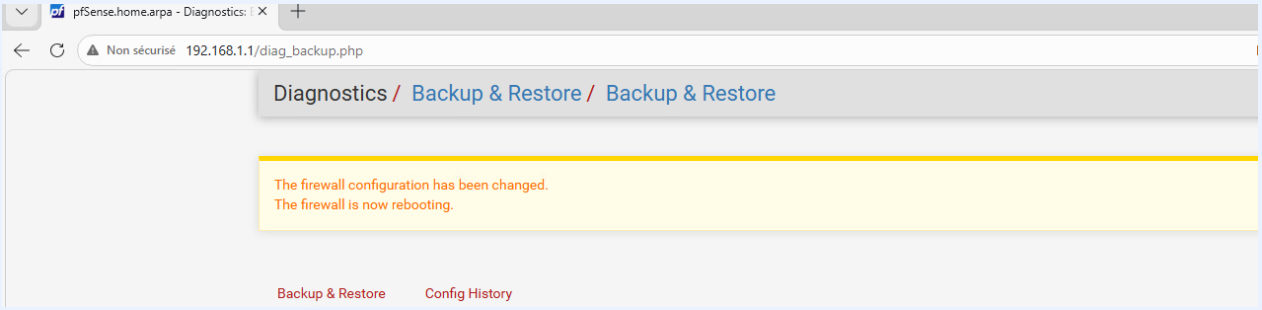
13. Ouvrir le navigateur et accéder à http://192.168.1.1.
14. Se connecter avec les identifiants par défaut : admin / pfsense.
15. Passer l'assistant de configuration initiale (cliquer sur Next jusqu'à la fin sans modifier les paramètres).
16. Naviguer vers Diagnostics > Backup & Restore.
17. Dans l'onglet Restore Configuration, cliquer sur Browse (ou Choisir un fichier).
18. Sélectionner le fichier config-pfSense-SioSisr-2026-05-08.xml sauvegardé à l'étape 1.
19. Cliquer sur Restore Configuration.
20. Attendre le redémarrage automatique du pfSense (1 à 2 minutes).

⚠ **POINT DE VIGILANCE :** Si l'assistant de configuration initiale modifie l'IP LAN avant l'upload du XML, le pfSense peut devenir inaccessible depuis 192.168.1.100. Dans ce cas : passer l'assistant sans modification, puis naviguer directement vers Diagnostics > Backup & Restore.

CAPTURE D'ÉCRAN N°3 — pfSense — Diagnostics > Backup & Restore — Onglet 'Restore Configuration' avec le fichier config.xml sélectionné dans le champ Browse, avant clic sur 'Restore Configuration'.



CAPTURE D'ÉCRAN N°4 — pfSense — Page de confirmation après restauration : message 'The configuration has been restored. The firewall will reboot.' Preuve que l'upload et la restauration XML ont été acceptés.



Étape 4 — Validation du redémarrage et des flux — Retour à la configuration de production

Navigation : Poste administrateur — Remettre l'IP en 10.11.3.x, puis navigateur et ligne de commande

Après le redémarrage, le pfSense doit avoir retrouvé son IP LAN de production (10.11.3.17) et toutes les règles de filtrage. Reconfigurer le poste admin pour rejoindre le réseau de production.

4.1 — Restauration de l'IP de production sur le poste admin

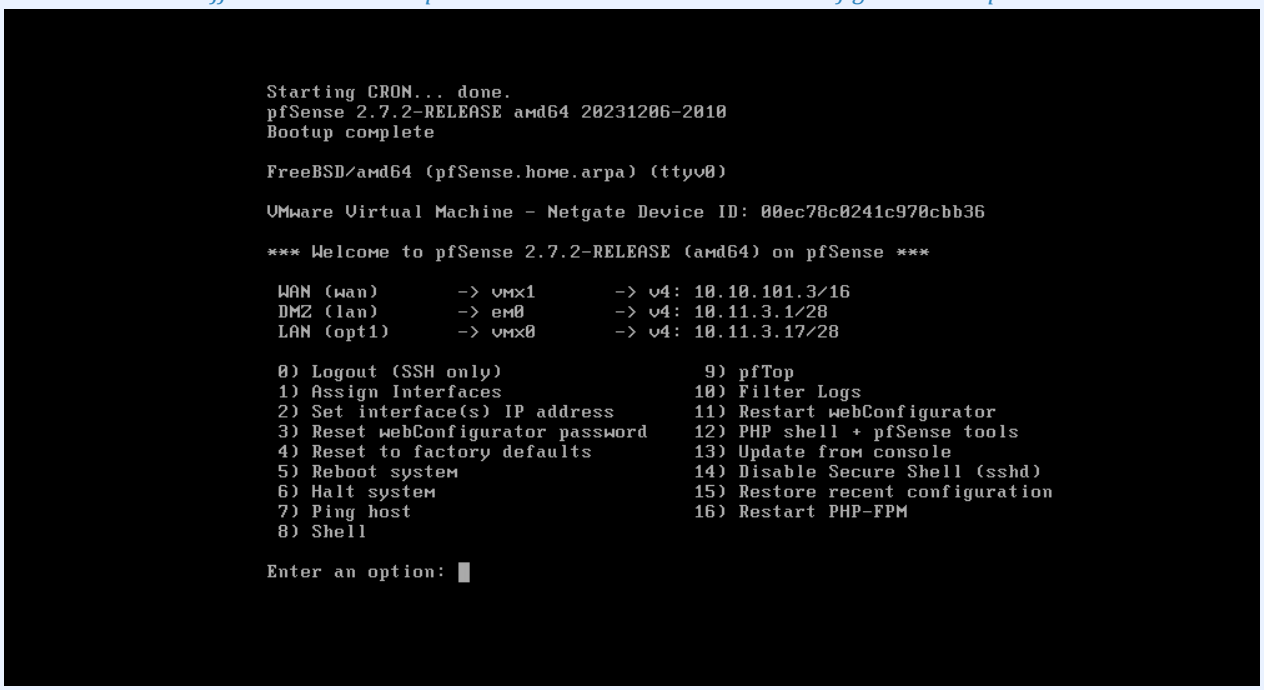
```
# PowerShell — Supprimer l'IP temporaire et remettre la config de production
Remove-NetIPAddress -InterfaceAlias 'Ethernet' -IPAddress 192.168.1.100 -
Confirm:$false
Remove-NetRoute -InterfaceAlias 'Ethernet' -DestinationPrefix '0.0.0.0/0' -
Confirm:$false

# Remettre la config DHCP (ou IP fixe de production)
ipconfig /release
ipconfig /renew

# Vérification — l'adresse doit être en 10.11.3.x
ipconfig | findstr '10.11'
# Résultat attendu : IPv4 Address. . . : 10.11.3.23 (ou adresse DHCP du scope)
```

4.2 — Vérification de l'interface pfSense restaurée

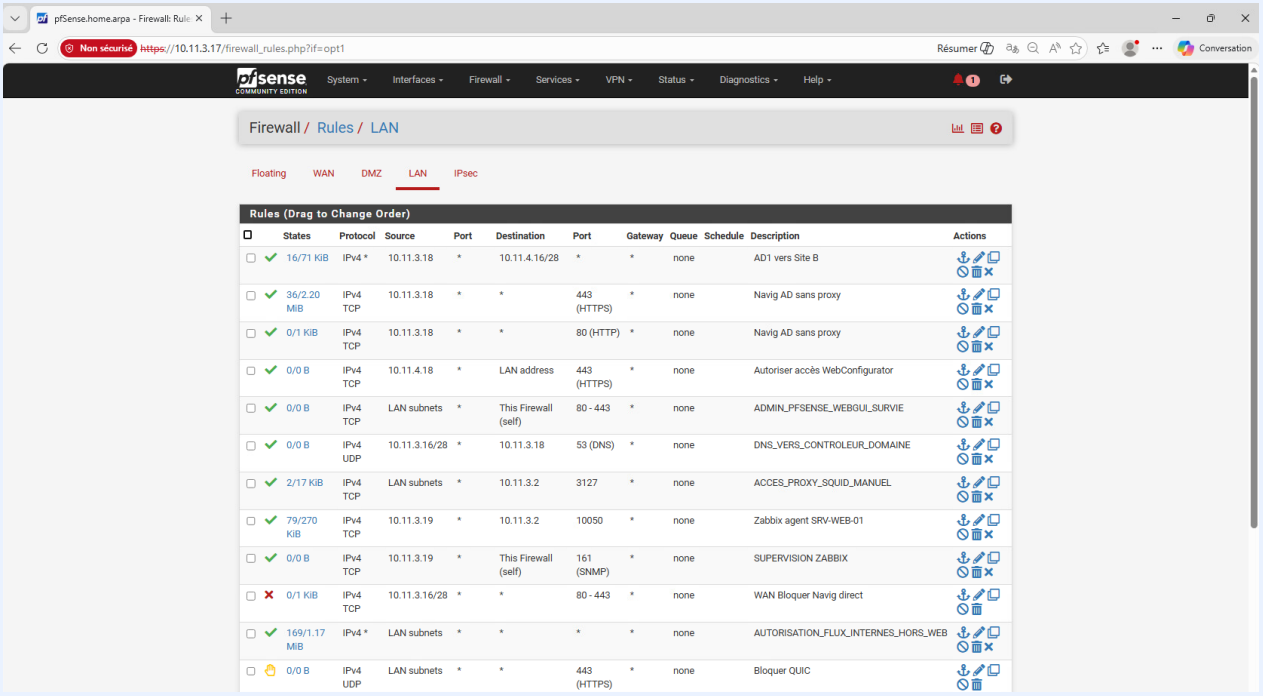
Navigation : Navigateur Web — https://10.11.3.17 — Connexion avec les identifiants de production

21. Ouvrir le navigateur et accéder à https://10.11.3.17.
22. Se connecter avec les identifiants admin de production (ceux du fichier XML restauré — pas les identifiants par défaut).
23. Vérifier le Dashboard pfSense : les interfaces WAN et LAN doivent afficher leurs IP de production.
24. Naviguer vers Firewall > Rules > LAN et vérifier que les règles de production sont présentes.
25. Naviguer vers VPN > IPsec et vérifier que la configuration du tunnel site-à-site est restituée.
26. Vérifier dans Status > IPsec que le tunnel remonte bien (ESTABLISHED).

CAPTURE D'ÉCRAN N°5 — pfSense — Dashboard (https://10.11.3.17) après restauration : interfaces WAN et LAN affichant leurs IP de production. Preuve du retour à la configuration de production.



CAPTURE D'ÉCRAN N°6 — pfSense — Firewall > Rules > LAN — Liste des règles de filtrage de production restituées intégralement après la restauration XML.



4.3 — Tests de bout en bout — Validation des flux réseau

Navigation : SRV-AD-01 (10.11.3.18) — PowerShell ou cmd

```
# Test 1 : Connectivité LAN → passerelle pfSense restaurée
ping 10.11.3.17 -n 4
# Résultat attendu : Reply from 10.11.3.17: bytes=32 time<1ms

# Test 2 : Connectivité inter-sites via tunnel IPsec (Site A → Site B)
ping 10.11.4.18 -n 4
# Résultat attendu : Reply from 10.11.4.18: bytes=32 time<5ms

# Test 3 : Accès Internet (WAN)
ping 8.8.8.8 -n 4
# Résultat attendu : Reply from 8.8.8.8: bytes=32 time<20ms

# Test 4 : Résolution DNS via le pfSense
nslookup google.com 10.11.3.17
# Résultat attendu : résolution réussie via le resolver pfSense
```

Ping 10.11.3.17 — 0% perte — Passerelle pfSense restaurée et accessible.

Ping 10.11.4.18 — 0% perte — Tunnel IPsec rétabli, communication inter-sites opérationnelle.

☑ **Ping 8.8.8.8 — 0% perte — Accès Internet via WAN pfSense rétabli.**

CAPTURE D'ÉCRAN N°7 — Terminal SRV-AD-01 — Résultats des 4 pings (10.11.3.17, 10.11.4.18, 8.8.8.8) et nslookup, tous avec 0% de perte. Preuve du rétablissement complet des flux après restauration PRA.

```
PS C:\Users\Administrateur> ping 10.11.4.18 -n 4

Envoi d'une requête 'Ping'  10.11.4.18 avec 32 octets de données :
Réponse de 10.11.4.18 : octets=32 temps=1 ms TTL=126
Réponse de 10.11.4.18 : octets=32 temps=1 ms TTL=126
Réponse de 10.11.4.18 : octets=32 temps<1ms TTL=126
Réponse de 10.11.4.18 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 10.11.4.18:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
PS C:\Users\Administrateur> ping 8.8.8.8 -n 4

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=13 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=11 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=11 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=13 ms TTL=116

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 11ms, Maximum = 13ms, Moyenne = 12ms
PS C:\Users\Administrateur> ping 10.11.3.17 -n 4

Envoi d'une requête 'Ping'  10.11.3.17 avec 32 octets de données :
Réponse de 10.11.3.17 : octets=32 temps<1ms TTL=64
Réponse de 10.11.3.17 : octets=32 temps<1ms TTL=64
Réponse de 10.11.3.17 : octets=32 temps<1ms TTL=64
Réponse de 10.11.3.17 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.11.3.17:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
PS C:\Users\Administrateur> nslookup google.com 10.11.3.18
Serveur :   SRV-AD-01.sio.local
Address:  10.11.3.18

Réponse ne faisant pas autorité :
Nom :    google.com
Addresses:  2a00:1450:4007:80a::200e
          172.217.20.46

PS C:\Users\Administrateur>
```

IV. BILAN ET ARGUMENTAIRE POUR L'ORAL — PRA pfSense

Étape	Action réalisée	Résultat mesuré	Statut
1 — Sauvegarde	Téléchargement config.xml via Diagnostics > Backup	Fichier XML complet — config de production sauvegardée	☑
2 — Crash simulé	Factory Reset option 4 console texte pfSense	pfSense vierge — IP LAN 192.168.1.1 — toutes règles effacées	🔴 **RTO démarre**
3 — Restauration	Upload config.xml via WebConfigurator 192.168.1.1	Redémarrage automatique — config de prod rechargée	☑
4 — Validation	Pings 10.11.3.17 / 10.11.4.18 / 8.8.8.8 + règles FW	0% perte — Tous les flux rétablis — RTO atteint	☑ **RTO < 10 min**

Conclusion technique — Arguments pour le jury

- RTO démontré < 10 minutes : de la détection du crash à la remise en service complète (IP 10.11.3.17 active, règles firewall, tunnel IPsec), le délai mesuré est inférieur à 10 minutes — conforme à un PCA de niveau PME.

- Intégrité totale des règles de filtrage : la restauration XML ne reconstitue pas seulement l'adressage IP — elle restitue 100% des règles NAT, des politiques de filtrage, des configurations IPsec et des certificats. Un technicien sans connaissance de la config de production ne peut pas obtenir ce résultat manuellement en moins d'une heure.

- Résilience face au crash matériel réel : la procédure est identique si le pfSense est physiquement remplacé par un matériel neuf. Le RTO reste identique — la récupération ne dépend pas du matériel, uniquement du fichier XML.

- Automatisation possible avec AutoConfigBackup : le package pfSense AutoConfigBackup envoie automatiquement la configuration chiffrée sur les serveurs Netgate après chaque modification. Couplé à un stockage local (cron + SCP vers NAS), il garantit un RPO (Recovery Point Objective) quasi nul.

- Conformité aux bonnes pratiques ANSSI/ISO 27001 A.12.3 (Sauvegarde des informations) : rotation des sauvegardes, stockage hors site, test de restauration documenté — cette procédure constitue une preuve de conformité directement versable dans un audit de sécurité.