

CATÉGORIE GLPI · JP CONSULTING

Playbook Réseau

Les runbooks de la catégorie GLPI Réseau

Jean-Philippe Rebischung

Sommaire

Ce playbook regroupe les runbooks de la catégorie GLPI **Réseau**. Un runbook par sous-catégorie ; chaque runbook décrit, cas par cas, la conduite à tenir pour un incident ou une demande.

Administration à distance **3**

Incident · SSH injoignable sur un serveur Windows 4

Connexion et adressage **9**

Incident · Un poste n'a plus d'adresse réseau (169.254) 10

Pare-feu **15**

Incident · Une règle de pare-feu reste sans effet 16

VPN **19**

Incident · Le tunnel entre les deux sites est tombé 20

Index par symptôme

Ce que je reçois	Runbook	Page
Un technicien : « SSH vers le serveur répond Connection timed out »	Administration à distance	4
Un utilisateur : « je n'ai plus accès à rien » (adresse en 169.254)	Connexion et adressage	10
Un technicien : « la règle est appliquée et le flux ne passe toujours pas »	Pare-feu	16
Un constat : le site B ne répond plus (Ansible, FreeIPA, pings)	VPN	20

> **Les champs à remplacer**
>
> Dans les commandes et les messages, un texte entre chevrons, comme **`<N°_TICKET>`** ou **`<NOM_DU_DOSSIER>`**, est **à remplacer par la valeur de ton cas**, **chevrons compris**. Exemple : **`E:\Restauration-<N°_TICKET>`** devient **`E:\Restauration-21`**.
>
> Avant de valider une commande, relis-la : s'il reste un chevron, elle n'est pas prête.

RUNBOOK · PLAYBOOK RÉSEAU

Administration à distance

L'accès d'administration aux serveurs : SSH depuis le PC hôte.

Cas traités dans ce runbook

INCIDENT SSH injoignable sur un serveur Windows.....4

Statut : non validé

SSH injoignable sur un serveur Windows

Niveau	N2.
Où	le PC hôte **`HOTE-VMWARE`** (seul poste autorisé) et le serveur visé (**`SRV-DC01 .1`**, **`SRV-WSUS01 .2`**, **`SRV-ADCS01 .3`**), compte **`JPCONSULTING\admin.domaine`**.
GLPI	type Incident · catégorie : Réseau › Administration à distance. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

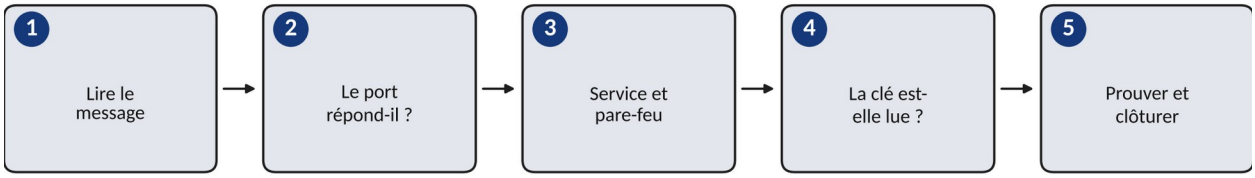
Les trois serveurs Windows s'administrent en **SSH*** depuis le PC hôte, avec une clé. Pour que ça marche, quatre choses doivent être vraies en même temps : le service **`sshd`** tourne, le pare-feu laisse entrer, la clé est lue, un interpréteur s'ouvre.

Ton travail : lire le message d'erreur, qui désigne une couche, puis prouver couche par couche.

Ce que tu reçois : le constat d'un technicien, par exemple « **`ssh`** vers le DC répond *Connection timed out* depuis ce matin ».

Regle d'or

Le message désigne la couche : *timed out* = rien n'a répondu ; *refused* = quelqu'un a répondu non ; mot de passe demandé = le réseau est bon, la clé n'est pas lue.



Les étapes de ce cas.

1 Lire le message

Ce que tu vois	Couche probable
`Connection timed out`	réseau ou pare-feu : le paquet est jeté en silence
`Connection refused`	rien n'écoute sur le port 22 : service **`sshd`**
Mot de passe demandé alors que la clé est posée	fichier de clés ignoré (droits trop larges)
Session ouverte sur **`cmd`** au lieu de PowerShell	**`DefaultShell`** absent du registre

Ticket : **Incident**, catégorie **Réseau › Administration à distance**.

2 Le port répond-il ?

Machine : HOTE-VMWARE (PC hôte, 192.168.20.70) | **Compte :** session Windows de l'hôte | **Outil :** PowerShell

```
Test-NetConnection <IP_DU_SERVEUR> -Port 22
```

Je dois voir

`TcpTestSucceeded : True` : le port répond, passe à l'étape 4. **`False`** : étape 3.

Depuis un **autre** poste que le PC hôte, **`False`** est normal : seul **`192.168.20.70`** est autorisé.

3 Service et pare-feu

SSH étant coupé, passe par la **console de la VM** dans VMware.

Machine : Le serveur (console VMware) | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-Service sshd | Select-Object Name, Status, StartType
```

Je dois voir

`Running` et **`Automatic`**. Sinon : **`Set-Service sshd -StartupType Automatic`** puis **`Start-Service sshd`**.

Machine : Le serveur (console VMware) | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-NetFirewallRule -Name SSH-PC-hote-In-TCP | Format-List Name, Enabled, Profile, Action
```

Je dois voir

`Enabled : True`, **`Profile : Domain`**, **`Action : Allow`**. La source se lit avec **`Get-NetFirewallRule -Name SSH-PC-hote-In-TCP | Get-NetFirewallAddressFilter`** : **`RemoteAddress`** = **`192.168.20.70`**.

Panne vécue : **`sshd`** arrêté, et la règle livrée **`OpenSSH-Server-In-TCP`** ne valait que pour le profil **Privé**, alors qu'un serveur du domaine est en profil **Domaine**.

4 La clé est-elle lue ?

Machine : Le serveur | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
icacls C:\ProgramData\ssh\administrators_authorized_keys
```

Je dois voir

Seuls **`SYSTEM`** et **`Administrators`** (ou **`Administrateurs`**). Avec des droits plus larges, OpenSSH ignore le fichier **sans message** et redemande le mot de passe.

Correction : **`icacls C:\ProgramData\ssh\administrators_authorized_keys /inheritance:r /grant 'SYSTEM:F' /grant 'Administrators:F'`**, puis **`Restart-Service sshd`**.

5 Prouver et clôturer

Machine : HOTE-VMWARE (PC hôte, 192.168.20.70) | **Compte :** session Windows de l'hôte | **Outil :** PowerShell

```
ssh -o BatchMode=yes -l admin.domaine@jpconsulting.lan <IP_DU_SERVEUR> hostname
```

Je dois voir

Le nom du serveur s'affiche **sans question** : c'est la clé qui a ouvert la session (`BatchMode` interdit toute demande de mot de passe).

Texte de la tâche (GLPI)

Serveur <NOM>, symptôme « <MESSAGE> » depuis <PC_HÔTE>. Port 22 : <RÉSULTAT>. `sshd` : <ÉTAT>. Règle `SSH-PC-hote-In-TCP` : <ÉTAT>. Droits du fichier de clés : <ÉTAT>. Correction : <ACTION>. Preuve : `ssh -o BatchMode=yes … hostname` rend <NOM> à <HEURE>.

Texte de la solution (GLPI)

La connexion SSH d'administration au serveur <NOM> est rétablie : <CAUSE_EN_MOTS_SIMPLES>.

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

SSH

Protocole d'administration à distance en ligne de commande, chiffré. Sur ce lab : port 22, depuis le seul PC hôte, avec une clé.

Profil réseau (Domaine, Privé, Public)

Catégorie que Windows donne à une connexion ; chaque règle du pare-feu ne vaut que pour certains profils.

Notes

RUNBOOK · PLAYBOOK RÉSEAU

Connexion et adressage

L'adressage des postes et le DHCP : un poste sans adresse, un réseau injoignable.

Cas traités dans ce runbook

INCIDENT Un poste n'a plus d'adresse réseau (169.254).....10

Statut : non validé

Un poste n'a plus d'adresse réseau (169.254)

Niveau	N1 (constater) puis N2 (serveur DHCP).
Où	le poste en panne, puis **`SRV-DC01`** (serveur DHCP), compte **`JPCONSULTING\admin.domaine`**.
GLPI	type Incident · catégorie : Réseau › Connexion et adressage.
	Statut : non validé

Ce que tu reçois et ce qu'on attend de toi

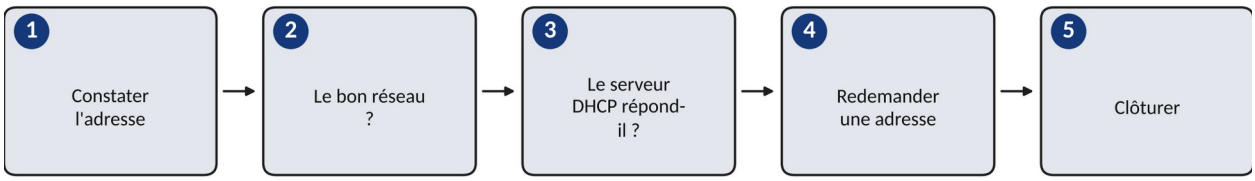
Un poste qui démarre demande une adresse au serveur **DHCP***. Si personne ne répond, il s'en invente une en **`169.254.x.x`** (**APIPA***) : elle ne passe aucun routeur, le poste ne voit plus ni le domaine, ni GLPI, ni Internet.

Ton travail : trouver **où la demande s'arrête** (le poste, son réseau, le serveur DHCP), dans cet ordre, sans redémarrer au hasard.

Ce que tu reçois, par exemple : « Je n'ai plus accès à rien, ni au réseau ni à GLPI. »

Regle d'or

Une adresse 169.254 ne dit pas « le réseau est cassé » : elle dit « personne n'a répondu à ma demande ».



Les étapes de ce cas.

1 Constater l'adresse

Machine : Le poste en panne | **Compte :** l'utilisateur ou un administrateur | **Outil :** Invite de commandes

```
ipconfig /all
```

Je dois voir

En panne : adresse **`169.254.x.x`**, aucune passerelle. Normal : adresse entre **`192.168.20.100`** et **`.200`**, passerelle **`.254`**, DNS **`.1`**.

Plusieurs postes touchés en même temps : le serveur DHCP est le premier suspect (étape 3).

Ticket : **Incident**, catégorie **Réseau › Connexion et adressage**. Priorité selon le nombre de postes touchés.

2 Le bon réseau ?

Pour une VM : dans VMware, **VM → Settings → Network Adapter** : **Custom: Specific virtual network** et **VMnet1**. Avec plusieurs réseaux « Host-only », le réglage générique ne désigne qu'un seul VMnet : la VM peut se retrouver seule sur un segment vide (panne vécue sur GLPI).

Machine : Le poste en panne | **Compte :** administrateur | **Outil :** PowerShell

```
Get-NetAdapter | Format-Table Name, Status, LinkSpeed, MacAddress
```

Je dois voir

`Status : Up`. `Disconnected` : la carte n'est pas reliée au commutateur virtuel.

3 Le serveur DHCP répond-il ?

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-Service DHCPServer | Select-Object Status, StartType
```

Je dois voir

`Running`. Attention : sur ce lab, le service a déjà été vu **Running mais en sommeil** après un démarrage du DC (incident vécu) : il avait vérifié son autorisation avant que l'annuaire soit prêt. Il est depuis en **démarrage différé**.

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-ChildItem C:\Windows\System32\dhcp\DhcpSrvLog-*.log | Sort-Object LastWriteTime |
Select-Object -Last 1 | Get-Content -Tail 20
```

Lire la commande

Journal d'audit du DHCP : un fichier par jour de la semaine. La commande prend le plus récent et affiche ses 20 dernières lignes.

Code `55` : serveur autorisé. Codes `50` puis `56` : échec de l'autorisation, le service ne distribue plus rien. Code `10` ou `11` : un bail attribué ou renouvelé.

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell (administrateur)

```
Get-DhcpServerv4ScopeStatistics -ScopeId 192.168.20.0
```

Je dois voir

Des adresses libres. Étendue pleine (`Free : 0`) : baux orphelins à nettoyer (escalade N2).

4 Redemander une adresse

Une fois la cause corrigée (VM sur le bon réseau, service DHCP redémarré par `Restart-Service DHCPServer` si le journal montre l'échec d'autorisation), redemande une adresse :

Machine : Le poste en panne | **Compte :** administrateur | **Outil :** Invite de commandes (administrateur)

```
ipconfig /renew
```

Je dois voir

Adresse entre `.100` et `.200`, passerelle `192.168.20.254`, DNS `192.168.20.1`. Puis la preuve par l'usage : le poste ouvre GLPI ou le partage.

5 Clôturer

Texte de la tâche (GLPI)

Poste(s) <NOMS> en APIPA (`169.254.x.x`) à <HEURE>. Réseau de la VM : <CONSTAT>. Service DHCP : <ÉTAT> ; journal : <CODES_LUS>. Étendue : <LIBRES>. Correction : <ACTION> à <HEURE>. Preuve : `ipconfig` rend <ADRESSE>, <APPLICATION> accessible.

Texte de la solution (GLPI), lisible par l'utilisateur

Bonjour <PRÉNOM>,

Votre poste n'avait pas reçu d'adresse réseau. Le problème est corrigé et vous avez de nouveau accès au réseau.

Cordialement,

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

DHCP

Service qui distribue automatiquement les adresses IP. Sur ce lab : le DC, adresses `.100` à `.200`, bail de 8 jours.

APIPA

Adresse `169.254.x.x` qu'un poste se donne seul quand aucun serveur DHCP ne répond. Elle ne passe aucun routeur.

Notes

RUNBOOK · PLAYBOOK RÉSEAU

Pare-feu

Les règles des deux pare-feux pfSense : un flux qui ne passe pas.

Cas traités dans ce runbook

INCIDENT Une règle de pare-feu reste sans effet..... 16

Statut : non validé

Une règle de pare-feu reste sans effet

Niveau	N2.
Où	la machine source du flux, puis PFSENSE01 ou PFSENSE02 (interface web depuis le PC hôte, ou shell), compte `admin` du pare-feu.
GLPI	type Incident · catégorie : Réseau › Pare-feu. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

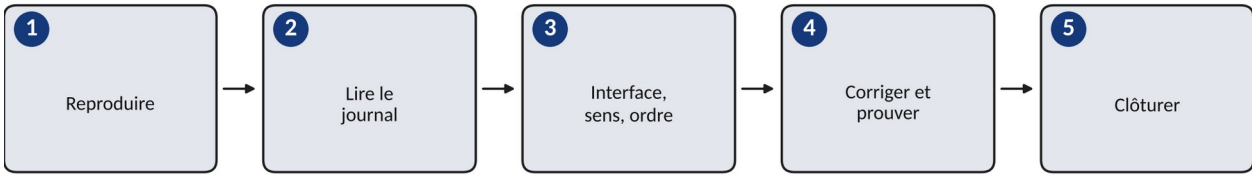
Le pare-feu lit ses règles **de haut en bas** et applique la première qui correspond. Une règle juste peut n'avoir aucun effet si une autre, plus haut, a déjà décidé.

Ton travail : prouver avec le **journal du pare-feu** quelle règle décide, au lieu de réécrire la règle au hasard.

Ce que tu reçois : « J'ai ajouté la règle, je l'ai appliquée, et le flux ne passe toujours pas. »

Regle d'or

On ne conclut jamais sans le journal : il donne le **numéro** de la règle qui a décidé.



Les étapes de ce cas.

1 Reproduire

Machine : La machine source du flux | **Compte :** selon la machine | **Outil :** PowerShell

```
Test-NetConnection <IP_DESTINATION> -Port <PORT>
```

Je dois voir

`TcpTestSucceeded : False` : le flux ne passe pas.

Un onglet de navigateur ouvert **avant** la règle continue de fonctionner (pare-feu à états*) : seule une connexion neuve prouve quelque chose.

Ticket : **Incident**, catégorie **Réseau › Pare-feu**. Note la source, la destination et le port.

2 Lire le journal

Interface web du pare-feu : **État → Journaux système → Pare-feu**. Filtre avec l'adresse seule dans *Adresse IP de destination* et le port dans *Port destination*. Repère l'interface, le sens, et la règle qui a bloqué.

Machine : PFSENSE01 ou PFSENSE02 (shell) | **Compte :** admin | **Outil :** SSH ou console

```
grep ',block,' /var/log/filter.log | tail -n 20
```

Lire la commande

Chaque ligne commence par le **numéro** de la règle qui a décidé. `pfctl -vvsr | grep '^@<NUMÉRO> '` affiche la règle correspondante.

3 Interface, sens, ordre

- Une règle ne voit que ce qui **entre** par son onglet (interface). Une règle sur le mauvais onglet n'a aucun effet, sans message.
- Un flux entre les deux sites traverse **deux** pare-feux : autorisé à l'entrée du tunnel (onglet de l'interface d'origine) **et** à la sortie (onglet IPsec d'en face).
- Un numéro de règle **bas** dans le journal : une règle placée avant la tienne décide ; ta règle n'est jamais lue.
- Les alias contiennent-ils ce que tu crois ? **Diagnostics → Tables**.

Attention

Exemple vécu : `Block private networks` interceptait le trafic avant la règle du port 443. Sur ce lab, le « WAN » est le réseau privé de la box : cette option est désactivée sur les deux pare-feux.

4 Corriger et prouver

Corrige (ordre, onglet, contenu), puis deux temps distincts : **Enregistrer**, puis **Appliquer les changements**.

Machine : La machine source du flux | **Compte :** selon la machine | **Outil :** PowerShell

```
Test-NetConnection <IP_DESTINATION> -Port <PORT>
```

Je dois voir

`TcpTestSucceeded : True`, et plus aucune ligne `block` pour ce flux dans le journal.

5 Clôturer

Texte de la tâche (GLPI)

Flux <SOURCE> → <DESTINATION>:<PORT>. Test initial : False. Journal : bloqué par la règle n° <N> (<DESCRIPTION>) sur l'interface <INTERFACE>. Correction : <ACTION>, enregistrée et appliquée à <HEURE>. Preuve : connexion neuve True, journal sans blocage. Export de la configuration avant modification : <OUI/NON>.

Texte de la solution (GLPI)

L'accès <SERVICE> depuis <SOURCE> est rétabli : une règle du pare-feu bloquait ce flux avant la règle prévue.

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

Pare-feu à états

Pare-feu qui garde en mémoire les connexions ouvertes : une connexion déjà établie continue après un changement de règle.

Alias

Nom donné dans pfSense à une liste d'adresses ou de ports, utilisé dans les règles (ex. **RFC1918**, **PORTS_SYSLOG**).

RUNBOOK · PLAYBOOK RÉSEAU

VPN

Le tunnel IPsec entre les deux sites et l'accès distant.

Cas traités dans ce runbook

INCIDENT Le tunnel entre les deux sites est tombé.....20

Statut : non validé

INCIDENT · VPN

Le tunnel entre les deux sites est tombé

Niveau	N2.
Où	**SRV-DC01** et SRV-FREEIPA01 (tests de bout en bout), PFSENSE01 et PFSENSE02 (interface web depuis le PC hôte, shell), compte **admin** des pare-feux.
GLPI	type Incident · catégorie : Réseau › VPN. *Statut : non validé*

Ce que tu reçois et ce qu'on attend de toi

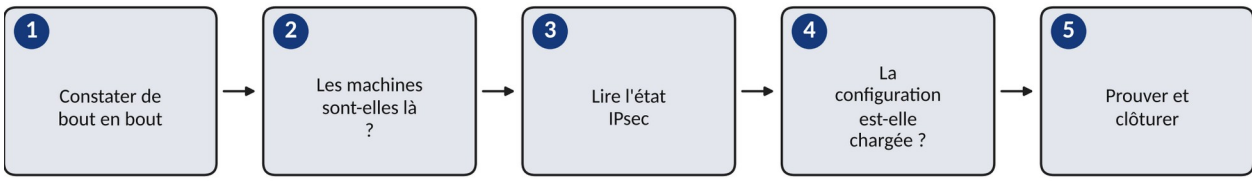
Les deux sites sont reliés par un tunnel **IPsec*** permanent entre PFSENSE01 et PFSENSE02. Il se monte en deux temps : les pare-feux s'identifient (**phase 1**), puis ouvrent un tunnel par paire de réseaux (**phases 2**). Ensuite, les règles décident ce qui passe.

Ton travail : lire l'état avant de conclure, et remonter les couches dans l'ordre. Aucune sonde Zabbix ne surveille le tunnel : il tombe **sans alerte**.

Ce que tu reçois, par exemple : « Le site B ne répond plus : Ansible échoue, FreeIPA est injoignable. »

Regle d'or

Lis avant de conclure. Lors de cette panne, la première hypothèse (veille du PC) était fausse : PFSENSE01 avait redémarré.



Les étapes de ce cas.

1 Constater de bout en bout

Machine : SRV-DC01 | **Compte :** JPCONSULTING\admin.domaine | **Outil :** PowerShell

```
ping -n 2 192.168.30.1
```

Je dois voir

Le sens B vers A se teste depuis SRV-FREEIPA01 : **ping -c 2 192.168.20.1**. Un seul sens en échec : pense **règles**. Les deux sens : pense **tunnel**.

Ticket : **Incident**, catégorie **Réseau › VPN**, priorité **Haute** si un site entier est coupé.

2 Les machines sont-elles là ?

- PC hôte allumé (il porte le site A et PFSENSE01).
- Proxmox **192.168.1.18** joignable, **VM 100 (PFSENSE02) démarrée**.

- Sur PFSENSE01, **Diagnostics → Ping** vers `192.168.1.254` (WAN de PFSENSE02).

3 Lire l'état IPsec

Sur les deux pare-feux : **État → IPsec**.

Ce que tu lis	Sens	Suite
Phase 1 `Established`, phases 2 `Installed`	Le tunnel est monté	Règles (onglet IPsec d'en face)
Phase 1 `Established`, phases 2 absentes	Sélecteurs de phase 2	Comparer les phases 2 des deux côtés
Phase 1 absente ou `Connecting`	Lien, authentification ou configuration non chargée	Étape 4

4 La configuration est-elle chargée ?

Machine : PFSENSE02 (shell : console VM 100 ou SSH depuis le PC hôte) | **Compte :** admin | **Outil :** swanctl

```
/usr/local/sbin/swanctl --list-conns
```

Je dois voir

Une connexion `con1:` listée. Rien : la configuration n'est pas chargée (panne connue au démarrage).

Machine : PFSENSE02 (shell) | **Compte :** admin | **Outil :** swanctl

```
/usr/local/sbin/swanctl --load-all --file /var/etc/ipsec/swanctl.conf
```

Lire la commande

Recharge la configuration. **Sans `--file`**, la commande ne la trouve pas : pfSense la range hors de l'emplacement standard. Une garde planifiée (toutes les 5 minutes) fait la même chose : `grep garde-ipsec /var/log/system.log` dit si elle est intervenue.

5 Prouver et clôturer

Je dois voir

État → IPsec des deux côtés : phase 1 `Established`, phases 2 `Installed`. Pings dans les deux sens. Sur SRV-FREEIPA01 : `sssctl domain-status jpconsulting.lan` rend `Online`.

Texte de la tâche (GLPI)

Symptôme : <DESCRIPTION> à <HEURE> (sens <A→B / B→A / LES DEUX>). Machines : <ÉTAT>. État IPsec : phase 1 <ÉTAT>, phases 2 <ÉTAT>. Cause : <CAUSE>. Action : <ACTION> à <HEURE>. Preuve : état Established/Installed, pings OK, trust Online. La clé pré-partagée n'est pas citée.

Texte de la solution (GLPI)

La liaison entre les deux sites est rétablie depuis <HEURE>. Les services du site B sont de nouveau joignables.

Lexique

Les mots marqués d'un astérisque (*) dans ce runbook.

IPsec

Protocole qui chiffre le trafic entre deux réseaux. Ici IKEv2, clé pré-partagée (jamais écrite), PFSENSE01 initiateur.

Phase 1 / phase 2

Phase 1 : les deux pare-feux s'authentifient ; phases 2 : un tunnel de données par paire de réseaux (`20.0/24` ↔ `30.0/24`, `40.0/24` ↔ `30.0/24`).