

Exemple de recettage — VPN WireGuard

Recette d'un VPN site à site WireGuard entre deux pare-feux pfSense : cas complet rédigé, du cahier de recette au procès-verbal

§ Un exemple à adapter

Ce document présente un **exemple rédigé** de recettage, appliqué à un cas concret. Il illustre la démarche décrite dans le livret « Le recettage informatique » : il ne s'agit pas d'un modèle unique à recopier.

Le nombre de tests, leur formulation et le niveau de détail doivent être **adaptés** à chaque installation et à chaque cahier des charges. La même démarche s'applique à un tunnel IPsec, en adaptant les commandes et les écrans. Les noms, adresses et versions sont fictifs ou indicatifs.

1. Présentation du cas

Une entreprise relie son siège (site A) et une agence (site B) par un VPN site à site WireGuard, configuré sur deux pare-feux pfSense CE. Les postes du siège doivent accéder au serveur de fichiers de l'agence, et uniquement à lui.

Environnement de recette

Élément	Site A (siège)	Site B (agence)	Remarque
Pare-feu	fw-sitea	fw-siteb	pfSense CE + paquet WireGuard
Adresse WAN	203.0.113.10	198.51.100.20	Plages de documentation
LAN	192.168.10.0/24	192.168.20.0/24	Passerelles en .254
Adresse de tunnel	10.10.10.1/30	10.10.10.2/30	Interface tun_wg0
Machine de test	pc-a01 (192.168.10.50)	srv-fic-b (192.168.20.10)	Poste Windows 11 / serveur de fichiers

Exigences retenues

Réf.	Exigence du cahier des charges
E1	Un tunnel WireGuard est établi entre fw-sitea et fw-siteb (UDP 51820).
E2	Les deux extrémités du tunnel communiquent (10.10.10.1 ↔ 10.10.10.2).
E3	Les postes du LAN A joignent le LAN B en passant par le tunnel.
E4	Depuis le LAN A, seuls le ping et le partage de fichiers (TCP 445) vers srv-fic-b sont autorisés.
E5	Sur le WAN de fw-siteb, seul le flux UDP 51820 provenant de fw-sitea est accepté ; l'interface d'administration n'est pas exposée.
E6	Les clés privées ne sont pas divulguées.

Réf.	Exigence du cahier des charges
E7	Le tunnel se rétablit automatiquement après le redémarrage d'un pare-feu.

Vigilance : sécurité des tests et des preuves

Les **clés privées** WireGuard ne doivent jamais apparaître dans un document : la commande `wg show` les masque d'elle-même, mais un export de configuration ou une capture de l'écran de paramétrage peut les révéler. Les clés publiques sont tronquées ici pour la lisibilité.

Les **analyses de ports** (test 5) sont réalisées uniquement sur l'infrastructure du laboratoire, avec autorisation : scanner un système sans autorisation est illégal.

2. Fiches de test et preuves

Test 1 — État du tunnel WireGuard

FICHE DE TEST N° 1	
Exigence couverte	E1, E6
Objectif du test	Vérifier que le tunnel est configuré et qu'une poignée de main récente a eu lieu avec le pair.
Type de test	Fonctionnel / Sécurité
Prérequis	Tunnel et pair configurés sur les deux pfSense.
Procédure	1. Sur fw-sitea, ouvrir Diagnostics > Command Prompt. 2. Exécuter <code>wg show</code> .
Résultat attendu	Pair 198.51.100.20:51820 ; réseaux autorisés 10.10.10.2/32 et 192.168.20.0/24 ; poignée de main de moins de 2 minutes ; clé privée non affichée.
Résultat obtenu	Conforme.
Preuve(s)	Capture 1
Statut	☒ Conforme
Anomalie / commentaire	Aucune.
Re-test après correction	Sans objet.

Capture 1 — Sortie de wg show sur fw-sitea

```
interface: tun_wg0
  public key: kP3x...Hc8=
  private key: (hidden)
  listening port: 51820

peer: Q9fZ...a2E=
  endpoint: 198.51.100.20:51820
  allowed ips: 10.10.10.2/32, 192.168.20.0/24
  latest handshake: 38 seconds ago
  transfer: 1.24 MiB received, 2.87 MiB sent
  persistent keepalive: every 30 seconds
```

 Explicitation

Contexte : pare-feu fw-sitea, interface web, menu Diagnostics > Command Prompt.

Action : exécution de `wg show`.

À observer : l'adresse du pair, les réseaux autorisés, la dernière poignée de main (38 secondes) et la mention « (hidden) » pour la clé privée.

Interprétation : une poignée de main récente prouve que les deux pare-feux se sont authentifiés mutuellement avec leurs clés : le tunnel est établi. Les réseaux autorisés correspondent au plan. **Test conforme.**

Données masquées : clés publiques tronquées (...); clé privée masquée par l'outil.

Test 2 — Communication entre les extrémités du tunnel

FICHE DE TEST N° 2	
Exigence couverte	E2
Objectif du test	Vérifier que les deux adresses de tunnel se joignent.
Type de test	Fonctionnel
Prérequis	Test 1 conforme.
Procédure	1. Sur fw-sitea, Diagnostics > Ping vers 10.10.10.2, source 10.10.10.1, 3 paquets.
Résultat attendu	3 réponses, 0 % de perte.
Résultat obtenu	Conforme.
Preuve(s)	Capture 2
Statut	☒ Conforme
Anomalie / commentaire	Aucune.
Re-test après correction	Sans objet.

Capture 2 — Ping de 10.10.10.1 vers 10.10.10.2

```
PING 10.10.10.2 (10.10.10.2) from 10.10.10.1: 56 data bytes
64 bytes from 10.10.10.2: icmp_seq=0 ttl=64 time=4.812 ms
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=4.655 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=4.701 ms
3 packets transmitted, 3 packets received, 0.0% packet loss
```

 Explicitation

Contexte : pare-feu fw-sitea, menu Diagnostics > Ping, adresse source 10.10.10.1.

Action : envoi de 3 requêtes ICMP vers l'autre extrémité du tunnel.

À observer : la dernière ligne : 3 paquets reçus, 0 % de perte.

Interprétation : les deux interfaces de tunnel communiquent. **Test conforme.**

Données masquées : aucune donnée sensible.

Test 3 — Routage entre les deux LAN

FICHE DE TEST N° 3	
Exigence couverte	E3
Objectif du test	Vérifier qu'un poste du LAN A joint le serveur du LAN B en passant par le tunnel.
Type de test	Fonctionnel
Prérequis	Tests 1 et 2 conformes ; route vers 192.168.20.0/24 via le tunnel.
Procédure	1. Sur pc-a01, ouvrir PowerShell. 2. Exécuter <code>tracert -d 192.168.20.10</code> .
Résultat attendu	Trois sauts : 192.168.10.254, puis 10.10.10.2, puis 192.168.20.10.
Résultat obtenu	Conforme.
Preuve(s)	Capture 3
Statut	☒ Conforme
Anomalie / commentaire	Aucune.
Re-test après correction	Sans objet.

Capture 3 — Itinéraire de pc-a01 vers srv-fic-b

```
PS C:\Users\test.user> tracert -d 192.168.20.10
Détermination de l'itinéraire vers 192.168.20.10 avec un maximum de 30 sauts.
 1    <1 ms    <1 ms    <1 ms  192.168.10.254
 2     5 ms     4 ms     5 ms  10.10.10.2
 3     5 ms     5 ms     5 ms  192.168.20.10
Itinéraire déterminé.
```

 Explicitation

Contexte : poste pc-a01 (LAN A), session de l'utilisateur de test, PowerShell.

Action : traçage de l'itinéraire vers srv-fic-b.

À observer : le 2e saut 10.10.10.2 (extrémité B du tunnel), puis la destination.

Interprétation : le passage par 10.10.10.2 prouve que le trafic emprunte bien le tunnel, et non un autre chemin. Un simple ping n'aurait pas permis de le démontrer. **Test conforme.**

Données masquées : aucune donnée sensible.

Test 4 — Filtrage des flux dans le tunnel

FICHE DE TEST N° 4	
Exigence couverte	E4
Objectif du test	Vérifier que seuls le ping et TCP 445 vers srv-fic-b sont autorisés depuis le LAN A.
Type de test	Sécurité
Prérequis	Test 3 conforme. Services 445 (SMB) et 3389 (RDP) actifs sur srv-fic-b.
Procédure	1. Sur pc-a01, tester le port 445 de srv-fic-b. 2. Tester le port 3389 (non autorisé).
Résultat attendu	Port 445 : TcpTestSucceeded True. Port 3389 : TcpTestSucceeded False.
Résultat obtenu	1er passage : 3389 joignable (non conforme). 2e passage : 3389 bloqué.
Preuve(s)	Captures 4a et 4b
Statut	☒ Conforme après correction
Anomalie / commentaire	Anomalie majeure (sécurité) : règle « autoriser tout » sur l'interface WireGuard de fw-siteb. Remplacée par des règles restrictives.
Re-test après correction	15/10/2026 — Conforme (capture 4b).

Capture 4a — Premier passage

```
PS C:\Users\test.user> Test-NetConnection 192.168.20.10 -Port 445 | Select-Object  
RemotePort, TcpTestSucceeded  
RemotePort TcpTestSucceeded  
-----  
445 True  
PS C:\Users\test.user> Test-NetConnection 192.168.20.10 -Port 3389 | Select-Object  
RemotePort, TcpTestSucceeded  
3389 True
```

 Explicitation — résultat non conforme

Contexte : poste pc-a01, PowerShell.

Action : test des ports 445 puis 3389 sur srv-fic-b.

À observer : le port 3389 répond (True) alors qu'il devrait être bloqué.

Interprétation : le tunnel laisse passer des flux non prévus : le bureau à distance du serveur est accessible depuis tout le LAN A. **Test non conforme** ; anomalie majeure de sécurité ouverte.

Données masquées : aucune donnée sensible.

Correction appliquée sur fw-siteb (Firewall > Rules > WireGuard)

Action	Source	Destination	Protocole / port
Avant	Tout	Tout	Tout (règle supprimée)

Action	Source	Destination	Protocole / port
Passer	192.168.10.0/24	192.168.20.10	ICMP echo-request
Passer	192.168.10.0/24	192.168.20.10	TCP 445
Bloquer	Tout	Tout	Tout (règle explicite, journalisée)

Capture 4b — Re-test après correction

```
PS C:\Users\test.user> Test-NetConnection 192.168.20.10 -Port 445 | Select-Object  
RemotePort, TcpTestSucceeded  
445 True  
PS C:\Users\test.user> Test-NetConnection 192.168.20.10 -Port 3389 | Select-Object  
RemotePort, TcpTestSucceeded  
AVERTISSEMENT : TCP connect to (192.168.20.10 : 3389) failed  
3389 False
```

 Explicitation

Contexte : poste pc-a01, après modification des règles de fw-siteb.

Action : mêmes tests qu'au premier passage.

À observer : 445 toujours True (le service attendu fonctionne), 3389 désormais False.

Interprétation : le filtrage est conforme : le flux autorisé passe et le flux interdit est bloqué. Le test du port 445 sert aussi de **non-régression** après la correction. **Test conforme.**

Données masquées : aucune donnée sensible.

Test 5 — Exposition du WAN de fw-siteb

FICHE DE TEST N° 5	
Exigence couverte	E5
Objectif du test	Vérifier que le pare-feu de l'agence n'expose rien d'autre que WireGuard au pair autorisé.
Type de test	Sécurité
Prérequis	Poste de test autorisé placé sur le réseau WAN du laboratoire (203.0.113.50), différent de fw-sitea.
Procédure	1. Relever la règle WAN de fw-siteb. 2. Depuis le poste de test, analyser les ports TCP d'administration de 198.51.100.20.
Résultat attendu	Une seule règle WAN : UDP 51820 depuis 203.0.113.10. Ports 22, 80 et 443 non joignables.
Résultat obtenu	Conforme.
Preuve(s)	Capture 5
Statut	☒ Conforme
Anomalie / commentaire	Aucune.
Re-test après correction	Sans objet.

Capture 5 — Règle WAN et analyse depuis l'extérieur

```
# Règle WAN de fw-siteb (relevée dans Firewall > Rules > WAN)
Pass IPv4 UDP source 203.0.113.10 dest. WAN address port 51820 « WireGuard site A »

test@poste-wan:~$ nmap -Pn -p 22,80,443 198.51.100.20
Nmap scan report for 198.51.100.20
PORT      STATE      SERVICE
22/tcp    filtered  ssh
80/tcp    filtered  http
443/tcp   filtered  https
```

 Explicitation

Contexte : interface web de fw-siteb pour la règle, puis poste de test « poste-wan » (203.0.113.50) sur le WAN du laboratoire.

Action : relevé de la règle WAN, puis analyse nmap des ports d'administration.

À observer : la source limitée à 203.0.113.10 dans la règle, et l'état « filtered » des trois ports.

Interprétation : seul le pair légitime peut joindre WireGuard, et l'interface web comme SSH restent invisibles depuis Internet. **Test conforme.**

Données masquées : aucune ; les adresses publiques sont des adresses de documentation.

Test 6 — Rétablissement après redémarrage

FICHE DE TEST N° 6	
Exigence couverte	E7
Objectif du test	Vérifier que le tunnel remonte seul après le redémarrage de fw-siteb.
Type de test	Robustesse
Prérequis	Tests 1 à 5 conformes.
Procédure	1. Sur pc-a01, lancer ping -t 192.168.20.10. 2. Redémarrer fw-siteb. 3. Observer la reprise, puis contrôler wg show sur fw-sitea.
Résultat attendu	Interruption pendant le redémarrage, puis reprise sans intervention ; nouvelle poignée de main.
Résultat obtenu	Interruption d'environ 1 min 30, reprise automatique.
Preuve(s)	Captures 6a et 6b
Statut	☒ Conforme
Anomalie / commentaire	Aucune.
Re-test après correction	Sans objet.

Capture 6a — Ping continu pendant le redémarrage (extrait)

```
Réponse de 192.168.20.10 : octets=32 temps=5 ms TTL=126
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
(... 44 lignes identiques non reproduites ...)
Réponse de 192.168.20.10 : octets=32 temps=6 ms TTL=126
Réponse de 192.168.20.10 : octets=32 temps=5 ms TTL=126
```

 Explicitation

Contexte : poste pc-a01, ping continu pendant le redémarrage de fw-siteb.

Action : ping -t puis redémarrage du pare-feu distant.

À observer : le passage des réponses aux délais dépassés, puis le retour des réponses.

Interprétation : la coupure correspond au redémarrage ; la reprise se fait sans aucune action manuelle.

Données masquées : aucune ; sortie abrégée, ce qui est signalé.

Capture 6b — wg show sur fw-sitea après la reprise (extrait)

```
peer: Q9fZ...a2E=
  endpoint: 198.51.100.20:51820
  latest handshake: 12 seconds ago
```

✓ **Explicitation**

Contexte : pare-feu fw-sitea, Diagnostics > Command Prompt.

Action : wg show après la reprise du ping.

À observer : une poignée de main de 12 secondes.

Interprétation : une nouvelle session a été négociée après le redémarrage : le tunnel s'est rétabli de lui-même. **Test conforme.**

Données masquées : aucune donnée sensible.

3. Synthèse des tests

N°	Test	Statut	Anomalie / réserve	Re-test
1	État du tunnel	Conforme	—	—
2	Extrémités du tunnel	Conforme	—	—
3	Routage entre LAN	Conforme	—	—
4	Filtrage des flux	Conforme après correction	Majeure : règle « tout autoriser »	Conforme
5	Exposition du WAN	Conforme	—	—
6	Rétablissement après redémarrage	Conforme	—	—

4. Procès-verbal de recette

PROCÈS-VERBAL DE RECETTE	
Projet / installation	VPN site à site WireGuard fw-sitea ↔ fw-siteb
Bilan des tests	6 tests réalisés : 6 conformes (dont 1 après correction), 0 non conforme, 0 avec réserve
Décision	☒ Recette prononcée sans réserve ☐ Recette prononcée avec réserves ☐ Recette refusée
Réserves éventuelles	Aucune.
Observation	Prévoir la sauvegarde des configurations des deux pfSense (fichiers chiffrés : ils contiennent les clés privées) et une supervision de l'état du tunnel.
Testeur	Nom Prénom — 15/10/2026 — signature
Valideur	Nom Prénom — 15/10/2026 — signature

✓ Ce que montre cet exemple

- Chaque exigence du cahier des charges est couverte par au moins un test.
- Un tunnel « qui marche » n'est pas forcément conforme : le test 4 révèle un **défaut de sécurité** invisible à l'usage.
- Le test qui suit une correction vérifie aussi que **rien n'a été cassé** (non-régression).
- Les preuves sont **explicitées**, et les clés privées n'apparaissent jamais.