

Passez votre site à HTTPS avec Nginx, sans casser vos URL

Suivez cette procédure courte pour activer une redirection HTTP vers HTTPS fiable. Elle vous aide à préserver les chemins et paramètres, éviter les boucles et contrôler le résultat avant mise en service.

Au sommaire

- 1 À vérifier avant toute modification
- 2 Configuration en 4 étapes
- 3 Repères de configuration à retenir
- 4 Tests après édition
- 5 Le mémo essentiel

À vérifier avant toute modification

- ☐ **Identifier le fichier de configuration réellement chargé par Nginx**
Contrôlez les directives include ou utilisez nginx -T si nécessaire.
- ☐ **Sauvegarder le fichier de site avant de l'éditer**
Préparez un retour rapide à une configuration connue.
- ☐ **Vérifier que le domaine pointe vers le bon serveur ou proxy**
- ☐ **Confirmer qu'un bloc HTTPS fonctionnel écoute déjà sur le port 443**
Le certificat et la clé privée doivent être accessibles à Nginx.
- ☐ **Déterminer si la validation ou le renouvellement du certificat utilise le webroot Certbot**
Une exception HTTP peut être nécessaire pour le défi ACME.



Requête HTTP



Bloc port 80



Retour 301

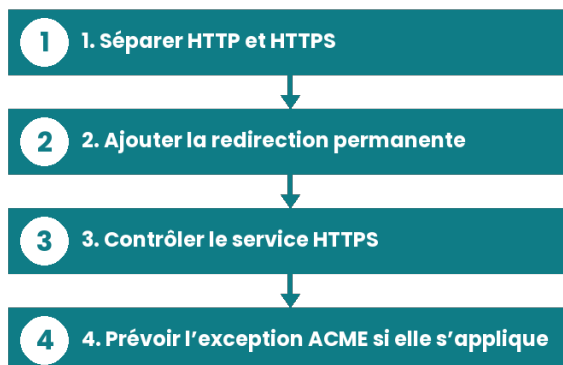


URL HTTPS
conservée



Réponse port 443

Configuration en 4 étapes



1. Séparer HTTP et HTTPS

Conservez un bloc serveur pour le port 80 et un autre pour le port 443. Le trafic HTTP doit uniquement orienter le visiteur vers la version sécurisée.

2. Ajouter la redirection permanente

Dans le bloc HTTP, utilisez une réponse 301 vers `https://$host$request_uri`. Cette destination conserve le nom d'hôte, le chemin demandé et la chaîne de paramètres.

3. Contrôler le service HTTPS

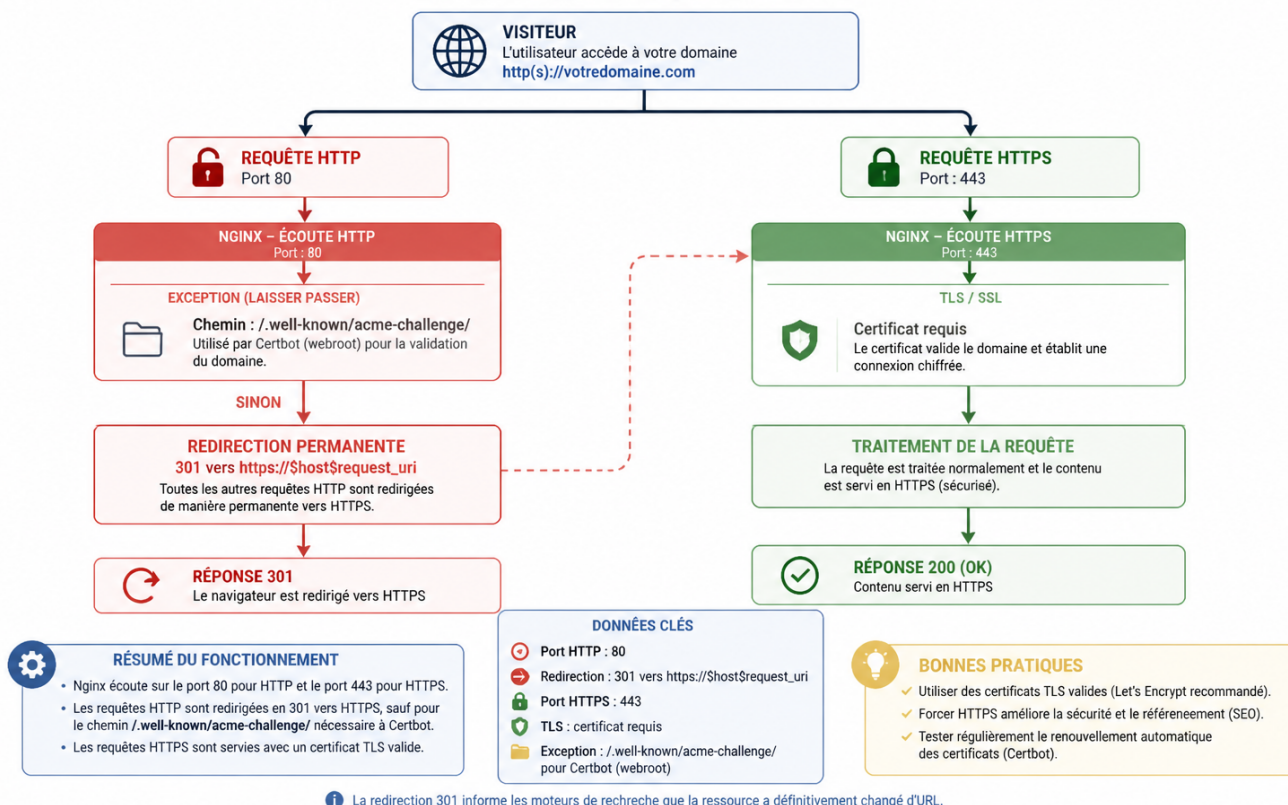
Vérifiez que le bloc port 443 active TLS et référence le certificat correspondant au domaine demandé. Le contenu du site ou le proxy applicatif doit rester servi depuis ce bloc HTTPS.

4. Prévoir l'exception ACME si elle s'applique

Si Certbot valide via webroot, laissez `/.well-known/acme-challenge/` accessible en HTTP avant d'appliquer la redirection au reste des requêtes.

REDIRECTION HTTP VERS HTTPS AVEC NGINX

Forcer les connexions sécurisées en redirigeant tout le trafic HTTP vers HTTPS



SCHEMA Redirection HTTP vers HTTPS avec une exception dédiée au défi ACME.

Repères de configuration à retenir

Élément	Rôle
Port 80	Reçoit les requêtes HTTP et renvoie la redirection.
<code>return 301 https://\$host\$request_uri</code>	Bascule durablement vers HTTPS en préservant l'URL demandée.
<code>\$host</code>	Conserve le nom d'hôte transmis par le client.
<code>\$request_uri</code>	Conserve le chemin et les paramètres de requête.
Port 443 avec TLS	Sert effectivement le site sécurisé avec son certificat.
<code>/well-known/acme-challenge/</code>	Peut rester disponible en HTTP pour une validation Certbot en mode webroot.

Tests après édition

- ☐ **Tester la syntaxe avec `sudo nginx -t`**
Ne rechargez pas Nginx tant que le test ne signale pas une configuration valide.
- ☐ **Recharger Nginx après validation de la syntaxe**
- ☐ **Vérifier qu'une URL HTTP répond par une redirection 301 vers son équivalent HTTPS**
- ☐ **Contrôler que le chemin et les paramètres sont inchangés**
Une URL de type `/produit?id=42` doit rester identique après le changement de protocole.

- ❑ **Tester l'accès HTTPS et la validité du certificat pour le domaine concerné**
- ❑ **Tester le chemin ACME si votre renouvellement repose sur le webroot**

! Évitez ces erreurs de migration

Ne forcez pas HTTPS avant que le site sécurisé ne réponde correctement. N'alternez pas entre HTTP et HTTPS : une page doit avoir une version canonique. Évitez aussi de modifier en même temps la redirection, les certificats et le routage applicatif, car le diagnostic devient plus difficile.

Le mémo essentiel

Une redirection 301 est adaptée lorsque le passage vers HTTPS est stabilisé.

Préserver `$request_uri` évite d'envoyer toutes les visites vers la page d'accueil.

Testez la configuration avant rechargement, puis vérifiez le comportement réel des en-têtes et des URL.

La redirection ne remplace pas la configuration TLS : certificat, clé privée et écoute sur le port 443 restent indispensables.

Une configuration présente sur le disque n'a aucun effet si elle n'est pas incluse et chargée par Nginx.

Adaptez les noms de domaine, chemins de certificats et répertoires webroot à votre installation réelle.