Ouvrir vers l'exterieur l'accès à Open-Prod

1. Principe général

L’objectif est de permettre à des utilisateurs autorisés d’accéder à Open-Prod depuis Internet, tout en conservant le serveur de production dans le réseau interne de l’entreprise. Le client, ou son prestataire informatique, choisit l’architecture adaptée à son contexte et met en place les composants réseau et sécurité nécessaires.

Message clé à retenir

> Open-Prod ne doit pas nécessairement être directement exposé sur Internet. Dans la majorité des cas, l’accès passe par des équipements intermédiaires : pare-feu, NAT, reverse proxy, VPN ou service de sécurité équivalent.

> **Le client mettra en place les mécanismes nécessaires, notamment DNS, routage, pare-feu, NAT, reverse proxy, VPN ou tout dispositif équivalent, afin de permettre un accès sécurisé depuis Internet au serveur Open-Prod de production hébergé sur son réseau interne. La configuration et la sécurisation de ce chemin d’accès relèvent de la responsabilité du client ou de son prestataire informatique. L’équipe 1Life pourra intervenir pour assister à la validation applicative une fois les accès réseau opérationnels.**

2. Choisir le scénario d’accès adapté

Scénario	Principe	Cas d’usage typique	Niveau de sécurité
Accès direct HTTPS	Le pare-feu redirige le flux HTTPS vers le serveur ou le service exposé.	Petite structure, architecture simple, faible nombre d’utilisateurs externes.	Sécurité à maîtriser, faible coût de mise en oeuvre. A utiliser obligatoirement si un service externe doit accéder de manière permanente à des ressources Open-Prod (Services de RFE, lien vers des services M365, etc.).
VPN	Les utilisateurs se connectent d’abord au réseau interne via VPN.	Cas recommandé pour la majorité des entreprises.	Permet de garantir une protection importante des accès externes et une authentification forte des utilisateurs en mobilité ou en connexion de sites à sites.

Reverse proxy	Un serveur intermédiaire reçoit les connexions Internet et relaie vers Open-Prod.	Cas recommandé pour la majorité des entreprises.	Bon niveau de sécurité et meilleure maîtrise. Solution plus complexe à maitriser car elle repose souvent sur une couche réseau et une couche applicative sur le serveur Open-Prod.
Reverse proxy + WAF	Ajout d'un filtrage applicatif avancé devant le service publié.	Entreprise avec exigences de sécurité fortes.	Renforcé.

3. Démarches à réaliser pas à pas

Étape 1 - Identifier le serveur Open-Prod à publier

Responsable principal : Client

Actions à réaliser :

- Identifier le nom du serveur Open-Prod de production.
- Relever son adresse IP interne.
- Confirmer les ports applicatifs utilisés.
- Vérifier que l'application fonctionne depuis le réseau local.

Livrable attendu : Nom du serveur, adresse IP interne, ports utilisés.

Étape 2 - Valider le besoin d'accès externe

Responsable principal : Client / Métier / DSI

Actions à réaliser :

- Identifier les profils ou services qui doivent accéder à Open-Prod depuis l'extérieur.
- Déterminer si l'accès concerne des salariés, agences, fournisseurs, clients ou prestataires, des services Web externes.
- Définir si l'accès doit être permanent, ponctuel ou limité à certaines plages horaires.

Livrable attendu : Liste des utilisateurs ou populations ou services web concernées et règles d'accès attendues.

Étape 3 - Choisir l'architecture d'exposition

Responsable principal : Client / Prestataire informatique

Actions à réaliser :

- Choisir entre accès direct HTTPS, reverse proxy, VPN, WAF ou hébergement externe.
- Prendre en compte les contraintes de sécurité internes.
- Valider l’architecture avec le responsable informatique ou le prestataire réseau.

Livrable attendu : Schéma cible ou description de l’architecture retenue.

Étape 4 - Vérifier la connectivité Internet entrante

Responsable principal : Client / Opérateur télécom

Actions à réaliser :

- Vérifier la disponibilité d’une adresse IP publique fixe ou d’un mécanisme équivalent.
- S’assurer que l’opérateur autorise les connexions entrantes nécessaires.
- Vérifier que l’équipement réseau frontal est administrable.

Livrable attendu : Adresse IP publique ou information de publication équivalente.

Étape 5 - Créer le nom DNS d’accès

Responsable principal : Client / Gestionnaire DNS

Actions à réaliser :

- Créer un nom DNS dédié, par exemple openprod.masociete.fr.
- Faire pointer ce nom vers l’adresse publique ou le point d’entrée retenu.
- Vérifier la résolution DNS depuis Internet.

Livrable attendu : Nom DNS définitif communiqué aux utilisateurs.

Étape 6 - Configurer le routage, le NAT et le pare-feu

Responsable principal : Client / Prestataire réseau

Actions à réaliser :

- Créer les règles de pare-feu nécessaires.
- Mettre en place le NAT ou la redirection vers le reverse proxy ou le serveur cible.
- Limiter l’exposition aux seuls ports nécessaires.
- Activer ou conserver la journalisation des accès.

Livrable attendu : Flux réseau opérationnels et filtrés.

Étape 7 - Mettre en place HTTPS et le certificat

Responsable principal : Client / Prestataire informatique

Actions à réaliser :

- Obtenir ou générer un certificat SSL/TLS valide.
- Installer le certificat sur le serveur Open-Prod.
- Vérifier que l'accès se fait en HTTPS sans alerte navigateur.

Livrable attendu : URL HTTPS valide, par exemple https://openprod.masociete.fr.

Étape 8 - Renforcer la sécurité

Responsable principal : Client / DSI

Actions à réaliser :

- Restreindre les accès lorsque cela est possible par adresse IP, VPN, MFA ou règles spécifiques.
- Maintenir les composants exposés à jour.
- Surveiller les journaux d'accès.
- Prévoir une procédure de coupure rapide en cas d'incident.

Livrable attendu : Mesures de durcissement validées.

Étape 9 - Réaliser les tests de validation

Responsable principal : Client + équipe Open-Prod

Actions à réaliser :

- Tester l'accès depuis un réseau externe.
- Contrôler le certificat HTTPS.
- Vérifier la connexion à Open-Prod et les principales fonctions métier.
- Contrôler les performances et les journaux côté infrastructure.

Livrable attendu : Validation technique et fonctionnelle de l'accès externe.

5. Check-list client avant sollicitation des équipes 1life

☐ Le serveur Open-Prod de production est identifié.
☐ L’adresse IP interne et les ports applicatifs sont connus.
☐ L’accès Open-Prod fonctionne sur le réseau local.
☐ Le scénario d’accès externe est choisi : reverse proxy, VPN, WAF, NAT direct ou hébergement externe.
☐ Le nom DNS public est défini ou en cours de création.
☐ L’adresse IP publique ou le point d’entrée Internet est connu.
☐ Les règles de pare-feu et de NAT sont préparées ou planifiées.
☐ Le certificat SSL/TLS est prévu ou déjà disponible.
☐ Les exigences de sécurité internes sont validées par la DSI ou le prestataire informatique.

7. Points de vigilance

Ne pas exposer inutilement plusieurs ports : limiter l’accès au strict nécessaire. Pour les écahnges depuis l'exterieur du réseau privilégier HTTPS avec certificat valide afin d’éviter les alertes navigateur et de chiffrer les échanges. Éviter, lorsque cela est possible, l’exposition directe du serveur applicatif : préférer un reverse proxy, un VPN ou un dispositif contrôlé. Prévoir une journalisation exploitable en cas d’incident ou d’audit. Documenter précisément l’architecture retenue pour faciliter le support et les évolutions futures.

8. Schéma de principe simplifié

Internet
  |
  v
Nom DNS public : openprod.monsociete.fr
  |
  v
Adresse IP publique / point d’entrée client
  |
  v
Pare-feu / NAT / Reverse proxy / VPN / WAF
  |
  v
Serveur Open-Prod de production sur le réseau interne

Revision #7
Created 2026-07-10 12:46:43 UTC by Jacques LEGAT
Updated 2026-07-16 16:24:55 UTC by Jacques LEGAT