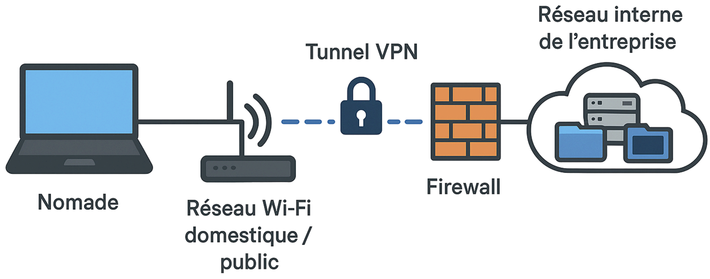
Note d'information Fortinet : La fin du VPN SSL

Johan Lemonnier
Chef de projet Marketing

Suite à la publication de sa nouvelle version FortiOS, Fortinet a communiqué à la mi-avril l'arrêt de support d'une fonctionnalité utilisée sur votre solution, voici quelques précisions :

Qu'est-ce que c'est : Un tunnel SSL VPN (Secure Sockets Layer Virtual Private Network) est une technologie de sécurité réseau qui permet de créer une connexion sécurisée entre un utilisateur et un réseau distant via Internet.

Pourquoi ça s'arrête : La fin de support du VPN SSL dans la version de FortiOS 7.6.3 s'explique par plusieurs failles de sécurité critiques qui ont été subies par les utilisateurs des tunnels SSL VPN au cours des dernières années.
Exemple : début 2024 ie CVE-2024-21762 a impacté environ 350K équipements Fortinet dans le monde.



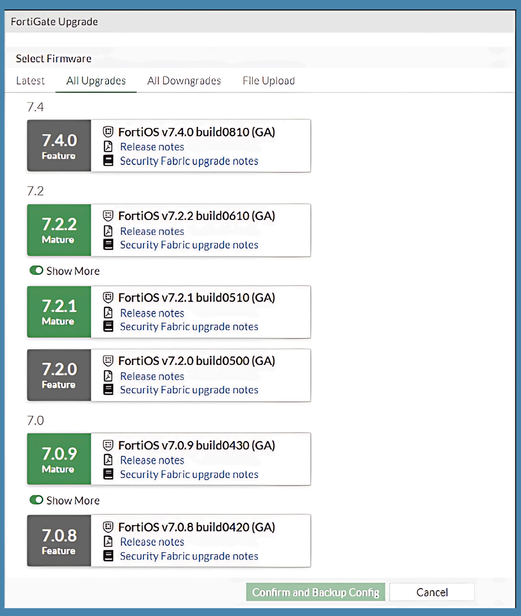
Quel impact pour vous ? : pour le moment rien. La version 7.6.3 est une version récente et n'est pas encore en production sur les équipements Fortinet managés par Linkt.
Fortinet déploie plusieurs versions de production, incluant des temps de stabilisation, du patching à long terme.

Les versions de production actuelles sont :

FortiOS 7.4.x (version la plus récente)
- Dernière version stable : 7.4.7, publiée le 12 février 2025
- Date de sortie initiale : 11 mai 2023
- Fin du support d'ingénierie : prévue pour le 11 mai 2026
- Fin du support complet (EOS) : prévue pour le 11 novembre 2027

FortiOS 7.2.x (version LTS – Long Term Support)
- Dernière version stable : 7.2.7, publiée le 7 février 2024
- Fin du support d'ingénierie : prévue pour le 31 mars 2025
- Fin du support complet (EOS) : prévue pour le 30 septembre 2026

FortiOS 6.4.x (version stable précédente)
- Dernière version stable : 6.4.10, publiée le 31 mars 2024
- Fin du support d'ingénierie : 31 mars 2023
- Fin du support complet (EOS) : 30 septembre 2024



La version 7.6.3 a été publiée le 17 Avril 2025 et est donc en phase de stabilisation. Elle ne sera pas conseillée en production avant mi-2026.

Quelles sont vos alternatives à partir de mi-2026 ?
Vous devrez réaliser une migration vers une solution de tunneling supportée par le constructeur.
Pour cela, deux solutions :

- VPN IPSEC : Solution de VPN classique avec une accessibilité sans licence supplémentaire pour des interconnexions site à site ou site à client (nomade). Le VPN IPSEC est une fonctionnalité accessible gratuitement depuis le FortiClient (Gratuit)
- ZTNA : Solution de tunneling avancé avec une gestion centralisée des accès sécurisés.
  - Gestion centralisée des clients VPN via FortiClient EMS (licence payante).
  - Authentification avancée (ex. SAML, LDAP via FortiAuthenticator, MFA).
  - Fonctions de sécurité avancées : antivirus, filtrage web, sandboxing, etc.

Pour cela, nos équipes seront disponibles pour vous conseiller sur la meilleure solution pour votre besoin.