



## FAQ de l'outil de migration Secure Firewall

- [Foire aux questions sur l'outil de migration de pare-feu sécurisé, à la page 1](#)

### Foire aux questions sur l'outil de migration de pare-feu sécurisé

- Q.** Quelles sont les nouvelles fonctionnalités prises en charge sur l'outil de migration Secure Firewall pour la version 3.0.1?
- A.** Les caractéristiques suivantes sont prises en charge avec la version 3.0.1 :
- Migration du protocole EIGRP (Enhanced Interior Gateway Routing Protocol) de l'ASA avec FPS.
  - La gamme Secure Firewall 3100 est prise en charge uniquement en tant que périphérique de destination pour la migration.
- Q.** Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration de pare-feu sécurisé pour la version 3.0 ?
- A.** Les caractéristiques suivantes sont prises en charge avec la version 3.0 :
- VPN d'accès à distance
  - Automatisation de clé pré-partagée VPN de site à site
- Q.** Quelles sont les nouvelles fonctionnalités prises en charge sur l'outil de migration Secure Firewall pour la version 2.5.1?
- A.** Les caractéristiques suivantes sont prises en charge avec la version 2.5.1 :
- Objets de routage dynamique
  - Protocole de passerelle frontière
- Q.** Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration de pare-feu sécurisé pour la version 2.4 ?
- A.** Les fonctionnalités suivantes sont prises en charge avec la version 2.4 :
- Migration ASA avec FPS vers la protection contre les menaces.

- Migration du VPN basé sur les certificats dans le centre de gestion.

- Q.** Vous disposez d'un centre de gestion avec huit zones de sécurité FPS, FPS1 avec cinq zones et FPS2 avec trois zones. Les politiques d'ACL associées au FPS1 utilisent une combinaison des zones FPS1 et FPS2 dans les règles d'accès. Les zones FPS1 et FPS2 seront-elles migrées vers la défense contre les menaces?
- A.** L'outil de migration Secure Firewall fera migrer les zones FPS1 vers les zones de défense contre les menaces. Il ne migrera pas les zones FPS2. Cependant, les listes de contrôle d'accès sources utilisant FPS2 seront partiellement migrées.
- Q.** Comment les ACL basées sur les utilisateurs FPS seront-elles migrées?
- A.** L'outil de migration de pare-feu sécurisé ne prend pas en charge la migration des ACL basées sur les utilisateurs FPS vers le centre de gestion. Il supprime le champ Users (Utilisateurs) et fait migrer les listes de contrôle d'accès à l'état désactivé. Vous devez ajouter manuellement le champ Users (Utilisateurs) et activer l'ACL dans le cadre de l'activité de post-migration sur le centre de gestion.

## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.