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. L’outil de migration Cisco Secure Firewall 3.0.1 prend désormais en charge Cisco Secure Firewall 3100 uniquement en tant qu’appareil de destination pour les migrations à partir de Fortinet.

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 :

- Migration vers le Centre de gestion du pare-feu en nuage.

Q. Quelles sont les nouvelles fonctionnalités prises en charge par l’outil de migration Secure Firewall pour la version 2.5.2 ?

A. Optimisation des listes de contrôle d’accès pour Fortinet.

Q. Quelles sont les plateformes source et cible qu’utilise l’outil de migration Cisco Secure Firewall 2.3 pour la migration des politiques?

A. L’outil de migration Cisco Secure Firewall peut dorénavant migrer les politiques de la plateforme du pare-feu Fortinet prise en charge vers la plateforme de protection contre les menaces. Pour en savoir plus, consultez Supported Platforms for Migration [plateformes de migration prises en charge].

Q. Quelles sont les nouvelles fonctions prises en charge par l’outil de migration Cisco Secure Firewall 2.3?

A. L’outil de migration Cisco Secure Firewall 2.3 peut migrer les politiques de la plateforme Fortinet prise en charge vers la plateforme de protection contre les menaces.

Q. Quels sont les périphériques sources et la version du code pris en charge?

A. Vous pouvez utiliser l’outil de migration de Cisco Secure Firewall pour migrer la configuration du pare-feu Fortinet à VDOM unique ou multiple au moyen de FortiOS 5.0 ou d’une version ultérieure.

Pour en savoir plus sur la liste des appareils pris en charge, consultez Supported Source Fortinet Platforms [plateformes Fortinet sources prises en charge].

Q. Le pare-feu Fortinet prend-il en charge les groupes d'interfaces?

A. Non. Le pare-feu Fortinet ne prend pas en charge les groupes d'interfaces pour la conversion en protection contre les menaces.

Q. Quelles sont les fonctionnalités prises en charge par l'outil de migration Secure Firewall pour la migration?

A. L'outil de migration de Cisco Secure Firewall prend en charge la migration de la configuration Fortinet L3/L4 vers la protection contre les menaces et peut migrer les configurations Fortinet suivantes :

- Objets et groupes réseau (à l'exception de quelques types d'objets non pris en charge)
- Objets de service, à l'exception des objets de service configurés pour une source et une destination
- Groupes d'objets de service, à l'exception des groupes d'objets de service imbriqués

Remarque Puisque l'imbrication n'est pas prise en charge sur le centre de gestion, l'outil de migration Cisco Secure Firewall élargit le contenu des règles référencées. Les règles, toutefois, sont migrées avec toutes les fonctionnalités.

- Objets et groupes FQDN IPv4 et IPv6
- Prise en charge de la conversion IPv6 (interface, routes statiques, objets, ACL et NAT)
- Règles d'accès
- Règles NAT
- NAT utilisant l'adresse VIP et un bassin d'adresses IP (la NAT centrale n'est pas prise en charge)
- Routes statiques et routes ECMP non migrées
- Interfaces physiques
- Sous-interfaces
- canaux de port
- Zones
- Objets temporels

Q. La NAT utilise le nom de domaine complet, qui n'est pas pris en charge par le centre de gestion. Que dois-je faire?

A. La commande FQDN-address-Object dans les champs de la NAT n'est pas prise en charge sur l'outil de migration Cisco Secure Firewall et le centre de gestion. Pour reproduire la même configuration que la

source, vous devez configurer manuellement, après la migration, l'ensemble des adresses IP mappées avec le nom de domaine complet.

Q. Que devrais-je faire si le pare-feu source comporte plus d'interfaces que la cible?

A. Si le pare-feu source a plus d'interfaces que la cible, créez des sous-interfaces sur la protection contre les menaces avant de lancer la migration.

Q. L'outil de migration de Cisco Secure Firewall migrera-t-il les interfaces agrégées (canaux de port)?

A. L'outil de migration de Cisco Secure Firewall ne migrera pas les interfaces agrégées (canaux de port). Vous devez configurer l'interface du canal de port sur le centre de gestion avant de lancer la migration.

Q. Que devrais-je faire avec les fichiers de configuration ignorés?

A. Les fichiers de configuration ignorés contiennent des lignes propres à Fortinet, qui ne sont pas pertinentes pour le centre de gestion. Pour cette raison, ils sont ignorés. Vous devez examiner attentivement la configuration des éléments ignorés. Tout détail non pertinent qui se reflète dans la section des éléments ignorés devrait être configuré manuellement sur le centre de gestion.

Q. J'obtiens une erreur dans le rapport préalable à la migration. Puis-je ignorer les interfaces et poursuivre?

A. Si vous choisissez de poursuivre sans les interfaces, les routes ne seront pas migrées non plus.

Q. Quelles sont les causes courantes de l'échec de l'analyse?

A. L'échec de l'analyse survient si les interfaces possèdent plusieurs adresses IP ou si les adresses IP sont attribuées avec les sous-réseaux, par exemple /32 ou /128. Pour poursuivre, vous devez corriger l'adresse IP et relancer la migration.

Q. Comment exporter une configuration Fortinet?

A. Vous pouvez exporter la configuration Fortinet en l'extrayant de l'appareil FortiGate ou de FortiManager s'il est géré par FortiManager. Pour en savoir plus, consultez la section Export the Configuration from Fortinet Networks Firewall [exporter la configuration du pare-feu Fortinet Networks].

Q. Y a-t-il une dépendance au centre de gestion pour utiliser les nouvelles fonctions introduites dans l'outil de migration Cisco Secure Firewall?

A. Oui. La fonction Objets temporels est prise en charge par le centre de gestion cible 6.6 et les versions ultérieures :

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.