FAQ de l'outil de migration Secure Firewall

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 Palo Alto Networks.

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 plateformes source et cible qu'utilise l'outil de migration Cisco Secure Firewall pour la migration de la politique?

A. L'outil de migration Cisco Secure Firewall peut migrer les politiques de la plateforme du pare-feu PAN prise en charge vers la plateforme défense contre les menaces virtuelles. Pour en savoir plus, consultez Supported Source PAN Platforms [plateformes PAN sources prises en charge].

Q. Quelles sont les limites matérielles pour la conversion de PAN en Threat Defense Virtual?

A. L'outil de migration Cisco Secure Firewall migrera la configuration si la version du système d'exploitation PAN est 6.1.x ou ultérieure.

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

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

Q. La NAT utilise le FQDN qui n'est pas pris en charge par Centre de gestion. Que dois-je faire?

A. Tout comme le FQDN dans la NAT qui n'est pas pris en charge par centre de gestion, dans la ligne semblable, le FQDN n'est pas pris en charge par l'outil de migration Cisco Secure Firewall. Pour

reproduire la même configuration que la source, vous devez configurer l'ensemble complet des adresses IP qui sont mappées manuellement avec le FQDN après la migration.

Q. Que faire si le pare-feu source a un plus grand nombre d'interfaces que la cible?
A. Si le pare-feu source a plus d'interfaces que la cible, créez alors des sous-interfaces sur défense contre les menaces virtuelles 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 centre de gestion avant de lancer la migration.

Q. Le routage Inter VR est-il pris en charge par Centre de gestion?
A. Toute route qui a Next Hop [saut suivant] en tant que route Next VR [VR suivante] n'est pas prise en charge.
Q. Quelle est la commande pour extraire le tableau des routes du PAN?
A. Utilisez la commande **Show routing route** [afficher la route de routage]. Une fois que vous avez collé la route dans le fichier *.txt*, assurez-vous que la mise en forme est correcte. En cas de systèmes multi-vsys, collez uniquement la route pour le *vsys* pertinent. Nous vous recommandons de supprimer les routes de tunnel, de boucle avec retour et VLAN du tableau des routes, car ces interfaces ne sont pas prises en charge par centre de gestion.
Q. Que devrais-je faire des fichiers de la configuration ignorée?
A. La configuration ignorée contient des balises XML qui sont propres à PAN seulement et qui ne sont pas pertinentes pour centre de gestion. Par conséquent, elles sont ignorées. Vous devez examiner attentivement la configuration ignorée. Les éléments imprévus qui sont indiqués dans la section ignorée devraient être configurés manuellement sur centre de gestion.
Q. J'obtiens un message d'erreur dans le rapport prémigration. Puis-je ignorer les interfaces et continuer?
A. Si vous choisissez de continuer sans les interfaces, les routes ne seront pas non plus migrées.
Q. Quelle est la cause courante de l'échec de l'analyse?
A. L'échec de l'analyse se produit si les interfaces ont plusieurs adresses IP ou des adresses IP attribuées à des sous-réseaux, par exemple /32 ou /128. Pour continuer, vous devez corriger l'adresse IP et relancer la migration.
Q. Pourquoi la NAT dans le résumé de préanalyse correspond-elle à zéro?
A. Consultez la section Parse Summary [analyse du résumé] pour en savoir plus.

Q. Comment peut-on exporter la configuration PAN?
A. La configuration doit être extraite de la passerelle si votre appareil est géré par Panorama. Il suffit de fusionner la configuration de Panorama avec la passerelle et d'extraire la configuration.

Pour en savoir plus, consultez la section Export the Configuration from Palo Alto Networks Firewall [exporter la configuration du pare-feu de Palo Alto Networks].

Q. En quoi le mappage d'applications consiste-t-il?
A. Le mappage d'applications vous permet de mapper des applications aux applications cibles correspondantes, comme HTTP ou SSH. Vous pouvez également migrer les règles basées sur l'application.

Pour en savoir plus, consultez la section Map Configurations with Applications [mapper des configurations avec les applications].

Q. Qu'advient-il des politiques affichant « application-default »?
A. Procédez comme suit:

- Si l'application est sélectionnée comme « any » et que le port est réglé sur « application-default », la politique n'est pas prise en charge et est migrée comme désactivée.

- Si l'application est sélectionnée comme « xyz » et que le port est réglé sur « application-default », la politique est migrée avec l'application « xyz » et le service « any ».

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.