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 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. 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 ACL pour Check Point.

Q. Quelles sont les limites matérielles pour la conversion de Check Point en protection contre les menaces?

A. Si les fichiers de configuration sont compatibles avec l'outil de visualisation Web Check Point et l'outil FMT-CP-Config-Extractor_v4.0.1-8248, vous devriez pouvoir migrer la solution Check Point source.

Q. Puis-je utiliser la configuration exportée de Check Point r76SP et la migrer vers les plateformes Firepower 4100 et 6100?

A. Oui. Toutes les plateformes sont prises en charge pour r75 à r77.30.

La plateforme est prise en charge tant que l'outil de visualisation Web Check Point est disponible.

Q. Comment gérez-vous les objets rejetés dans les règles de Check Point?

A. S'il s'agit d'un objet ou d'un groupe de type exclusion, la conversion de l'ACL suit la combinaison **allow** [autoriser] et **block** [bloquer]. Cette conversion est prise en charge par l'ACL, même si un objet ou un groupe réseau de type exclusion n'est pas pris en charge. Par exemple, si une règle Check Point ACE possède un groupe d'objets de type exclusion référencé.

- Si l'action découlant de la règle Check Point est **allow** [autoriser] :
  - L'ACE doit disposer d'une action **Deny** [refuser] pour le groupe ou l'objet référencé sous la balise XML **<exception></exception>** et ajouter un commentaire *Rule for Exception Object-Group* [règle pour le groupe ou l'objet d'exception].

- L'ACE doit disposer d'une action **Allow** [autoriser] pour le groupe d'objets référencé sous la balise XML *<base></base>* et ajouter un commentaire *Rule for Exception Object-Group* [règle pour le groupe d'objets d'exception].

- Si l'action découlant de la règle Check Point est **Deny/Reset** [refuser/réinitialiser] :
  - L'ACE doit disposer d'une action **permit** [permettre] pour le groupe d'objets référencé sous la balise XML **<exception></exception>** et ajouter un commentaire Rule for Exception Object-Group [règle pour le groupe d'objets d'exception].
  - L'ACE doit disposer d'une action **Block(Deny)/Block** [bloquer(refuser)/bloquer] avec **Reset (Reject)** [réinitialiser(refuser)] pour le groupe d'objets référencé sous la balise XML **<base></base>** et ajouter un commentaire *Rule for Exception Object-Group* [règle pour le groupe d'objets d'exception].

Q. L'outil de migration Cisco Secure Firewall prend-il en charge ACE avec la fonction Negate Cell [annuler la cellule]? Sinon, comment l'outil de migration Cisco Secure Firewall gère-t-il ces règles?

A. Les ACE dont certaines cellules sont annulées ne sont pas prises en charge par l'outil de migration Cisco Secure Firewall; elles sont donc converties en considérant l'ACE comme un ACE normal. Ces problèmes seront résolus dans les prochaines versions.

Q. Vous verrez un message d'échec de la liaison à la base de données. Accès refusé. Que feriez-vous?

A. Procédez comme suit:

- Ouvrez la console Check Point Gaia pour le serveur de gestion.
- Accédez aux paramètres d'utilisateurs et de rôles sur la console Gaia.
- Créez un nouveau nom d'utilisateur sur la console Gaia du serveur de gestion Check Point qui a un rôle d'administrateur avec le répertoire interne `/home` et les paramètres Shell `/etc/cli.sh`.

Q. Le nombre d'analyses est égal à 0 lors de l'analyse de la configuration de Check Point à l'aide de l'outil de migration Cisco Secure Firewall. Que feriez-vous?

A. Effectuez une des étapes suivantes :

Extrayez le fichier *networking.txt* au moyen de l'outil FMT-CP-Config-Extractor_v4.0.1-8248 et évitez le fichier *networking.txt* codé à la main.

Ou

Il se peut que la journalisation soit activée pour une raison quelconque sur la passerelle de sécurité du point de contrôle à partir de laquelle les sorties du fichier *networking.txt* sont exportées. Les renseignements superflus ajoutés au fichier *networking.txt* provoquent ce type de problème, car la journalisation est activée. Dans ce cas :

- Vérifiez le fichier *networking.txt*.
- Corrigez le fichier en supprimant la ligne du journal qui a été ajoutée.
- Chargez le nouveau fichier compressé (.zip) dans l'outil de migration Cisco Secure Firewall.

Q. Est-il possible de migrer la configuration à partir d'un point de vérification au moyen de VSX?

A. Vous pouvez exporter un paquet de politiques donné relatif aux systèmes virtuels, un système virtuel à la fois. Par exemple, si vous exportez la configuration au moyen de l'outil de visualisation Web (r75 à r77.30), les éléments de politique pour l'ensemble du système virtuel sont exportés. Par conséquent, ne

conservez que les fichiers NAT et les fichiers de politique pour le système virtuel que vous souhaitez migrer avec les fichiers *index.xml*, *communities.xml*, *network_objects.xml* et *networking.txt* (à partir de la passerelle de sécurité pour la politique visée par la migration) pour que la configuration soit complète.

Pour r80, sélectionnez le paquet de politiques pour un système virtuel en particulier si vous vous connectez au gestionnaire de sécurité Check Point par Live Connect, que vous souhaitez migrer à l'étape 5 lorsque vous sélectionnez le paquet de politiques Check Point et que vous procéder à la configuration.

Lorsque vous vous connectez également à la passerelle de sécurité Check Point, donnez les détails exacts du paquet du pare-feu Check Point du système virtuel Check Point correspondant au paquet de politiques Check Point.

Si vous éprouvez toujours des problèmes, communiquez avec le centre d'assistance technique Cisco pour créer un dossier concernant ces échecs.

Q. Est-il possible d'extraire la configuration de Check Point (r80) manuellement?

A. Non. Il n'est pas possible d'extraire la configuration de Check Point (r80) manuellement. Utilisez Live Connect dans l'outil de migration Cisco Secure Firewall pour obtenir la configuration r80 complète. Lorsque vous extrayez la configuration à l'aide de solutions de contournement manuelles ou au moyen d'une configuration Check Point (r80) qui n'est pas configurée dans l'outil de migration Cisco Secure Firewall, la configuration est incomplète. Elle est alors migrée comme une configuration qui n'est pas prise en charge ou est migrée partiellement ou encore cette situation entraîne l'échec des migrations.

Pour en savoir plus, consultez Export the Check Point Configuration Files for r80 [exporter les fichiers de configuration Check Point pour r80].

Q. Quelles sont les façons de préparer les données d'identification pour les différents types de déploiement de Check Point (r80)?

A. Vous pouvez configurer les données d'identification sur les appareils Check Point (r80) avant la migration en suivant l'une ou l'autre des étapes suivantes :

- Exportation à partir d'un déploiement distribué de Check Point
- Exportation à partir d'un déploiement autonome de Check Point
- Exportation d'un déploiement multi-domaine Check Point (r80)

Q. J'utilise un port API personnalisé sur Check Point r80 pour le gestionnaire de sécurité Check Point. Que dois-je faire pour extraire complètement la configuration?

A. Si vous utilisez un port API personnalisé sur Check Point Smart Manager, procédez comme suit :

- Cochez la case **Déploiement multidomaine Check Point** sur la page **Check Point Security Manager** de Live Connect.
- Ajoutez l'adresse IP de Check Point CMA et les détails du port API si vous utilisez le déploiement multidomaine.
- Gardez l'adresse IP du Check Point Security Manager si c'est un déploiement général et saisissez les détails du port API personnalisé.

Q. J'ai une passerelle Check Point de version r80.40, et l'extraction par Live Connect se passe bien. Toutefois, lors de l'analyse, le message d'erreur suivant s'affiche : « Blocked VSX Feature is UNSUPPORTED in FTD » [FTD ne prend PAS en charge la fonction VSX bloquée]. Que dois-je faire?

A. Cette erreur se produit, car la commande **fw vsx stat** est obsolète à partir de la version r80.40 de Check Point. L'outil de migration de Cisco Secure Firewall ne peut pas analyser les valeurs après l'exécution de la commande **fw vsx stat** lors de l'analyse du fichier *networking.txt*.

Voici comment contourner le problème :

1. Décompressez le fichier zip *config.zip*.
2. Ouvrez le fichier *networking.txt*.

   Voici un exemple de l'exemple de sortie :

   ```
   firewall> fw vsx stat
   Deprecated command, Please see sk144112 for alternative
   Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
   ```

   Faites le remplacement manuellement, comme suit :

   ```
   firewall> fw vsx stat
   VSX is not supported on this platform
   ```

3. Sélectionnez tous les fichiers et compressez-les de sorte qu'ils aient l'extension .zip.

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.