



Migration du pare-feu Check Point vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration

Première publication : 2022-11-17

Dernière modification : 2024-04-25

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. Tous droits réservés.



TABLE DES MATIÈRES

CHAPITRE 1

Mise en route de l'outil de migration Secure Firewall	1
À propos de l'outil de migration Secure Firewall	1
Quoi de neuf dans l'outil de migration Secure Firewall	4
Licence pour l'outil de migration Secure Firewall	11
Configuration requise pour l'outil de migration Cisco Secure Firewall	11
Exigences et conditions préalables pour les appareils Threat Defense	12
Soutien pour la configuration de Check Point	13
Lignes directrices et limites relatives à la licence	16
Plateformes prises en charge pour la migration	19
Centre de gestion des cibles pour la migration pris en charge	20
Versions logicielles prises en charge pour la migration	22

CHAPITRE 2

Flux de travail de la migration de Check Point vers Threat Defense	23
Procédure de bout en bout	23
Préalables pour la migration	25
Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com	26
Exporter les fichiers de configuration de Check Point	26
Exporter les fichiers de configuration Check Point pour r77	26
Exécuter la migration	30
Lancer l'outil de migration Secure Firewall	30
Utilisation du mode de démonstration dans l'outil de migration Cisco Secure Firewall	32
Exporter les fichiers de configuration Check Point pour r80	33
Pré-établissez les dispositifs Check Point (r80) pour l'extraction de la configuration à l'aide de Live Connect	33
Procédure pour exporter les fichiers de configuration Check Point pour r80	41
Extraire un autre fichier de configuration	44

	Téléversez le fichier de configuration Check Point	45
	Préciser les paramètres de destination pour l'outil de migration Secure Firewall	45
	Examiner le rapport pré-migration	48
	Mappez les configurations de ,Check Point du pare-feu et de avec les Défense contre les menacesinterfaces.	49
	Associez les interfaces Check Point à des zones de sécurité à des groupes d'interfaces	51
	Optimiser, examiner et valider la configuration	52
	Transférer la configuration migrée vers Centre de gestion	56
	Examiner le rapport de post-migration pour Check Point et terminer la migration	57
	Désinstaller l'outil de migration Secure Firewall	58
	Exemple de migration : avec vers Threat Defense 2100	58
	Tâches de la fenêtre de pré-maintenance	58
	Tâches de la fenêtre de maintenance	60
<hr/>		
CHAPITRE 3	Cisco Success Network - Données de télémétrie	61
	Cisco Success Network – Données de télémétrie	61
<hr/>		
CHAPITRE 4	Dépannage des problèmes de migration	71
	Dépannage de l'outil de migration de pare-feu sécurisé	71
	Journaux et autres fichiers utilisés pour le dépannage	72
	Résolution de problèmes liée aux échecs de chargement des fichiers Check Point	72
	Exemple de résolution de problèmes pour Check Point : Impossible de trouver le membre du groupe d'objets (pour les versions r75 à r77.30 seulement)	73
	Exemple de résolution de problèmes pour Check Point (r80) concernant Live Connect	74
<hr/>		
CHAPITRE 5	FAQ de l'outil de migration Secure Firewall	77
	Foire aux questions sur l'outil de migration de pare-feu sécurisé	77



CHAPITRE 1

Mise en route de l'outil de migration Secure Firewall

- À propos de l'outil de migration Secure Firewall, à la page 1
- Quoi de neuf dans l'outil de migration Secure Firewall, à la page 4
- Licence pour l'outil de migration Secure Firewall, à la page 11
- Configuration requise pour l'outil de migration Cisco Secure Firewall, à la page 11
- Exigences et conditions préalables pour les appareils Threat Defense, à la page 12
- Soutien pour la configuration de Check Point, à la page 13
- Lignes directrices et limites relatives à la licence, à la page 16
- Plateformes prises en charge pour la migration, à la page 19
- Centre de gestion des cibles pour la migration pris en charge, à la page 20
- Versions logicielles prises en charge pour la migration, à la page 22

À propos de l'outil de migration Secure Firewall

Ce guide contient des informations sur comment télécharger l'outil de migration Secure Firewall et terminer la migration. De plus, il vous offre des astuces de résolution de problèmes pour vous aider à résoudre les problèmes de migration que vous pourriez rencontrer.

L'exemple de procédure de migration ([Exemple de migration : avec vers Threat Defense 2100](#)) inclus dans ce livre aide à faciliter la compréhension du processus de migration.

L'outil de migration Cisco Secure Firewall convertit les configurations prises en charge de laCheck Point de en une plateforme Cisco Secure Firewall Threat Defense prise en charge. L'outil de migration Cisco Secure Firewall vous permet de migrer automatiquement les fonctions et les politiques de Check Point vers défense contre les menaces. Vous devez migrer manuellement toutes les caractéristiques non prises en charge.

L'outil de migration Secure Firewall recueille les informations sur Check Point, les analyses et les transmet au Cisco Secure Firewall Management Center. Pendant la phase d'analyse, l'outil de migration Secure Firewall génère un **rapport de pré-migration** qui identifie les éléments suivants :

- Lignes XML ou JSON de la configuration de Check Point avec des erreurs
- Check Point dresse la liste des lignes Check Point XML ou JSON que l'outil de migration Secure Firewall ne peut pas reconnaître. Signalez les lignes de configuration XML ou JSON sous la rubrique « erreur » dans le **rapport de pré-migration** et dans les journaux de la console; cela bloque la migration.

S'il y a des erreurs d'analyse, vous pouvez y remédier, télécharger à nouveau une nouvelle configuration, vous connecter au dispositif de destination, mapper les interfaces du Check Point dispositif géré par aux interfaces défense contre les menaces, mapper les zones de sécurité et les groupes d'interfaces, et procéder à l'examen et à la validation de votre configuration. Vous pouvez ensuite faire migrer la configuration vers le périphérique de destination.

Console

La console s'ouvre lorsque vous lancez l'outil de migration Secure Firewall. La console fournit des informations détaillées sur la progression de chaque étape dans l'outil de migration Secure Firewall. Le contenu de la console est aussi écrit dans le fichier journal de l'outil de migration Secure Firewall.

La console peut rester ouverte pendant que l'outil de migration Secure Firewall est en marche.



Important Lorsque vous quittez l'outil de migration Secure Firewall en fermant le navigateur sur lequel l'interface web est en cours d'exécution, la console continue de fonctionner en arrière-plan. Pour sortir complètement de l'outil de migration Secure Firewall, quittez la console en appuyant sur la touche Commande + C sur le clavier.

Journaux

L'outil de migration Secure Firewall crée un journal de chaque migration. Les journaux incluent les détails de ce qui se produit à chaque étape de la migration et peuvent vous aider à déterminer la cause de l'échec d'une migration.

Vous pouvez trouver les fichiers journaux pour l'outil de migration Secure Firewall à l'endroit suivant :

```
<migration_tool_folder>\logs
```

Ressources

L'outil de migration Cisco Secure Firewall enregistre une copie des **rapports prémigration**, des **rapports postmigration** et des configurations Check Point et de l', et les consigne dans le dossier des **ressources**.

Vous pouvez trouver le dossier des **ressources** à l'emplacement suivant : `<migration_tool_folder>\resources`

Fichier non analysé

Vous pouvez trouver le fichier analysé à l'emplacement suivant :

```
<migration_tool_folder>\resources
```

Recherche dans l'outil de migration Secure Firewall

Vous pouvez rechercher des items dans les tableaux affichés dans l'outil de migration Secure Firewall, tels que ceux sur la page **Optimiser, examiner et valider**.

Pour rechercher un item dans toute colonne ou rangée, cliquez sur le **Search** (🔍) au-dessus du tableau et saisissez le terme recherché dans le champ. L'outil de migration Secure Firewall filtre les rangées de tableaux et affiche celles contenant le terme recherché.

Pour rechercher un item dans une seule colonne, saisissez le terme recherché dans le champ **Recherche** fourni dans l'en-tête de la colonne. L'outil de migration Secure Firewall filtre les rangées de tableaux et affiche celles correspondant au terme recherché.

Ports

L'outil de migration Secure Firewall prend en charge la télémétrie lorsqu'il est exécuté sur l'un de ces 12 ports : les ports 8321-8331 et le port 8888. Par défaut, l'outil de migration Secure Firewall utilise le port 8888. Pour changer le port, mettez à jour l'information dans le fichier *app_config*. Après la mise à jour, assurez-vous de relancer l'outil de migration Secure Firewall pour que le changement de port prenne effet. Vous trouverez le fichier *app_config* à l'emplacement suivant : `<migration_tool_folder>\app_config.txt`.



Remarque Nous vous recommandons d'utiliser les ports 8321-8331 et le port 8888, puisque la télémétrie n'est prise en charge que sur ces ports. Si vous activez le Cisco Success Network, vous ne pouvez pas utiliser un autre port pour l'outil de migration Secure Firewall.

Cisco Success Network (Réseau de succès Cisco)

Cisco Success Network est un service en nuage activé par l'utilisateur. Lorsque vous activez Cisco Success Network, une connexion sécurisée est établie entre l'outil de migration Secure Firewall et Cisco Cloud pour diffuser des informations et des statistiques d'utilisation. La télémétrie en continu fournit un mécanisme permettant de sélectionner des données intéressantes à partir de l'outil de migration Secure Firewall et de les transmettre dans un format structuré à des stations de gestion à distance, ce qui présente les avantages suivants :

- Pour vous informer des caractéristiques offertes non utilisées qui peuvent améliorer l'efficacité du produit dans votre réseau.
- Pour vous informer des services de soutien technique supplémentaires et la supervision offerte pour votre produit.
- Pour aider Cisco à améliorer nos produits.

L'outil de migration Secure Firewall établit et maintient la connexion sécurisée et vous permet de vous inscrire au Cisco Success Network. Vous pouvez éteindre la connexion en tout temps en désactivant le Cisco Success Network, ce qui déconnectera l'appareil du nuage de Cisco Success Network.

Quoi de neuf dans l'outil de migration Secure Firewall

Version	Fonctionnalités prises en charge
6.0	

Version	Fonctionnalités prises en charge
	<p>Cette version comprend les nouvelles caractéristiques et améliorations suivantes :</p> <p>Migration de Cisco Secure Firewall ASA vers Secure Firewall Threat Defense</p> <ul style="list-style-type: none"> • Vous pouvez maintenant faire la migration des configurations WebVPN de votre Cisco Secure Firewall ASA vers les configurations de Cisco Zero Trust Access Policy sur un appareil de protection contre les menaces. Cochez bien la case WebVPN à la page Select Features [sélectionner les fonctions] et jetez un œil au nouvel onglet WebVPN à la page Optimize, Review and Validate Configuration [optimiser, examiner et valider la configuration]. L'appareil de protection contre les menaces et le centre de gestion cible doit fonctionner sur la version 7.4 ou une version ultérieure et doit exécuter Snort3 comme moteur de détection. • Vous pouvez désormais procéder à la migration des configurations des protocoles SNMP (Simple Network Management Protocol) et DHCP (Dynamic Host Configuration Protocol) vers un appareil de protection contre les menaces. Cochez bien les cases SNMP et DHCP à la page Select Features [sélectionner les fonctions]. Si vous avez configuré le protocole DHCP sur Cisco Secure Firewall ASA, notez que le serveur DHCP, ou l'agent de relais et les configurations du système DDNS, peuvent également être sélectionnés pour la migration. • Vous pouvez désormais effectuer la migration des configurations du routage ECMP (Equal-Cost Multipath) lors de la migration d'un appareil ASA en mode multicontexte vers un contexte unique et fusionné de protection contre les menaces. L'encadré Routes [routage] dans le résumé décomposé comprend également des zones ECMP, que vous pouvez valider dans l'onglet Routes [routage] de la page Optimize, Review and Validate Configuration [optimiser, examiner et valider les configurations]. • Vous pouvez désormais effectuer la migration des tunnels dynamiques à partir de l'interface DVTI (Dynamic Virtual Tunnel Interface), de votre Cisco Secure Firewall ASA vers un appareil de protection contre les menaces. Vous pouvez les faire correspondre à la page Map ASA Interfaces to Security Zones, Interface Groups, and VRFs [mapper les interfaces ASA aux zones de sécurité, aux groupes d'interfaces et aux VRF]. Assurez-vous d'avoir un ASA de version 9.19 (x) ou ultérieure pour que s'applique cette fonctionnalité. <p>Migration d'un appareil géré par FDM vers Cisco Secure Firewall Threat Defense</p> <ul style="list-style-type: none"> • Vous pouvez désormais effectuer la migration des politiques de sécurité de couche 7, y compris les protocoles SNMP et HTTP, ainsi que les configurations des politiques sur les programmes malveillants et les fichiers de votre appareil géré par FDM vers un appareil de protection contre les menaces. Assurez-vous d'avoir un centre de gestion cible de version 7.4 ou ultérieure et vérifiez que les cases des paramètres de la plateforme et de la politique sur les programmes malveillants et les fichiers à la page Select Features [sélectionner les fonctions] sont bien cochées. <p>Migration du pare-feu Check Point vers Cisco Secure Firewall Threat Defense</p>

Version	Fonctionnalités prises en charge
	<ul style="list-style-type: none"> • Vous pouvez dorénavant effectuer la migration des configurations VPN de site à site (basées sur les politiques) de votre pare-feu Check Point vers un appareil de protection contre les menaces. Notez que cette fonction s'applique aux versions Check Point R80 ou ultérieures, et aux versions 6.7 ou ultérieures du centre de gestion et de Threat Defense. Assurez-vous que la case Site-to-Site VPN Tunnels [tunnels VPN de site à site] est bien cochée à la page Select Features [sélectionner les fonctions]. Notez qu'étant donné qu'il s'agit d'une configuration propre à l'appareil, l'outil de migration n'affiche pas ces configurations si vous décidez de poursuivre sans FTD. <p>Migration de Fortinet Firewall vers Cisco Secure Firewall Threat Defense</p> <ul style="list-style-type: none"> • Vous pouvez dorénavant optimiser vos listes de contrôle d'accès (ACL) lorsque vous procédez à la migration des configurations d'un pare-feu Fortinet à votre appareil de protection contre les menaces. Utilisez le bouton Optimize ACL [optimiser l'ACL] à la page Optimize, Review and Validate Configuration [optimiser, examiner et valider la configuration] pour consulter la liste des ACL redondantes et dupliquées et pour télécharger le rapport d'optimisation qui détaille l'ACL.

Version	Fonctionnalités prises en charge
5.0.1	<p>Cette version comprend les nouvelles caractéristiques et améliorations suivantes :</p> <ul style="list-style-type: none"> • L'outil de migration Cisco Secure Firewall prend maintenant en charge la migration de plusieurs contextes de sécurité transparents en mode pare-feu à partir des appareils Cisco Secure Firewall ASA vers les appareils de protection contre les menaces. Vous pouvez fusionner au moins deux contextes transparents en mode pare-feu qui se trouvent dans votre appareil Cisco Secure Firewall ASA à une instance en mode transparent, et procéder ensuite à leur migration. <p>Là où au moins un de vos contextes dispose d'une configuration VPN, lors d'un déploiement ASA avec VPN configuré, vous pouvez choisir un seul contexte pour lequel vous souhaitez réaliser la migration de la configuration VPN vers l'appareil cible de protection contre les menaces. À partir des contextes que vous n'avez pas sélectionnés, seule la configuration VPN est ignorée, tandis que toutes les autres configurations font l'objet d'une migration.</p> <p>Consultez la rubrique Select the ASA Security Context [sélectionner le contexte de sécurité ASA] pour en savoir plus.</p> <ul style="list-style-type: none"> • Vous pouvez désormais procéder à la migration des configurations VPN de site à site et distantes à partir de vos pare-feu Fortinet et Palo Alto Networks vers la protection contre les menaces au moyen de l'outil de migration Cisco Secure Firewall. Depuis le panneau Select Features [sélectionner les fonctions], choisissez les fonctions VPN à migrer. Consultez la rubrique Specify Destination Parameters for the Secure Firewall Migration Tool [indiquer les paramètres de destination pour l'outil de migration Cisco Secure Firewall] dans les guides Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool [migration du pare-feu Palo Alto Networks vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration] et Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool [migration du pare-feu Fortinet vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration]. • Vous pouvez désormais sélectionner au moins un contexte de sécurité routé ou transparent en mode pare-feu à partir de vos appareils Cisco Secure Firewall ASA et procéder à la migration à un ou plusieurs contextes au moyen de l'outil de migration Cisco Secure Firewall.

Version	Fonctionnalités prises en charge
5.0	<ul style="list-style-type: none"> • L'outil de migration Cisco Secure Firewall prend maintenant en charge la migration de plusieurs contextes de sécurité à partir des appareils Cisco Secure Firewall ASA vers les appareils de protection contre les menaces. Vous pouvez choisir d'effectuer la migration de configurations à partir d'un de vos contextes ou fusionner les configurations de tous vos contextes routés en mode pare-feu, et ensuite procéder à leur migration. Un soutien sera bientôt offert pour la fusion des configurations de plusieurs contextes transparents en mode pare-feu. Consultez la rubrique Select the ASA Primary Security Context [sélectionner le contexte de sécurité primaire ASA] pour en savoir plus. • L'outil de migration tire maintenant profit de la fonctionnalité virtuelle de routage et de transfert afin de reproduire le flux de trafic divisé, qui est observé dans un environnement ASA à plusieurs contextes, lequel fera partie de la nouvelle configuration fusionnée. Vous pouvez vérifier le nombre de contextes qu'a détecté l'outil de migration dans un nouvel encadré Contexts [contextes] et pareillement après l'analyse, dans un nouvel encadré VRF de la page Parsed Summary [résumé décomposé]. De plus, l'outil de migration affiche les interfaces auxquelles sont mappés ces VRF, à la page Map Interfaces to Security Zones and Interface Groups [mapper les interfaces aux zones de sécurité et aux groupes d'interfaces]. • Vous pouvez désormais essayer l'intégralité du flux de travail de la migration au moyen du nouveau mode de démonstration de l'outil Cisco Secure Firewall et visualiser à quoi ressemble réellement votre migration. Consultez la rubrique Using the Demo Mode in Firewall Migration Tool [utilisation du mode de démonstration de l'outil de migration du pare-feu] pour en savoir plus. • Grâce aux nouvelles améliorations et à la correction des problèmes, l'outil de migration Cisco Secure Firewall offre maintenant une expérience améliorée et plus rapide lors de la migration du pare-feu Palo Alto Networks vers Threat Defense.
4.0.3	<p>L'outil de migration Secure Firewall 4.0.3 comprend des corrections de bogues et les nouvelles améliorations suivantes :</p> <ul style="list-style-type: none"> • L'outil de migration offre désormais un écran de mappage d'application amélioré pour la migration des configurations de PAN vers la défense contre les menaces. Reportez-vous à la section Mappage des configurations avec les applications lors de la <i>migration du pare-feu de Palo Alto Networks vers Secure Firewall Threat Defense avec le guide de l'outil de migration</i> pour plus d'informations.

Version	Fonctionnalités prises en charge
4.0.2	<p>L'outil de migration Secure Firewall 4.0.2 inclut les nouvelles caractéristiques et améliorations suivantes :</p> <ul style="list-style-type: none"> • Outil de migration Cisco Secure Firewall La version 4.0.2 présente l'outil d'extraction de configuration intégré, qui s'affiche désormais sur la page Extract Config Information (Extraire les informations de configuration). Cela facilite l'extraction de la configuration et élimine la tâche de téléchargement de l'outil d'extraction. Notez que l'outil FMT-CP-Config-Extractor n'est plus disponible en tant qu'application autonome à télécharger. Consultez la section Exporter la configuration du périphérique à l'aide de l'extracteur de configuration pour plus de renseignements. • L'outil de migration dispose désormais d'une télémétrie permanente; cependant, vous pouvez désormais choisir d'envoyer des données de télémétrie limitées ou élargies. Les données de télémétrie limitées comprennent peu de points de données, tandis que les données de télémétrie élargies envoient une liste plus détaillée de données de télémétrie. Vous pouvez modifier ce paramètre dans Paramètres > Envoyer les données de télémétrie à Cisco? .
4.0.1 ou ultérieure	<p>L'outil de migration Secure Firewall 4.0.1 inclut les nouvelles caractéristiques et améliorations suivantes :</p> <ul style="list-style-type: none"> • Vous pouvez maintenant faire migrer la configuration de Check Point R81 vers Secure Firewall Threat Defense. • Vous pouvez désormais choisir d'ajouter un ID de système virtuel lors de la connexion à la passerelle Check Point Security Gateway, pour exporter la configuration d'un déploiement VSX (Virtual System Extension) multi-domaines. • Vous pouvez extraire la configuration d'un Check Point VSX version R77 en exécutant quelques commandes manuellement. Pour plus d'informations, reportez-vous à la section Exporter la configuration des dispositifs à l'aide de l'outil FMT-CP-Config-Extractor_v4.0-7965 du guide <i>Migration de Check Point Firewall vers Threat Defense à l'aide de l'outil de migration</i>.
3.0.1	<ul style="list-style-type: none"> • Pour ASA avec FirePOWER Services, Check Point, Palo Alto Networks et Fortinet, Secure Firewall Série 3100 n'est pris en charge qu'en tant que dispositif de destination.
3.0	<p>L'outil de migration Secure Firewall 3.0 permet de migrer vers le centre de gestion de pare-feu de Check Point fourni dans le nuage si le centre de gestion de destination est 7.2 ou plus récent.</p>

Version	Fonctionnalités prises en charge
2.5.2	<p>L'outil de migration Secure Firewall 2.5.2 permet d'identifier et de séparer les ACL qui peuvent être optimisées (désactivées ou supprimées) de la base de règles du pare-feu sans avoir d'impact sur la fonctionnalité réseau des pare-feu Check Point</p> <p>L'optimisation d'ACL supporte les types d'ACL suivants :</p> <ul style="list-style-type: none"> • ACL redondante: lorsque deux ACL ont le même ensemble de configurations et de règles, la suppression de l'ACL non de base n'aura pas d'incidence sur le réseau. • ACL dupliquée: la première ACL masque complètement les configurations de la deuxième ACL. <p>Remarque L'optimisation est disponible pour le Check Point uniquement pour une action découlant d'une règle ACP.</p> <p>L'outil de migration Secure Firewall 2.5.2 supporte le protocole de passerelle frontière (BGP) et les objets de routage dynamique si la destination centre de gestion est 7.1 ou ultérieure.</p>
2,2	<ul style="list-style-type: none"> • Offre le support pour les versions r80 Check Point OS • Offre le support pour Live Connect pour extraire les configurations des appareils Check Point (r80). • Vous pouvez migrer les éléments de configuration Check Point pris en charge suivants vers défense contre les menaces pour r80 : <ul style="list-style-type: none"> • Interfaces • Routes statiques • Objets • NAT (Network Address Translation; Translation d'adresses de réseau) • Stratégies de contrôle d'accès <ul style="list-style-type: none"> • Politique globale — lorsque vous sélectionnez cette option, les zones source et destination de la politique ACL sont migrées comme Any car il n'y a pas de recherche d'itinéraire. • Politique basée sur les zones : lorsque vous sélectionnez cette option, les zones de source et de destination sont dérivées sur la base de la recherche prédictive d'itinéraires par le biais du mécanisme de routage pour les objets ou groupes de réseaux de source et de destination. <p>Remarque La recherche d'itinéraires est limitée aux itinéraires statiques et aux itinéraires dynamiques (à l'exclusion de PBR et NAT) et, en fonction de la nature des groupes d'objets réseau source et destination, cette opération peut entraîner une explosion des règles.</p> <p>Remarque La recherche d'itinéraires IPv6 pour les règles basées sur les zones n'est pas prise en charge.</p>

Version	Fonctionnalités prises en charge
2.0	<ul style="list-style-type: none"> • La nouvelle fonctionnalité d'optimisation de l'outil de migration Secure Firewall vous permet d'obtenir rapidement les résultats de la migration à l'aide des filtres de recherche. • L'outil de migration Secure Firewall vous permet de migrer les éléments de configuration Check Point pris en charge suivants vers défense contre les menaces : <ul style="list-style-type: none"> • Interfaces • Routes statiques • Objets • Politique de contrôle d'accès <ul style="list-style-type: none"> • Politique globale : lorsque vous sélectionnez cette option, les zones source et destination de la politique ACL sont migrées comme Any. • Politique basée sur les zones : lorsque vous sélectionnez cette option, les zones de source et de destination sont dérivées sur la base de la recherche prédictive d'itinéraires par le biais du mécanisme de routage pour les objets ou groupes de réseaux de source et de destination. <p>Remarque La recherche d'itinéraires est limitée aux itinéraires statiques et aux itinéraires dynamiques (à l'exclusion de PBR et NAT) et, en fonction de la nature des groupes d'objets réseau source et destination, cette opération peut entraîner une explosion des règles.</p> <ul style="list-style-type: none"> • NAT (Network Address Translation; Translation d'adresses de réseau) <ul style="list-style-type: none"> • Prend en charge les versions R75, R76, R77, R77.10, R77.20 et R77.30 du système d'exploitation Check Point.

Licence pour l'outil de migration Secure Firewall

L'application outil de migration Secure Firewall est gratuite et ne requiert pas de licence. Cependant, le centre de gestion doit avoir les licences requises pour les caractéristiques défense contre les menaces correspondantes afin d'enregistrer les appareils défense contre les menaces et d'y déployer les politiques.

Configuration requise pour l'outil de migration Cisco Secure Firewall

L'outil de migration Cisco Secure Firewall a les exigences en matière d'infrastructure et de plateforme suivantes:

- Fonctionne sur un système d'exploitation Microsoft Windows 10 64-bit ou sur une version macOS 10.13 ou une version récente
- Google Chrome comme navigateur par défaut du système
- (Windows) Comporte des paramètres de veille configurés dans la consommation et la veille pour ne jamais mettre l'ordinateur en veille, de sorte que le système ne se met pas en veille lors d'une migration importante
- (macOS) Comporte des paramètres d'économie d'énergie configurés de sorte que l'ordinateur et le disque dur ne se mettent pas en veille lors d'une migration importante

Exigences et conditions préalables pour les appareils Threat Defense

Lorsque vous migrez vers le centre de gestion, il se peut qu'un dispositif de défense contre les menaces cibles soit ajouté ou non. Vous pouvez faire migrer des stratégies partagées vers un centre de gestion en vue d'un déploiement ultérieur vers un dispositif de défense contre les menaces. Pour faire migrer des stratégies spécifiques à un appareil vers une défense contre les menaces, vous devez l'ajouter au centre de gestion. Tandis que vous envisagez la migration de la configuration de votre Check Point vers la protection contre les menaces, prenez en compte les conditions préalables et les exigences qui suivent :

- Le dispositif de défense contre les menaces cible doit être enregistré auprès du centre de gestion.
- Le dispositif de défense contre les menaces peut être un dispositif autonome ou une instance de conteneur. Il ne doit **pas** faire partie d'un cluster ou d'une configuration de haute disponibilité.
 - Le dispositif natif cible défense contre les menaces doit avoir au moins un nombre égal d'interfaces ou de sous-interfaces de canaux de données ou de ports physiques utilisés (à l'exception des interfaces de gestion uniquement) à celui du dispositif cible Check Point; sinon, vous devez ajouter le type d'interface requis sur le dispositif cible défense contre les menaces. Les sous-interfaces sont créées par l'outil de migration Secure Firewall sur la base d'un mappage physique ou d'un mappage de canaux de ports.
 - Si l'appareil de protection contre les menaces cible est une instance de conteneur, il doit utiliser au minimum un nombre égal d'interfaces et de sous-interfaces physiques et d'interfaces et de sous-interfaces de canal de port (sauf pour la gestion seulement) que celui de l', de l'Check Point ou du , de ou de l'. Si vous devez ajouter le type nécessaire d'interface sur l'appareil cible de protection contre les menaces.



Remarque

- Les sous-interfaces ne sont pas créées par l'outil de migration Secure Firewall, seul le mappage des interfaces est autorisé.
- Le mappage entre différents types d'interface est autorisé, par exemple : une interface physique peut être mappée à une interface de canal de port.

Soutien pour la configuration de Check Point

Configurations de Check Point prises en charge

- Interfaces (interfaces physique, VLAN et de liaison)
- Objets et groupes réseau : L'outil de migration Cisco Secure Firewall prend en charge la migration de tous les objets réseau de Check Point vers la protection contre les menaces.
- Objets de service
- NAT (Network Address Translation; Translation d'adresses de réseau)
- Prise en charge de la conversion IPv6 (interface, routes statiques et objets), à l'exception des ACL avec IPv6 et basée sur la zone
- Règles d'accès qui s'appliquent en général et qui prennent en charge la conversion des ACL globales en ACL basée sur la zone
- Routes statiques, à l'exception des routes configurées avec une portée considérée comme locale et avec des interfaces logiques en tant qu'interface de sortie pour une route statique sans l'adresse IP du saut suivant
- ACL assortie d'un type de journalisation supplémentaire
- VPN de site à site basé sur des politiques pour Check Point R80 et les versions ultérieures : IPv4 et authentification basée sur une clé prépartagée (PSK). Nous vous recommandons d'utiliser l'option **Live Connect** pour migrer les configurations VPN.



Remarque

Pour les ACE configurés dans Check Point qui ont des règles NAT correspondantes dans Check Point, l'outil de migration Cisco Secure Firewall ne mappe pas les adresses IP réelles avec les adresses IP traduites dans les règles ACE migrées correspondantes. L'outil de migration Cisco Secure Firewall ne mappe pas les adresses IP en raison du manque d'informations de référence entre la règle ACE et la règle NAT. Ainsi, lors de la validation de la configuration ACE et NAT migrée sur centre de gestion, vous devez valider et modifier manuellement les règles ACE qui correspondent au flux des paquets de la protection contre les menaces.



Remarque

Bien que l'outil de migration Cisco Secure Firewall ne migre pas les objets de service (configurés pour une source et une destination, et une combinaison de ports ayant le même type d'objets appelés dans un groupe d'objets), les règles ACL et NAT référencées sont migrées avec toutes leurs fonctionnalités.

Pour en savoir plus sur la configuration de Check Point qui n'est pas prise en charge, consultez la section [Unsupported Check Point Configuration](#) [configuration Check Point non prise en charge].

Configurations de Check Point prises en charge partiellement

L'outil de migration Cisco Secure Firewall prend partiellement en charge les configurations suivantes de Check Point pour la migration. Certaines de ces configurations comprennent des règles ayant des options

avancées, qui sont migrées sans ces options. Si le centre de gestion prend en charge ces options avancées, vous pouvez les configurer manuellement lorsque la migration sera terminée.

- Les routes statiques assorties de paramètres pour l'envoi de message Ping sont partiellement migrées.
- Les interface de liaison avec mode, XOR, sauvegarde active et circuit cyclique sont partiellement migrés vers le type LACP dans centre de gestion par l'outil de migration Cisco Secure Firewall.
- Les configurations des interfaces d'alias faisant partie d'interfaces parentes, comme l'interface physique ou l'interface de liaison, ainsi que la configuration des interfaces d'alias pour les attributs des interfaces ignorées et parentes sont migrées telles quelles.
- Le groupe d'objets réseau de type exclusion est pris en charge par une ACL afin de maintenir intacte la signification.
- ACL avec l'ajout du type de journalisation et ACL avec plage de temps.

Configurations de Check Point non prises en charge

L'outil de migration Cisco Secure Firewall ne prend pas en charge les configurations Check Point suivantes. Si ces configurations sont prises en charge dans le centre de gestion, vous pouvez les configurer manuellement lorsque la migration sera complétée.

- Interfaces d'alias, de pont, de tunnel 6IN4, de boucle avec retour et de PPPoE
- Objets et groupes réseau :
 - Passerelle de périphérie UTM-1
 - Hôte Check Point
 - Grappe de passerelles
 - Passerelles ou hôtes gérés à l'externe
 - Appareil OSE (Open Security Extension)
 - Serveurs logiques
 - Objets dynamiques
 - Domaines VoIP
 - Zone
 - Passerelle de sécurité CP
 - Serveur de gestion CP
 - Groupe d'objets réseau de type exclusion
- Objets de service :
 - RPC
 - DCE-RPC
 - TCP composé
 - GTP

- Autres objets de service propres à Check Point
- Politiques d'ACL avec :
 - Les types d'actions ACE non pris en charge (authentification client, authentification de session, authentification d'utilisateur et autres types d'authentification personnalisées) sont migrés avec le type d'action « Allow » (autorisation), mais à l'état désactivé
 - Politiques ACL basées sur l'identité
 - Politiques en fonction de la zone avec recherche de route IPv6
 - Règles de politique de contrôle d'accès basées sur l'utilisateur
 - Les règles du système multidomaine global ne peuvent pas être migrées



Remarque

Les configurations du système multidomaine global dans le déploiement multidomaine de Check Point ne peuvent pas être exportées. Par conséquent, les configurations appartenant à des CMA en particulier peuvent seulement être exportées et migrées.

- Objets dont le type et le code ICMP ne sont pas pris en charge
- Règles de contrôle d'accès basées sur le protocole de tunnellation
- Règles ACL implicites
- ACE avec paramètres d'annulation
- Zones destinées à l'ACE lorsque l'ACE en fonction de la zone est sélectionnée et que l'objet de plage ayant une valeur supérieure à 100 est migré et qu'il est marqué comme **Any** sans recherche, et ajouté au nom de l'ACE et au commentaire approprié
- Zone destinée à l'ACE avec une adresse IPv6 lorsque l'ACE en fonction de la zone sélectionnée est marquée comme **Any** et que l'ACE n'est pas prise en charge avec un commentaire approprié.

Règles NAT non prises en charge

L'outil de migration Cisco Secure Firewall ne prend pas en charge les règles NAT suivantes :

- Règles NAT automatiques qui se cachent derrière la passerelle
- Règle NAT manuelle utilisant la passerelle de sécurité Check Point.
- Règle NAT manuelle contenant des objets réseau avec une adresse IP à deux types
- Règles NAT manuelles contenant un groupe d'objets dont l'objet hérité possède une configuration IPv6
- Règle NAT manuelle avec un groupe de services
- Règles NAT IPv6

Routes statiques non prises en charge

- Routes statiques quand aucune interface de sortie n'est trouvée dans **netstat-rnv**
- Routes statiques qui ont la passerelle logique comme interface de sortie
- Routes statiques des types ECMP
- Routes statiques qui ont la portée locale comme interface de sortie

Lignes directrices et limites relatives à la licence

Durant la conversion, l'outil de migration Secure Firewall crée un mappage un-à-un de tous les objets et règles supportés, qu'ils soient utilisés en tant que règle ou politique. Toutefois, l'outil de migration Cisco Secure Firewall offre une caractéristique d'optimisation qui vous permet d'exclure la migration d'objets inutilisés (des objets qui ne sont cités en référence dans aucune ACL).

Voici comment l'outil de migration Cisco Secure Firewall traite les objets et les règles qui ne sont pas pris en charge :

- Les objets et les routes qui ne sont pas pris en charge ne sont pas migrés.
- Les règles ACL qui ne sont pas prises en charge sont migrées dans le centre de gestion en tant que règles désactivées.

Limites pour les configurations de Check Point

Voici les limites imposées à la migration de la configuration source de Check Point :

- La configuration système n'est pas migrée.
- La solution Live Connect du pare-feu est prise en charge seulement pour Check Point (r80) et les versions ultérieures.
- Toutes les politiques de sécurité explicites (qui figurent dans `Security_Policy.xml` pour les versions 77.30 et antérieures et dans le fichier de la politique de sécurité pour les versions r80 et ultérieures) sont migrées vers l'ACP sur le centre de gestion. Les règles d'un tableau de bord Check Point Smart ne sont pas migrées, car les règles implicites ne font pas partie de la configuration exportée.



Remarque

- Pour Check Point (r80) et les versions ultérieures, si une politique de couche d'application distincte est associée à la version ultérieure de la politique de sécurité L4, l'outil de migration Cisco Secure Firewall effectue leur migration comme s'ils n'étaient **pas pris en charge**. De plus, dans un tel cas, les configurations ACE seront accompagnées de deux fichiers : un pour la couche de sécurité et l'autre pour la couche d'application. L'outil de migration Cisco Secure Firewall effectue la migration en fonction des renseignements de priorité qui sont disponibles dans la couche d'accès, dans le fichier de configuration *index.json* compressé.
- Pour les versions de Check Point r80 et ultérieures dont le déploiement multidomaine est configuré et qui ont une politique globale ainsi qu'une politique précise pour le module complémentaire géré par le client (CMA), l'ordre qu'utilise l'outil de migration Cisco Secure Firewall pour la migration des configurations de Check Point sera légèrement différent de celui utilisé pour la configuration source. De plus, dans un tel cas, les configurations ACE seront accompagnées de deux fichiers : un pour la politique globale et l'autre pour la politique CMA. Les ACE configurés sous la couche de domaine seront migrés comme des ACE **non pris en charge**.
- La définition de l'ordre des règles ACE, configurée pour un CMA qui a « Action » comme couche de domaine dans le système multidomaine, est incomplète dans la configuration extraite. Par conséquent, si une politique globale est associée à une politique CMA précise dans la configuration source, validez l'index de numéros de règle dans la configuration extraite pour vous assurer que le bon ordre est utilisé.

-
- Certaines configurations Check Point, comme le routage dynamique et le VPN pour la protection contre les menaces, ne peuvent pas être migrées au moyen de l'outil de migration de Cisco Secure Firewall. Migrez manuellement ces configurations.
 - Les interfaces du pont, du tunnel et de l'alias de Check Point vers le centre de gestion ne peuvent pas être migrées.
 - Les groupes d'objets de service imbriqués ou les groupes de ports ne sont pas pris en charge par le centre de gestion. Dans le cadre de la conversion, l'outil de migration Secure Firewall étend le contenu du groupe objet imbriqué ou du groupe de port.
 - L'outil de migration Cisco Secure Firewall divise les groupes ou les objets de service aux ports sources et de destination configurés dans le même objet. Les références à de telles règles de contrôle d'accès sont converties en règles de centre de gestion ayant exactement la même signification.

Lignes directrices de la migration de Check Point

La migration de l'option de journalisation de Check Point respecte les bonnes pratiques de la protection contre les menaces. L'option de journalisation pour une règle est activée ou désactivée selon la configuration Check Point source. Pour les règles dont l'action est le **drop** [refuser] ou **reject** [rejeter], l'outil de migration Cisco Secure Firewall configure la journalisation au début de la connexion. Si l'action est la **permission**, l'outil de migration Secure Firewall configure la journalisation à la fin de la connexion.

Lignes directrices pour la migration d'objets

Les objets de service, qui sont appelés « objets de port » dans la protection contre les menaces, ont des lignes directrices différentes pour la configuration des objets. Par exemple, un ou plusieurs objets de service peuvent avoir le même nom dans Check Point, soit un nom d'objet en minuscule et l'autre en majuscule. Or, chaque objet doit porter un nom unique, quelle que soit la casse, comme dans la protection contre les menaces. L'outil de migration Cisco Secure Firewall analyse tous les objets Check Point et s'occupe de leur migration vers la protection contre les menaces d'une des manières suivantes :

- Chaque objet Check Point possède un nom et une configuration uniques. L'outil de migration Cisco Secure Firewall migre les objets avec succès sans changements.
- Le nom d'un objet de service Check Point comprend un ou plusieurs caractères spéciaux qui ne sont pas pris en charge par le centre de gestion. L'outil de migration Cisco Secure Firewall renomme les caractères spéciaux dans le nom de l'objet avec le caractère « _ » pour remplir le critère de dénomination d'objets du centre de gestion.
- Un objet de service Check Point porte le même nom et a la même configuration qu'un objet existant dans le centre de gestion. L'outil de migration Cisco Secure Firewall réutilise l'objet du centre de gestion pour la configuration de la protection contre les menaces et ne migre pas l'objet Check Point.
- Un objet de service Check Point porte le même nom, mais a une configuration différente de celle d'un objet existant dans le centre de gestion. L'outil de migration Cisco Secure Firewall rapporte un conflit d'objets et vous permet de résoudre le conflit en ajoutant un suffixe unique au nom de l'objet à des fins de migration.
- Plusieurs objets de service Check Point portent le même nom, mais dans des casses différentes. L'outil de migration Cisco Secure Firewall renomme des objets de ce type afin de remplir le critère de dénomination des objets.

Lignes directrices et limites relatives aux appareils Défense contre les menaces

Lorsque vous prévoyez de migrer votre configuration Check Point vers défense contre les menaces, tenez compte des lignes directrices et des limites qui suivent :

- S'il existe des configurations propres à l'appareil sur défense contre les menaces, comme des routes et des interfaces, lors de la migration poussée, l'outil de migration Cisco Secure Firewall nettoie automatiquement l'appareil et remplace la configuration Check Point.



Remarque Afin de prévenir toute perte indésirable de données de l'appareil (cible défense contre les menaces), nous vous recommandons de nettoyer manuellement l'appareil avant la migration.

Durant la migration, l'outil de migration Secure Firewall réinitialise la configuration de l'interface. Si vous utilisez ces interfaces dans des politiques, l'outil de migration Secure Firewall ne peut pas les réinitialiser et ainsi donc, la migration échoue.

- L'outil de migration Cisco Secure Firewall peut créer des sous-interfaces sur l'instance native de l'appareil défense contre les menaces en fonction de la configuration Check Point. Créez manuellement des interfaces et de interfaces de canaux de port sur l'appareil défense contre les menaces cible avant de débiter la migration Par exemple, si votre configuration Check Point est affectée aux interfaces et aux canaux de port suivants, vous devez les créer sur l'appareil défense contre les menaces cible avant la migration :

- Cinq interfaces physiques
- Cinq canaux de port
- Deux interfaces de gestion uniquement



Remarque Pour les instances de conteneurs de dispositifs défense contre les menaces, les sous-interfaces ne sont pas créées par l'outil de migration Secure Firewall, seul le mappage d'interface est autorisé.

Plateformes prises en charge pour la migration

Le et les plateformes défense contre les menaces suivantes sont pris en charge pour la migration avec l'outil de migration Cisco Secure Firewall : Pour plus d'informations sur les plateformes défense contre les menaces prises en charge, consultez le [Guide de compatibilité de Cisco Secure Firewall](#).



Remarque L'outil de migration Secure Firewall prend en charge la migration de la configuration du mode autonome ou du point de contrôle distribué vers un périphérique défense contre les menaces autonome uniquement.

Plateformes Défense contre les menaces cibles prises en charge

Vous pouvez utiliser l'outil de migration Secure Firewall pour migrer une source Check Point vers l'instance autonome ou conteneur suivante des platesdefence contre les menaces-formes :

- Firepower de Série 1000
- Série Firepower 2100
- Secure Firewall de Série 3100
- Firepower de série 4100
- Secure Firewall de Série 4200
- Série Firepower 9300 qui comprend :
 - SM-24
 - SM-36
 - SM-40
 - SM-44
 - SM-48
 - SM-56

- Threat Defense sur VMware, déployé à l'aide de VMware ESXi, VMware vSphere Web Client ou le client autonome vSphere
- Threat Defense Virtual sur Microsoft Azure Cloud ou AWS Cloud



Remarque

- Pour les conditions préalables et la préparation de défense contre les menaces virtuelles l'installation dans Azure, voir la section [Prise en main de Secure Firewall Threat Defense Virtual](#) et Azure.
- Pour les prérequis et la mise en place préalable de défense contre les menaces virtuelles dans AWS Cloud, voir les [prérequis virtuels de Threat Defense](#).

Pour chacun de ces environnements, une fois préétabli selon les exigences, l'outil de migration Secure Firewall nécessite une connectivité réseau pour se connecter au nuage Microsoft Azure ou AWS, puis pour faire migrer la configuration vers le centre de gestion nuage.



Remarque

Pour que la migration soit réussie, il est nécessaire de procéder à une mise en scène préalable de centre de gestion ou de la défense virtuelle contre les menaces avant d'utiliser l'outil de migration Secure Firewall.



Remarque

L'outil de migration Secure Firewall nécessite une connectivité réseau à tout appareil hébergé dans le nuage pour extraire la configuration source (CP (r80) Live Connect) ou faire migrer la configuration téléchargée manuellement vers centre de gestion dans le nuage. Par conséquent, la connectivité du réseau IP doit être établie au préalable avant d'utiliser l'outil de migration Secure Firewall.

Centre de gestion des cibles pour la migration pris en charge

L'outil de migration Secure Firewall prend en charge la migration vers des dispositifs de défense contre les menaces gérés par le centre de gestion et le centre de gestion de pare-feu en nuage.

Centre de gestion

Le centre de gestion est un puissant gestionnaire multi-appareils basé sur le Web qui fonctionne sur son propre matériel de serveur, ou comme un appareil virtuel sur un hyperviseur. Vous pouvez utiliser le centre de gestion sur site et le centre de gestion virtuel comme centre de gestion cible pour la migration.

Le centre de gestion devrait rencontrer les critères suivants pour la migration :

- La version du logiciel du Centre de gestion qui est prise en charge pour la migration, comme décrit dans [Versions logicielles prises en charge pour la migration, à la page 22](#).
- La version du logiciel centre de gestion qui est prise en charge pour la migration pour Check Point est 6.2.3.3 et les versions ultérieures.

- Vous avez obtenu et installé des licences intelligentes défense contre les menaces qui incluent toutes les fonctionnalités que vous prévoyez de migrer depuis ASA Check Point, comme décrit ci-dessous :
 - La section Mise en route du [compte Smart de Cisco](#) sur Cisco.com
 - [Enregistrez le Centre de gestion du pare-feu avec le Cisco Smart Software Manager.](#)
 - [Octroi de licences pour le système de pare-feu](#)
 - Vous avez activé l'API REST.centre de gestion
- Sur l'interface Web centre de gestion, allez à **System > Configuration [configuration du système] > Rest API Preferences [préférences REST API] > Enable Rest API**[activer REST API], puis cochez la case **Enable Rest API [activer REST API]**.



Important Vous devez détenir un rôle d'utilisateur administrateur dans centre de gestion pour activer REST API. Pour en savoir plus sur les rôles utilisateur dans le centre de gestion, consultez [User Roles](#) [rôles utilisateur].

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Le centre de gestion de pare-feu, disponible dans le nuage, est une plateforme de gestion pour les dispositifs de défense contre les menaces et est fourni par Cisco Defense Orchestrator Le centre de gestion de pare-feu en nuage offre un grand nombre de fonctions identiques à celles d'un centre de gestion.

Vous pouvez accéder au centre de gestion des pare-feux dans le nuage à partir de CDO. Le CDO se connecte au centre de gestion des pare-feux en nuage par l'intermédiaire du Secure Device Connector (SDC). Pour plus d'informations sur le centre de gestion des pare-feux dans le nuage, voir [Gestion des périphériques Cisco Secure Firewall Threat Defense avec le centre de gestion des pare-feux dans le nuage](#).

L'outil de migration Secure Firewall prend en charge le centre de gestion de pare-feu fourni dans le nuage en tant que centre de gestion de destination pour la migration. Pour sélectionner le centre de gestion de pare-feu fourni par le cloud comme centre de gestion de destination pour la migration, vous devez ajouter la région CDO et générer le jeton API à partir du portail CDO.

Régions CDO

CDO est offert dans trois régions différentes et les régions peuvent être identifiés avec l'extension URL.

Tableau 1 : Régions CDO et URL

Région	URL CDO
Région de l'Europe	https://defenseorchestrator.eu/
Région des É-U	https://defenseorchestrator.com/
Région APJC	https://www.apj.cdo.cisco.com/

Versions logicielles prises en charge pour la migration

Les outils de migration Secure Firewall, et les versions défense contre les menaces pour la migration sont les suivants :

Versions prises en charge de l'outil de migration Secure Firewall

Les versions affichées sur software.cisco.com sont les versions officiellement supportées par nos organisations d'ingénierie et de support. Nous vous recommandons vivement de télécharger la dernière version de l'outil de migration Secure Firewall à partir de software.cisco.com.

Versions Check Point prises en charge

L'outil de migration Secure Firewall prend en charge la migration vers défense contre les menaces qui utilisent les systèmes d'exploitation Check Point version r75-r77.30 et r80-r80.40. Sélectionnez la version de Check Point appropriée dans la page **Select Source (Sélectionner la source)**.

L'outil de migration Secure Firewall prend en charge la migration à partir des déploiements de Check Point Platform Gaia et Virtual System Extension (VSX).

Versions Centre de gestion prises en charge pour la configuration source du pare-feu Check Point

Pour le pare-feu Check Point, l'outil de migration Cisco Secure Firewall prend en charge la migration vers un périphérique défense contre les menaces géré par un centre de gestion qui exécute la version 6.2.3.3 ou une version récente.



Remarque

La migration vers l'appareil défense contre les menaces 6.7 n'est pas actuellement prise en charge. Par conséquent, la migration peut échouer si le périphérique est configuré avec une interface de données pour l'accès centre de gestion.

Versions Défense contre les menaces prises en charge

L'outil de migration Secure Firewall recommande de migrer vers un appareil fonctionnant défense contre les menaces avec la version 6.5 ou une version ultérieure.

Pour des informations détaillées sur la compatibilité du logiciel et du matériel du pare-feu Cisco, y compris les exigences en matière de système d'exploitation et d'environnement d'hébergement, pour défense contre les menaces, voir le [Guide de compatibilité du pare-feu Cisco](#).



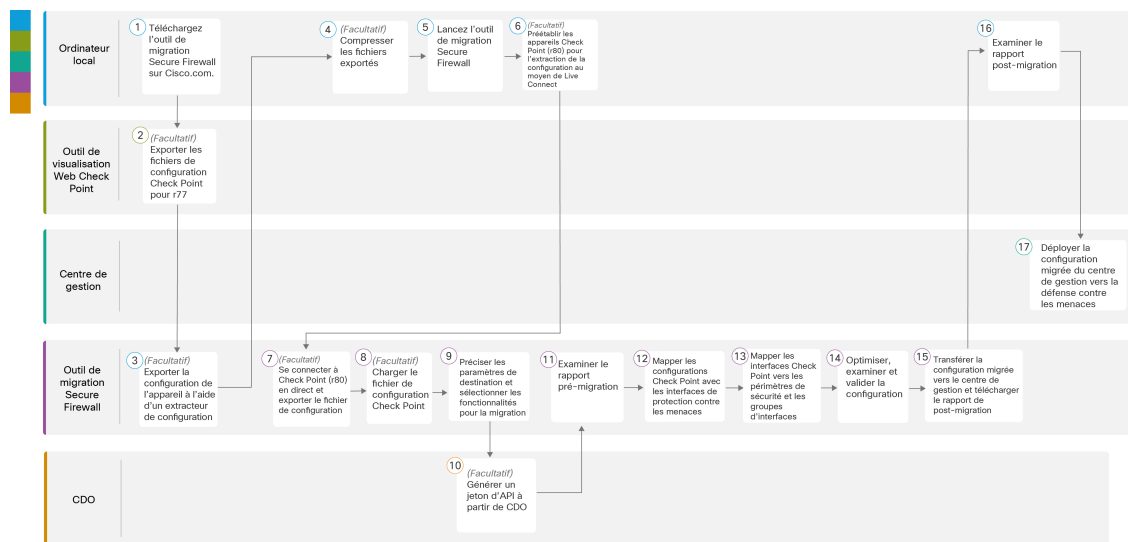
CHAPITRE 2

Flux de travail de la migration de Check Point vers Threat Defense

- Procédure de bout en bout, à la page 23
- Préalables pour la migration, à la page 25
- Exécuter la migration, à la page 30
- Désinstaller l'outil de migration Secure Firewall, à la page 58
- Exemple de migration : avec vers Threat Defense 2100 , à la page 58

Procédure de bout en bout

L'organigramme suivant illustre le flux de travail pour la migration d'un pare-feu Check Point vers la protection contre les menaces à l'aide de l'outil de migration Cisco Secure Firewall.



	Espace de travail	Étapes
1	Ordinateur local	Téléchargez l'outil de migration Secure Firewall sur Cisco.com. Pour les étapes détaillées, voir Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com

	Espace de travail	Étapes
2	Outil de visualisation Web Check Point	(Facultatif) Exportez le fichier de configuration Check Point pour la version r77 : Pour exporter les fichiers de configuration Check Point vers la version r77, consultez Exporter les fichiers de configuration Check Point pour r77, à la page 26 . Si vous avez l'intention d'exporter des fichiers de configuration pour la version 80 au moyen de la fonction Live Connect de l'outil de migration Cisco Secure Firewall, passez à l'étape 5.
3	Ordinateur local	Lancez l'outil de migration Cisco Secure Firewall sur votre ordinateur local et sélectionnez Check Point (r75–r77) ou Check Point (r80–r81) dans la liste déroulante Source Firewall Vendor [fournisseur du pare-feu source], selon vos besoins. Consultez la section Lancer l'outil de migration Secure Firewall [lancer l'outil de migration Cisco Secure Firewall] pour en savoir plus.
4	Outil de migration Secure Firewall	(Facultatif) Exporter la configuration de l'appareil à partir de Check Point (r75 à r77) : Pour exporter la configuration d'un appareil pour r77 au moyen de l' extracteur de configuration et d'une connexion à une passerelle sécurisée, consultez Exporter la configuration d'un appareil à l'aide d'un extracteur de configuration, à la page 27 .
5	Ordinateur local	(Facultatif) Compresser les fichiers exportés : Sélectionnez les fichiers de configuration exportés pour r77 et compressez-les dans un fichier ZIP. Pour la marche à suivre détaillée, consultez la section Compresser les fichiers exportés [compressez les fichiers exportés].
6	Ordinateur local	Préparez les appareils Check Point (r80) pour l'extraction de la configuration : Vous devez configurer les données d'identification sur les appareils Check Point (r80) avant d'utiliser Live Connect sur le pare-feu. Pour préparer les données d'identification sur un appareil Check Point (r80), consultez la section Pré-établissez les dispositifs Check Point (r80) pour l'extraction de la configuration à l'aide de Live Connect [préparer les appareil Check Point (r80) pour l'extraction de la configuration]. Cette étape n'est requise que si vous prévoyez de migrer les fichiers de configuration des appareils r80. Si vous prévoyez de migrer la configuration des périphériques r77, passez à l'étape 8.
7	Outil de migration Secure Firewall	(Facultatif) Connectez-vous à Check Point en direct (r80) et exportez le fichier de configuration : Pour exporter les fichiers de configuration de Check Point pour r80 en utilisant la fonction Live Connect, consultez la Procédure pour exporter les fichiers de configuration Check Point pour r80 .
8	Outil de migration Secure Firewall	(Facultatif) Chargez le fichier de configuration Check Point : Pour voir la marche à suivre détaillée du chargement d'un fichier de configuration Check Point, consultez la section Téléversez le fichier de configuration Check Point [charger le fichier de configuration Check Point].
9	Outil de migration Secure Firewall	Durant cette étape, vous pouvez spécifier les paramètres de destination pour la migration. Pour les étapes détaillées, référez-vous à Préciser les paramètres de destination pour l'outil de migration Secure Firewall .

	Espace de travail	Étapes
10	CDO	(Facultatif) Cette étape est facultative et obligatoire uniquement si vous avez sélectionné le centre de gestion de pare-feu fourni dans le nuage comme centre de gestion de destination. Pour connaître les étapes détaillées, consultez la section Préciser les paramètres de destination pour l'outil de migration Secure Firewall [indiquer les paramètres de destination de l'outil de migration Cisco Secure Firewall, étape 1].
11	Outil de migration Secure Firewall	Accédez à l'emplacement d'où vous avez téléchargé le rapport préalable à la migration, puis examinez le rapport. Pour les étapes détaillées, référez-vous à Examiner le rapport pré-migration
12	Outil de migration Secure Firewall	L'outil de migration Cisco Secure Firewall vous permet de mapper la configuration de Check Point avec les interfaces de la protection contre les menaces. Pour connaître la marche à suivre détaillée, consultez la section Mappez les configurations de ,Check Point du pare-feu et de avec les Défense contre les menaces interfaces . [mapper des configurations Check Point avec les interfaces Threat Defense du gestionnaire de l'appareil Cisco Secure Firewall].
13	Outil de migration Secure Firewall	Pour vous assurer que la configuration Check Point est correctement migrée, mappez les interfaces Check Point avec les objets d'interface de la protection contre les menaces, les périmètres de sécurité et les groupes d'interfaces appropriés. Pour connaître les étapes détaillées, consultez Associez les interfaces Check Point à des zones de sécurité à des groupes d'interfaces [mapper les interfaces Check Point avec les périmètres de sécurité et les groupes d'interfaces].
14	Outil de migration Secure Firewall	Optimisez et examinez soigneusement la configuration et vérifiez qu'elle est correcte et qu'elle correspond à la façon dont vous souhaitez configurer le dispositif de défense contre les menaces. Pour les étapes détaillées, référez-vous à Optimiser, examiner et valider la configuration .
15	Outil de migration Secure Firewall	Cette étape dans le processus de migration envoie la configuration migrée au centre de gestion et vous permet de télécharger le rapport de post-migration. Pour les étapes détaillées, référez-vous à Transférer la configuration migrée vers Centre de gestion .
16	Ordinateur local	Accédez à l'endroit où vous avez téléchargé le rapport de post-migration et examinez le rapport. Pour les étapes détaillées, référez-vous à Examiner le rapport de post-migration pour Check Point et terminer la migration .
17	Centre de gestion	Déployer la configuration migrée du centre de gestion vers la défense contre les menaces. Pour les étapes détaillées, référez-vous à Examiner le rapport de post-migration pour Check Point et terminer la migration .

Préalables pour la migration

Avant de faire faire migrer la configuration de votre dispositif Check Point géré par , exécutez les activités suivantes :

Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com

Avant de commencer

Vous devez disposer d'une machine Windows 10 64-bit ou macOS version 10.13 ou supérieure avec une connectivité internet à Cisco.com.

-
- Étape 1** Sur votre ordinateur, créez un dossier pour l'outil de migration Secure Firewall
- Nous vous recommandons de ne pas stocker d'autres fichiers dans ce dossier. Lorsque vous lancez l'outil de migration Secure Firewall, il place les journaux, ressources et tous les autres fichiers dans ce dossier.
- Remarque** Peu importe quand vous téléchargez la plus récente version de l'outil de migration Secure Firewall, assurez-vous de créer un nouveau fichier et de ne pas utiliser le dossier actuel.
- Étape 2** Naviguez vers <https://software.cisco.com/download/home/286306503/type> et cliquez sur **Outil de migration Firewall**
- Le lien ci-dessus vous amène à l'outil de migration Secure Firewall sous Firewall NGFW Virtual. Vous pouvez également télécharger l'outil de migration Secure Firewall à partir des zones de téléchargement des appareils défense contre les menaces.
- Étape 3** Téléchargez la version la plus récente de l'outil de migration Secure Firewall dans le dossier que vous avez créé.
- Téléchargez l'exécutable approprié de l'outil de migration Secure Firewall pour les machines Windows ou macOS.
-

Prochaine étape

[Exporter les fichiers de configuration de Check Point](#)

Exporter les fichiers de configuration de Check Point

Vous pouvez exporter la configuration Check Point pour ce qui suit :

- [Exporter les fichiers de configuration Check Point pour r77](#)
- [Exporter les fichiers de configuration Check Point pour r80](#)

Exporter les fichiers de configuration Check Point pour r77

Pour exporter les fichiers de configuration Check Point pour r77, procédez comme suit :

- [Exportez la configuration à l'aide de l'outil de visualisation Web de Check Point \(WVT\)](#)
- [Exporter la configuration d'un appareil à l'aide d'un extracteur de configuration, à la page 27](#)
- [Compresser les fichiers exportés](#)

Exportez la configuration à l'aide de l'outil de visualisation Web de Check Point (WVT)

- Étape 1** Ouvrez l'invite de commande sur le poste de travail qui a accès au server de gestion Check Point.

Étape 2 Téléchargez WVT à partir du [portail Check Point](#) correspondant à la version du pare-feu Check Point.

Étape 3 Décompressez le fichier zip WVT.

Étape 4 Créez un nouveau sous-dossier dans le même dossier racine où l'outil Check Point WVT est extrait.

Étape 5 Dans l'invite de commande, remplacez le répertoire par le répertoire où WVT est stocké et exécutez les commandes suivantes :

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name | -a certificate_file]
[-p password] [-o output_file_path] [-t table_names] [-c | -m gateway | -l package_names] [-gr]
[-go] [-w Web_Visualization_Tool_installation_directory]
```

Par exemple :

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 172.16.0.1 -u admin -p admin123 -o Outputs
```

Un total de sept fichiers sont créés dans le répertoire *Sorties* quand ces commandes sont exécutées, où :

Commande	Description
C:\Web_Visualisation_Tool	Le répertoire racine de l'outil WVT.
172.16.0.1	L'adresse IP du serveur de gestion Check Point.
admin	Le nom d'utilisateur du serveur de gestion Check Point.
Admin123	Le mot de passe du serveur de gestion Check Point.
Sorties	Le chemin relatif pour stocker les fichiers de sortie.

Remarque Les noms des fichiers Security Policy et NAT Policy doivent être respectivement `Security_Policy.xml` et `NAT_Policy.xml`. Si les noms de fichiers sont différents, renommez-les manuellement.

S'il existe plusieurs fichiers de politique de sécurité et de NAT, assurez-vous de sélectionner et de conserver uniquement les fichiers `Security_Policy.xml` et `NAT_Policy.xml` de l'appareil Check Point que vous souhaitez migrer.

Prochaine étape

[Exporter la configuration d'un appareil à l'aide d'un extracteur de configuration](#)

Exporter la configuration d'un appareil à l'aide d'un extracteur de configuration

Étape 1 Dans la page **Choisir la configuration de la source**, choisissez **Check Point (r75-r77)** et cliquez sur **Débuter la migration**.

Étape 2 Dans le volet **Extracteur de configuration**, cliquez sur **Connexion** à la passerelle de sécurité de Check Point pour laquelle les politiques doivent être migrées à l'aide de l'outil de migration Secure Firewall.

Pour vous connecter, vous avez besoin des informations suivantes :

- Adresse IP
- Port
- Nom d'utilisateur administrateur

- d) Mot de passe de l'administrateur
- e) Mot de passe expert
- f) (Facultatif) Numéro d'identification virtuel

Étape 3

Attendez jusqu'à ce que vous voyez un fichier `networking.txt` téléchargé sur votre machine locale.

Les commandes suivantes sont exécutées en arrière-plan par l'extracteur de configuration et sont téléchargées comme fichier `networking.txt` :

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

Par exemple, 172.16.0.1 est l'adresse IP de la passerelle du pare-feu Check Point pour laquelle les politiques doivent être migrées.

Étape 4

Si vous essayez d'exporter la configuration d'un Check Point VSX (Virtual System eXtension) version R77 ayant un ID virtuel, les commandes suivantes sont exécutées en arrière-plan :

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **fw vsx stat <vsid>**
- **set virtual system <vsid>**

Astuces **vsid** indique l'identifiant du système virtuel.

- **fw getifs**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**

- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

Étape 5 Déplacez le fichier .txt vers le dossier `Sorties`.

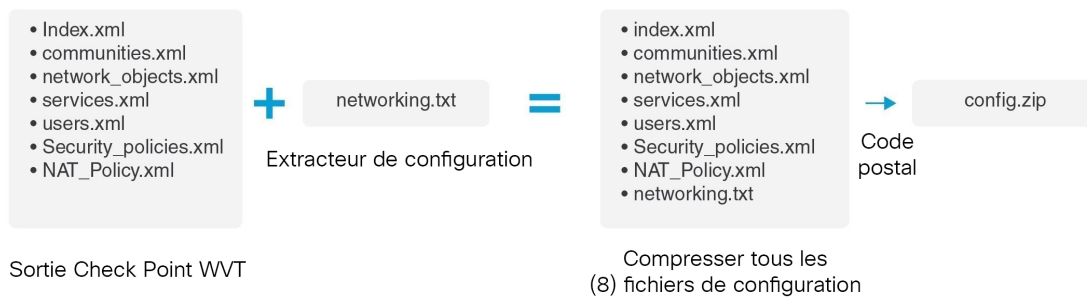
Prochaine étape

[Compresser les fichiers exportés](#)

Compresser les fichiers exportés

Choisissez les huit fichiers (sept de l'outil de visualisation web (WVT) et un fichier .txt de l'extracteur de configuration) et compressez-les dans un fichier zip.

Remarque Avant de compresser les fichiers pour la migration, assurez-vous que les fichiers `Security_Policy.xml` et `NAT_Policy.xml` sont pour le périphérique Check Point que vous souhaitez migrer vers la protection contre les menaces.



Remarque .tar ou les autres types de fichiers compressés ne sont pas pris en charge.

Prochaine étape

[Téléversez le fichier de configuration Check Point](#)

Exécuter la migration

Lancer l'outil de migration Secure Firewall

Cette tâche s'applique uniquement si vous utilisez la version de bureau de l'outil de migration de pare-feu sécurisé. Si vous utilisez la version en nuage de l'outil de migration hébergé sur CDO, passez à [Téléverser le fichier de configuration Check Point](#).



Remarque

Lorsque vous lancez l'outil de migration Secure Firewall, une console apparaît dans une fenêtre séparée. Au fur et à mesure de la migration, la console affiche la progression de l'étape en cours dans l'outil de migration Secure Firewall. Si vous ne voyez pas la console sur votre écran, il est fort probable qu'elle soit derrière l'outil de migration Secure Firewall.

Avant de commencer

- [Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com](#)
- Examiner et vérifier les exigences de la section [Centre de gestion des cibles pour la migration pris en charge, à la page 20](#).
- Assurez-vous que votre ordinateur dispose d'une version récente du navigateur Google Chrome pour exécuter l'outil de migration Secure Firewall. Pour plus d'informations sur la manière de définir Google Chrome comme navigateur par défaut, voir [Définir Chrome comme navigateur web par défaut](#).
- Si vous prévoyez de migrer un fichier de configuration volumineux, configurez les paramètres de mise en veille afin que le système ne se mette pas en veille pendant la poussée de migration.

Étape 1

Sur votre ordinateur, naviguez jusqu'au dossier où vous avez téléchargé l'outil de migration Secure Firewall.

Étape 2

Effectuez l'une des opérations suivantes :

- Sur votre machine Windows, double-cliquez sur l'exécutable de l'outil de migration Secure Firewall pour le lancer dans un navigateur Google Chrome.

Si vous y êtes invité, cliquez sur **Oui** pour autoriser l'outil de migration Secure Firewall à apporter des modifications à votre système.

L'outil de migration Secure Firewall crée et stocke tous les fichiers connexes dans le dossier où il réside, y compris les dossiers de journaux et de ressources.

- Sur votre Mac, déplacez le fichier *.command de l'outil de migration Secure Firewall dans le dossier souhaité, lancez l'application Terminal, naviguez jusqu'au dossier où l'outil de migration Secure Firewall est installé et exécutez les commandes suivantes :

```
# chmod 750 Firewall_Migration_Tool-version_number.command
# ./Firewall_Migration_Tool-version_number.command
```

L'outil de migration Secure Firewall crée et stocke tous les fichiers connexes dans le dossier où il réside, y compris les dossiers de journaux et de ressources.

Astuces Lorsque vous essayez d'ouvrir l'outil de migration Secure Firewall, vous obtenez une boîte de dialogue d'avertissement car l'outil de migration Secure Firewall n'est pas enregistré auprès d'Apple par un développeur identifié. Pour plus d'informations sur l'ouverture d'une application provenant d'un développeur non identifié, voir [Ouvrir une application provenant d'un développeur non identifié](#).

Remarque Utilisez la méthode zip du terminal MAC.

Étape 3 Sur la page **Contrat de licence de l'utilisateur final**, cliquez sur **J'accepte de partager des données avec Cisco Success Network** si vous souhaitez partager des informations de télémétrie avec Cisco, sinon cliquez sur **Je le ferai plus tard**.

Lorsque vous acceptez d'envoyer des statistiques au Cisco Success Network, vous êtes invité à vous connecter à l'aide de votre compte Cisco.com. Les informations d'identification locales sont utilisées pour se connecter à l'outil de migration Secure Firewall si vous choisissez de ne pas envoyer de statistiques à Cisco Success Network.

Étape 4 Sur la page de connexion de l'outil de migration Secure Firewall, effectuez l'une des opérations suivantes :

- Pour partager des statistiques avec le Cisco Success Network, cliquez sur le lien **Se connecter avec CCO** pour vous connecter à votre compte Cisco.com à l'aide de vos identifiants de connexion unique. Si vous n'avez pas de compte Cisco.com, créez-le sur la page de connexion de Cisco.com.

Passez à [l'étape 8](#) si vous avez utilisé votre compte Cisco.com pour vous connecter.

- Si vous avez déployé votre pare-feu dans un réseau isolé qui n'a pas d'accès à Internet, communiquez avec le centre d'assistance technique Cisco pour recevoir une version qui fonctionne avec les identifiants de l'administrateur. Prenez note que cette version n'enverra pas de statistiques d'utilisation à Cisco, et le centre d'assistance technique Cisco peut vous fournir les identifiants.

Étape 5 Sur la page **Réinitialiser le mot de passe**, entrez l'ancien mot de passe, votre nouveau mot de passe et confirmez le nouveau mot de passe.

Le nouveau mot de passe doit avoir 8 caractères ou plus et doit inclure des lettres en majuscule et en minuscule, des numéros et des caractères spéciaux.

Étape 6 Cliquez sur **Réinitialiser**.

Étape 7 Connectez-vous avec le nouveau mot de passe.

Remarque Si vous avez oublié le mot de passe, supprimez toutes les données existantes du dossier `<migration_tool_folder>` et réinstallez l'outil de migration Secure Firewall.

Étape 8 Passez en revue la liste de contrôle de pré-migration et assurez-vous que vous avez rempli tous les points énumérés. Si vous n'avez pas rempli un ou plusieurs points de la liste de contrôle, ne continuez pas tant que vous ne l'avez pas fait.

Étape 9 Cliquez sur **Nouvelle migration**.

Étape 10 Sur l'écran de **vérification de la mise à jour du logiciel**, si vous n'êtes pas sûr d'utiliser la version la plus récente de l'outil de migration Secure Firewall, cliquez sur le lien pour vérifier la version sur Cisco.com.

Étape 11 Cliquez sur **Procéder**.

Prochaine étape

Vous pouvez procéder à l'étape suivante :

- Si vous avez exporté la configuration de Check Point sur votre ordinateur, passez au [Téléversez le fichier de configuration Check Point](#).
- Si vous devez extraire des informations d'un Check Point (r77) à l'aide de l'outil de migration Secure Firewall, passez à la section [Exporter les fichiers de configuration Check Point pour r77](#).
- Si vous devez extraire des informations d'un Check Point (r80) à l'aide de l'outil de migration Secure Firewall, passez à la section [Exporter les fichiers de configuration Check Point pour r80](#).

Utilisation du mode de démonstration dans l'outil de migration Cisco Secure Firewall

Lorsque vous lancez l'outil de migration Cisco Secure Firewall et si vous vous trouvez à la page **Select Source Configuration** [sélectionner la configuration source], vous pouvez choisir d'amorcer une migration au moyen de **Start Migration** [commencer la migration] ou de saisir **Demo Mode** [mode de démonstration].

Le mode de démonstration donne l'occasion d'exécuter une migration en démonstration en utilisant des appareils fictifs et de visualiser le processus réel de migration. L'outil de migration déclenche le mode de démonstration en se basant sur votre sélection dans le menu **Source Firewall Vendor** [fournisseur du pare-feu source]. Vous pouvez également charger un fichier de configuration ou vous connecter à un appareil en direct pour poursuivre la migration. Vous pouvez procéder à la migration en démonstration en choisissant les appareils source et cible utilisés, comme les appareils FMC et FTD.



Mise en garde

Si vous choisissez le **mode de démonstration**, les processus de migration existants s'effacent, le cas échéant. Si vous utilisez le mode de démonstration pendant qu'une migration est active dans **Resume Migration** [reprendre la migration], votre migration active est abandonnée et devra être relancée du début lorsque vous en aurez fini avec le mode de démonstration.

Vous pouvez également télécharger et vérifier le rapport prémigration, mapper les interfaces, les périmètres de sécurité et les groupes d'interfaces, et réaliser toutes les autres actions que vous entreprendriez dans un processus de migration réel. Cependant, vous pouvez seulement exécuter une migration en démonstration jusqu'à la validation des configurations. Vous ne pouvez pas pousser les configurations vers les appareils cibles utilisés lors de la démonstration, car il s'agit seulement d'un mode de démonstration. Vous pouvez vérifier l'état de la validation et le résumé, puis cliquez sur **Exit Demo Mode** [quitter le mode de démonstration] pour retourner à la page **Select Source Configuration** [sélectionner la configuration source] afin de lancer la véritable migration.



Remarque

Le mode de démonstration vous permet de tirer profit de la totalité de l'ensemble de fonctions de l'outil de migration Cisco Secure Firewall, mais vous ne pouvez pas pousser les configurations, et faire un essai de la procédure de migration de bout en bout avant d'exécuter votre migration réelle.

Exporter les fichiers de configuration Check Point pour r80



Remarque L'exportation de la configuration Check Point r80 n'est prise en charge uniquement qu'avec la caractéristique Live Connect sur l'outil de migration Secure Firewall.

Pour configurer les identifiants requis pour la migration sur l'appareil Check Point et pour exporter les fichiers de configuration Check Point, effectuez ce qui suit :

- [Pré-établisiez les dispositifs Check Point \(r80\) pour l'extraction de la configuration à l'aide de Live Connect](#)
- [Procédure pour exporter les fichiers de configuration Check Point pour r80](#)

Pré-établisiez les dispositifs Check Point (r80) pour l'extraction de la configuration à l'aide de Live Connect

Vous pouvez configurer les informations d'identification sur les dispositifs Check Point (r80) avant la migration en suivant l'une des étapes suivantes :

- [Exportation à partir d'un déploiement distribué de Check Point](#) - Lorsque vous disposez d'une passerelle de sécurité Check Point indépendante et d'un gestionnaire de sécurité Check Point.
- [Exportation à partir d'un déploiement autonome de Check Point](#) - Lorsque vous disposez d'une passerelle de sécurité Check Point et d'un gestionnaire de sécurité Check Point en tant que dispositif unique.
- [Exportation d'un déploiement multi-domaine Check Point](#) - Lorsque vous disposez d'une passerelle de sécurité Check Point et d'un gestionnaire de sécurité Check Point avec une configuration de déploiement multi-domaine.

Exportation à partir d'un déploiement distribué de Check Point

Vous devez configurer les informations d'identification sur les appareils Check Point (r80) avant d'utiliser Live Connect sur l'outil de migration Secure Firewall pour extraire la configuration Check Point.

La procédure de mise à disposition préalable des informations d'identification dans le cadre d'un déploiement distribué de Check Point comprend les étapes suivantes :

Étape 1

Créez les éléments suivants sur la passerelle de sécurité de la console Gaia Check Point :

- a) Dans le navigateur Web, ouvrez l'application Gaia Console Check Point via une session HTTPS pour vous connecter à la passerelle de sécurité Check Point.
- b) Naviguez vers l'onglet **Gestion de l'utilisateur** et choisissez **Utilisateurs > Ajoutez**.
- c) Dans la fenêtre **Ajouter un utilisateur**, créez un nouveau nom d'utilisateur et mot de passe avec les détails suivants :
 - Dans la liste déroulante **Shell**, choisissez */etc/cli.sh*.
 - Dans **Rôles disponibles**, choisissez *adminRole*.
 - Conservez les valeurs par défaut pour les champs restants.
 - Cliquez sur **Ok**.

- d) Connectez-vous en SSH à votre passerelle de sécurité Check Point et créez un nouveau mot de passe à l'aide de la commande :

```
set expert-password <password>
```

- Remarque**
- Si vous avez déjà configuré le mot de passe expert sur l'appareil Check Point, réutilisez-le.
 - Vous aurez besoin de ces informations d'identification sur la page **Connexion à la passerelle de sécurité Check Point**, comme indiqué à l'étape 3.

Une fois que vous avez configuré le mot de passe de l'expert, la mise en place préalable des informations d'identification pour la passerelle Check Point r80 est terminée.

Pour plus d'informations, référez-vous à [Illustration 3 : Connectez-vous à la passerelle de sécurité Check Point](#).

Étape 2

Créez le nom d'utilisateur et le mot de passe sur le gestionnaire de sécurité Check Point pour r80 :

- a) Sur l'application SmartConsole, effectuez ces étapes :

1. Connectez-vous au gestionnaire de sécurité Check Point.
2. Naviguez vers **Gérer et Paramètres > Permissions et Administrateurs > Administrateurs**.
3. Cliquez sur * pour créer un nouveau nom d'utilisateur et un mot de passe et effectuez ces étapes :

- Choisissez **Méthode d'authentification** comme **mot de passe Check Point**.
- Cliquez sur **Définir un nouveau mot de passe** pour définir un nouveau mot de passe.

Remarque Assurez-vous de ne pas cocher la case **L'utilisateur doit modifier le mot de passe lors de la prochaine connexion**.

- Choisissez **Profil de permission** comme **Super utilisateur**.
- Choisissez l'**expiration** comme **Jamais**.

4. Cliquez sur **Publier** pour sauvegarder les changements de configuration sur l'application SmartConsole de Check Point.

- b) Sur la console Gaia pour le gestionnaire de sécurité Check Point, effectuez ces étapes :

Remarque Assurez-vous que le nom d'utilisateur et le mot de passe que vous créez maintenant est le même que celui créé à l'étape 2a (3) dans l'application SmartConsole.

1. Dans le navigateur Web, ouvrez l'application Gaia Console via une session HTTPS pour vous connecter à Check Point Security Manager.
2. Naviguez vers l'onglet **Gestion de l'utilisateur** et choisissez **Utilisateurs > Ajoutez**.
3. Créez un nom d'utilisateur et mot de passe qui est le même que celui créé dans l'étape 2a (3) de l'application SmartConsole
 - Dans la liste déroulante **Shell**, sélectionnez */bin/bash*.
 - Dans la liste déroulante des **rôles disponibles**, sélectionnez *adminRole*.
 - Conservez les valeurs par défaut pour les champs restants.
 - Cliquez sur **Ok**.

- Connectez-vous en SSH au gestionnaire de sécurité Check Point et créez un mot de passe expert à l'aide de la commande :

```
set expert-password <password>
```

- Remarque**
- Si vous avez déjà configuré le mot de passe expert, vous pouvez utiliser ce mot de passe.
 - Le nom d'utilisateur et le mot de passe créés dans l'étape 2b (3) et l'étape 2a (3) doivent être le même.

La mise en place préalable des informations d'identification sur Check Point dans le cadre d'un déploiement distribué pour le gestionnaire de sécurité Check Point est terminée.

Vous aurez besoin de ces informations d'identifiant sur la page **Connexion au gestionnaire de sécurité Check Point**, tel que montré dans l'étape 4.

Si vous utilisez un port API personnalisé sur le Check Point Smart Manager, voir [Vous utilisez un port API personnalisé pour Check Point \(r80\) Security Manager ?](#)

Prochaine étape

[Procédure pour exporter les fichiers de configuration Check Point pour r80](#)

Exportation à partir d'un déploiement autonome de Check Point

Vous devez configurer les informations d'identification sur les appareils Check Point (r80) avant d'utiliser Live Connect sur l'outil de migration Secure Firewall pour extraire la configuration Check Point.

La procédure de mise à disposition préalable des informations d'identification dans le cadre d'un déploiement autonome de Check Point comprend les étapes suivantes :

Étape 1

Dans le navigateur Web, ouvrez l'application Gaia Console via une session HTTPS pour vous connecter au dispositif Check Point autonome qui gère à la fois la passerelle de sécurité Check Point et le gestionnaire de sécurité Check Point.

Étape 2

Naviguez vers l'onglet **Gestion de l'utilisateur** et choisissez **Utilisateurs > Ajoutez**.

- Dans la fenêtre **Ajouter un utilisateur**, créez un nouveau nom d'utilisateur et mot de passe avec les détails suivants :
 - Dans la liste déroulante **Shell**, choisissez */etc/cli.sh*.
 - Dans la liste déroulante des **rôles disponibles**, sélectionnez *adminRole*.
 - Conservez les valeurs par défaut pour les champs restants.
 - Cliquez sur **Ok**.

Vous aurez besoin de ces informations d'identification sur la page **Connexion à la passerelle de sécurité Check Point**, comme indiqué à l'étape 3.

Pour plus d'informations, référez-vous à [Illustration 3 : Connectez-vous à la passerelle de sécurité Check Point](#).

- Dans la fenêtre **Ajouter un utilisateur**, créez un autre nom d'utilisateur et mot de passe avec les détails suivants :
 - Dans la liste déroulante **Shell**, sélectionnez */bin/bash*.

- Dans la liste déroulante des **rôles disponibles**, sélectionnez *adminRole*.
- Conservez les valeurs par défaut pour les champs restants.
- Cliquez sur **Ok**.

Étape 3

Créez les éléments suivants dans l'application SmartConsole pour r80 sur l'appareil Check Point :

Remarque Assurez-vous que le nom d'utilisateur et le mot de passe que vous créez maintenant sont les mêmes que ceux créés dans la console Check Point Gaia à l'étape précédente.

- Connectez-vous à l'application SmartConsole de l'appareil Check Point.
- Naviguez vers **Gérer et Paramètres > Permissions et Administrateurs > Administrateurs**.
- Cliquez sur ***** pour créer un nouveau nom d'utilisateur et mot de passe avec les détails suivants :

- Choisissez la **méthode d'authentification** comme **mot de passe Check Point**.
- Cliquez sur **Définir un nouveau mot de passe** pour définir un nouveau mot de passe.

Remarque Assurez-vous de ne pas cocher la case **L'utilisateur doit modifier le mot de passe lors de la prochaine connexion**.

- Choisissez le **profil de permission** comme **Super utilisateur**.
- Choisissez l'**expiration** comme **Jamais**.

Le nom d'utilisateur et mot de passe que vous avez créé ans l'étape b de l'étape 2 et l'étape c de l'étape 3 doivent être les mêmes.

Vous aurez besoin de ces informations d'identifiant sur la page **Connexion au gestionnaire de sécurité Check Point**, tel que montré dans l'étape 4.

- Cliquez sur **Publier** pour sauvegarder les changements de configuration sur l'application SmartConsole de Check Point.

Étape 4

Connectez-vous en SSH au périphérique Check Point et créez un mot de passe expert à l'aide de la commande :
set expert-password <password>

- Remarque**
- Si vous avez déjà configuré le mot de passe expert sur l'appareil Check Point, réutilisez-le.
 - Le nom d'utilisateur et mot de passe que vous avez créé ans l'étape b de l'étape 2 et l'étape c de l'étape 3 doivent être les mêmes.

La mise en place préalable des informations d'identification sur les dispositifs Check Point dans le cadre d'un déploiement autonome est terminée.

Si vous utilisez un port API personnalisé sur le Check Point Smart Manager, voir [Vous utilisez un port API personnalisé pour Check Point \(r80\) Security Manager ?](#)

Prochaine étape

[Procédure pour exporter les fichiers de configuration Check Point pour r80](#)

Exportation d'un déploiement multi-domaine Check Point


Vous devez configurer les informations d'identification sur les appareils Check Point (r80) à l'aide de Live Connect sur l'outil de migration Secure Firewall pour extraire la configuration Check Point.

La procédure de mise à disposition préalable des informations d'identification dans le cadre d'un déploiement multidomaine de Check Point comprend les étapes suivantes :

Étape 1

Créez les éléments suivants sur la passerelle de sécurité de la console Gaia Check Point :

- a) Dans le navigateur Web, ouvrez l'application Gaia Console via une session HTTPS pour vous connecter à la passerelle de sécurité Check Point.
- b) Naviguez vers l'onglet **Gestion de l'utilisateur** et choisissez **Utilisateurs > Ajoutez**.
- c) Dans la fenêtre **Ajouter un utilisateur**, créez un nouveau nom d'utilisateur et mot de passe avec les détails suivants :
 - Dans la liste déroulante **Shell**, choisissez */etc/cli.sh*.
 - Dans la liste déroulante des **rôles disponibles**, sélectionnez *adminRole*.
 - Conservez les valeurs par défaut pour les champs restants.
 - Cliquez sur **Ok**.
- d) Connectez-vous en SSH à votre passerelle de sécurité Check Point et créez un nouveau mot de passe à l'aide de la commande :
set expert-password <password>
La mise en place préalable des informations d'identification sur la passerelle de sécurité Check Point pour un déploiement multi-domaine est terminée.
- e) (Facultatif) Lors de l'exportation de la configuration d'un dispositif VSX (Virtual System Extension), cochez la **case ID du système virtuel** pour pouvoir saisir l'ID du système virtuel.

Illustration 1 : Se connecter à la passerelle de sécurité Check Point - Déploiement multi-domaines


Connect to Checkpoint Security Gateway

IP Address: 10.1.1.1 Port: 22

Admin Username: admin

Admin Password: ●●●●●●●●

Expert Password: ●●●●●●●●

Virtual System ID

Virtual ID Number: 2

[Login](#)

Étape 2

Créez le nom d'utilisateur et le mot de passe sur le gestionnaire de sécurité Check Point :

a) Sur l'application SmartConsole (mds), effectuez ces étapes :

1. Connectez-vous au gestionnaire de sécurité Check Point.
2. Naviguez vers **Gérer et Paramètres > Permissions et Administrateurs > Administrateurs**.
3. Cliquez sur *pour créer un nouveau nom d'utilisateur et mot de passer avec les détails suivants :

- Choisissez la **méthode d'authentification** comme **mot de passe Check Point**.
- Cliquez sur **Définir un nouveau mot de passe** pour définir un nouveau mot de passe.

Remarque Assurez-vous de ne pas cocher la case **L'utilisateur doit modifier le mot de passe lors de la prochaine connexion**.

- Choisissez le **profil de permission** comme **Super utilisateur multi-domaines**.
 - Choisissez l'**expiration** comme **Jamais**.
4. Cliquez sur **Publier** pour sauvegarder les changements de configuration sur l'application SmartConsole de Check Point.

Si vous utilisez un port API personnalisé sur le Check Point Smart Manager, voir [Vous utilisez un port API personnalisé pour Check Point \(r80\) Security Manager ?](#)

b) Sur la console Gaia pour le gestionnaire de sécurité Check Point, effectuez ces étapes :

Remarque Assurez-vous que le nom d'utilisateur et le mot de passe que vous allez créer est le même que celui créé à l'étape 2a (3) dans l'application SmartConsole.

1. Dans le navigateur Web, ouvrez l'application Gaia Console via une session HTTPS pour vous connecter à Check Point Security Manager.
2. Naviguez vers l'onglet **Gestion de l'utilisateur** et choisissez **Utilisateurs > Ajoutez**.
3. Créez un nom d'utilisateur et mot de passe qui est le même que celui créé dans l'étape 2a (3) de l'application SmartConsole
 - Dans la liste déroulante **Shell**, sélectionnez */bin/bash*.
 - Dans la liste déroulante des **rôles disponibles**, sélectionnez *adminRole*.
 - Conservez les valeurs par défaut pour les champs restants.
 - Cliquez sur **Ok**.
4. Connectez-vous en SSH à votre gestionnaire de sécurité Check Point et créez un nouveau mot de passe à l'aide de la commande :

```
set expert-password <password>
```

- Remarque**
- Si vous avez déjà configuré le mot de passe expert sur l'appareil Check Point, réutilisez-le.
 - Le nom d'utilisateur et le mot de passe créés dans l'étape 2a (3) et l'étape 2b (3) doivent être le même.

La mise en place préalable des informations d'identification sur le gestionnaire de sécurité Check Point dans le cadre d'un déploiement multidomaine est terminée.

Vous aurez besoin des identifiants pour vous connecter à Live Connect comme dans [Illustration 2 : Se connecter au gestionnaire de sécurité Check Point - Déploiement multi-domaines](#).

Illustration 2 : Se connecter au gestionnaire de sécurité Check Point - Déploiement multi-domaines

Remarque

- Si vous utilisez un port API personnalisé sur le Check Point Smart Manager, voir [Vous utilisez un port API personnalisé pour Check Point \(r80\) Security Manager ?](#)
- L'extraction du paquet de stratégies globales pour le déploiement multi-domaines n'est pas possible. Par conséquent, les objets, les règles ACE et les règles NAT configurés dans le cadre de la configuration sous Check Point CMA sont uniquement exportés et migrés.

Prochaine étape

[Procédure pour exporter les fichiers de configuration Check Point pour r80](#)

Vous utilisez un port API personnalisé pour Check Point (r80) Security Manager ?



- Remarque** Si vous utilisez un port API personnalisé sur le Check Point Smart Manager, effectuez ces actions :
- 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.

Procédure pour exporter les fichiers de configuration Check Point pour r80

Avant de commencer

Il est obligatoire de mettre en place les dispositifs Check Point au préalable. Pour des informations détaillées sur la configuration des informations d'identification sur les dispositifs Check Point (r80) avant la migration, voir [Pré-établissee les dispositifs Check Point \(r80\) pour l'extraction de la configuration à l'aide de Live Connect](#).



- Remarque**
- Nous vous recommandons d'utiliser Live Connect pour extraire les configurations Check Point (r80).
 - L'utilisation d'une configuration Check Point (r80) qui n'est pas exportée à l'aide de Live Connect dans l'outil de migration Secure Firewall entraîne la migration de la configuration comme non prise en charge, la migration partielle ou l'échec de la migration.
- Si les informations dans l'exportation de la configuration sont incomplètes, certaines configurations ne sont pas migrées et sont marquées comme **non prises en charge**.

Pour exporter les fichiers de configuration Check Point pour r80, procédez comme suit :

Étape 1 Choisissez Check Point (r80) de la page **Choisissez la configuration source**.

Étape 2 Cliquez sur **Connect (connexion)**.

Remarque Live Connect est offerte uniquement pour Check Point (r80).

Étape 3 Connectez-vous à la passerelle de sécurité Check Point. Procédez comme suit:

- a) Saisissez les informations suivantes dans la passerelle de sécurité Check Point r80 :
- Adresse IP
 - Port SSH
 - Nom d'utilisateur administrateur
 - Mot de passe de l'administrateur

- Mot de passe expert

Illustration 3 : Connectez-vous à la passerelle de sécurité Check Point

Connect to Checkpoint Security Gateway

IP Address: 10.10.1.1 Port: 22

Admin Username: admin

Admin Password: *****

Expert Password: *****

Login

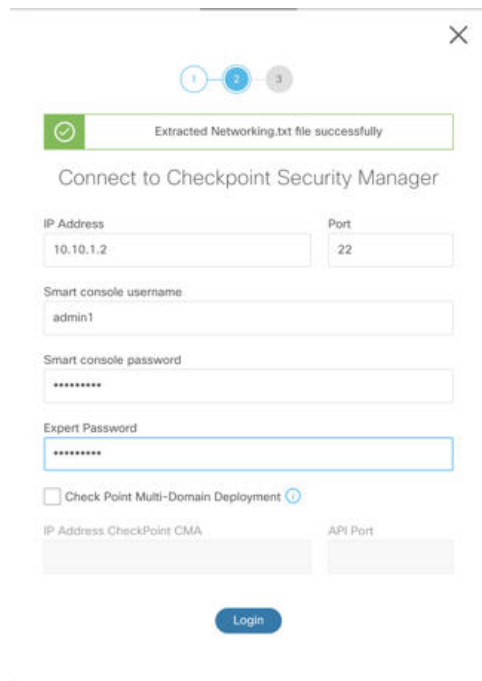
- b) Cliquez sur **Ouvrir une session**.

L'outil de migration Secure Firewall génère le fichier *networking.txt* qui contient les configurations spécifiques à l'appareil, telles que les configurations d'interface et de route. Stockez le fichier *networking.txt* dans un répertoire local pour la session en cours de l'outil de migration Secure Firewall.

Étape 4

Connectez-vous au gestionnaire de sécurité Check Point. Procédez comme suit:

- a) Saisissez les informations suivantes dans le gestionnaire de sécurité Check Point r80 :
- Adresse IP
 - Port SSH
 - Nom de l'utilisateur de la console Smart
 - Mot de passe de la console Smart
 - Mot de passe expert

Illustration 4 : Connectez-vous au gestionnaire de sécurité Check Point

b) Cliquez sur **Ouvrir une session**.

L'outil de migration Secure Firewall génère le fichier *Extracted-objects.json* qui capture la configuration complète du réseau et des objets de service disponibles dans le gestionnaire de sécurité Check Point.

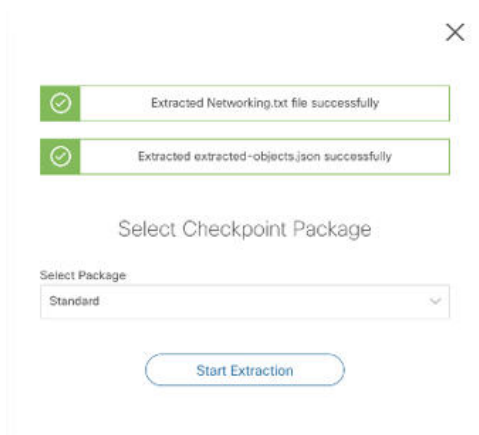
Stockez le fichier *Extracted-objects.json* dans un répertoire local pour la session actuelle de l'outil de migration Secure Firewall.

Remarque Si vous avez connecté l'outil de migration Secure Firewall au gestionnaire de sécurité Check Point, la liste des paquets de politiques offertes dans le gestionnaire de sécurité Check Point est affichée.

Étape 5 Sélectionnez le Paquet de politique Check Point que vous souhaitez migrer dans la liste **Choisir le paquet Check Point**, puis cliquez sur **Débuter l'extraction**.

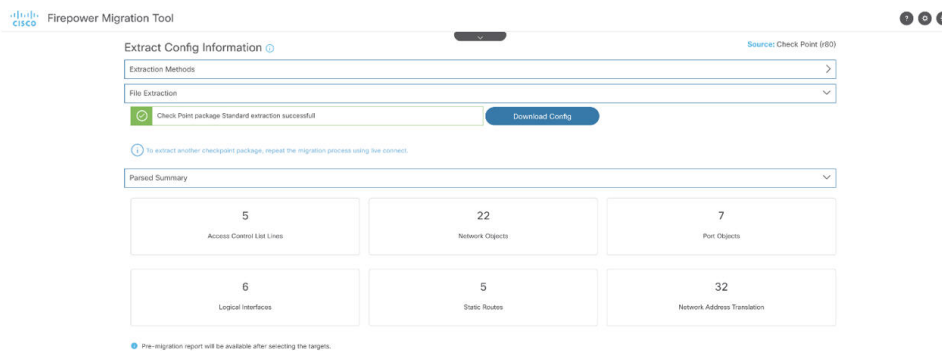
Extraire un autre fichier de configuration

Illustration 5 : Extraire le paquet de politique Check Point



Étape 6 Téléchargez la configuration et procédez avec la migration.

Illustration 6 : Extraction de la configuration complète de Check Point pour un déploiement distribué et autonome



Étape 7 Cliquez sur **Suivant** pour procéder à la migration de la configuration Check Point (r80).

Prochaine étape

[Téléversez le fichier de configuration Check Point](#)

Extraire un autre fichier de configuration

Pour extraire un autre fichier de configuration :

- Cliquez sur **Back to source selection** [retour à la sélection de la source] afin d'extraire une nouvelle configuration pour un autre paquet de politiques ou de vous connecter à un autre pare-feu Check Point (r80).
- Téléchargez la configuration actuelle si vous devez migrer plus tard la configuration Check Point (r80) extraite.



Remarque Le fichier de configuration actuel est téléchargé à un emplacement par défaut, défini par le navigateur.

Vous pouvez utiliser l'approche de la chaîne de montage pour extraire la configuration r80 :

- Exécutez Live Connect pour extraire le fichier de configuration Check Point (r80) pour chaque paquet de pare-feu ou pour différents pare-feu.
- Créez un référentiel pour plusieurs configurations.
- Utilisez l'option **Start Migration later** [lancer la migration plus tard] au moyen d'un chargement manuel afin de poursuivre la migration ultérieurement.

Téléversez le fichier de configuration Check Point

Avant de commencer

Exporter le fichier de configuration en format .zip.

-
- Étape 1** Sur l'écran **Extraire les informations de configuration**, dans la section **Téléversement manuel**, cliquez sur **Téléverser** pour téléverser le fichier de configuration Check Point.
- Étape 2** Naviguez vers l'endroit où le fichier de configuration est conservé. Le fichier de configuration est extrait pour Check Point (r77) et téléchargé en utilisant Live Connect pour Check Point (r80) Cliquez sur **Ouvrir**
- L'outil de migration Secure Firewall téléverse le fichier de configuration. Pour les fichiers de configuration volumineux, cette étape prend plus de temps.
- Le processus d'analyse préalable est maintenant terminé.
- La section Résumé de l'analyse affiche le statut de l'analyse.
- Étape 3** Examinez le résumé des éléments détectés et analysés par l'outil de migration Secure Firewall dans le fichier de configuration téléversé.
- Étape 4** Cliquez sur **Suivant** pour choisir les paramètres cibles.
-

Prochaine étape

[Préciser les paramètres de destination pour l'outil de migration Secure Firewall](#)

Préciser les paramètres de destination pour l'outil de migration Secure Firewall

Avant de commencer

- Obtenez l'adresse IP de centre de gestion pour le centre de gestion du pare-feu sur place
- À partir de l'outil de migration Secure Firewall 3.0, vous pouvez choisir entre le centre de gestion des pare-feux sur site et le centre de gestion des pare-feux en nuage.

- Pour le centre de gestion de pare-feu en nuage, la région et le jeton API doivent être fournis. Pour en savoir plus, consultez le [Centre de gestion cible pour la migration pris en charge](#).
- (Facultatif) Si vous souhaitez faire migrer des configurations spécifiques à un dispositif, comme des interfaces et des itinéraires, ajoutez la défense contre les menaces cible au centre de gestion. Référez-vous à [Ajoutez des dispositifs au Firewall Management Center](#)
- S'il est nécessaire d'appliquer un IPS ou une politique de fichier à l'ACL dans la page **Examiner et valider**, nous vous recommandons vivement de créer une politique sur centre de gestion avant la migration. Utilisez la même politique, alors que l'outil de migration Secure Firewall récupère la politique du centre de gestion connecté. Créer une nouvelle politique et l'assigner à des listes de contrôles d'accès peut dégrader la performance et causer l'échec du transfert.

Étape 1

Sur l'écran **Sélectionner la cible**, dans la section **Gestion** du pare-feu, procédez comme suit : vous pouvez choisir de migrer vers un centre de gestion de pare-feu sur site ou un centre de gestion de pare-feu en nuage .

- Pour migrer vers un centre de gestion sur place, faites ce qui suit :

- Cliquez sur le bouton radio **FMC sur place**
- Saisissez l'adresse IP ou le nom de domaine entièrement qualifié (FQDN) du centre de gestion.
- Dans la liste déroulante **Domaine**, sélectionnez le domaine vers lequel vous effectuez la migration.

Si vous voulez migrer vers un appareil défense contre les menaces, vous pouvez seulement migrer vers les appareils défense contre les menaces offerts dans le domaine sélectionné.

- Cliquez sur **Connecter** et procédez à l'**étape 2**.

- Pour migrer vers un centre de gestion de pare-feu en nuage, faites ce qui suit :

- Cliquez sur le bouton radio **FMC en nuage**.
- Choisissez la région et collez le jeton API CDO. Pour générer le jeton API du CO, suivez les étapes ci-dessous :
 - Connectez-vous au portail CDO
 - Naviguez vers **Paramètres > Paramètres généraux** et copiez le jeton API.
- Cliquez sur **Connecter** et procédez à l'**étape 2**.

Étape 2

Dans la boîte de dialogue Connexion du **Centre de gestion du pare-feu**, entrez le nom d'utilisateur et le mot de passe du compte dédié à l'outil de migration Secure Firewall, puis cliquez sur **Connexion**.

L'outil de migration Secure Firewall se connecte au centre de gestion et récupère une liste des appareils défense contre les menaces qui sont gérés par centre de gestion. Vous pouvez voir la progression de cette étape dans la console.

Étape 3

Cliquez sur **Procéder**.

Étape 4

Dans la section **Choisir la défense contre les menaces**, faites l'une de ces choses :

- Cliquez sur la liste déroulante **Sélectionner un dispositif de défense contre les menaces de pare-feu** et cochez le dispositif sur lequel vous souhaitez faire migrer la configuration de Check Point du .

Les dispositifs dans le domaine centre de gestion choisi sont listés par **adresse IP** et par **nom**.

Remarque Au minimum, le dispositif défense contre les menaces natif que vous choisissez doit avoir le même nombre d'interfaces physiques ou de canaux de port que la configuration de l'Check Point que vous migrez. Au minimum, l'instance de conteneur du dispositif défense contre les menaces doit avoir le même nombre d'interfaces et de sous-interfaces physiques ou de canaux de port. Vous devez configurer l'appareil avec le même mode de pare-feu que . Cependant, ces interfaces n'ont pas à avoir le même nom sur les deux dispositifs.

Remarque Uniquement lorsque la plateforme de défense contre les menaces cible prise en charge est le Firewall 1010 avec la version 6.5 ou ultérieure du centre de gestion. 6.5, la prise en charge de la migration FDM 5505 est applicable pour les politiques partagées et non pour les politiques spécifiques au dispositif. Lorsque vous procédez sans défense contre les menaces, l'outil de migration de Secure Firewall ne transfère aucune configuration ou politique à la défense contre les menaces. Ainsi, les interfaces et les itinéraires, ainsi que le VPN site à site, qui sont des configurations spécifiques aux dispositifs de défense contre les menaces, ne seront pas migrés. Cependant, toutes les autres configurations prises en charge (stratégies et objets partagés), telles que NAT, ACL et objets de port, seront migrées. Le VPN d'accès à distance est une politique partagée et peut être migré même sans défense contre les menaces.

L'outil de migration Secure Firewall prend en charge la migration du pare-feu Check Point vers la version 6.7 centre de gestion ou défense contre les menaces ou ultérieure avec l'option de déploiement à distance activée. La migration des interfaces et des itinéraires doit être faite manuellement.

- Cliquez sur **Proceed without FTD** (continuer sans FTD) pour amorcer la migration vers centre de gestion.

Lorsque vous procédez sans défense contre les menaces, l'outil de migration de Secure Firewall ne transfère aucune configuration ou politique vers défense contre les menaces. Ainsi, les interfaces et les routes ainsi que le VPN site à site, qui sont des configurations propres à l'appareil défense contre les menaces, ne seront pas migrés et devront être configurés manuellement sur centre de gestion. Cependant, toutes les autres configurations prises en charge (stratégies et objets partagés), telles que NAT, ACL et objets de port, seront migrées. Le VPN d'accès à distance est une politique partagée et peut être migré même sans défense contre les menaces.

Étape 5

Cliquez sur **Procéder**.

En fonction de la destination vers laquelle vous migrez, l'outil de migration Secure Firewall vous permet de sélectionner les fonctionnalités que vous souhaitez migrer.

Étape 6

Cliquez sur la section **Sélectionner les fonctionnalités** pour examiner et sélectionner les fonctionnalités que vous souhaitez migrer vers la destination.

- Si vous effectuez une migration vers un dispositif de destination défense contre les menaces, l'outil de migration Secure Firewall sélectionne automatiquement les fonctionnalités disponibles pour la migration à partir de la configuration de Check Point dans les sections **Configuration du dispositif** et **Configuration partagée**. Vous pouvez modifier la sélection par défaut, selon vos besoins.
- Si vous effectuez une migration vers un centre de gestion, l'outil de migration Cisco Secure Firewall sélectionnera automatiquement les fonctions disponibles pour la migration à partir Check Point dans les sections **Device Configuration** [configuration de l'appareil], **Shared Configuration** [configuration partagée] et **Optimization** [optimisation]. Vous pouvez modifier la sélection par défaut, selon vos besoins.
- Pour Check Point, sous **Configuration partagée**, sélectionnez l'option **Contrôle d'accès** appropriée :
 - Politique globale : lorsque vous sélectionnez cette option, la zone source et les zones de destination de la politique ACL sont migrées comme **Any**.

- Politique basée sur les zones : lorsque vous sélectionnez cette option, les zones de source et de destination sont dérivées sur la base de la recherche prédictive d'itinéraires par le biais du mécanisme de routage pour les objets ou groupes de réseaux de source et de destination.

Remarque La recherche d'itinéraires est limitée aux itinéraires statiques et aux itinéraires dynamiques (PBR et NAT ne sont pas pris en compte) et, en fonction de la nature des groupes d'objets réseau source et destination, cette opération peut entraîner une explosion des règles.

L'information de routage est obtenu par le fichier `networking.txt`. Ce fichier est la sortie de l'outil `FMT-CP-Config-Extractor_v4.0.1-8248` qui utilise la commande `netstat -rnv` pour rassembler la table de routage. Pour plus d'informations, référez-vous à [Exporter la configuration d'un appareil à l'aide d'un extracteur de configuration](#)

La recherche d'itinéraires IPv6 pour les politiques basées sur les zones n'est pas prise en charge dans cette version. Assurez-vous que toutes les règles de la politique globale ou des politiques basées sur les zones soient migrées avec succès.

Dans **Device Configuration** [configuration de l'appareil], choisissez les interfaces, les routes et les configurations des tunnels VPN de site à site à migrer à partir de votre pare-feu Check Point. Notez que la migration est possible seulement pour une configuration des tunnels VPN de site à site basée sur les politiques (carte cryptographique).

- (Facultatif) Dans la section **Optimisation**, sélectionnez **Migrer uniquement les objets référencés** pour ne migrer que les objets référencés dans une stratégie de contrôle d'accès et une stratégie NAT.

Remarque Lorsque vous sélectionnez cette option, les objets non référencés dans la configuration de l' Check Point de ne seront pas migrés. Cela optimise le temps de migration et nettoie les objets inutilisés de la configuration.

Étape 7 Cliquez sur **Procéder**.

Étape 8 Dans la section **Conversion de règle/Configuration de processus**, cliquez sur **Débuter la conversion** pour initier la conversion.

Étape 9 Examiner le sommaire des éléments que l'outil de migration Secure Firewall a converti.

Pour vérifier si votre fichier de configuration a été téléversé et analysé avec succès, téléchargez et vérifiez le rapport de **pré-migration** avant de continuer avec la migration.

Étape 10 Cliquez sur **Télécharger le rapport** et sauvegardez le **rapport de pré-migration**.

Une copie du rapport **pré-migration** est aussi sauvegardée dans le dossier `Ressources` au même endroit que l'outil de migration Secure Firewall.

Prochaine étape

[Examiner le rapport pré-migration, à la page 48](#)

Examiner le rapport pré-migration

Étape 1 Naviguez vers où vous avez téléchargé le **rapport pré-migration**.

Une copie du rapport **pré-migration** est aussi sauvegardée dans le dossier `Ressources` au même endroit que l'outil de migration Secure Firewall.

Étape 2 Ouvrez le **rapport pré-migration** et examiner attentivement son contenu pour identifier tout problème pouvant causer l'échec de la migration.

Le **rapport pré-migration** inclut les informations suivantes :

- **Résumé de la migration** - Résumé général des éléments de configuration Check Point pris en charge qui peuvent être migrés avec succès vers Firepower Threat Defense. Par exemple, les noms de politiques, le nombre de règles, etc.
- **Détails des erreurs d'analyse** - Met en évidence la configuration qui a entraîné un échec de l'analyse. Ceci aide à modifier et mettre à jour la configuration pour un autre essai.
- **Configuration non prise en charge** - Liste de tous les éléments de configuration qui ne sont pas pris en charge pour la migration par FMT et qui sont présentés de manière plus détaillée. Par exemple, une boucle avec retour, les interfaces Alias, les objets de domaine.
- **Configuration partiellement prise en charge** - Liste de tous les éléments de configuration Check Point qui ne peuvent être que partiellement migrés. Par exemple, les routes statiques avec les paramètres Ping.
- **Configuration ignorée** - Liste de tous les éléments de configuration Check Point qui sont ignorés par FMT pendant la migration et qui ne seront pas signalés sur le système cible.

Pour plus d'informations à propos des caractéristiques prises en charge dans centre de gestion et Défense contre les menaces, consultez le [Guide de configuration du centre de FMC](#).

Étape 3 Si le **rapport de pré-migration** recommande des actions correctives, effectuez ces corrections sur le Check Point, exportez à nouveau le fichier de configuration du Check Point et téléchargez le fichier de configuration mis à jour avant de poursuivre.

Étape 4 Une fois que le fichier de configuration Check Point a été téléchargé et analysé avec succès, revenez à l'outil de migration Secure Firewall et cliquez sur **Suivant** pour poursuivre la migration.

Mappez les configurations de ,Check Point du pare-feu et de avec les Défense contre les menaces interfaces.

L'appareil défense contre les menaces doit avoir un nombre d'interfaces physiques et de canaux de port égal ou supérieur à celui utilisé par ASACheck Point. Ces interfaces ne doivent pas avoir les mêmes noms sur les deux appareils. Vous pouvez choisir comment associer les interfaces.

À la page **Map FTD Interface** [mapper l'interface FTD], l'outil de migration Cisco Secure Firewall récupère une liste des interfaces de l'appareil défense contre les menaces. Par défaut, l'outil de migration Secure Firewall mappe les interfaces dans ASACheck Point avec leet le dispositif défense contre les menaces en fonction de leurs identités d'interface. Par exemple, l'interface « gestion seule » de l'interface du Check Point est automatiquement mappée à l'interface « gestion seule » du défense contre les menacesdispositif et n'est pas modifiable.

Le mappage de l'interface de l' Check Pointavec à l'interface défense contre les menaces diffère en fonction du type de périphérique défense contre les menaces :

- Si la cible défense contre les menaces est de type natif :

- Le défense contre les menaces doit avoir un nombre égal ou supérieur d'interfaces Check Point ou d'interfaces de données de canal de port (PC) utilisées (à l'exclusion des interfaces de gestion uniquement et des sous-interfaces dans la configuration de dispositifs gérés par un Check Point). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre les menaces cible.
- Les sous-interfaces sont créées par l'outil de migration du pare-feu sécurisé sur la base de l'interface physique ou du mappage du canal de port.
- Si la cible défense contre les menaces est de type contenant :
 - Le défense contre les menaces doit avoir un nombre égal ou supérieur d'interfaces Check Point ou de sous-interfaces physiques utilisées, de canal de port ou de sous-interfaces de canal de port (à l'exclusion des interfaces de gestion uniquement et des sous-interfaces dans la configuration de dispositifs gérés par un Check Point). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre les menaces cible. Par exemple, si le nombre d'interfaces physiques et de sous-interfaces physiques sur la cible défense contre les menaces est inférieur de 100 à celui de l'Check Point , vous pouvez créer des interfaces physiques ou des sous-interfaces physiques supplémentaires sur la cible défense contre les menaces.
 - Les sous-interfaces ne sont pas créés par l'outil de migration Secure Firewall Seul le mappage d'interface est autorisé entre les interfaces physiques, les canaux de port ou les sous-interfaces.

Avant de commencer

Assurez-vous de vous être connecté au centre de gestion et choisi la destination comme défense contre les menaces Pour en savoir plus, consultez [Préciser les paramètres de destination pour l'outil de migration Secure Firewall](#), à la page 45.



Remarque

Cette étape n'est pas applicable si vous migrez vers un centre de gestion sans un dispositif défense contre les menaces.

Étape 1

Si vous souhaitez modifier le mappage d'une interface, cliquez sur la liste déroulante du **nom de l'interface FTD** et choisissez l'interface que vous souhaitez mapper à l'interface de l' et de l'Check Point.

Vous ne pouvez pas modifier le mappage des interfaces de gestion. Si une interface défense contre les menaces a déjà été attribuée à une interface de périphérique Check Point, vous ne pouvez pas choisir cette interface dans la liste déroulante. Toutes les interfaces sont grisées et indisponibles.

Vous n'avez pas besoin de mapper les sous-interfaces. L'outil de migration Secure Firewall fait correspondre les sous-interfaces du dispositif défense contre les menaces à toutes les sous.

Étape 2

Lorsque vous avez mappé chaque interface de périphérique Check Point à une interface défense contre les menaces, cliquez sur **Suivant**.

Prochaine étape

Mappez les interfaces des Check Point aux objets d'interface, aux zones de sécurité et aux groupes d'interfaces appropriés pour la défense contre les menaces. Pour plus d'informations, voir [Associez les interfaces Check Point à des zones de sécurité à des groupes d'interfaces](#).

Associez les interfaces Check Point à des zones de sécurité à des groupes d'interfaces

Pour que la configuration de l'outil de migration de l'interface de l'interface et Check Point géré par FDM soit migrée correctement, mappez les interfaces de Check Point aux objets d'interface, aux zones de sécurité, aux groupes d'interfaces. Dans une configuration Check Point de l'interface, les politiques de contrôle d'accès et les politiques NAT utilisent des noms d'interface (nameif). Dans le centre de gestion, ces politiques utilisent des objets d'interface. De plus, les politiques du centre de gestion regroupent les objets d'interface ainsi :

- Zones de sécurité - Une interface ne peut appartenir qu'à une seule zone de sécurité.
- Groupes d'interfaces - Une interface peut appartenir à plusieurs groupes d'interfaces.

L'outil de migration Cisco Secure Firewall permet le mappage individuel des interfaces avec les zones de sécurité et les groupes d'interfaces. Lorsqu'une zone de sécurité ou un groupe d'interfaces est mappé à une interface, il n'est pas disponible pour le mappage à d'autres interfaces, bien que le centre de gestion le permette. Pour en savoir plus sur les zones de sécurité et les groupes d'interfaces dans le centre de gestion, consultez la section [Security Zones and Interface Groups](#) [zones de sécurité et groupes d'interfaces] du *guide de configuration d'appareil de Cisco Secure Firewall Management Center*.

-
- Étape 1** Sur l'écran **Mapper les zones de sécurité et les groupes d'interfaces**, passez en revue les interfaces, les zones de sécurité et les groupes d'interfaces disponibles.
- Étape 2** Pour mapper des interfaces à des zones de sécurité et à des groupes d'interfaces qui existent dans le centre de gestion, ou qui sont disponibles dans les fichiers de configuration de l'interface en tant qu'objets de type zone de sécurité et qui sont disponibles dans la liste déroulante, procédez comme suit :
- a) Dans la colonne **Zones de sécurité**, choisissez la zone de sécurité pour cette interface.
 - b) Dans la colonne **Groupes d'interface**, choisissez le groupe d'interface pour cette interface.
- Étape 3** Pour mapper des interfaces à des zones de sécurité et à des groupes d'interfaces qui existent dans le centre de gestion, ou qui sont disponibles dans les fichiers de configuration de Check Point (r80) en tant qu'objets de type zone de sécurité et qui sont disponibles dans la liste déroulante, procédez comme suit :
- a) Dans la colonne **Zones de sécurité**, choisissez la zone de sécurité pour cette interface.
 - b) Dans la colonne **Groupes d'interface**, choisissez le groupe d'interface pour cette interface.
- Étape 4** Vous pouvez mapper manuellement ou auto-créez les zones de sécurité et les groupes d'interface.
- Étape 5** Pour mapper manuellement les zones de sécurité et les groupes d'interface, faites ce qui suit :
- a) Cliquez sur **Ajouter ZS & GI**
 - b) Dans la boîte de dialogue **Ajouter ZS & GI**, cliquez sur **Ajouter** pour ajouter une nouvelle zone de sécurité ou groupe d'interface.
 - c) Saisissez le nom de la zone de sécurité dans la colonne **Zone de sécurité**. Le nombre maximal de caractères est de 48. Vous pouvez, de même, ajouter un groupe d'interface.
 - d) Cliquez sur **Close** (Fermer).
- Pour mapper les zones de sécurité et les groupes d'interface par auto-création, faites ce qui suit :

- a) Cliquez sur **Auto-cr  er**.
- b) Dans la bo  te de dialogue **Auto-cr  er**, cochez une ou les deux cases **Groupes d'interface** et **Mappage de zone**.
- c) Cliquez sur **Auto-cr  er**.

L'outil de migration Secure Firewall donne    ces zones de s  curit   le m  me nom que l'interface Check Point, comme    **l'ext  rieur** ou    **l'int  rieur**, et affiche un « (A) » apr  s le nom pour indiquer qu'il a   t   cr  e par l'outil de migration Secure Firewall. Les groupes d'interface ont un suffixe `_ig` ajout  , tel que **outside_ig** ou **inside_ig**. De plus, les zones de s  curit   et les groupes d'interface ont le m  me mode que l'interface Check Point. Par exemple, si l'interface logique Check Point est mode L3, la zone de s  curit   et le groupe d'interface cr  es pour l'interface sont   galement en mode L3.

  tape 6

Lorsque vous avez mapp   toutes les interfaces aux zones de s  curit   et groupes d'interface appropri  s, cliquez sur **Suivant**.

Optimiser, examiner et valider la configuration

Avant de transf  rer la configuration Check Point de vers centre de gestion, optimisez et examinez soigneusement la configuration et v  rifiez qu'elle est correcte et qu'elle correspond    la fa  on dont vous souhaitez configurer l'appareil d  fense contre les menaces. Un onglet clignotant indique que vous devez passer    l'action suivante.



Remarque

Si vous fermez l'outil de migration Secure Firewall    l'  cran **Optimiser, examiner et valider la configuration**, cela sauvegarde votre progression et vous permet de continuer la migration plus tard. Si vous fermez l'outil de migration Secure Firewall avant cet   cran, votre progression ne sera pas sauvegard  e. S'il y a un   chec apr  s l'analyse, relancer l'outil de migration Secure Firewall continue    partir de l'  cran **Mappage des interfaces**.

Ici, l'outil de migration Cisco Secure Firewall r  cup  re les politiques du syst  me de pr  vention des intrusions (IPS) et les politiques des fichiers qui sont d  j   pr  sentes dans le centre de gestion et qui vous permet de les associer aux r  gles de contr  le d'acc  s que vous migrez.

Une strat  gie de fichiers est un ensemble de configurations que le syst  me utilise pour effectuer une protection avanc  e contre les logiciels malveillants pour les r  seaux et le contr  le des fichiers, dans le cadre de votre configuration globale de contr  le d'acc  s. Cette association fait en sorte qu'avant que le syst  me passe un fichier dans le trafic correspondant aux conditions de la r  gle de contr  le d'acc  s, le fichier est d'abord inspect  .

De m  me, vous pouvez utiliser une politique IPS comme derni  re ligne de d  fense du syst  me avant que le trafic ne soit autoris      se rendre    destination. Les politiques d'intrusion r  gissent la mani  re dont le syst  me inspecte le trafic    la recherche de violations de la s  curit   et, dans les d  ploiements en ligne, peuvent bloquer ou modifier le trafic malveillant. Chaque fois que le syst  me utilise une politique d'intrusion pour   valuer le trafic, il utilise un ensemble de variables associ  . La plupart des variables d'un ensemble repr  sentent des valeurs couramment utilis  es dans les r  gles d'intrusion pour identifier les adresses IP et les ports source et destination. Vous pouvez   galement utiliser des variables dans les politiques d'intrusion pour repr  senter les adresses IP dans les   tats de suppression de r  gles et de r  gles dynamiques.

Pour rechercher des   l  ments de configuration sp  cifiques dans un onglet, saisissez le nom de l'  l  ment dans le champ situ   en haut de la colonne. Les rang  es du tableau sont filtr  es pour afficher seulement les   l  ments correspondant au terme de recherche.



Remarque Par défaut, l'option du Groupement en ligne est activée.

Si vous fermez l'outil de migration Secure Firewall à l'écran **Optimiser, examiner et valider la configuration**, cela sauvegarde votre progression et vous permet de continuer la migration plus tard. Si vous fermez ceci avant cet écran, votre progression ne sera pas sauvegardée. S'il y a un échec après l'analyse, relancer l'outil de migration Secure Firewall continue à partir de l'écran **Mappage des interfaces**.

Présentation de l'optimisation ACL de l'outil de migration Secure Firewall

L'outil de migration Secure Firewall permet d'identifier et de séparer les ACL qui peuvent être optimisées (désactivées ou supprimées) de la base de règles du pare-feu sans avoir d'impact sur la fonctionnalité du réseau.

L'optimisation d'ACL supporte les types d'ACL suivants :

- **ACL redondante:** lorsque deux ACL ont le même ensemble de configurations et de règles, la suppression de l'ACL non de base n'aura pas d'incidence sur le réseau. Par exemple, si deux règles autorisent le trafic FTP et IP sur le même réseau sans qu'aucune règle ne soit définie pour refuser l'accès, la première règle peut être supprimée.
- **ACL dupliquée:** la première ACL masque complètement les configurations de la deuxième ACL. Si deux règles ont un trafic similaire, la deuxième règle n'est appliquée à aucun trafic lorsqu'elle apparaît plus loin dans la liste d'accès. Si les deux règles spécifient des actions différentes pour le trafic, vous pouvez soit déplacer la règle masquée, soit modifier l'une des règles pour mettre en œuvre la politique requise. Par exemple, la règle de base peut refuser le trafic IP et la règle masquée peut autoriser le trafic FTP pour une source ou une destination donnée.

L'outil de migration Secure Firewall utilise les paramètres suivants lors de la comparaison des règles pour l'optimisation des ACL :



Remarque L'optimisation est disponible pour le Check Point uniquement pour une action découlant d'une règle ACP.

- Les ACL désactivés ne sont pas considérés durant le processus d'optimisation.
- Les ACLs sources sont développées en ACEs correspondants (valeurs en ligne), puis comparées pour les paramètres suivants :
 - Zones source et de destination
 - Réseau source et de destination
 - Port source et de destination

Cliquez sur **Download Report** [télécharger le rapport] pour revoir le nom de l'ACL et les ACL redondantes et dupliquées correspondantes figurant dans un fichier Excel. Utilisez la feuille **Detailed ACL Information** [information détaillée sur les ACL] pour afficher plus de détails sur les ACL.

Optimisation de l'objet

Les objets suivants sont pris en considération lors de l'optimisation des objets dans le cadre du processus de migration :

- Objets non référencés - Vous pouvez choisir de ne pas migrer les objets non référencés au début de la migration.
- Objets en double - Si un objet existe déjà sur centre de gestion, au lieu de créer un objet en double, la politique est réutilisée.
- Objets incohérents - si des objets ont des noms similaires mais un contenu différent, les noms des objets sont modifiés par l'outil de migration Secure Firewall avant la poussée de migration.

Étape 1

(Facultatif) Sur l'écran **Optimiser, examiner et valider la configuration**, cliquez sur **Optimiser l'ACL** pour exécuter le code d'optimisation et effectuez les opérations suivantes :

- Pour télécharger les règles d'optimisation d'ACL, cliquez sur **Télécharger**.
- Sélectionnez les règles et choisissez **Actions > Migrer comme désactivé** ou **Ne pas migrer** et appliquez l'une des actions.
- Cliquez sur **Save** (enregistrer).

L'opération de migration passe de **Ne pas migrer** à **désactivé** ou vice-versa.

Vous pouvez effectuer une sélection en bloc des règles à l'aide des options suivantes

- Migrer - Pour migrer vers le statut par défaut.
- Ne pas migrer - Pour ignorer la migration des ACL
- Migrer comme désactivé - Pour migrer les ACL avec le champ **État** réglé à **Désactiver**
- Migrer comme activé - Pour migrer les ACL avec le champ **État** réglé à **Activer**

Étape 2

À la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration], cliquez sur **Access Control Rules** [règles de contrôle d'accès] et faites comme suit :

- Pour chaque entrée dans le tableau, examinez les mappages et vérifiez qu'ils soient corrects.

Une règle de politique d'accès migrée utilise le nom de l'ACL comme préfixe et y ajoute le numéro de la règle de l'ACL pour faciliter le mappage vers le fichier de configuration Check Point. Par exemple, si une ACL Check Point est nommée « inside_access », la première ligne de règle (ou ACE) de l'ACL sera nommée « inside_access_#1 ». Si une règle doit être étendue en raison de combinaisons TCP ou UDP, d'un objet de service étendu ou pour toute autre raison, l'outil de migration Secure Firewall ajoute un suffixe numéroté au nom. Par exemple, si la règle d'autorisation est développée en deux règles de migration, elles sont nommées « inside_access_#1-1 » et « inside_access_#1-2 ».

Pour toute règle comprenant un objet non pris en charge, l'outil de migration Secure Firewall ajoute un suffixe « _UNSUPPORTED » au nom.

- Si vous ne souhaitez pas migrer une ou plusieurs politiques de liste de contrôle d'accès, cochez la case des lignes concernées, choisissez **Actions [actions] > Do not migrate [ne pas migrer]**, puis **Save** [enregistrer].

Toutes les règles que vous choisirez de ne pas migrer sont grisées dans le tableau.

- Si vous souhaitez appliquer une politique de fichiers centre de gestion à une ou plusieurs politiques de contrôle d'accès, cochez la case des lignes appropriées, puis sélectionnez **Actions > Politique de fichiers**.

Dans la boîte de dialogue **Stratégie de fichier**, sélectionnez la stratégie de fichier appropriée et appliquez-la aux stratégies de contrôle d'accès sélectionnées, puis cliquez sur **Enregistrer**.

- Si vous souhaitez appliquer une politique IPS centre de gestion à une ou plusieurs politiques de contrôle d'accès, cochez la case des lignes appropriées, puis sélectionnez **Actions > Politique de fichiers**.

Dans la boîte de dialogue **Politique IPS**, sélectionnez la politique IPS appropriée et son ensemble de variables correspondant, appliquez-la aux politiques de contrôle d'accès sélectionnées et cliquez sur **Enregistrer**.

- e) Si vous souhaitez modifier les options de journalisation d'une règle de contrôle d'accès pour laquelle la journalisation est activée, cochez la case de la ligne correspondante et sélectionnez **Actions > Journal**.

Dans la boîte de dialogue **Journal**, vous pouvez activer l'enregistrement des événements au début ou à la fin d'une connexion, ou les deux. Si vous activez la journalisation, vous devez choisir d'envoyer les événements de connexion soit à **l'observateur d'événements**, soit au **Syslog**, soit aux deux. Lorsque vous choisissez d'envoyer les événements de connexion à un serveur syslog, vous pouvez choisir les stratégies syslog déjà configurées sur le centre de gestion dans le menu déroulant **Syslog**.

- f) Si vous souhaitez modifier les actions pour les règles de contrôle d'accès migrées dans le tableau Contrôle d'accès, cochez la case de la ligne appropriée et sélectionnez **Actions > Action découlant d'une règle**.

Astuces Les politiques IPS et les politiques de fichiers joints à une règle de contrôle d'accès seront automatiquement supprimées pour les actions découlant d'une règle, à l'exception de l'option **Allow** [autoriser].

Vous pouvez filtrer le nombre d'ACE dans l'ordre croissant ou décroissant, ou pour voir les résultats égaux, supérieurs et inférieurs.

Pour effacer les critères de filtrage existants et charger une nouvelle recherche, cliquez sur **Effacer le filtre**.

Remarque L'ordre dans lequel vous trie l'ACL en fonction de l'ACE est uniquement destiné à la visualisation. Les ACL sont transférés selon l'ordre chronologique selon lequel ils se produisent.

Étape 3

Cliquez sur les onglets suivants et examinez les éléments de configuration :

- **Contrôle d'accès**
- **Objets (objets de réseau, objets de port)**
- **NAT**
- **Interfaces**
- **Routs**
- **Tunnels de réseau privé virtuel (VPN) de site à site**

Si vous ne souhaitez pas migrer une ou plusieurs règles NAT ou interfaces de routage, cochez la case des lignes concernées, choisissez **Actions [actions] > Do not migrate [ne pas migrer]**, puis **Save** [enregistrer].

Toutes les règles que vous choisirez de ne pas migrer sont grisées dans le tableau.

Étape 4

Vous pouvez afficher les routes à partir de la zone **Routes** [routes] et sélectionner les routes que vous ne souhaitez pas migrer, en sélectionnant une entrée et en choisissant **Actions [actions] > Do not migrate** [ne pas migrer].

Étape 5

À la section **Site-to-Site VPN Tunnels** [tunnels VPN de site à site], les tunnels VPN des configurations du pare-feu source sont indiqués. Passez en revue les données du tunnel VPN, comme les configurations de **l'interface source**, du **type VPN**, **IKEv1** et **IKEv2** pour chaque ligne, et assurez-vous de fournir les valeurs des clés prépartagées pour toutes les lignes.

Étape 6

(Facultatif) Pour télécharger les détails pour chaque élément de configuration dans la grille, cliquez sur **Télécharger**.

Étape 7

Après avoir complété votre examen, cliquez sur **Valider**. Prenez note que les champs obligatoires qui requièrent votre attention clignoteront jusqu'à ce que vous les remplissiez. Vous pourrez cliquer sur le bouton **Valider** [valider] seulement après que vous aurez rempli tous les champs obligatoires.

Durant la validation, l'outil de migration Secure Firewall se connecte à centre de gestion, examine les objets existants et les compare à une liste d'objets à migrer. Si un objet existe déjà dans centre de gestion, l'outil de migration Secure Firewall fait ce qui suit :

- Si un objet a le même nom et configuration, l'outil de migration Secure Firewall réutilise l'objet existant et ne crée pas de nouvel objet dans centre de gestion.
- Si l'objet a le même nom mais une configuration différente, l'outil de migration Secure Firewall rapporte un conflit d'objet.

Vous pouvez voir la progression de la validation dans la console.

Étape 8

Lorsque la validation est terminée, si la boîte de dialogue **Statut de la validation** montre un ou plusieurs conflits d'objets, faites ce qui suit :

a) Cliquez sur **Résoudre les conflits**

L'outil de migration Secure Firewall affiche une icône d'avertissement dans l'onglet **Objets réseau** ou **Objets port**, ou les deux, selon l'endroit où les conflits d'objets ont été signalés.

b) Cliquez sur l'onglet et examinez les objets.

c) Vérifiez l'entrée pour chaque objet qui présente un conflit et sélectionnez **Actions > Résoudre les conflits**.

d) Dans la fenêtre **Résoudre les conflits**, complétez l'action recommandée.

Par exemple, on pourrait vous demander d'ajouter un suffixe au nom de l'objet pour éviter un conflit avec l'objet centre de gestion existant. Vous pouvez accepter le suffixe par défaut ou le remplacer par un des vôtres.

e) Cliquez sur **Résoudre**

f) Lorsque vous avez résolu tous les conflits d'objet sur un onglet, cliquez sur **Sauvegarder**

g) Cliquez sur **Valider** pour revalider la confirmation et confirmer que vous avez résolu tous les conflits d'objet.

Étape 9

Lorsque la validation est terminée et que la boîte de dialogue **Statut de la validation** affiche le message **Validé avec succès**, continuez avec [Transférer la configuration migrée vers Centre de gestion](#), à la page 56

Transférer la configuration migrée vers Centre de gestion

Vous ne pouvez pas pousser la configuration de Check Point migré avec un vers centre de gestion si vous n'avez pas validé la configuration et résolu tous les conflits d'objets.

Cette étape dans le processus de migration envoie la configuration migrée vers centre de gestion. Elle ne déploie pas la configuration vers l'appareil Défense contre les menaces. Cependant, toute configuration existante sur le Défense contre les menaces est supprimée durant cette étape.



Remarque

Ne faites pas de changements de configuration ou ne déployez pas vers tout appareil pendant que l'outil de migration Secure Firewall envoie la configuration migrée vers centre de gestion.

Étape 1

Dans la boîte de dialogue **Statut de validation**, examinez le sommaire de la validation.

Étape 2

Cliquez sur **Transférer la configuration** pour envoyer la configuration du dispositif migré Check Point à centre de gestion.

L'outil de migration Secure Firewall affiche un sommaire de la progression de la migration. Vous pouvez voir la progression détaillée, ligne par ligne des composants étant transférés vers centre de gestion dans la console.

Étape 3 Une fois la migration terminée, cliquez sur **Télécharger le rapport** pour télécharger et sauvegarder le rapport post-migration.

Une copie du **rapport post-migration** est également sauvegardée dans le dossier **Ressources** au même endroit que l'outil de migration Secure Firewall

Étape 4 Si la migration a échoué, examinez attentivement le rapport post-migration, le fichier journal et le fichier non analysé pour comprendre la cause de l'échec.

Vous pouvez également contacter l'équipe de soutien technique pour la résolution de problèmes.

Assistance à l'échec de migration

Si votre migration a échoué, contactez le soutien technique.

1. Sur l'écran **Migration terminée**, cliquez sur le bouton **Soutien technique**.

La page de soutien technique apparaît.

2. Cochez la case **Offre groupée de soutien**, puis sélectionnez les fichiers de configuration à télécharger.

Remarque Les fichiers journaux et dB sont choisis pour téléchargement par défaut.

3. Cliquez sur **Télécharger**.

Le fichier d'assistance est téléchargé sous la forme d'un fichier .zip dans votre chemin d'accès local. Extrayez le dossier Zip pour voir les fichiers journaux, la base de données et les fichiers de configuration.

4. Cliquez sur **Envoyer** pour envoyer les détails de la panne à l'équipe technique.

Vous pouvez aussi joindre les fichiers d'assistance téléchargés à votre courriel.

5. Cliquez sur **Visiter la page TAC** pour créer une demande TAC dans la page de soutien de Cisco

Remarque Vous pouvez soumettre une demande TAC en tout temps durant la migration à partir de la page de soutien technique.

Examiner le rapport de post-migration pour Check Point et terminer la migration

Étape 1 Naviguez vers où vous avez téléchargé le rapport post-migration.

Étape 2 Ouvrez le rapport de post-migration et examinez attentivement son contenu pour comprendre comment la configuration de votre ASA a été migrée :

- **Résumé de la migration** - Un résumé de la configuration qui a été migrée avec succès de Check Point à Firepower Threat Defense.
- **Migration sélective des politiques** - Des détails sur les fonctionnalités Check Point spécifiques sélectionnées pour la migration et le mappage d'interface sont disponibles.
- **Conversions des migrations** - Détails des conversions et des transferts incluant ce qui suit :
 - Gestion des objets de réseau/service

- Liste des configurations partiellement migrées avec les raisons
- Liste des configurations non prises en charge avec motif
- Règles de contrôle d'accès étendues

Désinstaller l'outil de migration Secure Firewall

Tous les composants sont stockés dans le même dossier que l'outil de migration Secure Firewall.

- Étape 1** Naviguez jusqu'au dossier où vous avez téléchargé l'outil de migration Secure Firewall.
- Étape 2** Si vous voulez sauvegarder les journaux, coupez ou copiez et collez le dossier `journal` vers un endroit différent.
- Étape 3** Si vous voulez sauvegarder les rapports pré-migration et les rapports post-migration, coupez ou copiez et collez le dossier `ressources` vers un endroit différent.
- Étape 4** Supprimez le dossier où vous avez placé l'outil de migration Secure Firewall.
- Astuces** Le fichier `journal` est associée avec la fenêtre de la console. Si la fenêtre de la console pour l'outil de migration Secure Firewall est ouverte, le fichier `journal` et le dossier ne peuvent pas être supprimés.

Exemple de migration : avec vers Threat Defense 2100



- Remarque** Créez un plan test que vous pouvez exécuter sur le dispositif cible une fois la migration terminée.
- [Tâches de la fenêtre de pré-maintenance](#)
 - [Tâches de la fenêtre de maintenance](#)

Tâches de la fenêtre de pré-maintenance

Avant de commencer

Assurez-vous d'avoir installé et déployé un centre de gestion Pour plus d'informations, consultez le [Guide d'installation du matériel du centre de gestion](#) approprié et le [Guide de démarrage du centre de gestion](#) approprié.

- Étape 1** Utilisez l'outil de visualisation Web et `FMT-CP-Config-Extractor_v4.0.1-8248` l'outil Check Point pour collecter les configurations des dispositifs Check Point que vous essayez de migrer et enregistrez une copie des fichiers de configuration Check Point.
- Étape 2** Examinez le fichier zip de la configuration de Check Point.

- Étape 3** Déployez l'appareil Série Firepower 2100 dans votre réseau, connectez les interfaces et mettez l'appareil sous tension. Pour plus d'informations, consultez le [Guide de démarrage rapide Cisco Threat Defense pour la série 2100 en utilisant le centre de gestion](#).
- Étape 4** Inscrivez l'appareil Série Firepower 2100 qui sera géré par le centre de gestion. Pour plus d'informations, consultez [Ajouter des appareils au centre de gestion](#).
- Étape 5** (Facultatif) Si votre configuration source Check Point possède des interfaces de liaison, créez des canaux de port (EtherChannels) sur l'appareil cible Série Firepower 2100. Pour plus d'informations, consultez [Configurez des EtherChannels et les interfaces redondantes](#).
- Étape 6** Téléchargez et exécutez la version la plus récente de l'outil de migration Secure Firewall de <https://software.cisco.com/download/home/286306503/type>. Pour en savoir plus, consultez [Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com, à la page 26](#).
- Étape 7** Lorsque vous lancez l'outil de migration Secure Firewall et que vous spécifiez les paramètres de destination, assurez-vous de sélectionner l'appareil Série Firepower 2100 que vous avez enregistré vers le centre de gestion. Pour en savoir plus, consultez [Préciser les paramètres de destination pour l'outil de migration Secure Firewall, à la page 45](#).
- Étape 8** Mappez les ASA les Check Point interfaces avec les interfaces Défense contre les menaces.
- Remarque** L'outil de migration Secure Firewall vous permet de mapper un d'interface Check Point au type Défense contre les menaces d'interface.
- Par exemple, vous pouvez mapper une interface de liaison dans Check Point à une interface physique dans Défense contre les menaces.
- Pour plus d'informations, voir [Mappez les configurations de ,Check Point du pare-feu et de avec les Défense contre les menaces interfaces.](#)
- Étape 9** Lors du mappage des interfaces logiques aux zones de sécurité, cliquez sur **Création automatique** pour permettre à l'outil de migration Secure Firewall de créer de nouvelles zones de sécurité. Pour utiliser les zones de sécurité existantes, mappez manuellement les interfaces logiques de aux zones de sécurité.
- Pour plus d'informations, voir [Associez les interfaces Check Point à des zones de sécurité à des groupes d'interfaces](#).
- Étape 10** Suivez les instructions de ce guide pour examiner et valider de manière séquentielle la configuration à migrer, puis pour pousser la configuration vers le centre de gestion.
- Étape 11** Examinez le rapport post-migration, installez manuellement et déployez les autres configurations vers le Défense contre les menaces et complétez la migration.
- Pour plus de renseignements, consultez la section [Examiner le rapport de post-migration pour Check Point et terminer la migration, à la page 57](#).
- Étape 12** Testez l'appareil Série Firepower 2100 à l'aide du plan de test que vous avez créé lors de la planification de la migration.
-

Tâches de la fenêtre de maintenance

Avant de commencer

Assurez-vous d'avoir complété toutes les tâches devant être effectuées avant la fenêtre d'entretien. Consultez [Tâches de la fenêtre de pré-maintenance](#), à la page 58.

- Étape 1** Connectez-vous à la passerelle de sécurité Check Point via la console Gaia
- Étape 2** Arrêtez les interfaces Check Point de la passerelle de sécurité prévue via la console Gaia.
- Étape 3** (Facultatif) Accédez au centre de gestion et configurez le routage dynamique, les paramètres de plate-forme et les autres fonctions qui ne sont pas migrées par l'outil de migration Secure Firewall et qui sont nécessaires manuellement pour le dispositif Firepower 2100 Series.
- Étape 4** Effacez le cache du protocole de résolution d'adresses (ARP) sur l'infrastructure de commutation environnante
- Étape 5** Effectuez des tests ping de base depuis l'infrastructure de commutation environnante jusqu'aux adresses IP de l'interface de l'appareil Série Firepower 2100, afin de vous assurer qu'elles sont accessibles.
- Étape 6** Effectuez des tests de ping de base à partir d'appareils qui nécessitent un routage de couche 3 vers les adresses IP de l'interface de l'appareil Série Firepower 2100.
- Étape 7** Si vous attribuez une nouvelle adresse IP à l'appareil Série Firepower 2100 et ne réutilisez pas l'adresse IP attribuée à l'appareil Check Point géré par , procédez comme suit :
1. Mettez à jour toutes les routes statiques qui réfèrent aux adresses IP afin qu'elles puissent maintenant pointer vers l'adresse IP de l'appareil Série Firepower 2100.
 2. Si vous utilisez des protocoles de routage, assurez-vous que les voisins voient l'adresse IP de l'appareil Série Firepower 2100 comme le prochain saut vers les destinations attendues.
- Étape 8** Exécutez un plan de test complet et surveillez les journaux dans le cadre de la gestion de centre de gestion pour votre appareil Firepower 2100.
-



CHAPITRE 3

Cisco Success Network - Données de télémétrie

- [Cisco Success Network – Données de télémétrie, à la page 61](#)

Cisco Success Network – Données de télémétrie

Cisco Success Network est une fonctionnalité permanente de collecte d'informations et de mesures d'utilisation de l'outil de migration de pare-feu sécurisé, qui collecte et transmet des statistiques d'utilisation par l'intermédiaire d'une connexion sécurisée dans le nuage entre l'outil de migration et le nuage de Cisco. Ces statistiques nous aident à fournir une assistance supplémentaire sur les fonctionnalités inutilisées et à améliorer nos produits. Lorsque vous lancez un processus de migration dans l'outil de migration de pare-feu sécurisé, le fichier de données de télémétrie correspondant est généré et stocké dans un emplacement fixe.

Lorsque vous poussez la configuration migrée avec FPSCheck Point vers centre de gestion, le service de transfert lit le fichier de données de télémétrie à partir de l'emplacement et le supprime une fois les données téléchargées avec succès dans le nuage.

L'outil de migration offre deux options au choix pour la diffusion en continu des données de télémétrie : **limitée** et **étendue**.

Lorsque **Cisco Success Network** est défini sur **Limitée**, les points de données de télémétrie suivants sont collectés :

Tableau 2 : Télémétrie limitée

Point de données	Description	Exemple de valeur
Durée	L'heure et la date de collecte des données de télémétrie	2023-04-25 10:39:19
Type de source	Le type de périphérique source	ASA
Numéro de modèle de l'appareil	Numéro de modèle de l'ASA	ASA5585-SSP-10, 5969 Mo de RAM, CPU Xeon série 5500 2000 MHz, 1 CPU (4 cœurs)
Version source	Version d'ASA	9.2 (1)
Version de gestion des cibles	La version cible du centre de gestion	6.5 ou plus récent

Point de données	Description	Exemple de valeur
Type de gestion cible	Le type de périphérique de gestion cible, à savoir le centre de gestion	Centre de gestion
Version du périphérique cible	La version du périphérique cible	75
Modèle de l'appareil cible	Le modèle du périphérique cible	Cisco Secure Firewall Threat Defense pour VMware
Version de l'outil de migration	La version de l'outil de migration	1.1.0.1912
État de la migration	L'état de la migration de la configuration ASA vers le centre de gestion	SUCCÈS

Les tableaux suivants fournissent des informations sur les points de données de télémétrie, leurs descriptions et des exemples de valeurs, lorsque **Cisco Success Network** est défini sur **Étendue** :

Tableau 3 : Télémétrie étendue

Point de données	Description	Exemple de valeur
Système d'exploitation	Système d'exploitation qui exécute l'outil de migration de pare-feu sécurisé. Il peut s'agir de Windows7/Windows10 64 bits/macOS High Sierra	Windows 7 :
Navigateur	Navigateur utilisé pour lancer l'outil de migration de pare-feu sécurisé. Il peut s'agir de Mozilla/5.0, de Chrome/68.0.3440.106 ou de Safari/537.36.	Mozilla/5.0

Tableau 4 : Informations sur le point de vérification source

Point de données	Description	Exemple de valeur
Durée	L'heure et la date de collecte des données de télémétrie	2023-04-25 10:39:19
Type de source	Le type de périphérique source	Check Point
Numéro de série du périphérique source	Numéro de série de Check Point	Numéro de série de l'appareil, s'il existe.
Numéro de modèle du périphérique source	Numéro de modèle de Check Point	
Version du périphérique source	Version de Check Point	R77.30
Nombre de configurations sources	Le nombre total de lignes dans la configuration source	504

Point de données	Description	Exemple de valeur
Mode pare-feu	Le mode de pare-feu configuré sur Check Point - routé ou transparent	ROUTAGE
Mode contextuel	Le mode contextuel de Check Point. Il peut s'agir d'un contexte unique ou multiple.	UNIQUE
Statistiques de configuration de point de contrôle :		
Nombre d'ACL	Le nombre d'ACL associées au groupe d'accès	46
Nombre de règles d'accès	Le nombre total de règles d'accès	46
Nombre de règles NAT	Le nombre total de règles NAT	17
Compte d'objets réseau	Le nombre d'objets réseau configurés dans Check Point	34
Nombre de groupes d'objets réseau	Le nombre de groupes d'objets réseau dans Check Point	6
Compte d'objets de port	Le nombre d'objets de port	85
Compte de groupes d'objets de port	Le nombre de groupes d'objets de port	37
Nombre de règles d'accès non prises en charge	Le nombre total de règles d'accès non prises en charge	3
Nombre de règles NAT non prises en charge	Le nombre total de règles d'accès NAT non prises en charge	0
Nombre de règles d'accès basées sur FQDN	Le nombre de règles d'accès basées sur le nom de domaine complet (FQDN)	7
Nombre de règles d'accès basées sur une plage de temps	Le nombre de règles d'accès basées sur une plage de temps	1
Nombre de règles d'accès basées sur SGT	Le nombre de règles d'accès basées sur SGT	0
Résumé des lignes de configuration que l'outil n'est pas en mesure d'analyser		
Nombre de configurations non analysées	Le nombre de lignes de configuration non reconnues par l'analyseur syntaxique	68
Nombre total de règles d'accès non analysées	Le nombre total de règles d'accès non analysées	3

Tableau 5 : Informations sur le périphérique de gestion cible (Centre de gestion)

Point de données	Description	Exemple de valeur
Version de gestion des cibles	La version cible de centre de gestion	6.2.3.3 (build 76)

Point de données	Description	Exemple de valeur
Type de gestion cible	Le type de périphérique de gestion cible, à savoir, centre de gestion	Centre de gestion
Version du périphérique cible	La version du périphérique cible	75
Modèle de l'appareil cible	Le modèle du périphérique cible	Cisco Secure Firewall Threat Defense pour VMware
Version de l'outil de migration	La version de la migration aussi	1.1.0.1912

Tableau 6 : Résumé de la migration

Point de données	Description	Exemple de valeur
Stratégie de contrôle d'accès		
Nom	Le nom de la stratégie de contrôle d'accès	N'existe pas
Nombre de règles d'accès	Le nombre total de règles d'ACL migrées	0
Nombre de règles d'ACL partiellement migrées	Le nombre total de règles d'ACL partiellement migrées	3
Nombre de règles ACP étendu	Le nombre de règles ACP étendues	0
Fonction NAT		
Titre du champ	Le nom de la politique de NAT	N'existe pas
Nombre de règles NAT	Le nombre total de règles NAT migrées	0
Nombre de règles NAT partiellement migrées	Le nombre total de règles NAT partiellement migrées	0
Plus de détails sur la migration...		
Nombre d'interfaces	Le nombre d'interfaces mises à jour	0
Nombre de sous-interfaces	Le nombre de sous-interfaces mises à jour	0
Nombre de routes statiques	Le nombre de routes statiques	0
Nombre d'objets	Le nombre d'objets créés	34
Nombre de groupes d'objet	Le nombre de groupes d'objets créés	6
Nombre de groupes d'interfaces	Le nombre de groupes d'interfaces créés	0
Nombre de zones de sécurité	Le nombre de zones de sécurité créées	3
Nombre d'objets réseau réutilisés	Le nombre d'objets réutilisés	21
Nombre de renommages d'objets réseau	Le nombre d'objets qui sont renommés	1

Point de données	Description	Exemple de valeur
Nombre d'objets de port réutilisés	Le nombre d'objets de port qui sont réutilisés	0
Nombre d'objets de port renommés	Le nombre d'objets de port qui sont renommés	0

Tableau 7 : Données de performance de l'outil de migration de pare-feu sécurisé

Point de données	Description	Exemple de valeur
Temps de conversation	Le temps nécessaire pour analyser Check Point (en minutes)	14
Temps de la migration	Le temps total nécessaire pour la migration de bout en bout (en minutes)	592
Temps de transfert de la configuration	Le temps nécessaire pour transférer la configuration finale (en minutes)	7
État de la migration	L'état de la migration de la configuration Check Point vers centre de gestion	SUCCÈS
Message d'erreur	Le message d'erreur affiché par l'outil de migration de pare-feu sécurisé	null (nul)
Description de l'erreur	La description de l'étape où l'erreur s'est produite et la cause première possible	null (nul)

Fichier d'exemple de point de contrôle de télémétrie pour r77

Voici un exemple de fichier de données de télémétrie sur la migration de la configuration de Check Point vers défense contre les menaces :

```
{
  "metadata": {
    "contentType": "application/json",
    "topic": "migrationtool.telemetry"
  },
  "payload": {
    "Check Point_config_stats": {
      "Ipv6_access_rule_counts": 0,
      "Ipv6_bgp_count": 0,
      "Ipv6_nat_rule_count": 0,
      "Ipv6_network_counts": 24,
      "Ipv6_static_route_counts": 6,
      "access_rules_counts": 63,
      "acl_counts": 63,
      "fqdn_based_access_rule_counts": 0,
      "nat_rule_counts": 0,
      "network_object_counts": 143,
      "network_object_group_counts": 31,
      "no_of_fqdn_based_objects": 0,
      "ospfv3_count": 0,
      "port_object_counts": 370,
      "port_object_group_counts": 55,
      "sgt_based_access_rules_count": 0,
    }
  }
}
```

```

    "timerange_based_access_rule_counts": 0,
    "total_unparsed_access_rule_counts": 0,
    "tunneling_protocol_based_access_rule_counts": 0,
    "unparsed_config_count": 15,
    "unsupported_access_rules_count": 0,
    "unsupported_nat_rule_count": 0
  },
  "context_mode": "SINGLE",
  "error_description": null,
  "error_message": null,
  "firewall_mode": "ROUTED",
  "log_info_acl_count": 0,
  "migration_status": "SUCCESS",
  "migration_summary": {
    "access_control_policy": [
      [
        {
          "access_rule_counts": 63,
          "apply_file_policy_rule_counts": 0,
          "apply_ips_policy_rule_counts": 0,
          "apply_log_rule_counts": 0,
          "do_not_migrate_rule_counts": 0,
          "enable_Global-ACL-Policy": true,
          "enable_Zone-Specific-ACL-Policy": false,
          "enable_hit_count": false,
          "expanded_acp_rule_counts": 1,
          "name": "FTD-Mig-1566804327",
          "partially_migrated_acl_rule_counts": 0,
          "update_rule_action_counts": 0
        }
      ]
    ]
  },
  "interface_counts": 12,
  "interface_group_counts": 0,
  "interface_group_manually_created_counts": 0,
  "nat_Policy": [
    [
      {
        "NAT_rule_counts": 0,
        "do_not_migrate_rule_counts": 0,
        "name": "Doesn't Exist",
        "partially_migrated_nat_rule_counts": 0
      }
    ]
  ],
  "network_object_rename_counts": 0,
  "network_object_reused_counts": 0,
  "object_group_counts": 15,
  "objects_counts": 54,
  "port_object_rename_counts": 0,
  "port_object_reused_counts": 5,
  "security_zone_counts": 13,
  "security_zone_manually_created_counts": 0,
  "static_routes_counts": 22,
  "sub_interface_counts": 11
},
"migration_tool_version": "2.0.3169",
"rule_change_acl_count": 0,
"source_config_counts": 0,
"source_device_model number": "Check Point Model Not Exists",
"source_device_serial_number": null,
"source_device_version": "R77.30",
"source_type": "Check Point",
"system_information": {

```

```

    "browser": "Chrome/76.0.3809.100",
    "operating_system": "Windows NT 10.0; Win64; x64"
  },
  "target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
  "target_device_version": "76",
  "target_management_type": "6.4.0.4 (build 31)",
  "target_management_version": "6.4.0.4 (build 31)",
  "template_version": "1.1",
  "time": "2019-08-26 12:55:40",
  "tool_analytics_data": {
    "objectsplit_100_count": 0
  },
  "tool_performance": {
    "config_push_time": 725,
    "conversion_time": 29,
    "migration_time": 1020
  }
},
"version": "1.0"
}

```

Fichier d'exemple de point de contrôle de télémétrie pour r80

Voici un exemple de fichier de données de télémétrie sur la migration de la configuration de Check Point vers défense contre les menaces :

```

{
  "Check Point_config_stats":{
    "Ipv6_access_rule_counts":0,
    "Ipv6_bgp_count":0,
    "Ipv6_nat_rule_count":0,
    "Ipv6_network_counts":3,
    "Ipv6_static_route_counts":0,
    "access_rules_counts":726,
    "acl_category_count":0,
    "acl_counts":726,
    "fqdn_based_access_rule_counts":0,
    "nat_rule_counts":335,
    "network_object_counts":7645,
    "network_object_group_counts":268,
    "no_of_fqdn_based_objects":0,
    "port_object_counts":1051,
    "port_object_group_counts":66,
    "s2s_vpn_tunnel_counts":0,
    "sgt_based_access_rules_count":0,
    "timerange_based_access_rule_counts":0,
    "total_unparsed_access_rule_counts":0,
    "tunneling_protocol_based_access_rule_counts":0,
    "unparsed_config_count":234,
    "unsupported_access_rules_count":0,
    "unsupported_nat_rule_count":0},
    "context_mode":"SINGLE",
    "error_description":"No data.",
    "error_message":"push failed for object network",
    "firewall_mode":"ROUTED",
    "log_info_acl_count":0,
    "migration_status":"FAIL",
    "migration_summary":{
      "access_control_policy":[
        [
          {
            "access_rule_counts":0,
            "apply_file_policy_rule_counts":0,
            "apply_ips_policy_rule_counts":0,

```

```

        "apply_log_rule_counts":0,
        "do_not_migrate_rule_counts":0,
        "enable_Global-ACL-Policy":true,
        "enable_Zone-Specific-ACL-Policy":false,
        "enable_hit_count":false,
        "expanded_acp_rule_counts":1,
        "name":"Doesn't Exist",
        "partially_migrated_acl_rule_counts":0,
        "total_acl_element_counts":389416,
        "update_rule_action_counts":0
    }
]
],
"interface_counts":11,
"interface_group_counts":0,
"interface_group_manually_created_counts":0,
"nat_Policy":[
[
{
    "NAT_rule_counts":0,
    "do_not_migrate_rule_counts":0,
    "name":"Doesn't Exist",
    "partially_migrated_nat_rule_counts":0
}
]
],
"network_object_rename_counts":0,
"network_object_reused_counts":0,
"object_group_counts":222,"objects_counts":7148,
"port_object_rename_counts":2,
"port_object_reused_counts":30,
"prefilter_control_policy":[
[
{
    "do_not_migrate_rule_counts":0,
    "name":null,
    "partially_migrated_acl_rule_counts":0,
    "prefilter_rule_counts":0
}
]
]
],
"security_zone_counts":11,
"security_zone_manually_created_counts":0,
"static_routes_counts":0,
"sub_interface_counts":8,
"time_out":false},
"migration_tool_version":"2.1.4283",
"mtu_info":{"interface_name":null,
"mtu_value":null},
"rule_change_acl_count":0,
"selective_policy":
{
    "acl":true,
    "acl_policy":true,
    "application":false,
    "csm":false,
"interface":true,
"interface_groups":true,
"migrate_tunneled_routes":false,
"nat":true,
"network_object":true,
"policy_assignment":true,
"populate_sz":false,
"port_object":true,

```



```
"routes":true,
"security_zones":true,
"unreferenced":true},
"source_config_counts":0,
"source_device_model_number":"Check Point Model Not Exists",
"source_device_serial_number":null,
"source_device_version":"R77.30",
"source_type":"Check Point",
"system_information":
{
  "browser":"Chrome/80.0.3987.163","operating_system":
  "Macintosh; Intel Mac OS X 10_15_4",
  "target_device_model":"Cisco Firepower 4110 Threat Defense",
  "target_device_version":"76",
  "target_management_type":"6.5.0 (build 63)",
  "target_management_version":"6.5.0 (build 63)",
  "template_version":"1.1",
  "time":"2020-04-16 04:50:05",
  "tool_analytics_data":{"objectsplit_100_count":6},
  "tool_performance":
  {
    "config_push_time":1457,
    "conversion_time":279,
    "migration_time":2637
  }
}
```




CHAPITRE 4

Dépannage des problèmes de migration

- [Dépannage de l'outil de migration de pare-feu sécurisé, à la page 71](#)
- [Journaux et autres fichiers utilisés pour le dépannage, à la page 72](#)
- [Résolution de problèmes liée aux échecs de chargement des fichiers Check Point, à la page 72](#)

Dépannage de l'outil de migration de pare-feu sécurisé

Une migration échoue généralement lors du Check Point chargement du fichier de configuration de ou lors du transfert de la configuration migrée vers centre de gestion.

Voici certains des scénarios courants où le processus de migration échoue pour une configuration Check Point :

- Fichiers manquants dans le fichier Check Point Config.zip.
- Les fichiers non valides sont détectés par l'outil de migration de pare-feu sécurisé dans le fichier Check Point Cofig.zip
- Si le fichier de configuration de Check Point est d'un type de fichier compressé autre que .zip.

Offre groupée de soutien pour l'outil de migration de pare-feu sécurisé

L'outil de migration Secure Firewall offre la possibilité de télécharger un ensemble d'assistance pour extraire des informations de dépannage précieuses comme les fichiers journaux, la base de données et les fichiers de configuration. Procédez comme suit:

1. Sur l'écran **Migration terminée**, cliquez sur le bouton **Soutien technique**.

La page de soutien technique apparaît.

2. Cochez la case **Offre groupée de soutien**, puis sélectionnez les fichiers de configuration à télécharger.



Remarque Les fichiers journaux et dB sont choisis pour téléchargement par défaut.

3. Cliquez sur **Télécharger**.

Le fichier d'assistance est téléchargé sous la forme d'un fichier .zip dans votre chemin d'accès local. Extrayez le dossier Zip pour voir les fichiers journaux, la base de données et les fichiers de configuration.

4. Cliquez sur **Envoyer** pour envoyer les détails de la panne à l'équipe technique.
Vous pouvez aussi joindre les fichiers d'assistance téléchargés à votre courriel.
5. Cliquez sur **Visiter la page TAC** pour créer une demande TAC dans la page de soutien de Cisco



Remarque Vous pouvez soumettre une demande TAC en tout temps durant la migration à partir de la page de soutien technique.

Journaux et autres fichiers utilisés pour le dépannage

Vous pouvez trouver des informations utiles pour identifier et résoudre les problèmes dans les fichiers suivants.

Fichier	Emplacement
Fichier de journalisation	<migration_tool_folder>\journaux
Rapport pré-migration	<migration_tool_folder>\ressources
Rapport post-migration	<migration_tool_folder>\ressources
fichier non analysé	<migration_tool_folder>\ressources

Résolution de problèmes liée aux échecs de chargement des fichiers Check Point

Si le chargement de votre fichier de configuration Check Point échoue, c'est généralement parce que l'outil de migration Cisco Secure Firewall n'a pas pu analyser une ou plusieurs lignes du fichier.

Vous pouvez trouver des informations sur les erreurs qui ont causé l'échec du chargement et de l'analyse aux emplacements suivants :

- Fichier non analysé : Examinez la fin du fichier pour repérer la dernière ligne ignorée du fichier de configuration de Check Point qui a été analysée avec succès.
- Fichier inattendu : Fichier non valide détecté pour Check Point. Par exemple, lors de la compression à l'aide de Mac OS, les fichiers système Mac sont créés. Supprimez les fichiers Mac.
- (Pour r75 à r77.30 seulement) Fichiers incorrectement nommés : Lorsque les fichiers de la politique de sécurité et ceux de la politique NAT ne sont pas nommés correctement pour Check Point. Renommez correctement les fichiers ACL et NAT.
- Fichiers manquants : Il manque certains fichiers dans le fichier config.zip de Check Point. Ajoutez les fichiers requis.



Remarque Pour r77, extrayez manuellement le fichier de configuration manquant. Pour en savoir plus, consultez [Exporter les fichiers de configuration Check Point pour r77](#) [exporter les fichiers de configuration Check Point pour r77].

Pour r80, utilisez Live Connect pour extraire le fichier de configuration approprié pour l'outil de migration de Cisco Secure Firewall. Pour en savoir plus, consultez [Exporter les fichiers de configuration Check Point pour r80](#) [exporter les fichiers de configuration Check Point pour r80].

Exemple de résolution de problèmes pour Check Point : Impossible de trouver le membre du groupe d'objets (pour les versions r75 à r77.30 seulement)

Dans cet exemple, le chargement et l'analyse du fichier de configuration Check Point ont échoué en raison d'une erreur dans la configuration d'un élément.

Étape 1 Consultez les messages d'erreur pour identifier le problème.

Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	<p>Les fichiers de configuration Check Point ont été analysés et comportent des erreurs.</p> <p>Consultez la section sur les erreurs du Examiner le rapport pré-migration pour connaître les erreurs d'analyse et le Examiner le rapport de post-migration pour Check Point et terminer la migration pour connaître les erreurs de transmission qui sont survenues pendant l'étape de transmission.</p>
Fichier de journalisation	<pre>[ERROR objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;"</pre> <pre>[INFO objectGroupRules] > "Parsing object-group service:[services_gvxs06]"</pre> <pre>[INFO objectGroupRules] > "Parsing object-group service:[services_iphigenia]"</pre> <pre>[INFO objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"</pre>

Étape 2 Ouvrez le fichier Check Point `services.xml`.

Étape 3 Cherchez le groupe d'objets dont le nom est `services_gvxs06`.

Étape 4 Créez le membre manquant pour le groupe d'objets au moyen du tableau de bord intelligent.

Étape 5 Exporter de nouveau le fichier de configuration. Pour en savoir plus, consultez [Exporter les fichiers de configuration Check Point pour r77](#) [exporter les fichiers de configuration Check Point].

Étape 6 S'il n'y a plus d'erreurs, chargez le nouveau fichier de configuration Check Point compressé dans l'outil de migration Cisco Secure Firewall pour poursuivre la migration.

Exemple de résolution de problèmes pour Check Point (r80) concernant Live Connect

Exemple 1 : Demandez des détails sur le gestionnaire de sécurité Check Point.

Dans cet exemple, l'outil de migration Cisco Secure Firewall demande des détails pour le gestionnaire de sécurité Check Point.

Consultez les messages d'erreur pour identifier le problème. Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	Filtrer les demandes de détails pour le gestionnaire de sécurité Check Point.
Fichier de journalisation	[ERREUR connect_cp]> « Unable to extract the Extracted-objects.json file due to credentials with insufficient privileges, time-out issues and so on. Refer Secure Firewall migration tool UG for more info » [impossible d'extraire le fichier Extracted-objects.json en raison des données d'identification ayant des privilèges insuffisants, des délais d'expiration, etc. Consultez le guide de l'utilisateur de l'outil de migration Cisco Secure Firewall pour en savoir plus.] 127.0.0.1 - - [20/Jul/2020 17:20:43] "POST /api/CP/connect HTTP/1.1" 500 -

Vos informations d'authentification sont erronées. Suivez les étapes mentionnées pour préparer les données d'identification. Les données d'identification utilisées doivent avoir un profil Shell */bin/bash* sur Check Point Gaia pour le gestionnaire de sécurité Check Point. Les mêmes données d'identification doivent être repérées sur l'application de console Check Point Smart pour le gestionnaire de sécurité Check Point ayant des privilèges de superutilisateur dans le cadre d'un déploiement normal. Les privilèges doivent être « super utilisateur » si vous utilisez un déploiement multidomaine. Pour en savoir plus, consultez la section [Pré-établisiez les dispositifs Check Point \(r80\) pour l'extraction de la configuration à l'aide de Live Connect](#) [préparer les appareils Check Point (r80) pour l'extraction de la configuration au moyen de Live Connect].

Exemple 2 : Mauvais format de fichier

Dans le présent exemple, l'outil de migration Cisco Secure Firewall est bloqué en raison d'un mauvais format de fichier.

Consultez les messages d'erreur pour identifier le problème. Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	Bloqué

Emplacement	Message d'erreur
Fichier de journalisation	[ERROR cp_device_connection] > "Bad file format" 2020-07-20 17:10:57,347 [ERROR connect_cp] > "Unable to download .tar file". 127.0.0.1 - - [20/Jul/2020 17:10:57] "GET /api/CP/generate_tar_file?package=Standard HTTP/1.1" 500 -

Vos informations d'authentification sont erronées. Suivez les étapes mentionnées pour préparer les données d'identification. Les données d'identification utilisées doivent avoir un profil Shell */bin/bash* sur Check Point Gaia pour le gestionnaire de sécurité Check Point. Les mêmes données d'identification doivent être repérées sur l'application de console Check Point Smart pour le gestionnaire de sécurité Check Point ayant des privilèges de superutilisateur. Les privilèges de super utilisateur doivent être octroyés si vous utilisez un déploiement multidomaine. Pour en savoir plus, consultez la section [Pré-établissee les dispositifs Check Point \(r80\) pour l'extraction de la configuration à l'aide de Live Connect](#) [préparer les appareils Check Point (r80) pour l'extraction de la configuration au moyen de Live Connect].

Exemple 3 : La fonction VSX bloquée n'est PAS prise en charge par Threat Defense

Ici, dans l'exemple, l'outil de migration Cisco Secure Firewall échoue en raison du blocage de la fonction VSX dans la protection contre les menaces.

Consultez les messages d'erreur pour identifier le problème. Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	La fonction VSX bloquée n'est PAS prise en charge par FTD.
Fichier de journalisation	[ERROR config_upload] > "VSX Feature is UNSUPPORTED in FTD" Recherche de la source (appel le plus récent)

Description du problème : Cette erreur se produit, car la commande **fw vsx stat** est obsolète à partir de la version r80.40 de Check Point.

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*.



CHAPITRE 5

FAQ de l'outil de migration Secure Firewall

- [Foire aux questions sur l'outil de migration de pare-feu sécurisé, à la page 77](#)

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 procédez 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 [Procédure pour exporter les fichiers de configuration Check Point pour 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](#)
- 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.