Mise en route de l'outil de migration Secure Firewall

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 : Check Pointdu 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 détaillés 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 filtres 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 filtres 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
	Cette version comprend les nouvelles caractéristiques et améliorations suivantes : **Migration de Cisco Secure Firewall ASA vers Secure Firewall Threat Defense** • 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. **Migration d'un appareil géré par FDM vers Cisco Secure Firewall Threat Defense** • 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. **Migration du pare-feu Check Point vers Cisco Secure Firewall Threat Defense**

Version	Fonctionnalités prises en charge
	• 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**. **Migration de Fortinet Firewall vers Cisco Secure Firewall Threat Defense** • 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	Cette version comprend les nouvelles caractéristiques et améliorations suivantes : • 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. 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. Consultez la rubrique Select the ASA Security Context [sélectionner le contexte de sécurité ASA] pour en savoir plus. • 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	• 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	L'outil de migration Secure Firewall 4.0.3 comprend des corrections de bogues et les nouvelles améliorations suivantes : • 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 *migration du pare-feu de Palo Alto Networks vers Secure Firewall Threat Defense avec le guide de l'outil de* migration pour plus d'informations.

Version	Fonctionnalités prises en charge
4.0.2	L'outil de migration Secure Firewall 4.0.2 inclut les nouvelles caractéristiques et améliorations suivantes : • 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	L'outil de migration Secure Firewall 4.0.1 inclut les nouvelles caractéristiques et améliorations suivantes : • 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 *Migration de Check Point Firewall vers Threat Defense à l'aide de l'outil* de migration.
3.0.1	• 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	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.

Version	Fonctionnalités prises en charge
2.5.2	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-feuCheck Point 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. • ACL dupliquée: la première ACL masque complètement les configurations de la deuxième ACL. **Remarque** L'optimisation est disponible pour le Check Point uniquement pour une action découlant d'une règle ACP. 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 gestionest 7.1 ou ultérieure.

2,2	• 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 versdéfense contre les menaces pour r80 :
	  • Interfaces
	  • Routes statiques
	  • Objets
	  • NAT (Network Address Translation; Translation d'adresses de réseau)
	  • Stratégies de contrôle d'accès
	  • 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.
	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.
	Remarque La recherche d'itinéraires IPv6 pour les règles basées sur les zones n'est pas prise en charge.

Version	Fonctionnalités prises en charge

2.0	• 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 :
	  • Interfaces
	  • Routes statiques
	  • Objets
	  • Politique de contrôle d'accès
	  • 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.
	  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.
	  • NAT (Network Address Translation; Translation d'adresses de réseau)
	• 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 y 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 menacesdoit 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 contenant, 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 tunnellisation
- 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 migrées 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 menacescible avant de débuter 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 Pointvers l'instance autonome ou conteneur suivante des platesdéfense 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 virtuellesl'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 virtuellesdans 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 centre de gestionconnecter au nuage Microsoft Azure ou AWS, puis pour faire migrer la configuration vers le centre de gestionnuage.

Remarque Pour que la migration soit réussie, il est nécessaire de procéder à une mise en scène préalable de centre de gestionou 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 menacesqui 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).

VersionsCentre de gestionprises 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.

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.