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 : du vers Threat defense 2100) inclus dans ce livre aide à faciliter la compréhension du processus de migration.

L'outil de migration Secure Firewall convertit les configurations des des vers une plateforme défense contre des menaces prise en charge. L'outil de migration Secure Firewall vous permet de migrer automatiquement les fonctionnalités et les politiques des ASA avec FPS versdéfense contre des menaces. Vous devez migrer manuellement toutes les caractéristiques non prises en charge.

L'outil de migration Secure Firewall recueille les informations sur les des , les analyse 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 :

- Les items de configuration ASA avec FPS (services de pare-feu) qui sont pleinement migrés, partiellement migrés, non prises en charge pour la migration et ignorés pour la migration.
- lignes de configuration avec erreurs, qui répertorie les CLI que l'outil de migration Secure Firewall ne peut pas reconnaître, ce qui 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 dispositif géré par aux interfaces défense contre des 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 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 Secure Firewall enregistre une copie des **rapports de pré-migration**, des **rapports de post**-migration, avec et des journaux dans le dossier des `ressources`.

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

Fichier non analysé

L'outil de migration Secure Firewall note les informations à propos des lignes de configuration ayant été ignorées dans le fichier non analysé. L'outil de migration Secure Firewall crée ce fichier lorsqu'il analyse le fichier de configuration d'ASA avec FPS.

Vous pouvez trouver le fichier non analysé à l'endroit 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
4.0.2	L'outil de migration Secure Firewall 4.0.2 inclut les nouvelles caractéristiques et améliorations suivantes : • 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 **les Paramètres** > **Envoyer les données de télémétrie à Cisco?** .

Version	Fonctionnalités prises en charge
4.0.1 ou ultérieure	L'outil de migration Secure Firewall 4.0.1 inclut les nouvelles caractéristiques et améliorations suivantes : L'outil de migration Secure Firewall analyse maintenant tous les objets et groupes d'objets selon leur nom et leur configuration et réutilise les objets qui ont le même nom et configuration. Seuls les objets réseaux et les groupes d'objets réseaux sont analysés selon leur nom et configuration antérieure. À noter que les profils XML dans les VPN d'accès à distance sont toujours valides uniquement à l'aide de leur nom.
3.0.2	L'outil de migration Secure Firewall 3.0.2 inclut des corrections de bogues pour la migration de la configuration VPN d'accès à distance Pare-feu ASA avec services FirePOWERà partir des Centre de gestionversions 7.2 ou supérieures.
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 prend en charge :
	
	• Migration VPN de l'accès à distance à partir de Pare-feu ASA avec services FirePOWERsi le centre de gestion de destination est 7.2 ou plus récent. Vous pouvez effectuer la migration VPN AD avec ou sans Secure Firewall Threat Defense. Si vous sélectionnez la migration avec défense contre les menaces, la version de la défense contre les menaces doit être 7.0 ou ultérieure.
	
	• Automatisation de la clé pré-partagée du VPN site à site à partir de Pare-feu ASA avec services FirePOWER.
	
	• Les points suivants doivent être effectués dans le cadre de l'activité pré-migration :
	
	  • Les points de confiance de Pare-feu ASA avec services FirePOWER doivent être migrés manuellement vers le centre de gestion en tant qu'objets PKI.
	
	  • Les paquets AnyConnect, les fichiers Hostscan (Dap.xml, Data.xml, Hostscan Package), les paquets External Browser et les profils AnyConnect doivent être récupérés à partir de la source ASA.
	
	  • Les paquets AnyConnect peuvent être téléversés vers le centre de gestion.
	
	  • Les profils AnyConnect doivent être directement téléversés vers le centre de gestion ou à partir de l'outil de migration Secure Firewall.
	
	  • La commande **ssh scopy enable** doit être activée sur le Pare-feu ASA avec services FirePOWER pour permettre la récupération des profils à partir de l'ASA Live Connect.

Version	Fonctionnalités prises en charge
2.4	

Version	Fonctionnalités prises en charge
	L'outil de migration Secure Firewall prend en charge la migration des configurations des défense contre des menacesservices de pare-feu Cisco (FPS) si la cible centre de gestionet défense contre des menaces est la version 6.5 ou ultérieure. • Migrer ASA avec les règles d'accès FPS en tant centre de gestionque règles de préfiltrage - mappage des règles d'accès vers centre de gestion pour une inspection approfondie sur mesure par le pare-feu. La politique d'accès contient des règles avec des IP et des ports. **Remarque** Vous pouvez utiliser le pré-filtrage et la stratégie de contrôle d'accès pour bloquer ou permettre le trafic. Les règles d'accès à partir de l'ASA sont migrés comme centre de gestiondes règles de pré-filtrage Les règles d'accès à partir des FPS sont migrées dans centre de gestioncomme stratégie de contrôle d'accès • Les ASA avec des règles FPS sont migrés comme suit : Les ACL de redirection de l'ASA vers le FPS sont migrées en tant que règles de préfiltrage (conditionnelles). **Remarque** Vous pouvez migrer les règles FPS en utilisant l'outil de migration Secure Firewall seulement si le module FPS est géré via centre de gestion. • Si l'ACL de redirection de la source a **Action=REFUSER**—migré comme centre de gestionrègle de préfiltre avec **Action=Fastpath**. Aussi, cet ACL particulier est placé comme la première règle ACL dans l'état DÉSACTIVÉ. • Si l'ACL de redirection de la source a la valeur **Action=Permis**, elle ne sera pas migrée par l'outil de migration Secure Firewall. • L'outil de migration Secure Firewall ne prend pas en charge la migration des règles FPS gérées par ASDM dans l'outil de migration Secure Firewall. Par conséquent, vous devez connaître les informations de configuration avant de procéder à la migration en sélectionnant la configuration source (ASA avec FPS). La configuration ASA VPN suivante est une migration vers défense contre des menaces: • VPN basé sur une carte cryptographique (statique/dynamique) à partir de l'ASA • ASA VPN basé sur les routes (VTI) • Migration vers un VPN basé sur des certificats à partir d'ASA **Remarque** • Le point de confiance ou les certificats ASA sont migrés manuellement et font partie de l'activité de pré-migration. • Les points de confiance ASA doivent être migrés en tant centre de gestionqu'objets PKI. Les objets PKI sont utilisés dans l'outil de migration Secure Firewall lors de la création de topologies VPN basées sur des certificats.

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 des menaces correspondantes afin d'enregistrer les appareils défense contre des 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 sont-ils 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 le fichier de configuration du pare-feu

Vous pouvez obtenir un fichier de configuration soit manuellement ou en vous connectant à un en fonction à partir de l'outil de migration Secure Firewall.

La migration du fichier de configuration de l'ASA avec FPS dans l'outil de migration Secure Firewall se fait en deux étapes :

- Vous pouvez importer le fichier de configuration en utilisant la méthode manuelle ou la méthode connexion directe.
- Vous devez importer le fichier de configuration FPS en vous connectant au centre de gestion qui gère le FPS et en choisissant la politique ACL source nécessaire devant être migrée.

Le fichier de configuration que vous devez importer manuellement dans l'outil de migration Secure Firewall doit rencontrer les pré-requis suivants :

- Possède une configuration en cours d'exécution qui est exportée d'un appareil dans une configuration en mode unique ou dans un contexte spécifique d'une configuration en mode contexte multiple. Consultez Exporter le fichier de configuration d'ASA avec FPS.
- Comprend le numéro de version.
- Contient uniquement les configurations CLI de valides.

- Ne contient pas d'erreurs de syntaxe.
- Possède une extension de fichier de `.cfg` ou `.txt`.
- Utilise un encodage de fichier UTF-8
- N'a pas été codé à la main ou modifié manuellement. Si vous modifiez la configuration du pare-feu , nous vous recommandons de tester le fichier de configuration modifié sur l'appareil pare-feu pour vous assurer que sa configuration soit valide.
- Ne contient pas le mot clé « --Plus-- » comme texte.

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 migrer des stratégies partagées vers un centre de gestion en vue d'un déploiement ultérieur vers un dispositif de défense contre les menaces. Pour migrer des stratégies spécifiques à un appareil vers une défense contre les menaces, vous devez l'ajouter au centre de gestion. Lorsque vous planifiez la migration de votre configuration de dispositifs gérés par le vers la défense contre les menaces, tenez compte des exigences et des conditions préalables suivantes :

- 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 de défense contre les menaces natif cible doit avoir au moins un nombre égal d'interfaces physiques de données et de canaux de port utilisées (à l'exclusion des interfaces de gestion uniquement et des sous-interfaces) à celui du ; si ce n'est pas le cas, vous devez ajouter le type d'interface requis sur le dispositif de défense contre les menaces cible. 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 le dispositif de défense contre les menaces cible est une instance de conteneur, il doit au moins disposer d'un nombre égal d'interfaces physiques, de sous-interfaces physiques, d'interfaces de canal de port et de sous-interfaces de canal de port utilisées (à l'exception de "gestion uniquement") à celui du dispositif géré par ; si ce n'est pas le cas, vous devez ajouter le type d'interface requis sur le dispositif de défense contre les menaces cible.

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.

Assistance à la configuration

Configurations prises en charge

L'outil de migration Secure Firewall peut totalement migrer les configurations suivantes :

- Objets et des groupes de réseau
- Objets de service, à l'exception des objets de service configurés pour une source et une destination

Remarque Bien que l'outil de migration de pare-feu sécurisé ne migre pas les objets de service élargis (configurés pour une source et une destination), les règles ACL et NAT référencées sont migrées avec toutes leurs fonctionnalités.

- Groupes d'objets de service, à l'exception des groupes d'objets de service imbriqués

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

- Objets et groupes FQDN IPv4 et IPv6
- Prise en charge de la conversion IPv6 (interface, routes statiques, objets, ACL et NAT)
- Règles d'accès appliquées aux interfaces dans la direction entrante et ACL globales
- NAT automatique, NAT manuel et NAT d'objet (conditionnel)
- Routes statiques, routes ECMP non migrées
- Interfaces physiques
- VLANs secondaires sur les interfaces non migrées vers Défense contre les menaces.
- Sous-interfaces (l'ID de sous-interface est toujours défini sur le même numéro que l'ID de VLAN lors de la migration)
- canaux de port
- Virtual tunnel interface (VTI)
- Groupes de ponts (mode transparent uniquement)
- IP SLA Monitor

  L'outil de migration Cisco Secure Firewall crée des objets IP SLA, mappe les objets avec les routes statiques spécifiques et fait migrer ces objets vers centre de gestion.

  Le moniteur SLA IP définit une stratégie de connectivité à une adresse IP surveillée et suit la disponibilité d'une route vers l'adresse IP. La disponibilité des routes statiques est vérifiée périodiquement en envoyant des demandes d'écho ICMP et en attendant la réponse. Si les demandes d'écho sont dépassées, les routes

statiques sont supprimées de la table de routage et remplacées par une route de secours. Les tâches de surveillance SLA démarrent immédiatement après le déploiement et continuent de s'exécuter à moins que vous ne supprimiez le moniteur SLA de la configuration de l'appareil, c'est-à-dire qu'elles ne vieillissent pas. Les objets du moniteur IP SLA sont utilisés dans le champ Route Tracking d'une stratégie de route statique IPv4. Les routes IPv6 n'ont pas la possibilité d'utiliser le moniteur SLA via le suivi de route.

Remarque IP SLA Monitor n'est pas pris en charge pour les non-flux Défense contre les menaces.

- Recherche groupée d'objets

  L'activation de la recherche de groupe d'objets réduit les besoins en mémoire pour les stratégies de contrôle d'accès qui incluent des objets réseau. Nous vous recommandons d'activer la recherche par groupe d'objets qui permet d'optimiser l'utilisation de la mémoire par la politique d'accès sur Défense contre les menaces.

Remarque

- La recherche de groupe d'objets n'est pas disponible pour la version antérieure à 6.6.centre de gestionDéfense contre les menaces
- La recherche de groupe d'objets ne sera pas prise en charge pour les non-flux et sera désactivée.Défense contre les menaces

- Objets temporels

  Lorsque l'outil de migration Secure Firewall détecte des objets temporels référencés par des règles d'accès, il migre les objets temporels et les associe aux règles d'accès correspondantes. Vérifier les objets contre les règles dans la page **Examiner et valider la configuration**.

  Les objets temporels sont des types de listes d'accès qui autorisent l'accès au réseau sur la base d'une période de temps. Il est utile lorsque vous devez imposer des restrictions au trafic sortant ou entrant en fonction d'une heure particulière de la journée ou de certains jours de la semaine.

Remarque

- Vous devez migrer manuellement la configuration du fuseau horaire du vers le FTD cible
- L'objet temporel n'est pas pris en charge pour les non-flux et sera désactivé.Défense contre les menaces
- Les objets temporels sont pris en charge sur les versions 6.6 et ultérieures.centre de gestion

- Tunnels de réseau privé virtuel (VPN) de site à site
  - VPN site à site - Lorsque l'outil de migration Secure Firewall détecte une configuration de carte cryptographique dans le source, l'outil de migration Secure Firewall migre la carte cryptographique vers le VPN centre de gestion en tant que topologie point à point.
  - VPN basé sur une carte cryptographique (statique/dynamique) à partir de l'ASA

- VPN ASA basé sur les routes (VTI)
- Migration vers un VPN basé sur des certificats à partir d'ASA
- La migration des points de confiance ou des certificats ASA vers le centre de gestiondoit être effectuée manuellement et fait partie de l'activité de pré-migration.

- Objets de routage dynamique, BGP et EIGRP
  - Liste de politiques
  - Liste des préfixes
  - Liste de communautés
  - Chemin du système autonome (AS)

- VPN d’accès à distance
  - Protocoles SSL et IKEv2
  - Méthodes d’authentification : AAA uniquement, certificat client uniquement, SAML, AAA et certificat client
  - AAA - Radius, Local, LDAP et AD.
  - Profils de connexion, stratégies de groupe, Dynamic Access Policy, mappage des attributs LDAP et mappage des certificats
  - ACL standard et élargi
  - Attributs personnalisés de RA VPN et équilibrage de charge VPN
  - Dans le cadre des activités préalables à la migration, effectuez les opérations suivantes:
    - Faites migrer manuellement les points de confiance ASA verscentre de gestion les objets PKI.
    - Récupérez les paquets AnyConnect, les fichiers Hostscan (Dap.xml, Data.xml, Hostscan Package), les paquets External Browser et les profils AnyConnect doivent être récupérés à partir de la source ASA.
    - Chargez tous les packages AnyConnect sur lecentre de gestion.
    - Chargez les profils AnyConnect directement vers centre de gestion ou à partir de l’outil de migration Cisco Secure Firewall.
    - Activez la commande **ssh scopy enable** sur l’ASA pour permettre la récupération des profils à partir de l’ASA Live Connect.

Configurations partiellement prises en charge

L'outil de migration Secure Firewall prend partiellement en charge les configurations suivantes pour migration : Certaines de ces configurations comprennent des règles avec 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.

- Règles de politique de contrôle d'accès configurées avec des paramètres de journalisation avancés, tels que la gravité et l'intervalle de temps.
- Routes statiques qui sont configurées avec l'option de suivi.
- Migration vers un VPN basé sur des certificats.
- Objets de routage dynamique, EIGRP et BGP
    - Route-Carte

Configurations non prises en charge

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

- Règles de politique de contrôle d'accès basées sur SGT
- Objets basés sur SGT
- Règles de politique de contrôle d'accès basées sur l'utilisateur
- Règles NAT configurées avec l'option d'allocation de bloc
- 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

Remarque Prise en charge d'un préfiltre sur l'outil de migration Secure Firewall et centre de gestion 6.5.

- Règles NAT configurées avec SCTP
- Règles NAT configurées avec l'hôte « 0.0.0.0 »
- Route par défaut obtenue par DHCP ou PPPoE avec suivi SLA
- Calendrier du suivi SLA
- Mode de transport IPsec transform-set
- Migration du point de confiance ASA vers centre de gestion
- Les ACL FPS basées sur l'utilisateur ne sont pas prises en charge pour la migration et sont migrées comme désactivées.
- Mode de pare-feu transparent pour BGP

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. L'outil de migration Secure Firewall offre une

caractéristique d'optimisation qui vous permet d'exclure la migration d'objets inutilisés (des objets non référencés dans quelconques ACL ou NAT)

L'outil de migration Secure Firewall traite les objets et règles non supportés comme suit :

- Les objets et règles NAT non supportés ne sont pas migrés.
- Les règles ACL non supportées sont migrées comme des règles désactivés dans le centre de gestion.
- Les ACL sortantes ne sont **pas prises en charge** et ne seront pas migrées verscentre de gestion. Si le pare-feu source a des ACL sortantes, ceci sera signalé dans la section **ignorée** du **rapport pré-migration**.
- Toutes les cartes cryptographiques VPN prises en charge seront migrées en tant quecentre de gestion topologie point à point.
- Les topologies VPN cryptographiques non supportées ou incomplètes ne seront pas migrées.
- Les ACL FPS basées sur l'utilisateur ne sont pas prises en charge pour la migration et sont migrées comme désactivées.

Limites de configuration

La migration de votre configuration source a les limites suivantes :

- L'outil de migration Secure Firewall supporte la migration des contextes de sécurité individuels à partir du en tant qu'appareils séparésDéfense contre les menaces.
- La configuration système n'est pas migrée.
- L'outil de migration Secure Firewall ne supporte pas la migration d'une seule politique ACL qui est appliqué sur **plus** de 50 interfaces. Faites migrer manuellement les politiques ACL étant appliquées à 50 interfaces ou plus.
- Vous ne pouvez pas migrer certaines configurations, par exemple, le routage dynamique vers Défense contre les menaces. Faites migrer manuellement ces configurations.
- Vous ne pouvez pas migrer des appareils en mode routée avec une interface virtuelle de point (BVI), une interface redondante ou une interface tunnelisée. Par contre, vous pouvez migrer des appareils en mode transparent avec le BVI.
- Les groupes d'objets de service imbriqués ou les groupes de ports ne sont pas pris en charge sur 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 Secure Firewall divise l'objet ou les groupes de service étendus avec la source et les ports de destination qui se trouvent sur une ligne en différents objets sur plusieurs lignes. Les références à de telles règles de contrôle d'accès sont converties en centre de gestionrègles avec la même signification.
- Si la configuration source à des règles de contrôle d'accès qui ne réfèrent pas à des protocoles de tunnelage spécifique (comme GRE, IP-dans-IP et IP6-dans-IP), mais que ces règles correspondent à un trafic de tunnelage non crypté sur le , alors, en migration vers le Défense contre les menaces, les règles correspondantes ne se comporteront pas de la même manière qu'elles le font sur le . Nous vous conseillons de créer des règles de tunnelage spécifique pour celles-ci dans la politique Préfiltrage, sur le Défense contre les menaces.
- Les cartes cryptographiques supportées sont migrées comme topologie point par point.

- Si un objet AS-Path portant le même nom apparaîtcentre de gestion, la migration s'arrête avec le message d'erreur suivant :

  « Conflit de noms d'objets AS-Path détecté dans centre de gestion, veuillez résoudre le conflit dans centre de gestion pour continuer »

- La redistribution d'OSPF et du protocole d'information de routage (RIP) vers EIGRP n'est pas supportée.

Limites pour la migration AD VPN

La migration d'accès à distance VPN est supporté avec les limites suivantes :

- La migration des paramètres SSL n'est pas prise en charge en raison des limitations de l'API.
- Le serveur LDAP est migré avec le type de chiffrement « aucun ».
- DfltGrpPolicy n'est pas migré puisque la politique n'est pas applicable pour tout le centre de gestion. Vous pouvez faire les changements nécessaires directement sur le centre de gestion.
- Pour un serveur radius, si l'autorisation dynamique est activée, la connectivité du serveur AAA doit être assurée par une interface et non par le routage dynamique. Si Pare-feu ASA avec services FirePOWERune configuration est trouvée avec un serveur AAA dont l'autorisation dynamique est activée sans interface, l'outil de migration Secure Firewall ignore l'autorisation dynamique. Vous devez activer manuellement l'autorisation dynamique après avoir choisi une interface dans le centre de gestion.
- La configuration de Pare-feu ASA avec services FirePOWERpeut avoir une interface tout en appelant l'ensemble des adresses sous le groupe tunnel. Mais la même chose n'est pas supportée dans le centre de gestion. Si une interface est détectée dans la configuration Pare-feu ASA avec services FirePOWER, elle est ignorée par l'outil de migration Secure Firewall et l'ensemble des adresses est migré sans l'interface.
- Pare-feu ASA avec services FirePOWER peut avoir un mot-clé **link-selection/subnet-selection** pour le serveur dhcp sous le groupe de tunnels. Mais la même chose n'est pas supportée dans le centre de gestion. Si un serveur dhcp est détectée dans la configuration Pare-feu ASA avec services FirePOWERavec ces mots-clés, cela est ignoré par l'outil de migration Secure Firewall et le serveur dhcp est transféré sans les mots-clés
- La configuration Pare-feu ASA avec services FirePOWERpeut avoir une interface tout en appelant le groupe de serveurs d'authentification, le groupe de serveurs d'authentification secondaire, le groupe de serveurs d'autorisation sous le groupe de tunnels. Mais la même chose n'est pas supportée dans le centre de gestion. Si une interface est détectée dans la configuration Pare-feu ASA avec services FirePOWER, elle est ignorée par l'outil de migration Secure Firewall et les commandes sont transférés sans l'interface.
- La configuration Pare-feu ASA avec services FirePOWERn'associe pas Redirect ACL à un serveur radius. Donc, il est impossible de le récupérer à partir de l'outil de migration Secure Firewall. Si rediriger l'ACL est utilisé dans Pare-feu ASA avec services FirePOWER, cela est donc laissé vide et vous devez ajouter et l'associer manuellement dans le centre de gestion.
- Pare-feu ASA avec services FirePOWER supporte une valeur de 0 - 720 pour le délai de réutilisation locale de vpn-addr-assign. Mais le centre de gestion supporte une valeur de 0 - 480. Si une valeur plus haute que 480 est trouvée dans la configuration de Pare-feu ASA avec services FirePOWER, elle est réglée à la valeur supportée maximum de 480 dans le centre de gestion.
- La configuration de l'ensemble IPv4 et des paramètres DHCP useSecondaryUsernameforSession dans le profil de connexion n'est pas prise en charge en raison de problèmes d'API.

- L'option de contournement du contrôle d'accès sysopt permit-vpn n'est pas activée dans le cadre de la politique AD VPN. Par contre, si nécessaire, vous pouvez l'activer à partir du centre de gestion.
- Les valeurs du module client AnyConnect et du profil peuvent être mises à jour dans le cadre de la stratégie de groupe uniquement lorsque les profils sont téléchargés depuis l'outil de migration Secure Firewall vers le centre de gestion.
- Vous devez associer les certificats directement dans le centre de gestion.
- Les paramètres IKEv2 ne sont pas migrés par défaut. Vous devez les ajouter dans le centre de gestion.

Lignes directrices pour la migration des services de pare-feu (FPS)

L'outil de migration Secure Firewall utilise les meilleures pratiques pour les configurations de Défense contre les menaces, incluant ceci :

- La migration de l'option de journalisation ACL suit les meilleures pratiques pour Défense contre les menaces. L'option de journalisation pour une règle est activée ou désactivée selon la configuration de la source. Pour les règles dont l'action est le **refus**, l'outil de migration 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.
- L'ASA avec les règles FPS est migrée comme suit :

  Les ACL de redirection pour ASA avec FPS sont migrés comme des règles de préfiltrage (conditionnelles)

Remarque Vous pouvez migrer les règles FPS en utilisant l'outil de migration Secure Firewall seulement si le module FPS est géré via centre de gestion.

  - Si l'ACL de redirection de la source a **Action=REFUSER**—migré comme centre de gestionrègle de préfiltre avec **Action=Fastpath**. Aussi, cet ACL particulier est placé comme la première règle ACL dans l'état DÉSACTIVÉ.
  - Si l'ACL de redirection de la source a la valeur **Action=Permis**, elle ne sera pas migrée par l'outil de migration Secure Firewall.

Lignes directrices pour la migration d'objets

et défense contre les menaces ont des lignes directrices de configuration différentes pour les objets. Par exemple, un ou plusieurs objets peuvent avoir le même nom dans avec un nom d'objet en minuscule et l'autre nom d'objet en majuscule, mais chaque objet doit avoir un nom unique, peu importe le scénario dans défense contre les menaces Pour accommoder de telles différences, l'outil de migration Secure Firewall analyse tous les objets et s'occupe de leur migration d'une des manières suivantes :

- Chaque objet a un nom et une configuration unique — L'outil de migration Secure Firewall migre les objets avec succès sans changements.
- Le nom d'un objet inclut un ou plusieurs caractères spéciaux qui ne sont pas supportés par le centre de gestion— L'outil de migration Secure Firewall renomme les caractères spéciaux dans le nom de l'objet avec un caractère « _ » pour rencontrer le critère de dénomination d'objets du centre de gestion.

- Un objet a le même nom et configuration qu'un objet existant dans le centre de gestion— L'outil de migration Cisco Secure Firewall Management CenterSecure Firewall réutilise l'objet pour la Cisco Secure Firewall Threat Defenseconfiguration et ne migre pas l'objet.
- Un objet a le même nom mais une configuration différente d'un objet existant dans Cisco Secure Firewall Management Center— L'outil de migration Secure Firewall rapporte un conflit d'objet et vous permet de résoudre le conflit en ajoutant un suffixe unique au nom de l'objet pour des besoins de migration.
- De multiples objets ont le même nom mais dans des scénarios différents — L'outil de migration Secure Firewall renomme de tels objets pour rencontrer le Cisco Secure Firewall Threat Defensecritère de dénomination de l'objet

Important L'outil de migration Secure Firewall analyse le nom et la configuration de tous les objets et groupes d'objets. Par contre, les profils XML dans les configurations VPN d'accès à distance sont analysés uniquement par le nom.

Remarque L'outil de migration Secure Firewall prend en charge la migration d'objets de masques de réseau discontigus (masques Wildcard) si le Centre de gestion du pare-feu de destination est la version 7.1 ou une version ultérieure.

```
ASA example:
object network wildcard2
subnet 2.0.0.2 255.0.0.255
```

Lignes directrices et limites relatives aux Défense contre les menacesappareils

Lorsque vous prévoyez de migrer votre configuration ASA avec FPSvers défense contre des menaces, tenez compte des lignes directrices et des limitations suivantes :

- S'il existe des configurations spécifiques à l'appareil, telles que défense contre des menaces des routes, des interfaces, etc., lors de la migration push, l'outil de migration Secure Firewall nettoie automatiquement l'appareil et remplace la configuration ASA par la configuration FPS.

Remarque Afin de prévenir toute perte indésirable de données de l'appareil (cible défense contre des 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 Secure Firewall peut créer des sous-interfaces sur l'instance native de défense contre des menacesl'appareil en fonction de la configuration de l'ASA avec FPS. Créez manuellement des interfaces et de interfaces défense contre des menacesde canaux de port sur l'appareil cible avant de débuter la migration. Par exemple, si votre configuration ASA avec FPS est affectée aux interfaces et canaux de port suivants, vous devez les créer sur le dispositif défense contre des menaces cible avant la migration :

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

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

- L'outil de migration Secure Firewall peut créer des sous-interfaces et des interfaces virtuelles Bridge-Group (mode transparent) sur défense contre des menacesl'instance native du dispositif basé sur ASA avec FPS. Créez manuellement des interfaces et de interfaces défense contre des menacesde canaux de port sur l'appareil cible avant de débuter la migration. Par exemple, si votre configuration ASA avec FPS est affectée aux interfaces et canaux de port suivants, vous devez les créer sur le dispositif défense contre des 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 des 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 des menacessuivantes sont pris en charge pour la migration avec l'outil de migration Cisco Secure Firewall : Pour plus d'informations sur les plateformes défense contre des menaces prises en charge, consultez le Guide de compatibilité de Cisco Secure Firewall.

Remarque L'outil de migration de Cisco Secure Firewall prend en charge la migration des périphériques ASA autonomes avec FPS vers un périphérique défense contre des menaces autonome uniquement.

Modèles ASA source pris en charge pour ASA avec migration FPS:

Le module Cisco ASA FirePOWER est déployé sur les périphériques suivants:

- ASA5506-X
- ASA5506H-X
- ASA5506W-X

- ASA5508-X
- ASA 5512-X
- ASA 5515-X
- ASA5516-X
- ASA5525-X
- ASA5545-X
- ASA 5555-X
- ASA5585-X-SSP-10
- ASA5585-X-SSP-20
- ASA5585-X-SSP-40
- ASA5585-X-SSP-60

Plateformes Défense contre les menaces cibles prises en charge

Vous pouvez utiliser l'outil de migration Secure Firewall pour migrer une source ASA avec une configuration FPS vers l'instance autonome ou conteneur suivante des platesdéfense contre des menaces-formes :

- Firepower de Série 1000
- Série Firepower 2100
- Secure Firewall de Série 3100
- Firepower de série 4100
- 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 virtuelle contre les menacesl'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 virtuelle contre les menacesdans 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 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 tous les dispositifs hébergés dans le nuage pour 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 20.
- Vous avez obtenu et installé des licences intelligentes défense contre des menacesqui incluent toutes les fonctionnalités que vous prévoyez de migrer depuis l'interface ASA avec FPS, 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

Astuces Sur l'interface web centre de gestion, naviguez vers. **Configuration du** > **système** > **Préférences Rest API** > **Activer Rest API**et cocher la case **Activer Rest API**.

- Vous avez créé un utilisateur dédié avec des privilèges REST centre de gestionAPI pour l'outil de migration Secure Firewall, comme décrit dans Comptes d'utilisateur pour l'accès à la gestion .

Versions logicielles prises en charge pour la migration

Les outils de migration Secure Firewall, ASA avec dispositif FDS et les versions défense contre des menacespour 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.

ASA pris en charge avec les versions FPS

L'outil de migration Cisco Secure Firewall prend en charge la migration à partir d'un périphérique qui exécute ASA avec le logiciel FPS version 9.2.2 et ultérieure.

Pour plus de détails, consultez la section Compatibilité du module ASA FirePOWER dans le guide de compatibilité Cisco ASA.

Versions Centre de gestion prises en charge pour la source ASA avec configuration FPS

Pour les ASA avec FPS, le Outil de migration de pare-feu prend en charge la migration vers un appareilDéfense contre les menaces géré parcentre de gestion qui utilise la version 6.5+.

Versions Défense contre les menaces prises en charge

L'outil de migration Secure Firewall recommande de migrer vers un appareil fonctionnant défense contre des menacesavec 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 des 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.