



Migration de pare-feu ASA avec les services FirePOWER (FPS) vers Firewall Threat Defense avec l'outil de migration

Première publication : 2022-11-14

Dernière modification : 2023-07-27

Americas Headquarters

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

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

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

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

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

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

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

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

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

© 2022 Cisco Systems, Inc. Tous droits réservés.



TABLE DES MATIÈRES

CHAPITRE 1

Mise en route de l'outil de migration Secure Firewall	1
À propos de l'outil de migration Secure Firewall	1
Quoi de neuf dans l'outil de migration Secure Firewall	3
Licence pour l'outil de migration Secure Firewall	7
Configuration requise pour l'outil de migration Cisco Secure Firewall	7
Exigences et conditions préalables pour le fichier de configuration du pare-feu	7
Exigences et conditions préalables pour les appareils Threat Defense	8
Assistance à la configuration	9
Lignes directrices et limites relatives à la licence	12
Plateformes prises en charge pour la migration	17
Centre de gestion des cibles pour la migration pris en charge	19
Versions logicielles prises en charge pour la migration	20

CHAPITRE 2

Flux de travail de migration ASA avec FPS vers Threat Defense	21
Procédure de bout en bout	21
Préalables pour la migration	23
Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com	23
Obtenir le fichier de configuration d'ASA avec FPS	24
Exporter le fichier de configuration d'ASA avec FPS	24
Exporter le certificat PKI à partir d'ASA avec services FirePOWER et l'importer dans le centre de gestion	25
Récupérer les paquets et les profils AnyConnect	26
Exécuter la migration	26
Lancer l'outil de migration Secure Firewall	26
Téléverser ASA avec le fichier de configuration FPS	28
Se connecter à l'ASA à partir de l'outil de migration de pare-feu sécurisé	29

Préciser les paramètres de destination pour l'outil de migration de pare-feu sécurisé	31
Groupement en ligne	35
Examiner le rapport pré-migration	37
Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager	38
Mapper les interfaces ASA à des zones de sécurité et à des groupes d'interfaces	39
Optimiser, examiner et valider la configuration	41
Transférer la configuration migrée vers Centre de gestion	46
Examiner le rapport de post-migration et terminer la migration	48
Désinstaller l'outil de migration Secure Firewall	51
Exemple de migration : ASA avec vers Threat Defense 2100	52
Tâches de la fenêtre de pré-maintenance	52
Tâches de la fenêtre de maintenance	53
<hr/>	
CHAPITRE 3	Cisco Success Network - Données de télémétrie 55
	Cisco Success Network – Données de télémétrie 55
<hr/>	
CHAPITRE 4	Dépannage des problèmes de migration 63
	Dépannage de l'outil de migration de pare-feu sécurisé 63
	Journaux et autres fichiers utilisés pour le dépannage 64
	Dépannage de l'ASA avec les échecs de chargement de fichier FPS 64
<hr/>	
CHAPITRE 5	FAQ de l'outil de migration Secure Firewall 65
	Foire aux questions sur l'outil de migration de pare-feu sécurisé 65



CHAPITRE 1

Mise en route de l'outil de migration Secure Firewall

- À propos de l'outil de migration Secure Firewall, à la page 1
- Quoi de neuf dans l'outil de migration Secure Firewall, à la page 3
- Licence pour l'outil de migration Secure Firewall, à la page 7
- Configuration requise pour l'outil de migration Cisco Secure Firewall, à la page 7
- Exigences et conditions préalables pour le fichier de configuration du pare-feu, à la page 7
- Exigences et conditions préalables pour les appareils Threat Defense, à la page 8
- Assistance à la configuration, à la page 9
- Lignes directrices et limites relatives à la licence, à la page 12
- Plateformes prises en charge pour la migration, à la page 17
- Centre de gestion des cibles pour la migration pris en charge, à la page 19
- Versions logicielles prises en charge pour la migration, à la page 20

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 : ASA avec 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 vers défense 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 détaillées sur la progression de chaque étape dans l'outil de migration Secure Firewall. Le contenu de la console est aussi écrit dans le fichier journal de l'outil de migration Secure Firewall.

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



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

Journaux

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

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

```
<migration_tool_folder>\logs
```

Ressources

L'outil de migration 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 filtre les rangées de tableaux et affiche celles contenant le terme recherché.

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

Ports

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

```
<migration_tool_folder>\app_config.txt.
```



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

Cisco Success Network (Réseau de succès Cisco)

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

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

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

Quoi de neuf dans l'outil de migration Secure Firewall

Version	Fonctionnalités prises en charge
4.0.2	<p>L'outil de migration Secure Firewall 4.0.2 inclut les nouvelles caractéristiques et améliorations suivantes :</p> <ul style="list-style-type: none"> • 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	<p>L'outil de migration Secure Firewall 4.0.1 inclut les nouvelles caractéristiques et améliorations suivantes :</p> <p>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.</p>
3.0.2	<p>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 FirePOWER à partir des Centre de gestion versions 7.2 ou supérieures.</p>
3.0.1	<ul style="list-style-type: none"> • Pour ASA avec FirePOWER Services, Check Point, Palo Alto Networks et Fortinet, Secure Firewall Série 3100 n'est pris en charge qu'en tant que dispositif de destination.
3.0	<p>L'outil de migration Secure Firewall 3.0 prend en charge :</p> <ul style="list-style-type: none"> • Migration VPN de l'accès à distance à partir de Pare-feu ASA avec services FirePOWER si 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 : <ul style="list-style-type: none"> • 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
	<p>L'outil de migration Secure Firewall prend en charge la migration des configurations des défenses contre des menaces services de pare-feu Cisco (FPS) si la cible centre de gestion et défense contre des menaces est la version 6.5 ou ultérieure.</p> <ul style="list-style-type: none"> Migrer ASA avec les règles d'accès FPS en tant que centre de gestion que 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. <p>Remarque Vous pouvez utiliser le pré-filtrage et la stratégie de contrôle d'accès pour bloquer ou permettre le trafic.</p> <p>Les règles d'accès à partir de l'ASA sont migrées comme centre de gestion des règles de pré-filtrage. Les règles d'accès à partir des FPS sont migrées dans le centre de gestion comme stratégie de contrôle d'accès.</p> <ul style="list-style-type: none"> Les ASA avec des règles FPS sont migrés comme suit : <p>Les ACL de redirection de l'ASA vers le FPS sont migrées en tant que règles de préfiltrage (conditionnelles).</p> <p>Remarque Vous pouvez migrer les règles FPS en utilisant l'outil de migration Secure Firewall seulement si le module FPS est géré via le centre de gestion.</p> <ul style="list-style-type: none"> Si l'ACL de redirection de la source a Action=REFUSER—migré comme centre de gestion règle de préfiltrage 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. <ul style="list-style-type: none"> 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). <p>La configuration ASA VPN suivante est une migration vers la défense contre des menaces:</p> <ul style="list-style-type: none"> 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 de l'ASA <p>Remarque</p> <ul style="list-style-type: none"> 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 que centre de gestion qu'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, à la page 24](#).
- 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 gestion Défense 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 gestion doit 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 vers centre 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 le centre 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 tunnellation



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 vers centre 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 que centre 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 séparés Défense 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 gestion règles avec la même signification.
- Si la configuration source a 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 apparaît dans le centre de gestion, la migration s'arrête avec le message d'erreur suivant :
« Conflit de noms d'objets AS-Path détecté dans le centre de gestion, veuillez résoudre le conflit dans le 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 supportée 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 FirePOWER une 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 FirePOWER peut 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 détecté dans la configuration Pare-feu ASA avec services FirePOWER avec 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 FirePOWER peut 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 transférées sans l'interface.
- La configuration Pare-feu ASA avec services FirePOWER n'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 Center Secure Firewall réutilise l'objet pour la Cisco Secure Firewall Threat Defense configuration 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 Defense critère 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 discontinus (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 menaces appareils

Lorsque vous prévoyez de migrer votre configuration ASA avec FPS vers 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 menaces l'appareil en fonction de la configuration de l'ASA avec FPS. Créez manuellement des interfaces et de interfaces défense contre des menaces de canaux de port sur l'appareil cible avant de débiter 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 de 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.

- L'outil de migration Secure Firewall peut créer des sous-interfaces et des interfaces virtuelles Bridge-Group (mode transparent) sur défense contre des menaces l'instance native du dispositif basé sur ASA avec FPS. Créez manuellement des interfaces et de interfaces de défense contre des menaces de canaux de port sur l'appareil cible avant de débiter 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 de 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 de 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 de défense contre des menaces suivantes sont prises en charge pour la migration avec l'outil de migration Cisco Secure Firewall : Pour plus d'informations sur les plateformes de 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 de 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 plates-défense 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 menaces l'installation dans Azure, voir la section [Prise en main de Secure Firewall Threat Defense Virtual](#) et Azure.
- Pour les prérequis et la mise en place préalable de défense virtuelle contre les menaces dans AWS Cloud, voir les [prérequis virtuels de Threat Defense](#).

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



Remarque

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



Remarque

L'outil de migration Secure Firewall nécessite une connectivité réseau à tous les dispositifs hébergés dans le nuage pour migrer la configuration téléchargée manuellement vers le 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 de défense contre des menaces qui 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 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.

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 appareil Défense contre les menaces géré par centre 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 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 des menaces, voir le [Guide de compatibilité du pare-feu Cisco](#).



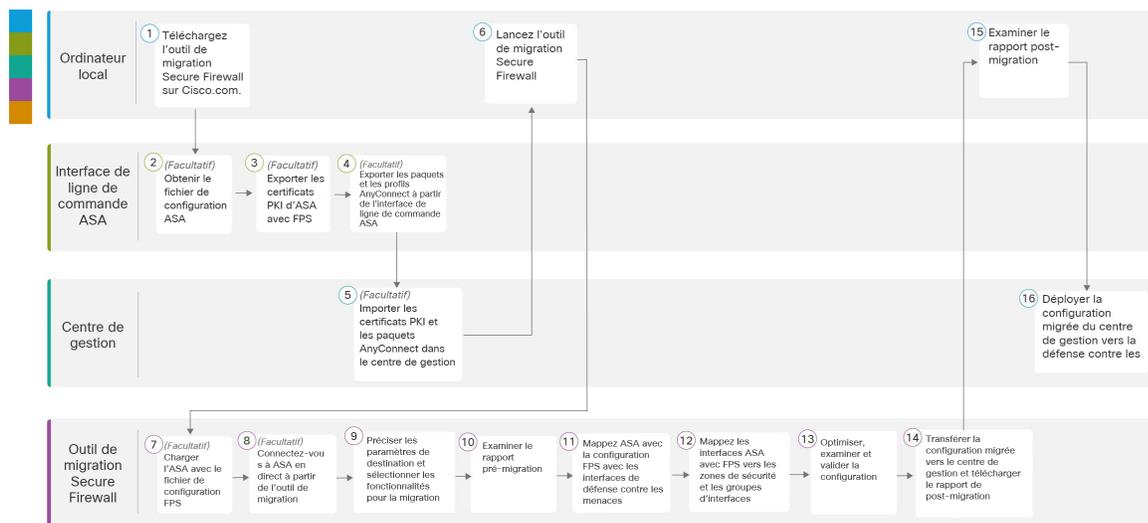
CHAPITRE 2

Flux de travail de migration ASA avec FPS vers Threat Defense

- Procédure de bout en bout, à la page 21
- Préalables pour la migration, à la page 23
- Exécuter la migration, à la page 26
- Désinstaller l'outil de migration Secure Firewall, à la page 51
- Exemple de migration : ASA avec vers Threat Defense 2100 , à la page 52

Procédure de bout en bout

L'organigramme suivant illustre le flux de travail de migration d'un ASA avec FPS vers la protection contre les menaces à l'aide de l'outil de migration de pare-feu sécurisé.



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

	Espace de travail	Étapes
2	Interface de ligne de commande ASA	(Facultatif) Obtenez le fichier de configuration ASA avec FPS : pour obtenir le fichier de configuration ASA avec FPS à partir de l'interface de ligne de commande ASA, consultez Obtenir le fichier de configuration ASA . Obtenir le fichier de configuration d'ASA avec FPS, à la page 24 Si vous avez l'intention de connecter l'ASA à partir de l'outil de migration Secure Firewall, sautez à l'étape 3.
3	Interface de ligne de commande ASA	(Facultatif) Exporter les certificats PKI à partir du CLI ASA : cette étape n'est requise que si vous prévoyez de migrer les fonctions VPN site à site et VPN RA de l'ASA vers la défense contre les menaces. Pour exporter les certificats PKI à partir de l'ASA CLI, voir Exporter le certificat PKI à partir d' Pare-feu ASA avec services FirePOWER et l'importer dans le centre de gestion . Si vous ne prévoyez pas de migrer le VPN site à site et l'AD VPN, passez à l'étape 7.
4	Interface de ligne de commande ASA	(Facultatif) Exportez les paquets et les profils AnyConnect à partir de l'interface de ligne de commande ASA : cette étape n'est requise que si vous envisagez de migrer les fonctionnalités AD VPN d'ASA avec FPS vers la défense contre les menaces. Pour exporter les paquets et profils AnyConnect à partir de l'ASA CLI, voir Récupérer les paquets et les profils AnyConnect . Si vous ne prévoyez pas de migrer le VPN site à site et l'AD VPN, passez à l'étape 7.
5	Centre de gestion	(Facultatif) Importez les certificats PKI et les paquets Anyconnect dans le centre de gestion : pour importer les certificats PKI dans le centre de gestion, reportez-vous aux sections Exporter le certificat PKI et importer dans le centre de gestion du pare-feu, étape 2 , et Récupérer les paquets et les profils AnyConnect, étape 2 . Exporter le certificat PKI à partir d' Pare-feu ASA avec services FirePOWER et l'importer dans le centre de gestion, à la page 25 Récupérer les paquets et les profils AnyConnect, à la page 26
6	Ordinateur local	Lancez l'outil de migration Secure Firewall sur votre machine locale, voir Lancer l'outil de migration Secure Firewall .
7	Outil de migration Secure Firewall	(Facultatif) Téléversez l'ASA avec le fichier de configuration FPS obtenu à partir de l'interface de ligne de commande de l'ASA. Téléverser ASA avec le fichier de configuration FPS Si vous prévoyez de vous connecter à l'ASA en direct avec FPS, passez à l'étape 8.
8	Outil de migration Secure Firewall	Vous pouvez vous connecter à ASA en direct avec FPS directement à partir de l'outil de migration de pare-feu sécurisé. Pour plus d'informations, consultez Connexion à l'ASA avec FPS à partir de l'outil de migration de pare-feu sécurisé . Se connecter à l'ASA à partir de l'outil de migration de pare-feu sécurisé, à la page 29
9	Outil de migration Secure Firewall	Durant cette étape, vous pouvez spécifier les paramètres de destination pour la migration. Pour les étapes détaillées, référez-vous à Préciser les paramètres de destination pour l'outil de migration de pare-feu sécurisé .

	Espace de travail	Étapes
10	Outil de migration Secure Firewall	Accédez à l'endroit où vous avez téléchargé le rapport de postmigration et examinez le rapport. Pour les étapes détaillées, référez-vous à Examiner le rapport pré-migration
11	Outil de migration Secure Firewall	L'outil de migration de pare-feu sécurisé vous permet de mapper l'ASA avec la configuration du FPS avec les interfaces de défense contre les menaces. Pour connaître les étapes détaillées, consultez Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager
12	Outil de migration Secure Firewall	Pour vous assurer que la configuration ASA avec FPS est migrée correctement, mappez les interfaces ASA avec FPS aux objets d'interface de défense contre les menaces, aux zones de sécurité et aux groupes d'interfaces appropriés. Pour connaître les étapes détaillées, reportez-vous à Mappage d'ASA avec des interfaces FPS vers des zones de sécurité et des groupes d'interfaces. Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager, à la page 38
13	Outil de migration Secure Firewall	Optimisez et examinez soigneusement la configuration et vérifiez qu'elle est correcte et qu'elle correspond à la façon dont vous souhaitez configurer le dispositif de défense contre les menaces. Pour les étapes détaillées, référez-vous à Optimiser, examiner et valider la configuration .
14	Outil de migration Secure Firewall	Cette étape dans le processus de migration envoie la configuration migrée au centre de gestion et vous permet de télécharger le rapport de post-migration. Pour les étapes détaillées, référez-vous à Transférer la configuration migrée vers Centre de gestion .
15	Ordinateur local	Accédez à l'endroit où vous avez téléchargé le rapport de post-migration et examinez le rapport. Pour les étapes détaillées, référez-vous à Examiner le rapport de post-migration et terminer la migration .
16	Centre de gestion	Déployer la configuration migrée du centre de gestion vers la défense contre les menaces. Pour les étapes détaillées, référez-vous à Examiner le rapport de post-migration et terminer la migration .

Préalables pour la migration

Avant de migrer la configuration de votre dispositif ASA avec FPS géré par , exécutez les activités suivantes :

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

Avant de commencer

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

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

Obtenir le fichier de configuration d'ASA avec FPS

Vous pouvez utiliser une des méthodes suivantes pour obtenir un fichier de configuration :

- [Exporter le fichier de configuration d'ASA avec FPS, à la page 24](#)
- [Se connecter à l'ASA à partir de l'outil de migration de pare-feu sécurisé, à la page 29](#)

Exporter le fichier de configuration d'ASA avec FPS

Cette tâche n'est requise uniquement que si vous voulez téléverser manuellement un fichier de configuration. Si vous voulez vous connecter à un à partir de l'outil de migration Secure Firewall, passez à [Se connecter à l'ASA à partir de l'outil de migration de pare-feu sécurisé, à la page 29](#).



Remarque

Ne pas coder à la main ou apporter des modifications à la configuration après avoir exporté le fichier. Ces changements ne seront pas migrés vers défense contre les menaces et ils créeront des erreurs dans la migration ou causeront son échec. Par exemple, ouvrir et sauvegarder le fichier de configuration dans le terminal peut ajouter un espace blanc ou des lignes vides que l'outil de migration Secure Firewall ne peut pas analyser.

Assurez-vous que le fichier de configuration exporté ne contient pas le mot-clé "--More--" en tant que texte, car cela peut faire échouer la migration.

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 ASA 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 des pare-feux qui gère le FPS et en sélectionnant la politique ACL source requise qui doit être migrée.

-
- Étape 1** Utilisez la commande **show running-config** pour le dispositif ASA ou le contexte que vous migrez et copiez la configuration à partir de là. Voir [Afficher la configuration en cours d'exécution](#).
- Vous pouvez également utiliser Adaptive Security Device Manager (ASDM) pour le dispositif ADA ou le contexte que vous souhaitez migrer et choisir **Fichier > Afficher la configuration en cours d'exécution dans une nouvelle fenêtre** pour obtenir le fichier de configuration.
- Remarque** Pour un multi-contexte, vous pouvez utiliser la commande **show tech-support** pour obtenir la configuration de tous les contextes dans un seul fichier.
- Étape 2** Sauvegardez la configuration soit comme `.cfg` ou `.txt`.
- Vous ne pouvez pas téléverser la configuration vers l'outil de migration Secure Firewall si elle a une extension différente.
- Étape 3** Transférez le fichier de configuration vers votre ordinateur où vous avez téléchargé l'outil de migration Secure Firewall.
-

Exporter le certificat PKI à partir d' Pare-feu ASA avec services FirePOWER et l'importer dans le centre de gestion

Avant de commencer

L'outil de migration Secure Firewall prend en charge la migration des VPN basés sur des certificats vers le centre de gestion.

Pare-feu ASA avec services FirePOWER utilise le modèle du point de confiance pour stocker les certificats dans la configuration. Un point de confiance est un conteneur dans lequel les certificats sont stockés. Le point de confiance Pare-feu ASA avec services FirePOWER peut stocker jusqu'à deux certificats.

Le point de confiance Pare-feu ASA avec services FirePOWER ou les certificats dans le fichier de configuration Pare-feu ASA avec services FirePOWER contiennent des valeurs de hachage. Ainsi donc, vous ne pouvez pas directement les importer dans un centre de gestion.

Dans le centre de gestion de destination, migrez manuellement le point de confiance Pare-feu ASA avec services FirePOWER ou les certificats VPN en tant qu'objets PKI dans le cadre de l'activité de pré-migration.

-
- Étape 1** Utilisez la commande suivante pour exporter le certificat PKI via la CLI à partir de la configuration Pare-feu ASA avec services FirePOWER source avec les clés vers un fichier PKCS12.
- ```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```
- Étape 2** Importez le certificat PKI dans un centre de gestion (**Gestion d'objet Objets PKI**).
- Pour plus d'informations, référez-vous au [guide de configuration du pare-feu](#) pour obtenir plus de renseignements.
- Les objets PKI créés manuellement peuvent maintenant être utilisés dans l'outil de migration Secure Firewall dans la **page de révision et de validation** sous la section **Point de confiance** dans **Accès à distance VPN**.
-

## Récupérer les paquets et les profils AnyConnect

Les profils AnyConnect sont facultatifs et peuvent être téléversés via le centre de gestion ou l'outil de migration Secure Firewall.

### Avant de commencer

- Le VPN d'accès à distance sur le centre de gestion demande au moins un paquet AnyConnect.
- Si la configuration consiste en un paquet de navigateur Hostscan et externe, vous devez téléverser ces paquets.
- Tous les paquets doivent être ajoutés au centre de gestion en tant qu'activité pré-migration.
- Dap.xml et Data.xml doivent être ajoutés via l'outil de migration Secure Firewall

### Étape 1

Utilisez la commande suivante pour copier le paquet demandé de la source ASA vers un serveur FTP ou TFTP.

```
Copy <source file location:/source file name> <destination>
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Example of copying
Anyconnect Package.
ASA# copy disk0:/ external-ss0- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Example of copying
External Browser Package.
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example of copying Hostscan
Package.
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect Profile.
```

### Étape 2

Importer les paquets téléchargés dans le centre de gestion (**fichier de gestion des objets > VPN > AnyConnect**)

1. Les fichiers Dap.xml et Data.xml doivent être téléchargés vers le centre de gestion à partir de l'outil de migration Secure Firewall dans la section **Examiner et valider > fichier VPN AnyConnect > pour l'accès à distance**.
2. Les profils AnyConnect peuvent être téléchargés directement vers le centre de gestion ou via l'outil de migration Secure Firewall dans la section **Examiner et valider > fichier VPN AnyConnect > pour l'accès à distance**.

Les fichiers téléversés manuellement peuvent maintenant être utilisés dans l'outil de migration Secure Firewall.

## Exécuter la migration

### Lancer l'outil de migration Secure Firewall



#### Remarque

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

### Avant de commencer

- [Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com](#)
- Examiner et vérifier les exigences de la section [Centre de gestion des cibles pour la migration pris en charge](#), à la page 19.
- Assurez-vous que votre ordinateur dispose d'une version récente du navigateur Google Chrome pour exécuter l'outil de migration Secure Firewall. Pour plus d'informations sur la manière de définir Google Chrome comme navigateur par défaut, voir [Définir Chrome comme navigateur web par défaut](#).
- Si vous prévoyez de migrer un fichier de configuration volumineux, configurez les paramètres de mise en veille afin que le système ne se mette pas en veille pendant la poussée de migration.

### Étape 1

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

### Étape 2

Effectuez l'une des opérations suivantes :

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

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

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

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

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

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

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

**Remarque** Utilisez la méthode zip du terminal MAC.

### Étape 3

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

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

### Étape 4

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

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

**Remarque** Si vous n'avez pas de compte Cisco.com, créez-le sur la page de connection de Cisco.com.

- Connectez-vous avec les identifiants par défaut suivants :
  - **Nom d'utilisateur** : admin
  - **Mot de passe** : Admin123

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

- Étape 5** Sur la page **Réinitialiser le mot de passe**, entrez l'ancien mot de passe, votre nouveau mot de passe et confirmez le nouveau mot de passe.
- Le nouveau mot de passe doit avoir 8 caractères ou plus et doit inclure des lettres en majuscule et en minuscule, des numéros et des caractères spéciaux.
- Étape 6** Cliquez sur **Réinitialiser**.
- Étape 7** Connectez-vous avec le nouveau mot de passe.
- Remarque** Si vous avez oublié le mot de passe, supprimez toutes les données existantes du dossier `<migration_tool_folder>` et réinstallez l'outil de migration Secure Firewall.
- Étape 8** Examinez la liste de contrôle de pré-migration et assurez-vous que vous avez rempli tous les points énumérés. Si vous n'avez pas rempli un ou plusieurs points de la liste de contrôle, ne continuez pas tant que vous ne l'avez pas fait.
- Étape 9** Cliquez sur **Nouvelle migration**.
- Étape 10** Sur l'écran de **vérification de la mise à jour du logiciel**, si vous n'êtes pas sûr d'utiliser la version la plus récente de l'outil de migration Secure Firewall, cliquez sur le lien pour vérifier la version sur Cisco.com.
- Étape 11** Cliquez sur **Procéder**.

### Prochaine étape

Vous pouvez procéder à l'étape suivante :

- Si vous avez exporté la configuration sur votre ordinateur, passez au [Téléverser ASA avec le fichier de configuration FPS](#).
- Si vous souhaitez extraire des informations d'un dossier en utilisant l'outil de migration Secure Firewall, passez à [Se connecter à l'ASA à partir de l'outil de migration de pare-feu sécurisé, à la page 29](#)

## Téléverser ASA avec le fichier de configuration FPS

### Avant de commencer

Exporter le fichier de configuration au format `.cfg` ou `.txt` à partir de l'appareil ASA avec FPS.



**Remarque** Ne téléversez pas un fichier de configuration codé à la main ou modifié manuellement. Les éditeurs de texte ajoutent des lignes vides et d'autres éléments au fichier qui peuvent faire échouer la migration.

- 
- Étape 1** Dans l'écran **Extraire Cisco ASA (9.2.2+)** avec les informations FPS, dans la section **Téléversement manuel**, cliquez sur **Téléverser** pour charger l'ASA avec le fichier de configuration FPS.
- Étape 2** Naviguez vers où le fichier de configuration est situé et cliquez sur **Ouvrir**
- L'outil de migration Secure Firewall téléverse le fichier de configuration. Pour les fichiers de configuration volumineux, cette étape prend plus de temps. La console fournit un journal ligne par ligne de la progression, y compris la ligne de configuration ASA avec FPS qui est en cours d'analyse. Si vous ne voyez pas la console, vous pouvez la trouver dans une fenêtre séparée derrière l'outil de migration Secure Firewall. La section **Choix de contexte** identifie si la configuration téléversée correspond au multi-contexte.
- Étape 3** Dans le champ **Adresse IP/Nom d'hôte du centre de gestion du pare-feu**, saisissez les informations pertinentes :
- ASA à contexte unique avec FPS - Adresse IP ou nom d'hôte de gestion
  - ASA à contexte multiple avec FPS - Adresse IP du contexte administrateur ou nom d'hôte
- Étape 4** Cliquez sur **Connect (connexion)**.
- Saisissez les informations suivantes dans l'écran de **connexion du centre de gestion du pare-feu**.
- Nom d'utilisateur
  - Mot de passe
  - Cliquez sur **Connexion** pour vous connecter au centre de gestion du pare-feu
- Étape 5** La liste déroulante **Choisir le dispositif FPS** affiche une liste de dispositifs FPS attachés au centre de gestion concerné. Chaque périphérique affiche le nom du périphérique avec la politique ACL associée.
- Étape 6** Examinez la section **Sélection du contexte** et choisissez le contexte que vous voulez migrer.
- Étape 7** Cliquez sur **Procéder**.
- Les règles d'accès sont récupérées du dispositif
- Étape 8** La section **Résumé de l'analyse** affiche le statut de l'analyse.
- Étape 9** Passez en revue le récapitulatif des éléments du fichier de configuration chargé que l'outil de migration Secure Firewall a détectés et analysés.
- Étape 10** Cliquez sur **Suivant** pour choisir les paramètres cibles.
- 

### Prochaine étape

[Préciser les paramètres de destination pour l'outil de migration de pare-feu sécurisé, à la page 31](#)

## Se connecter à l'ASA à partir de l'outil de migration de pare-feu sécurisé

L'outil de migration Secure Firewall peut se connecter à un dispositif que vous souhaitez migrer et extraire les informations de configuration requises.

### Avant de commencer

- Télécharger et lancer l'outil de migration Secure Firewall.

- Pour les ASA à contexte unique, obtenez l'adresse IP de gestion, les informations d'identification de l'administrateur et le mot de passe d'activation.
- Pour les ASA en mode multi-contexte, obtenez l'adresse IP du contexte **d'administration**, les informations d'identification de l'administrateur et le mot de passe d'activation.




---

**Remarque** Si l'ASA n'est pas configuré avec l'option **Activer le mot de passe**, vous pouvez laisser le champ vide dans l'outil de migration Secure Firewall.

---

- Étape 1** Sur l'écran **Extraire Cisco ASA (9.2.2+) avec informations FPS**, dans la section **Connecter à l'ASA**, cliquez sur **Connecter** pour vous connecter à l'appareil ASA que vous voulez migrer.
- Étape 2** Sur l'écran **Connexion à l'ASA**, saisissez les informations suivantes :
1. Dans le champ **Adresse IP/Nom d'hôte de l'ASA**, entrez l'adresse IP de gestion ou le nom d'hôte (pour un ASA à contexte unique) ou l'adresse IP du contexte d'administration ou le nom d'hôte (pour un ASA à contextes multiples).
  2. Dans les champs **Nom d'utilisateur**, **Mot de passe** et **Activer le mot de passe**, saisissez les informations d'identifiant administrateur appropriés.
- Remarque** Si l'ASA n'est pas configuré avec l'option **Activer le mot de passe**, vous pouvez laisser le champ vide dans l'outil de migration Secure Firewall.
3. Cliquez sur **Ouvrir une session**.
- Lorsque l'outil de migration Secure Firewall se connecte à l'ASA, il affiche message de connexion réussie au message ASA Pour un ASA multicontexte, l'outil de migration Secure Firewall identifie et liste les contextes.
- Étape 3** Choisissez le contexte que vous voulez migrer à partir de la liste déroulante **Contexte**
- Étape 4** (Facultatif) Sélectionnez **Collecter les comptes de résultat**.
- Lorsque cette case est cochée, cet outil calcule le nombre de fois qu'une règle ASA a été utilisée et la dernière fois que la règle a été utilisée depuis la mise en service de l'ASA ou le dernier redémarrage de l'ASA, et affiche ces informations sur la page **Examiner et valider**. Cela vous permet d'évaluer l'efficacité et la pertinence de la règle avant la migration.
- Étape 5** Cliquez sur **Débuter l'extraction**
- L'outil de migration Secure Firewall se connecte à l'ASA et débute l'extraction des informations de configuration. Lorsque l'extraction se termine avec succès, la section **Sélection du contexte** identifie si la configuration téléversée correspond à un ASA à contexte simple ou multiple.
- Étape 6** Examinez la section **Sélection** du contexte et choisissez le contexte ASA que vous voulez migrer.
- Étape 7** Dans le champ **Adresse IP/Nom d'hôte du centre de gestion du pare-feu**, saisissez les informations pertinentes :
- ASA à contexte unique avec FPS - Adresse IP ou nom d'hôte de gestion
  - ASA à contexte multiple avec FPS - Adresse IP du contexte administrateur ou nom d'hôte
- Étape 8** Cliquez sur **Connect (connexion)**.
- Saisissez les informations suivantes dans l'écran de **connexion du centre de gestion du pare-feu** :

- Nom d'utilisateur
- Mot de passe
- Cliquez sur **Connexion** pour vous connecter au centre de gestion du pare-feu

- Étape 9** La liste déroulante **Choisir le dispositif FPS** affiche une liste de dispositifs FPS attachés au centre de gestion concerné. Chaque périphérique affiche le nom du périphérique avec la politique ACL associée.
- Étape 10** Cliquez sur **Procéder**.  
Les règles d'accès sont récupérées du dispositif
- Étape 11** La section **Résumé de l'analyse** affiche le statut de l'analyse. L'outil de migration Secure Firewall analyse le fichier de configuration et le déconnecte de l'ASA.
- Étape 12** Examinez le résumé des éléments détectés et analysés par l'outil de migration Secure Firewall dans le fichier de configuration téléversé.
- Étape 13** Cliquez sur **Suivant** pour choisir les paramètres cibles.

---

#### Prochaine étape

[Préciser les paramètres de destination pour l'outil de migration de pare-feu sécurisé, à la page 31](#)

## Préciser les paramètres de destination pour l'outil de migration de pare-feu sécurisé

#### Avant de commencer

- Obtenez l'adresse IP de centre de gestion pour le centre de gestion du pare-feu sur place
- Créez un compte dédié à l'outil de migration Secure Firewall dans centre de gestion avec des privilèges suffisants pour accéder à l'API REST, comme décrit dans la section [Comptes d'utilisateur pour l'accès à la gestion](#).
- (Facultatif) Si vous souhaitez migrer des configurations spécifiques à un dispositif, comme des interfaces et des itinéraires, ajoutez le défense contre des menaces cible au centre de gestion. Référez-vous à [Ajoutez des dispositifs au Firewall Management Center](#)
- S'il est nécessaire d'appliquer un IPS ou une politique de fichier à l'ACL dans la page **Examiner et valider**, nous vous recommandons vivement de créer une politique sur centre de gestion avant la migration. Utilisez la même politique, alors que l'outil de migration Secure Firewall récupère la politique du centre de gestion connecté. Créer une nouvelle politique et l'assigner à de listes de contrôles d'accès peut dégrader la performance et causer l'échec du transfert.

- 
- Étape 1** Sur l'écran **Sélectionner la cible**, dans la section **Gestion** du pare-feu, procédez comme suit : .
- a) Cliquez sur le bouton radio **FMC sur place**
  - b) Saisissez l'adresse IP ou le nom de domaine entièrement qualifié (FQDN) du centre de gestion.
  - c) Dans la liste déroulante **Domaine**, sélectionnez le domaine vers lequel vous effectuez la migration.

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

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

### Étape 2

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

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

### Étape 3

Sur l'écran **Sélectionner la cible**, dans la section **Choisir la défense contre les menaces**, vous pouvez soit sélectionner un dispositif de défense contre des menaces vers lequel vous souhaitez migrer, soit, si vous n'avez pas de dispositif de défense contre des menaces, migrer les stratégies partagées (listes de contrôle d'accès, NAT et objets) de la configuration vers le centre de gestion.

### Étape 4

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

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

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

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

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

**Tableau 1 : ASA avec FPS Fonctionnalités et versions Centre de gestion ou Défense contre les menaces prises en charge du pare-feu**

| Fonctionnalités de pare-feu                                       | Version du centre de gestion ou de la défense contre les menaces prise en charge |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------|
| avec déploiement à distance                                       | 6.7 ou plus récent                                                               |
| VPN carte cryptographique site-à-site                             | 6.6 ou plus récent                                                               |
| Virtual Tunnel Interface (VTI) et basée sur les itinéraires (VTI) | 6.7 ou plus récent                                                               |
| ASA avec déploiement FPS                                          | 6.5 ou plus récent                                                               |
| Objets de routage dynamique et BGP                                | 7.1 ou plus récent                                                               |

| Fonctionnalités de pare-feu | Version du centre de gestion ou de la défense contre les menaces prise en charge                                                      |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| VPN d'accès à distance      | <ul style="list-style-type: none"> <li>• Centre de gestion 7.2 ou plus récent</li> <li>• Threat Defense 7.0 ou plus récent</li> </ul> |
| EIGRP                       | <ul style="list-style-type: none"> <li>• Centre de gestion 7.2 ou plus récent</li> <li>• Threat Defense 7.0 ou plus récent</li> </ul> |

**Remarque** Pour migrer les interfaces VPN site à site, VTI et basées sur les routes (VTI), défense contre des menaces doit être configuré sur centre de gestion.

- Pour l'ASA 5505, les configurations spécifiques à l'appareil (interface et routes) et les stratégies partagées (NAT, ACL et objets) ne peuvent être migrées que lorsque la plateforme de défense contre des menaces cible prise en charge est Firewall 1010 avec la version centre de gestion 6.5 ou ultérieure.

**Remarque**

- Si la cible défense contre des menaces n'est pas FPR-1010 ou si la cible centre de gestion est antérieure à la version 6.5, la prise en charge de la migration de l'ASA 5505 ne s'applique qu'aux politiques partagées. Les caractéristiques de l'appareil ne seront pas migrées.

- Vous pouvez sélectionner uniquement FPR-1010 dans la liste déroulante **Choisir l'appareil** car la configuration source est ASA 5505.

- La prise en charge de la migration ASA-SM ne concerne que les stratégies partagées. Les caractéristiques de l'appareil ne seront pas migrées.

- Cliquez sur **Continuer sans défense** contre les menaces pour migrer la configuration vers centre de gestion.

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

## Étape 5

Cliquez sur **Procéder**.

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

## Étape 6

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

- Si vous effectuez une migration vers un dispositif de destination défense contre des menaces, l'outil de migration Secure Firewall sélectionne automatiquement les fonctionnalités disponibles pour la migration à partir de la configuration de ASA avec FPS du dans les sections **Configuration du dispositif** et **Configuration partagée**. Vous pouvez modifier la sélection par défaut, selon vos besoins.
- Si vous effectuez une migration vers un centre de gestion, l'outil de migration Secure Firewall sélectionne automatiquement les fonctionnalités disponibles pour la migration à partir de la configuration de ASA avec FPS du dans la section **Configuration partagée**. Vous pouvez modifier la sélection par défaut, selon vos besoins.

**Remarque** La section **Configuration de l'appareil** n'est pas disponible lorsque vous n'avez pas choisi d'appareil destinataire défense contre des menaces vers où migrer

**Remarque** La section **Configuration de l'appareil** n'est pas disponible lorsque vous avez choisi **Migrer le gestionnaire d'appareil Firepower (Configurations partagées uniquement)**.

- L'outil de migration Secure Firewall prend en charge les fonctions de contrôle d'accès suivantes pendant la migration :

- Remplir les zones de sécurité de destination—Active le mappage des zones de destination pour l'ACL pendant la migration.

La logique de recherche de route est limitée aux routes statiques et aux routes connectées, et les PBR, les routes dynamiques et les NAT ne sont pas pris en compte. La configuration du réseau de l'interface est utilisée pour dériver les informations de l'itinéraire connecté.

Compte tenu de la nature des groupes d'objets réseau Source et Destination, cette opération peut entraîner une explosion des règles.

- Migrer les règles des tunnels non chiffrés (ASA) en tant que politique de préfiltrage - Le mappage des règles du protocole de tunnel encapsulé ASA en règles de tunnel de préfiltrage présente les avantages suivants :
  - Inspection en profondeur - Pour le trafic encapsulé et pour améliorer les performances avec le fastpathing.
  - Amélioration des performances : vous pouvez accélérer ou bloquer toutes les autres connexions qui bénéficient d'un traitement anticipé.

L'outil de migration Secure Firewall identifie les règles de trafic du tunnel encapsulé dans la configuration source et les migre en tant que règles de tunnel préfiltré. Vous pouvez vérifier la règle de tunnel migré sous la politique Préfiltrer La politique Préfiltrer est associée à la stratégie de contrôle d'accès sur centre de gestion.

Les protocoles étant migrés comme des règles de tunnel préfiltrés sont les suivants :

- GRE (47)
- Encapsulation IPv4 (4)
- Encapsulation IPv6 (41)
- Tunnellisation Teredo (UDP : 3544)

**Remarque** Si vous choisissez de ne pas choisir l'option Préfiltrer, toutes les règles de trafic tunnelisé seront migrées comme des règles non prises en charge.

Les règles de tunnel ACL (GRE et IPnIP) dans la configuration de l' ASA avec FPS sont actuellement migrées comme bidirectionnelles par défaut. Vous pouvez maintenant spécifier la direction de la règle pour la destination comme bidirectionnelle ou unidirectionnelle dans l'option d'état du contrôle d'accès.

- L'outil de migration Secure Firewall prend en charge les interfaces et les objets suivants pour la migration des tunnels VPN :
  - Basée sur la règle (carte cryptographique) - Si le centre de gestion et défense contre des menaces cible est la version 6.6 ou plus récente.

- Basée sur l'itinéraire (VTI) - Si le centre de gestion et défense contre des menaces est la version 6.7 ou plus récente.
  - L'outil de migration Secure Firewall prend en charge la migration du VPN d'accès à distance si le centre de gestion cible est 7.2 ou plus récent. Le VPN d'accès à distance est une politique partagée et peut être migré sans défense contre les menaces. Si la migration est sélectionnée avec la défense contre les menaces, la version de la défense contre les menaces doit être 7.0 ou ultérieure.
  - (Facultatif) Dans la section **Optimisation**, sélectionnez **Migrer uniquement les objets référencés** pour ne migrer que les objets référencés dans une stratégie de contrôle d'accès et une stratégie NAT.
 

**Remarque** Lorsque vous sélectionnez cette option, les objets non référencés dans la configuration de l'ASA avec FPS de ne seront pas migrés. Cela optimise le temps de migration et nettoie les objets inutilisés de la configuration.
  - (Facultatif) Dans la section **Optimisation**, sélectionnez **Recherche de groupe d'objets** pour une utilisation optimale de la mémoire par politique d'accès sur défense contre des menaces.
  - (Facultatif) Dans la section **Groupement en ligne**, l'outil de migration Secure Firewall vous permet d'effacer les règles d'accès des noms d'objets réseau et service prédéfinis qui commencent par CSM ou DM. Si vous décochez cette option, les noms d'objets prédéfinis seront conservés durant la migration. Pour plus d'informations, référez-vous à [Groupement en ligne](#).
- Remarque** Par défaut, l'option du Groupement en ligne est activée.

**Étape 7**

Cliquez sur **Procéder**.

**Étape 8**

Cliquez sur **Débuter la conversion** pour initier la conversion.

**Étape 9**

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

**Étape 10**

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

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

**Étape 11**

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

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

**Prochaine étape**

[Examiner le rapport pré-migration, à la page 37](#)

**Groupement en ligne****Groupement d'objet par ASDM et ASA géré par CSM**

Lorsque vous saisissez plusieurs éléments (objets ou valeurs en ligne) dans l'adresse source ou de destination, ou dans le service source ou de destination, CSM ou ASDM crée automatiquement un groupe d'objets. Les conventions d'appellation de ces groupes d'objets utilisés par CSM et ASDM sont respectivement CSM\_INLINE et DM\_INLINE lors du déploiement de la configuration sur l'appareil ASA concerné.



**Remarque** Pour modifier le comportement du regroupement d'objets, dans **Outils > Préférences**, sélectionnez **Développement automatique des objets de réseau et de service avec la préférence de table de règles de préfixe spécifiée**.

Voici l'extrait de configuration extrait à l'aide de la commande **show run** sur une ASA gérée par ASDM.

```
object network host1
 host 10.1.1.100
object network fqdn_obj1
 fqdn abc.cisco.com
object-group network DM_INLINE_NETWORK_1
 network-object 10.21.44.189 255.255.255.255
 network-object 10.21.44.190 255.255.255.255
object-group network DM_INLINE_NETWORK_2
 network-object 10.21.44.191 255.255.255.255
 network-object object host1
 network-object object fqdn_obj1
```

```
access-list CSM_DM_ACL extended permit tcp object-group DM_INLINE_NETWORK_1 object-group
DM_INLINE_NETWORK_2
```

Dans l'exemple ci-dessus, la liste d'accès CSM\_DM\_ACL sur l'interface ASDM n'affiche pas le groupe DM\_INLINE comme réseau source et destination de la règle, mais affiche le contenu du groupe DM\_INLINE.

### Groupement en ligne - ASDM/CSM

La fonctionnalité de regroupement en ligne de l'outil de migration Secure Firewall vous permet d'analyser la **configuration en cours d'exécution** des dispositifs ASA gérés par ASDM ou CSM. Il fournit une option pour préserver la même représentation de l'interface utilisateur des règles de liste d'accès que sur ASDM ou CSM. Si cette option n'est pas retenue, les règles migrées feront référence aux groupes DM\_INLINE, comme indiqué dans le document ASA **show running-configuration**.



**Remarque** Le fichier de configuration de l'ASA source utilisé par l'outil de migration Secure Firewall serait toujours **show run** ou **show tech** collecté à partir de l'ASA ou via une connexion en direct à l'ASA (SSH). L'outil de migration Secure Firewall ne prend pas en charge aucune autre forme de fichiers ou méthodes de configuration.

Les figures suivantes montrent comment les champs Source et Réseau destination de l'ACE ou de la RULE changent en fonction de l'activation ou de la désactivation de l'option de regroupement en ligne.

**Illustration 1 : Avec regroupement en ligne-ASDM/CSM activé**

| ■                        | #   | Name          | SOURCE  |                            |      | DESTINATION |                                |      | State | Action |
|--------------------------|-----|---------------|---------|----------------------------|------|-------------|--------------------------------|------|-------|--------|
|                          |     |               | Zone    | Network                    | Port | Zone        | Network                        | Port |       |        |
| <input type="checkbox"/> | 121 | CSM_DM_ACL_#1 | outside | 10.21.44.189, 10.21.44.190 | ANY  | ANY         | 10.21.44.191, host1, fqdn_obj1 | ANY  | ✓     | Allow  |

**Illustration 2 : Avec regroupement en ligne-ASDM/CSM désactivé**

| ■                        | #   | Name          | SOURCE  |                     |      | DESTINATION |                     |      | State | Action |
|--------------------------|-----|---------------|---------|---------------------|------|-------------|---------------------|------|-------|--------|
|                          |     |               | Zone    | Network             | Port | Zone        | Network             | Port |       |        |
| <input type="checkbox"/> | 121 | CSM_DM_ACL_#1 | outside | DM_INLINE_NETWORK_1 | ANY  | ANY         | DM_INLINE_NETWORK_2 | ANY  | ✓     | Allow  |

## Examiner le rapport pré-migration

Si vous avez oublié de télécharger les rapports de pré-migration pendant la migration, utilisez le lien suivant pour les télécharger :

Rapport de pré-migration Télécharger le point final—[http://localhost:8888/api/downloads/pre\\_migration\\_summary\\_html\\_format](http://localhost:8888/api/downloads/pre_migration_summary_html_format)



---

**Remarque** Vous pouvez télécharger les rapports seulement lorsque l'outil de migration Secure Firewall est en cours d'exécution.

---

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

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

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

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

- **Résumé général** — Méthode utilisée pour extraire les informations de configuration de l'ASA avec FPS ou téléchargement manuel pour l'ASA avec FPS.  
  
Si vous vous connectez à une ASA active, le mode de pare-feu détecté sur ASA avec FPS, et pour le mode de contexte multiple, le contexte que vous avez choisi pour la migration.  
  
Un résumé des éléments de configuration des dispositifs ASA avec FPS qui peuvent être migrés avec succès et des défenses contre des menaces fonctionnalités spécifiques des ASA avec FPS sélectionnées pour la migration.  
  
Lors de la connexion à un dispositif géré par FDM, le résumé comprend des informations sur le nombre d'occurrences - le nombre de fois où une règle de dispositif géré par l'ASA a été rencontrée et les informations sur l'horodatage.
- **Lignes de configuration avec des erreurs** - Détails des éléments de configuration ASA avec FPS qui ne peuvent pas être migrés avec succès car l'outil de migration Secure Firewall n'a pas pu les analyser. Corrigez ces erreurs dans l'ASA avec FPS, exportez un nouveau fichier de configuration, puis téléchargez le nouveau fichier de configuration dans l'outil de migration Secure Firewall avant de continuer.
- **Configuration partiellement prise en charge** - Détails des éléments de configuration des dispositifs ASA avec FPS gérés par qui ne peuvent être que partiellement migrés. Ces éléments de configuration comprennent des règles et des objets avec des options avancées, alors que la règle ou l'objet peut être migré sans les options avancées. Examinez ces lignes, vérifiez si les options avancées sont prises en charge dans centre de gestion, et si c'est le cas, prévoyez de configurer ces options manuellement après avoir terminé la migration à l'aide de l'outil de migration Secure Firewall.
- **Configuration non prise en charge** - Détails des éléments de configuration des qui ne peuvent pas être migrés car l'outil de migration Secure Firewall ne prend pas en charge la migration de ces fonctionnalités. Examinez ces lignes, vérifiez si chaque fonctionnalité est prise en charge dans centre de gestion, et si c'est le cas, prévoyez de configurer les fonctionnalités manuellement après avoir terminé la migration à l'aide de l'outil de migration Secure Firewall.
- **Configuration ignorée** - Détails des éléments de configuration des dispositifs ASA avec FPS qui sont ignorés parce qu'ils ne sont pas pris en charge par centre de gestion l'outil de migration Secure Firewall. L'outil de migration

Secure Firewall n'analyse pas ces lignes. Examinez ces lignes, vérifiez si chaque fonctionnalité est prise en charge dans centre de gestion, et si c'est le cas, prévoyez de configurer les fonctionnalités manuellement.

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

**Étape 3** Si le rapport de **pré-migration** recommande des actions correctives, effectuez ces corrections sur l'interface ASA avec FPS, exportez à nouveau le fichier de configuration d'ASA et téléchargez le fichier de configuration mis à jour avant de poursuivre.

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

### Prochaine étape

[Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager](#)

## Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager

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

Sur l'écran **Associer l'interface Threat Defense**, l'outil de migration Secure Firewall récupère une liste des interfaces sur l'appareil défense contre des menaces. Par défaut, l'outil de migration Secure Firewall mappe les interfaces dans ASA avec FPS avec le dispositif défense contre des menaces en fonction de leurs identités d'interface. Par exemple, l'interface « gestion seule » de l'interface du est automatiquement mappée à l'interface « gestion seule » du défense contre des menacesdispositif et n'est pas modifiable.

Le mappage de l'interface de l'ASA avec FPS avec à l'interface défense contre des menaces diffère en fonction du type de périphérique défense contre des menaces :

- Si la cible défense contre des menaces est de type natif :
  - Le défense contre des menaces doit avoir un nombre égal ou supérieur d'interfaces ASA avec FPS ou d'interfaces de données de canal de port (PC) utilisées (à l'exclusion des interfaces de gestion uniquement et des sous-interfaces dans la configuration de dispositifs gérés par un ASA avec FPS ). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre des menaces cible.
  - Les sous-interfaces sont créées par l'outil de migration du pare-feu sécurisé sur la base de l'interface physique ou du mappage du canal de port.
- Si la cible défense contre des menaces est de type contenant :
  - Le défense contre des menaces doit avoir un nombre égal ou supérieur d'interfaces ASA avec FPS ou de sous-interfaces physiques utilisées, de canal de port ou de sous-interfaces de canal de port (à l'exclusion des interfaces de gestion uniquement et des sous-interfaces dans la configuration de dispositifs gérés par un ). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre des menaces cible. Par exemple, si le nombre d'interfaces physiques et de sous-interfaces

physiques sur la cible défense contre des menaces est inférieur de 100 à celui de l'ASA avec FPS , vous pouvez créer des interfaces physiques ou des sous-interfaces physiques supplémentaires sur la cible défense contre des menaces.

- Les sous-interfaces ne sont pas créés par l'outil de migration Secure Firewall Seul le mappage d'interface est autorisé entre les interfaces physiques, les canaux de port ou les sous-interfaces.

### Avant de commencer

Assurez-vous de vous être connecté au centre de gestion et choisi la destination comme défense contre des menaces Pour en savoir plus, consultez [Préciser les paramètres de destination pour l'outil de migration de pare-feu sécurisé](#), à la page 31.



---

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

---

### Étape 1

Si vous souhaitez modifier le mappage d'une interface, cliquez sur la liste déroulante du **nom de l'interface de défense contre les menaces** et choisissez l'interface que vous souhaitez mapper à l'interface de ASA avec FPS.

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

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

### Étape 2

Lorsque vous avez mappé chaque interface de périphérique ASA avec FPS à une interface de défense contre des menaces, cliquez sur **Suivant**.

---

### Prochaine étape

Mappez les interfaces des ASA avec FPS aux objets d'interface, aux zones de sécurité et aux groupes d'interfaces appropriés défense contre des menaces. Pour plus d'informations, voir [Mapper les interfaces ASA à des zones de sécurité et à des groupes d'interfaces](#).

## Mapper les interfaces ASA à des zones de sécurité et à des groupes d'interfaces



---

**Remarque** Si la configuration de votre ASA avec FPS ne comprend pas de listes d'accès ni de règles NAT ou si vous choisissez de ne pas migrer ces règles, vous pouvez ignorer cette étape et passer à [Optimiser, examiner et valider la configuration](#), à la page 41.

---

Pour s'assurer que la configuration d'ASA avec FPS est migrée correctement, mappez les interfaces du aux objets d'interface, aux zones de sécurité défense contre des menaces. Dans une configuration ASA avec FPS

de , les politiques de contrôle d'accès et les politiques NAT utilisent des noms d'interface (nameif). Dans centre de gestion, ces politiques utilisent des objets d'interface. De plus, les politiques centre de gestion regroupent les objets d'interface ainsi :

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

L'outil de migration Secure Firewall permet le mappage un à un des interfaces avec les zones de sécurité et les groupes d'interfaces ; lorsqu'une zone de sécurité ou un groupe d'interfaces est mappé à une interface, il n'est pas disponible pour le mappage à d'autres interfaces, bien que centre de gestion le permette. Pour plus d'informations sur les zones de sécurité et les groupes d'interface dans centre de gestion, référez-vous à [Objets d'interface : groupes d'interfaces et zones de sécurité](#) .

**Étape 1**

Sur l'écran **Mapper les zones de sécurité et les groupes d'interfaces**, passez en revue les interfaces, les zones de sécurité et les groupes d'interfaces disponibles.

**Étape 2**

Pour mapper des interfaces à des zones de sécurité et à des groupes d'interfaces qui existent dans centre de gestion, ou qui sont disponibles dans les fichiers de configuration de ASA avec FPS des en tant qu'objets de type zone de sécurité et qui sont disponibles dans la liste déroulante, procédez comme suit :

- Dans la colonne **Zones de sécurité**, choisissez la zone de sécurité pour cette interface.
- Dans la colonne **Groupes d'interface**, choisissez le groupe d'interface pour cette interface.

**Étape 3**

Vous pouvez mapper manuellement ou auto-créez les zones de sécurité et les groupes d'interface.

**Étape 4**

Pour mapper manuellement les zones de sécurité et les groupes d'interface, faites ce qui suit :

- Cliquez sur **Ajouter ZS & GI**
- Dans la boîte de dialogue **Ajouter ZS & GI**, cliquez sur **Ajouter** pour ajouter une nouvelle zone de sécurité ou groupe d'interface.
- Saisissez le nom de la zone de sécurité dans la colonne **Zone de sécurité**. Le nombre maximal de caractères est de 48. De même, vous pouvez ajouter un groupe d'interfaces.
- Cliquez sur **Close** (Fermer).

**Pour la migration d'ASA avec FPS :**

- Le type de zone de sécurité ASA vers le type de zone de sécurité Routé/Commuté (Défense contre les menaces pris en charge) est pris en charge pour la migration.
- Comme centre de gestion n'accepte que des noms de zone de sécurité uniques, la nouvelle zone de sécurité Défense contre les menaces prise en charge ne peut pas avoir le même nom que l'ASA source avec les zones FPS.
- Pour toutes les zones de type ASA de l'ASA sélectionné avec FPS existant dans la centre de gestion source, une nouvelle zone Défense contre les menaces (Routé/Commuté) est créée dans l'outil de migration Secure Firewall sous la page **Cartographie des zones**. Contrairement à l'ASA pour la migration centre de gestion, dans l'ASA avec des scénarios FPS, les zones de sécurité sont extraites de la politique FPS et ne sont pas créées en fonction du nom logique Défense contre les menaces (nom ASA).
- Les groupes d'interface seront migrées en utilisant le nom logique Défense contre les menaces et ainsi donc, il n'y aura aucun impact sur le NAT.

La colonne **Zones FPS** affiche les zones de sécurité qui seront mappées à l'interface logique ASA.

**Remarque** Cette colonne affiche uniquement les ASA sélectionnés avec des zones de dispositifs FPS et les répertorie par rapport à leurs interfaces respectives.

Si un ASA avec zone FPS est connecté à plus d'une interface du même ASA avec le dispositif FPS, divisez la zone en deux zones Défense contre les menaces prises en charge.

Pour mapper les zones de sécurité et les groupes d'interface par auto-création, faites ce qui suit :

- Cliquez sur **Auto-créer**.
- Dans la boîte de dialogue **Auto-créer**, cochez une ou les deux cases **Groupes d'interface** et **Mappage de zone**.
- Cliquez sur **Auto-créer**.

L'outil de migration Secure Firewall donne à ces zones de sécurité le même nom que l'interface ASA avec FPS, comme à **l'extérieur** ou à **l'intérieur**, et affiche un « (A) » après le nom pour indiquer qu'il a été créé par l'outil de migration du pare-feu sécurisé. Les groupes d'interface ont un suffixe `_ig` ajouté, tel que **outside\_ig** ou **inside\_ig**. En outre, les zones de sécurité et les groupes d'interface ont le même mode que l'interface ASA avec FPS du . Par exemple, si l'interface logique ASA avec FPS du est en mode L3, la zone de sécurité et le groupe d'interface créés pour l'interface sont également en mode L3.

**Étape 5** Lorsque vous avez mappé toutes les interfaces aux zones de sécurité et groupes d'interface appropriés, cliquez sur **Suivant**.

## Optimiser, examiner et valider la configuration

**Étape 1** (Facultatif) Sur l'écran, cliquez sur **Optimiser l'ACL** pour exécuter le code d'optimisation et effectuez les opérations suivantes :

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

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

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

**Étape 2** Sur l'écran **Optimiser, examiner et valider la configuration**, cliquez sur **Règles de contrôle d'accès** et faites ceci :

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

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

exemple, si la règle d'autorisation est développée en deux règles de migration, elles sont nommées « inside\_access\_#1-1 » et « inside\_access\_#1-2 ».

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

- b) Si vous ne souhaitez pas migrer une ou plusieurs stratégies de liste de contrôle d'accès, cochez la case des lignes concernées, choisissez **Actions > Ne pas migrer**, puis cliquez sur **Enregistrer**.

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

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

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

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

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

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

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

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

Dans la boîte de dialogue **Action découlant d'une règle**, dans le menu déroulant **Actions**, vous pouvez choisir les onglets **SCA** ou **Préfiltre** :

- **SCA** - Chaque règle de contrôle d'accès comporte une action qui détermine la manière dont le système traite et enregistre le trafic correspondant. Vous pouvez effectuer une action d'autorisation, de confiance, de surveillance, de blocage ou de blocage avec réinitialisation sur une règle de contrôle d'accès.
- **Préfiltre** - L'action découlant d'une règle détermine comment le système traite et enregistre le trafic correspondant. Vous pouvez faire soit un fastpath ou un bloc.

**Astuces** Les stratégies IPS et de fichiers attachées à une règle de contrôle d'accès seront automatiquement supprimées pour toutes les actions de la règle, à l'exception de l'option Autoriser.

**Catégorie de règle ACL** - L'outil de migration Secure Firewall préserve les sections de règle dans la configuration ASA gérée par CSM et les migre en tant que catégories ACL sur centre de gestion.

**Avertissement relatif à la capacité et à la limite des règles** - L'outil de migration Secure Firewall compare le nombre total d'ACE pour les règles migrées avec la limite d'ACE prise en charge sur la plate-forme cible.

En fonction du résultat de la comparaison, l'outil de migration Secure Firewall affiche un indicateur visible et un message d'avertissement si le nombre total d'ACE migrés dépasse le seuil ou s'il s'approche du seuil de la limite supportée par le dispositif cible.

Vous pouvez optimiser ou décider de ne pas migrer si les règles dépassent la colonne Compte ACE. Vous pouvez aussi terminer la migration et utiliser ces informations pour optimiser les règles après un transfert sur le centre de gestion avant le déploiement.

**Remarque** L'outil de migration Secure Firewall ne bloque aucune migration malgré l'avertissement.

Vous pouvez désormais filtrer le nombre d'ACE dans l'ordre croissant, décroissant, égal, supérieur et inférieur.

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

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

### Étape 3

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

- **Règles NAT**
- **Objets (objets de liste d'accès, objets de réseau, objets de port, objets VPN et objets de route dynamique)**
- **Interfaces**
- **Routs**
- **Tunnels de réseau privé virtuel (VPN) de site à site**
- **VPN d'accès à distance**

Les objets Liste d'accès affichent les listes d'accès standard et étendues utilisées dans BGP, EIGRP et AD VPN.

Si vous ne souhaitez pas migrer une ou plusieurs règles NAT ou interfaces de routage, cochez la case des lignes concernées, choisissez **Actions > Ne pas migrer**, puis cliquez sur **Enregistrer**.

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

### Étape 4

(Facultatif) Tout en révisant votre configuration, vous pouvez renommer un ou plusieurs objets réseau, port ou VPN dans l'onglet **Objets réseau** ou dans l'onglet **Objets port**, ou dans l'onglet **Objets VPN** en choisissant **Actions > Renommer**.

Les règles d'accès et politiques NAT référant aux objets renommés sont aussi mises à jour avec de nouveaux noms d'objet.

### Étape 5

Dans la section **Objets de routage dynamique**, tous les objets pris en charge étant migrés sont affichés :

- Liste de politiques
- Liste des préfixes
- Route-Carte
- Liste de communautés
- Chemin d'accès AS
- Accès-Liste

### Étape 6

Dans la section **Routes**, les routes suivantes sont affichées :

- Statiques - Affiche toutes les routes statiques IPv4 et IPv6
- BGP - Affiche toutes les routes BGP.

- EIGRP - Affiche toutes les routes EIGRP.

Pour EIGRP, les clés d'authentification sont obtenues si la configuration `more system:running` est téléchargée et que les clés ne sont pas chiffrées. Si la clé est chiffrée dans la configuration de la source, vous pouvez fournir manuellement la clé dans la section de l'interface dans EIGRP. Vous pouvez choisir le type d'authentification (chiffrée, non chiffrée, autorisée ou aucune) et fournir la clé selon le cas.

- ECMP - Affiche toutes les zones ECMP.

**Remarque** La seule action pouvant être effectuée dans cette section est de renommer les zones ECMP.

- PBR - Affiche toutes les routes PBR.

## Étape 7

Dans la section **VPN d'accès à distance**, tous les objets correspondant au VPN d'accès à distance sont migrés de l'ASA vers le centre de gestion et sont affichés :

- **Fichiers Anyconnect** - 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 du dispositif ASA source et doivent être disponibles pour la migration.

Dans le cadre de l'activité de pré-migration, téléchargez tous les paquets AnyConnect vers le centre de gestion. Vous pouvez téléverser directement les profils AnyConnect vers le centre de gestion ou à partir de l'outil de migration Secure Firewall.

Sélectionnez les paquets AnyConnect, Hostscan ou External Browser préexistants récupérés depuis le centre de gestion. Vous devez sélectionner au moins un paquet AnyConnect. Vous devez sélectionner Hostscan, dap.xml, data.xml, ou un navigateur externe si disponible dans la configuration source. Les profils AnyConnect sont facultatifs.

Dap.xml doit être le bon fichier à récupérer de l'ASA. Les validations sont effectuées sur dap.xml qui sont disponibles dans le fichier de configuration. Vous devez téléverser et choisir tous les fichiers nécessaires pour la validation. Si la mise à jour n'est pas effectuée, elle sera considérée comme incomplète et l'outil de migration Secure Firewall ne procédera pas à la validation.

- **AAA** - Les serveurs d'authentification de type Radius, LDAP, AD, LDAP, SAML et Local Realm sont affichés. Mettez à jour les clés pour tous les serveurs AAA. À partir de l'outil de migration Secure Firewall 3.0, les clés pré-partagées sont récupérées automatiquement pour un ASA Live Connect. Vous pouvez aussi téléverser la configuration source avec les clés cachés utilisant le fichier **more system: running-config**. Pour récupérer la clé d'authentification AAA en format texte clair, suivez les étapes ci-dessous :

**Remarque** Ces étapes devraient être effectuées à l'extérieur de l'outil de migration Secure Firewall

1. Connectez-vous à l'ASA via la console SSH.
2. Entrez la commande `more system:running-config`.
3. Allez à la section **aaa-server et utilisateur local** pour trouver toute la configuration AAA et les valeurs de clé respectives en format texte clair.

```
ciscoASA#more system:running-config
!
aaa-server Test-RADIUS (inside) host 2.2.2.2
 key <key in clear text> <-----The radius key is now displayed in clear text format.
aaa-server Test-LDAP (inside) host 3.3.3.3
```

```
ldap-login-password <Mot de passe en clair> <-----Le mot de passe LDAP/AD/LDAPS est désormais
affiché en clair.
```

```
username Test_User password <Password in clear text> <-----The Local user
password is shown in clear text.
```

**Remarque** Si le mot de passe de l'utilisateur local est crypté, vous pouvez vérifier en interne le mot de passe ou en configurer un nouveau dans l'outil de migration Secure Firewall.

- LDAPS nécessite le domaine dans le centre de gestion. Vous devez mettre à jour le domaine pour le type de chiffrement LDAPS.
- Le domaine unique primaire AD est requis pour centre de gestion sur un serveur AD. Si un domaine unique est identifié, il sera affiché sur l'outil de migration Secure Firewall. S'il y a conflit, vous devez saisir un domaine primaire AD unique pour transférer avec succès les objets

Pour un serveur AAA avec le chiffrement réglé à LDAPS, ASA supporte l'adresse IP et le nom d'hôte ou le domaine mais le centre de gestion prend en charge seulement le nom d'hôte ou le domaine. Si la configuration ASA contient le nom d'hôte ou le domaine, celui-ci est récupéré et affiché. Si la configuration de l'ASA contient l'adresse IP pour LDAPS, entrez un domaine dans la section **AAA sous VPN d'accès à distance**. Vous devez saisir le domaine qui peut être résolu à l'adresse IP du serveur AAA.

Pour les serveurs AAA de type AD (le type de serveur est Microsoft dans la configuration de l'ASA), le **domaine primaire AD** est un champ obligatoire à configurer sur un centre de gestion. Ce champ n'est pas configuré séparément sur l'ASA et est extrait de la configuration LDAP-base-dn sur l'ASA.

Si le ldap-base-dn est : ou=Test-Ou,dc=gcevpn,dc=com

Le **domaine primaire AD** est le champ commençant par dc, avec dc=gcevpn et dc=com qui forme le domaine primaire. Le domaine primaire AD serait gcevpn.com.

Fichier exemple de LDAP-base-dn :

```
cn=asa,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:
```

Ici, dc=abec, et dc=com seraient combinés comme abc.com pour former le domaine primaire AD.

```
cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:
```

Le domaine primaire AD est fwsecurity.cisco.com.

Le domaine primaire AD est récupéré automatiquement et affiché sur l'outil de migration Secure Firewall.

**Remarque** La valeur du domaine primaire AD doit être unique pour chaque objet Realm. En cas où un conflit serait détecté ou si l'outil de migration Firewall est incapable de trouver la valeur dans la configuration ASA, vous devez saisir un domaine primaire AD pour le serveur spécifique. Saisissez le domaine primaire AD pour valider la configuration.

- **Ensemble des adresses** - Tous les ensembles IPv4 et IPv6 sont affichés ici.
- **Stratégies de groupe** - Cette section affiche les stratégies de groupe avec les profils de client, les profils de gestion, les modules de client et les stratégies de groupe sans profils. Si le profil a été ajouté dans la section du fichier AnyConnect, il est affiché tel que pré-sélectionné. Vous pouvez choisir ou enlever le profil d'utilisateur, le profil de gestion et le profil de module de client.
- **Profil de connexion** - Tous les profils de connexions/groupes tunnels sont affichés ici.
- **Point de confiance** - La migration des points de confiance ou objets PKI de l'ASA vers le centre de gestion fait partie de l'activité de pré-migration et est nécessaire à la réussite de la migration du VPN AD. Mettez en

correspondance le point de confiance pour Global SSL, IKEv2 et l'interface dans la section **Interface d'accès à distance** pour passer aux étapes suivantes de la migration. Les points de confiance Global SSL et IKEv2 sont obligatoires si le protocole LDAPS est activé. Si un objet SAML existe, les points de confiance pour SAML IDP et SP peuvent être mappés dans la section SAML. Le certificat SP est facultatif. Le point de confiance peut également être modifié pour un groupe de tunnels spécifique. Si la configuration du point de confiance SAML outrepasé est disponible dans l'ASA source, elle peut être sélectionnée dans l'option **Passer outre SAML**.

Pour plus d'informations sur l'exportation de certificats PKI à partir d'ASA, voir [Exporter le certificat PKI à partir d' Pare-feu ASA avec services FirePOWER et l'importer dans le centre de gestion](#) et l'importer dans ce dernier.

- **Cartes de certificats** - Les cartes de certificats sont affichées ici.

**Étape 8** (Facultatif) Pour télécharger les détails pour chaque élément de configuration dans la grille, cliquez sur **Télécharger**.  
**Étape 9** Après avoir complété votre examen, cliquez sur **Valider**.

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

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

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

**Étape 10** Lorsque la validation est terminée, si la boîte de dialogue **Statut de la validation** montre un ou plusieurs conflits d'objets, faites ce qui suit :

a) Cliquez sur **Résoudre les conflits**

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

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

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

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

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

e) Cliquez sur **Résoudre**

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

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

**Étape 11** Lorsque la validation est terminée et que la boîte de dialogue **Statut de la validation** affiche le message **Validé avec succès**, continuez avec [Transférer la configuration migrée vers Centre de gestion, à la page 46](#)

## Transférer la configuration migrée vers Centre de gestion

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

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



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

**Étape 1** Dans la boîte de dialogue **Statut de validation**, examinez le sommaire de la validation.

**Étape 2** Cliquez sur **Transférer la configuration** pour envoyer la configuration du dispositif migré ASA avec FPS à centre de gestion.

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 permet également d'optimiser le téléchargement des fichiers CSV et d'appliquer les actions par page ou sur toutes les règles.

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

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

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

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

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

#### Assistance à l'échec de migration

Si votre migration a échoué, contactez le soutien technique.

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

La page de soutien technique apparaît.

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

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

3. Cliquez sur **Télécharger**.

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

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

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

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

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

## Examiner le rapport de post-migration et terminer la migration

Le rapport de post-migration fournit des détails sur le nombre d'ACL dans différentes catégories, l'optimisation des ACL et la vue d'ensemble de l'optimisation effectuée sur le fichier de configuration. Pour plus de renseignements, consultez [Optimiser, examiner et valider la configuration, à la page 41](#)

Examiner et vérifier les objets :

- **Catégorie**

- Règles ACL totales (Configuration Source)
- Règles ACL totales considérées pour optimisation Par exemple, Redondant, Dupliquée et ainsi de suite.
- Comptes ACL pour optimisation indique le nombre total de règles ACL comptées avant et après l'optimisation.

Si vous avez oublié de télécharger les rapports de post-migration pendant la migration, utilisez le lien suivant pour les télécharger :

Rapport de post-migration Télécharger le point final—[http://localhost:8888/api/downloads/post\\_migration\\_summary\\_html\\_format](http://localhost:8888/api/downloads/post_migration_summary_html_format)



**Remarque** Vous pouvez télécharger les rapports seulement lorsque l'outil de migration Secure Firewall est en cours d'exécution.

### Étape 1

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

### Étape 2

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

- **Résumé de la migration** - Résumé de la configuration qui a été migrée avec succès de ASA avec FPS de vers Défense contre les menaces, y compris des informations sur , centre de gestionle nom d'hôte et le domaine, le dispositifDéfense contre les menaces cible (le cas échéant) et les éléments de configuration qui ont été migrés avec succès.
- **Migration sélective des règles** : les détails de la fonction spécifique de ASA avec FPS de sélectionné pour la migration sont disponibles dans trois catégories : Fonctions de configuration du dispositif, Fonctions de configuration partagées et Optimisation.
- **Mappage de l'interface de ASA avec FPS du dispositif géré par vers l'interface de défense contre les menaces** - Détails des interfaces migrées avec succès et de la manière dont vous avez mappé les l'ASA avec FPS du vers les Défense contre les menanceinterfaces du dispositif. Confirmez que ces mappages rencontrent vos attentes.

**Remarque** Cette section ne s'applique pas aux migrations sans dispositif de destination Défense contre les menacesou si les **interfaces**ne sont **pas** sélectionnées pour la migration.

- **Noms d'interface source vers les zones de sécurité et les groupes d'interfaces de défense contre les menaces** - Détails des interfaces logiques et des noms des ASA avec FPS du migrés avec succès et comment vous les avez mappés vers les zones de sécurité et les groupes d'interfaces dans Défense contre les menaces. Confirmez que ces mappages rencontrent vos attentes.

**Remarque** Cette section ne s'applique pas si les **listes de contrôle d'accès** et le **NAT** ne sont **pas** sélectionnés pour la migration.

- **Gestion des conflits d'objets** - Détails de ASA avec FPS des objets de qui ont été identifiés comme ayant des conflits avec des objets existants dans centre de gestion. Si les objets ont le même nom et configuration, l'outil de migration Secure Firewall a réutilisé l'objet centre de gestion. Si les objets ont le même nom mais une configuration différente, vous avez renommé ces objets. Examinez ces objets attentivement et vérifiez que les conflits aient été résolu adéquatement.
- **Règles de contrôle d'accès, NAT et routes que vous avez choisi de ne pas migrer** - Détails des règles que vous avez choisi de ne pas migrer avec l'outil de migration Secure Firewall. Examinez ces règles qui ont été désactivées par l'outil de migration Secure Firewall et qui n'ont pas été migrées. Examinez ces lignes et vérifiez que toutes les règles que vous avez choisies sont listées dans cette section. Si désiré, vous pouvez configurer manuellement ces règles.
- **Configuration partiellement migrée** - Détails des règles de ASA avec FPS qui n'ont été que partiellement migrées, y compris les règles avec des options avancées lorsque la règle pouvait être migrée sans les options avancées. Examinez ces lignes, vérifiez que les options avancées soient prises en charge dans centre de gestion, et si oui, configurez manuellement ces options.
- **Configuration non prise en charge** - détails des éléments de configuration des ASA avec FPS de qui n'ont pas été migrés car l'outil de migration Secure Firewall ne prend pas en charge la migration de ces fonctionnalités. Examinez ces lignes, vérifiez que chaque caractéristique soit prise en charge dans Défense contre les menaces. Si oui, configurez manuellement ces options dans centre de gestion.
- **Règles de politique de contrôle d'accès étendues** - Détails des règles de politique de contrôle d'accès des ASA avec FPS de qui ont été étendues d'une seule règle de point en plusieurs règles Défense contre les menaces au cours de la migration.
- **Actions prises sur les règles de contrôle d'accès**
  - **Règles d'accès que vous avez choisi de ne pas migrer** - Détails des règles de contrôle d'accès de ASA avec FPS que vous avez choisi de ne pas migrer avec l'outil de migration Secure Firewall. Examinez ces lignes et vérifiez que toutes les règles que vous avez choisies sont listées dans cette section. Si désiré, vous pouvez configurer manuellement ces règles.
  - **Règles d'accès avec modification de l'action de la règle** - Détails de toutes les règles de politique de contrôle d'accès dont l'action de la règle a été modifiée à l'aide de l'outil de migration Secure Firewall. Les valeurs d'action de la règle sont les suivantes - Autoriser, Faire confiance, Surveiller, Bloquer, Bloquer avec réinitialisation. Examinez ces lignes et vérifiez que toutes les règles que vous avez choisies sont listées dans cette section. Si désiré, vous pouvez configurer manuellement ces règles.
  - **Règles de contrôle d'accès auxquelles la politique IPS et l'ensemble de variables sont appliqués** - Détails de toutes ASA avec FPS de auxquelles la politique IPS est appliquée. Examinez attentivement ces règles et déterminez si la caractéristique est supportée dans Défense contre les menaces.
  - **Règles de contrôle d'accès auxquelles s'applique la politique de gestion des fichiers** - Détails de toutes les règles de contrôle d'accès d' ASA avec FPS auxquelles s'applique la politique de gestion des fichiers. Examinez attentivement ces règles et déterminez si la caractéristique est supportée dans Défense contre les menaces.

- **Règles de contrôle d'accès dont le paramètre « Journal » a été modifié** - Détails des règles de contrôle ASA avec FPS dont le paramètre « Journal » a été modifié à l'aide de l'outil de migration Secure Firewall. Les valeurs de réglage du journal sont : False, Event Viewer, Syslog. Examinez ces lignes et vérifiez que toutes les règles que vous avez choisies sont listées dans cette section. Si désiré, vous pouvez configurer manuellement ces règles.
- **Règles de contrôle d'accès qui ont échoué la recherche de zone**- Détails des règles ASA avec FPS de qui échouent à l'opération Recherche de route et qui sont renseignées dans le **rapport de post-migration**. L'outil de migration Secure Firewall effectue l'opération de recherche de route sur la base des informations de route (statique et connectée) dans la configuration source pour remplir les zones de sécurité de destination dans les règles d'accès.
- **Règles de contrôle d'accès pour les protocoles tunnelisés** - Détails des règles tunnelisées qui sont migrées en tant que règles tunnelisées de préfiltrage lors de la migration.

**Remarque** Une règle non supportée n'ayant pas été migrée cause des problèmes avec du trafic non désiré à travers votre pare-feu. Nous vous recommandons de configurer une règle dans centre de gestion qui assurera le blocage du trafic dans Défense contre les menaces.

**Remarque** S'il est nécessaire d'appliquer un IPS ou une politique de fichier à l'ACL dans la page **Examiner et valider**, il est fortement recommandé de créer une politique sur le centre de gestion avant la migration. Utilisez la même politique, alors que l'outil de migration Secure Firewall récupère la politique du centre de gestion connecté. Créer une nouvelle politique et l'assigner à de multiples politiques peut dégrader la performance et causer l'échec du transfert.

Pour plus d'informations à propos des caractéristiques prises en charge dans centre de gestion et Défense contre les menaces, consultez le [Guide de configuration du centre de gestion, Version 6.2.3](#).

### Étape 3

Ouvrez le **rapport de pré-migration** et notez tous les éléments de configuration des ASA avec FPS que vous devez migrer manuellement sur le Défense contre les menaces dispositif.

### Étape 4

Dans centre de gestion, faites ceci :

- Examinez la configuration migrée dans l'appareil Défense contre les menaces pour confirmer que toutes les règles attendues et autres articles de configuration, incluant ce qui suit, ont été migrés :
  - Listes de contrôle d'accès (ACL)
  - Règles de traduction d'adresse réseau
  - Port et objets réseau
  - Routs
  - Interfaces
  - Objets IP SLA
  - Recherche groupée d'objets
  - Objets temporels
  - Objets VPN
  - Tunnels de réseau privé virtuel (VPN) de site à site
  - Objets de routage dynamique

- b) Configurez tout élément et règle partiellement pris en charge, non pris en charge, ignoré et désactivé qui n'a pas été migré.

Pour plus d'informations sur comment configurer ces éléments et règles, référez-vous à [Guide de configuration du centre de gestion](#) Voici des exemples d'items de configuration demandant une configuration manuelle :

- Paramètres de la plateforme, y compris l'accès SSH et HTTPS, comme décrit dans Paramètres de la [plateforme pour la défense contre les menaces](#)
- Paramètres Syslog, comme décrit dans la section [Configurer Syslog](#)
- Routage dynamique, tel que décrit dans la section [Vue d'ensemble du routage pour la défense](#) contre les menaces
- Les politiques de service, telles que décrites dans les [politiques FlexConfig](#)
- Configuration VPN, comme décrit dans [Threat Defense VPN](#)
- Paramètres du journal des connexions, tels que décrits dans la section [Journal des connexions](#)

#### Étape 5

Après avoir complété votre révision, déployez la configuration migrée de centre de gestion vers l'appareil Défense contre les menaces.

Vérifier que les données sont correctement reflétées dans le **rapport post-migration** pour les règles non prises en charge et partiellement prises en charge.

L'outil de migration Secure Firewall assigne les politiques à l'appareil Défense contre les menaces. Vérifiez que les changements soient reflétés dans la configuration en cours d'exécution. Pour vous aider à identifier les politiques migrées, la description de ces politiques inclut le nom d'hôte de la configuration de ASA avec FPS de .

---

## Désinstaller l'outil de migration Secure Firewall

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

---

#### Étape 1

Naviguez jusqu'au dossier où vous avez téléchargé l'outil de migration Secure Firewall.

#### Étape 2

Si vous voulez sauvegarder les journaux, coupez ou copiez et collez le dossier `journal` vers un endroit différent.

#### Étape 3

Si vous voulez sauvegarder les rapports pré-migration et les rapports post-migration, coupez ou copiez et collez le dossier `ressources` vers un endroit différent.

#### Étape 4

Supprimez le dossier où vous avez placé l'outil de migration Secure Firewall.

**Astuces** Le fichier `journal` est associée avec la fenêtre de la console. Si la fenêtre de la console pour l'outil de migration Secure Firewall est ouverte, le fichier `journal` et le dossier ne peuvent pas être supprimés.

# Exemple de migration : ASA avec vers Threat Defense 2100



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

## Tâches de la fenêtre de pré-maintenance

### Avant de commencer

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

- Étape 1** Utilisez la commande `show running-config` pour le ou le contexte que vous faites migrer et enregistrez une copie de la configuration d'ASA avec FPS. Voir [Afficher la configuration en cours d'exécution](#).
- Vous pouvez également utiliser Adaptive Security Device Manager (ASDM) pour le dispositif ou le contexte que vous souhaitez migrer et choisir **Fichier > Afficher la configuration en cours d'exécution dans une nouvelle fenêtre** pour obtenir le fichier de configuration.
- Remarque** Pour un contexte multiple, vous pouvez utiliser la commande `show tech-support` pour obtenir la configuration de tous les contextes dans un seul fichier.
- Étape 2** Examinez le fichier de configuration d'ASA avec FPS.
- Étape 3** Déployez Série Firepower 2100 l'appareil dans votre réseau, connectez les interfaces et mettez l'appareil sous tension. Pour plus d'informations, consultez le [Guide de démarrage rapide Cisco Threat Defense pour la série 2100 en utilisant le centre de gestion](#).
- Étape 4** Inscrivez l'appareil Série Firepower 2100 qui sera géré par le centre de gestion. Pour plus d'informations, consultez [Ajouter des appareils au centre de gestion](#).
- Étape 5** (Facultatif) Si la configuration du dispositif géré par le des canaux de port, créez des canaux de port (EtherChannels) sur le dispositif cible Série Firepower 2100. Pour plus d'informations, consultez [Configurez des EtherChannels et les interfaces redondantes](#).
- Étape 6** Téléchargez et exécutez la version la plus récente de l'outil de migration Secure Firewall de <https://software.cisco.com/download/home/286306503/type>. Pour en savoir plus, consultez [Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com, à la page 23](#).
- Étape 7** Lorsque vous lancez l'outil de migration Secure Firewall et que vous spécifiez les paramètres de destination, assurez-vous de sélectionner l'appareil Série Firepower 2100 que vous avez enregistré vers le centre de gestion. Pour en savoir plus, consultez [Préciser les paramètres de destination pour l'outil de migration de pare-feu sécurisé, à la page 31](#).

- Étape 8** Mappez les interfaces ASA avec FPS avec les interfaces avec les interfaces Défense contre les menaces.
- Remarque** L'outil de migration Secure Firewall vous permet de mapper un d'interface ASA ASA avec FPS au type Défense contre les menaces d'interface.
- Par exemple, vous pouvez mapper un canal de port dans un à une interface physique dans Défense contre les menaces.
- Pour plus d'informations, voir [Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager](#).
- Étape 9** Lors du mappage des interfaces logiques aux zones de sécurité, cliquez sur **Création automatique** pour permettre à l'outil de migration Secure Firewall de créer de nouvelles zones de sécurité. Pour utiliser les zones de sécurité existantes, mappez manuellement les logiques de l'ASA ASA avec un géré par FDM aux zones de sécurité.
- Pour plus d'informations, voir [Mapper les interfaces ASA à des zones de sécurité et à des groupes d'interfaces](#).
- Étape 10** Suivez les instructions de ce guide pour examiner et valider de manière séquentielle la configuration à migrer, puis pour pousser la configuration vers le centre de gestion.
- Étape 11** Examinez le rapport post-migration, installez manuellement et déployez les autres configurations vers le Défense contre les menaces et complétez la migration.
- Pour plus de renseignements, consultez la section [Examiner le rapport de post-migration et terminer la migration](#), à la page 48.
- Étape 12** Testez l'appareil Série Firepower 2100 à l'aide du plan de test que vous avez créé lors de la planification de la migration.
- 

## Tâches de la fenêtre de maintenance

### Avant de commencer

Assurez-vous d'avoir complété toutes les tâches devant être effectuées avant la fenêtre d'entretien. Consultez [Tâches de la fenêtre de pré-maintenance](#), à la page 52.

---

- Étape 1** Connectez-vous via la console SSH et changez pour le mode de configuration d'interface.
- Étape 2** Arrêtez les interfaces du à l'aide de la commande **shutdown**.
- Étape 3** (Facultatif) Accédez au centre de gestion et configurez le routage dynamique pour le dispositif Série Firepower 2100.
- Pour plus d'informations, référez-vous à [Routage dynamique](#)
- Étape 4** Effacez le cache du protocole de résolution d'adresses (ARP) sur l'infrastructure de commutation environnante
- Étape 5** Effectuez des tests ping de base depuis l'infrastructure de commutation environnante jusqu'aux adresses IP de l'interface de l'appareil Série Firepower 2100, afin de vous assurer qu'elles sont accessibles.
- Étape 6** Effectuez des tests de ping de base à partir d'appareils qui nécessitent un routage de couche 3 vers les adresses IP de l'interface de l'appareil Série Firepower 2100.
- Étape 7** Si vous attribuez une nouvelle adresse IP à l'appareil Série Firepower 2100 et ne réutilisez pas l'adresse IP attribuée à l'appareil géré par ASA avec FPS, procédez comme suit :
1. Mettez à jour toutes les routes statiques qui réfèrent aux adresses IP afin qu'elles puissent maintenant pointer vers l'adresse IP de l'appareil Série Firepower 2100.
  2. Si vous utilisez des protocoles de routage, assurez-vous que les voisins voient l'adresse IP de l'appareil Série Firepower 2100 comme le prochain saut vers les destinations attendues.

**Étape 8** Exécutez un plan de test complet et surveillez les journaux dans le cadre de la gestion de centre de gestion pour votre appareil Firepower 2100.

---



## CHAPITRE 3

# Cisco Success Network - Données de télémétrie

- [Cisco Success Network – Données de télémétrie, à la page 55](#)

## Cisco Success Network – Données de télémétrie

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

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

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

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

**Tableau 2 : Télémétrie limitée**

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

| Point de données                | Description                                                              | Exemple de valeur                                |
|---------------------------------|--------------------------------------------------------------------------|--------------------------------------------------|
| Version de gestion des cibles   | La version cible du centre de gestion                                    | 6.5 ou plus récent                               |
| Type de gestion cible           | Le type de périphérique de gestion cible, à savoir le centre de gestion  | Centre de gestion                                |
| Version du périphérique cible   | La version du périphérique cible                                         | 75                                               |
| Modèle de l'appareil cible      | Le modèle du périphérique cible                                          | Cisco Secure Firewall Threat Defense pour VMware |
| Version de l'outil de migration | La version de l'outil de migration                                       | 1.1.0.1912                                       |
| État de la migration            | L'état de la migration de la configuration ASA vers le centre de gestion | SUCCÈS                                           |

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

**Tableau 3 : Télémétrie étendue**

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

**Tableau 4 : Informations sur le source**

| Point de données                        | Description                                              | Exemple de valeur   |
|-----------------------------------------|----------------------------------------------------------|---------------------|
| Durée                                   | L'heure et la date de collecte des données de télémétrie | 2023-04-25 10:39:19 |
| Type de source                          | Le type de périphérique source                           |                     |
| Numéro de série du périphérique source  | Numéro de série de l'ASA                                 | JAF1528ACAD         |
| Numéro de modèle du périphérique source | Numéro de modèle de l'ASA                                | ASA 5505-X          |
| Version du périphérique source          | Version d'ASA avec FPS                                   | 9.2(2)              |
| Nombre de configurations sources        | Le nombre total de lignes dans la configuration source   | 504                 |

| Point de données                                                                     | Description                                                                   | Exemple de valeur |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------|
| Mode pare-feu                                                                        | Le mode de pare-feu configuré sur ASA - routé ou transparent                  | ROUTAGE           |
| Mode contextuel                                                                      | Le mode de contexte d'ASA. Il peut s'agir d'un contexte unique ou multiple.   | UNIQUE            |
| <b>Statistiques de configuration ASA :</b>                                           |                                                                               |                   |
| Nombre d'ACL                                                                         | Le nombre d'ACL associées au groupe d'accès                                   | 46                |
| Nombre de règles d'accès                                                             | Le nombre total de règles d'accès                                             | 46                |
| Nombre de règles NAT                                                                 | Le nombre total de règles NAT                                                 | 17                |
| Compte d'objets réseau                                                               | Le nombre d'objets réseau configurés dans ASA                                 | 34                |
| Nombre de groupes d'objets réseau                                                    | Le nombre de groupes d'objets réseau dans ASA                                 | 6                 |
| Compte d'objets de port                                                              | Le nombre d'objets de port                                                    | 85                |
| Compte de groupes d'objets de port                                                   | Le nombre de groupes d'objets de port                                         | 37                |
| Nombre de règles d'accès non prises en charge                                        | Le nombre total de règles d'accès non prises en charge                        | 3                 |
| Nombre de règles NAT non prises en charge                                            | Le nombre total de règles d'accès NAT non prises en charge                    | 0                 |
| Nombre de règles d'accès basées sur FQDN                                             | Le nombre de règles d'accès basées sur le nom de domaine complet (FQDN)       | 7                 |
| Nombre de règles d'accès basées sur une plage de temps                               | Le nombre de règles d'accès basées sur une plage de temps                     | 1                 |
| Nombre de règles d'accès basées sur SGT                                              | Le nombre de règles d'accès basées sur SGT                                    | 0                 |
| <b>Résumé des lignes de configuration que l'outil n'est pas en mesure d'analyser</b> |                                                                               |                   |
| Nombre de configurations non analysées                                               | Le nombre de lignes de configuration non reconnues par l'analyseur syntaxique | 68                |
| Nombre total de règles d'accès non analysées                                         | Le nombre total de règles d'accès non analysées                               | 3                 |
| <b>Plus de détails sur la configuration ASA...</b>                                   |                                                                               |                   |
| Le VPN d'accès à distance est-il configuré                                           | Si le VPN d'accès à distance est configuré sur ASA                            | faux              |
| Le VPN S2S est-il configuré                                                          | Si le VPN de site à site est configuré sur ASA                                | faux              |

| Point de données                   | Description                                | Exemple de valeur |
|------------------------------------|--------------------------------------------|-------------------|
| Le BGP est-il configuré            | Si BGP est configuré sur ASA               | faux              |
| L'EIGRP est-il configuré           | Si EIGRP est configuré sur ASA             | faux              |
| Le protocole OSPF est-il configuré | Si OSPF est configuré sur ASA              | faux              |
| Comptes d'utilisateurs locaux      | Le nombre d'utilisateurs locaux configurés | 0                 |

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

| Point de données                | Description                                                           | Exemple de valeur                                |
|---------------------------------|-----------------------------------------------------------------------|--------------------------------------------------|
| Version de gestion des cibles   | La version cible de centre de gestion                                 | 6.5 ou plus récent                               |
| Type de gestion cible           | Le type de périphérique de gestion cible, à savoir, centre de gestion | Centre de gestion                                |
| Version du périphérique cible   | La version du périphérique cible                                      | 75                                               |
| Modèle de l'appareil cible      | Le modèle du périphérique cible                                       | Cisco Secure Firewall Threat Defense pour VMware |
| Version de l'outil de migration | La version de la migration aussi l                                    | 2.3.4                                            |

Tableau 6 : Résumé de la migration

| Point de données                             | Description                                           | Exemple de valeur |
|----------------------------------------------|-------------------------------------------------------|-------------------|
| <b>Stratégie de contrôle d'accès</b>         |                                                       |                   |
| Nom                                          | Le nom de la stratégie de contrôle d'accès            | N'existe pas      |
| Nombre de règles d'accès (FPS)               | Le nombre total de règles d'ACL FPS migrées           | 10                |
| Nombre de règles d'ACL partiellement migrées | Le nombre total de règles d'ACL partiellement migrées | 3                 |
| Nombre de règles ACP étendu                  | Le nombre de règles ACP étendues                      | 0                 |
| <b>Fonction NAT</b>                          |                                                       |                   |
| Titre du champ                               | Le nom de la politique de NAT                         | N'existe pas      |
| Nombre de règles NAT                         | Le nombre total de règles NAT migrées                 | 0                 |
| Nombre de règles NAT partiellement migrées   | Le nombre total de règles NAT partiellement migrées   | 0                 |
| <b>Plus de détails sur la migration...</b>   |                                                       |                   |
| Nombre d'interfaces                          | Le nombre d'interfaces mises à jour                   | 0                 |
| Nombre de sous-interfaces                    | Le nombre de sous-interfaces mises à jour             | 0                 |

| Point de données                     | Description                                      | Exemple de valeur |
|--------------------------------------|--------------------------------------------------|-------------------|
| Nombre de routes statiques           | Le nombre de routes statiques                    | 0                 |
| Nombre d'objets                      | Le nombre d'objets créés                         | 34                |
| Nombre de groupes d'objet            | Le nombre de groupes d'objets créés              | 6                 |
| Nombre de groupes d'interfaces       | Le nombre de groupes d'interfaces créés          | 0                 |
| Nombre de zones de sécurité          | Le nombre de zones de sécurité créées            | 3                 |
| Nombre d'objets réseau réutilisés    | Le nombre d'objets réutilisés                    | 21                |
| Nombre de renommages d'objets réseau | Le nombre d'objets qui sont renommés             | 1                 |
| Nombre d'objets de port réutilisés   | Le nombre d'objets de port qui sont réutilisés   | 0                 |
| Nombre d'objets de port renommés     | Le nombre d'objets de port qui sont renommés     | 0                 |
| Nombre de règles du préfiltre        | Le nombre de règles de préfiltre provenant d'ASA | 44                |

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

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

### Fichier d'exemple de télémétrie ASA avec FPS

Voici un exemple de fichier de données de télémétrie sur la migration de la configuration ASA avec FPS vers défense contre des menaces :

```
"Verbatim_Comments": "Very good!",
"asa_config_stats": {
"Ipv6_access_rule_counts": 0,
"Ipv6_bgp_count": 0,
```

```

"Ipv6_nat_rule_count": 0,
"Ipv6_network_counts": 10,
"Ipv6_static_route_counts": 3,
"access_rules_counts": 39,
"acl_category_count": 0,
"acl_counts": 60,
"cert_based_auth": false,
"dm_inline_applied": 0,
"dm_inline_present": 0,
"dynamic_crypto_map": false,
"fqdn_based_access_rule_counts": 0,
"ikev1_count": 0,
"ikev2_count": 0,
"is_aaa_configured": false,
"is_anyconnect_configured": false,
"is_bgp_configured": false,
"is_eigrp_configured": false,
"is_ipv6_configured": true,
"is_multicast_configured": false,
"is_ospf_configured": false,
"is_pbr_configured": false,
"is_ra_vpn_configured": false,
"is_s2s_vpn_configured": false,
"is_snmp_configured": false,
"is_ssl_server_version_configured": false,
"is_webvpn_configured": false,
"local_users_counts": 1,
"nat_rule_counts": 38,
"network_object_counts": 76,
"network_object_group_counts": 10,
"no_of_fqdn_based_objects": 6,
"ospfv3_count": 0,
"port_object_counts": 10,
"port_object_group_counts": 26,
"s2s_vpn_tunnel_counts": 0,
"s2s_vpn_vti": false,
"sgt_based_access_rules_count": 0,
"timerange_based_access_rule_counts": 0,
"total_unparsed_access_rule_counts": 3,
"tunneling_protocol_based_access_rule_counts": 0,
"unparsed_config_count": 115,
"unsupported_access_rules_count": 9,
"unsupported_nat_rule_count": 2,
"vpn_object_count": 0
},
"context_mode": "SINGLE",
"error_description": null,
"error_message": null,
"feedback_score": "5",
"firewall_mode": "ROUTED",
"log_info_acl_count": 0,
"migration_status": "SUCCESS",
"migration_summary": {
 "access_control_policy": [
 [
 {
 "access_rule_counts": 16,
 "apply_file_policy_rule_counts": 1,
 "apply_ips_policy_rule_counts": 2,
 "apply_log_rule_counts": 0,
 "do_not_migrate_rule_counts": 0,
 "enable_hit_count": false,
 "expanded_acp_rule_counts": 0,
 "name": "Doesn't Exist",
 "partially_migrated_acl_rule_counts": 9,

```

```
"time_based_acl_count": 0,
"total_acl_element_counts": 98,
"update_rule_action_counts": 0
}]
],
"interface_counts": 0,
"interface_group_counts": 0,
"interface_group_manually_created_counts": 0,
"ip_sla_monitor_count": 0,
"nat_Policy": [
 [
 [
 "NAT_rule_counts": 0,
 "do_not_migrate_rule_counts": 0,
 "name": "Doesn't Exist",
 "partially_migrated_nat_rule_counts": 1
]
]
],
"network_object_rename_counts": 0,
"network_object_reused_counts": 83,
"object_group_counts": 10,
"objects_counts": 90,
"port_object_rename_counts": 0,
"port_object_reused_counts": 0,
"prefilter_control_policy": [
 [
 [
 "do_not_migrate_rule_counts": 0,
 "name": "Doesn't Exist",
 "partially_migrated_acl_rule_counts": 0,
 "prefilter_rule_counts": 44
]
]
],
"security_zone_counts": 8,
"security_zone_manually_created_counts": 0,
"static_routes_counts": 0,
"sub_interface_counts": 0,
"time_out": false
},
"migration_tool_version": "2.4",
"mtu_info": {
 "interface_name": null,
 "mtu_value": null
},
"rule_change_acl_count": 0,
"selective_policy": {
 "acl": false,
 "acl_policy": false,
 "application": false,
 "csm": true,
 "fps_acl": true,
 "interface": false,
 "interface_groups": true,
 "migrate_tunneled_routes": false,
 "nat": false,
 "network_object": true,
 "policy_assignment": true,
 "policy_based_crypto_map": false,
 "populate_sz": false,
 "port_object": false,
 "remote_deployment_enabled": false,
 "route_based_vti": false,
 "routes": false,
 "s2s_vpn_flag": false,
 "security_zones": true,
 "unreferenced": false
}
```

```
},
"source_config_counts": 813,
"source_device_model_number": " ASAv, 8192 MB RAM, CPU Xeon E5 series 2600 MHz, 1 CPU (4
cores)",
"source_device_serial_number": "9A2EPUNLD80",
"source_device_version": "9.6(3)1",
"source_type": "ASAFPS",
"system_information": {
"browser": "Chrome/91.0.4472.124",
"operating_system": "Windows NT 10.0; Win64; x64"
},
"target_device_model": "Not Exists",
"target_device_version": "Not Exists",
"target_management_type": "6.6.1 (build 91)",
"target_management_version": "6.6.1 (build 91)",
"template_version": "1.1",
"time": "2021-07-14 19:10:59",
"tool_analytics_data": {
"objectsplit_100_count": 0
},
"tool_performance": {
"config_push_time": 6,
"conversion_time": 34,
"migration_time": 334
}
```



## CHAPITRE 4

# Dépannage des problèmes de migration

- [Dépannage de l'outil de migration de pare-feu sécurisé, à la page 63](#)
- [Journaux et autres fichiers utilisés pour le dépannage, à la page 64](#)
- [Dépannage de l'ASA avec les échecs de chargement de fichier FPS, à la page 64](#)

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

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

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

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

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

La page de soutien technique apparaît.

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



---

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

---

3. Cliquez sur **Télécharger**.

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

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

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

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



---

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

---

## Journaux et autres fichiers utilisés pour le dépannage

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

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

## Dépannage de l'ASA avec les échecs de chargement de fichier FPS

### ASA avec échec d'extraction du fichier de configuration FPS

L'outil de migration de pare-feu sécurisé ne prend pas en charge la migration des règles de FPS gérées par ASDM vers l'outil de migration de pare-feu sécurisé. Par conséquent, vous devez connaître les informations de configuration avant de migrer lors de la sélection de la configuration source (ASA ou ASA avec FPS). Dans ce cas, vous devez utiliser la source en tant que Cisco ASA au début de la migration.



## CHAPITRE 5

# FAQ de l'outil de migration Secure Firewall

- [Foire aux questions sur l'outil de migration de pare-feu sécurisé, à la page 65](#)

## Foire aux questions sur l'outil de migration de pare-feu sécurisé

- Q.** Quelles sont les nouvelles fonctionnalités prises en charge sur l'outil de migration Secure Firewall pour la version 3.0.1?
- A.** Les caractéristiques suivantes sont prises en charge avec la version 3.0.1 :
- Migration du protocole EIGRP (Enhanced Interior Gateway Routing Protocol) de l'ASA avec FPS.
  - La gamme Secure Firewall 3100 est prise en charge uniquement en tant que périphérique de destination pour la migration.
- Q.** Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration de pare-feu sécurisé pour la version 3.0 ?
- A.** Les caractéristiques suivantes sont prises en charge avec la version 3.0 :
- VPN d'accès à distance
  - Automatisation de clé pré-partagée VPN de site à site
- Q.** Quelles sont les nouvelles fonctionnalités prises en charge sur l'outil de migration Secure Firewall pour la version 2.5.1?
- A.** Les caractéristiques suivantes sont prises en charge avec la version 2.5.1 :
- Objets de routage dynamique
  - Protocole de passerelle frontière
- Q.** Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration de pare-feu sécurisé pour la version 2.4 ?
- A.** Les fonctionnalités suivantes sont prises en charge avec la version 2.4 :
- Migration ASA avec FPS vers la protection contre les menaces.

- Migration du VPN basé sur les certificats dans le centre de gestion.

- Q.** Vous disposez d'un centre de gestion avec huit zones de sécurité FPS, FPS1 avec cinq zones et FPS2 avec trois zones. Les politiques d'ACL associées au FPS1 utilisent une combinaison des zones FPS1 et FPS2 dans les règles d'accès. Les zones FPS1 et FPS2 seront-elles migrées vers la défense contre les menaces?
- A.** L'outil de migration Secure Firewall fera migrer les zones FPS1 vers les zones de défense contre les menaces. Il ne migrera pas les zones FPS2. Cependant, les listes de contrôle d'accès sources utilisant FPS2 seront partiellement migrées.
- Q.** Comment les ACL basées sur les utilisateurs FPS seront-elles migrées?
- A.** L'outil de migration de pare-feu sécurisé ne prend pas en charge la migration des ACL basées sur les utilisateurs FPS vers le centre de gestion. Il supprime le champ Users (Utilisateurs) et fait migrer les listes de contrôle d'accès à l'état désactivé. Vous devez ajouter manuellement le champ Users (Utilisateurs) et activer l'ACL dans le cadre de l'activité de post-migration sur le centre de gestion.

## 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.