Migration d'un appareil géré par FDM vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration

Première publication : 2023-02-02

Dernière modification : 2024-04-26

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

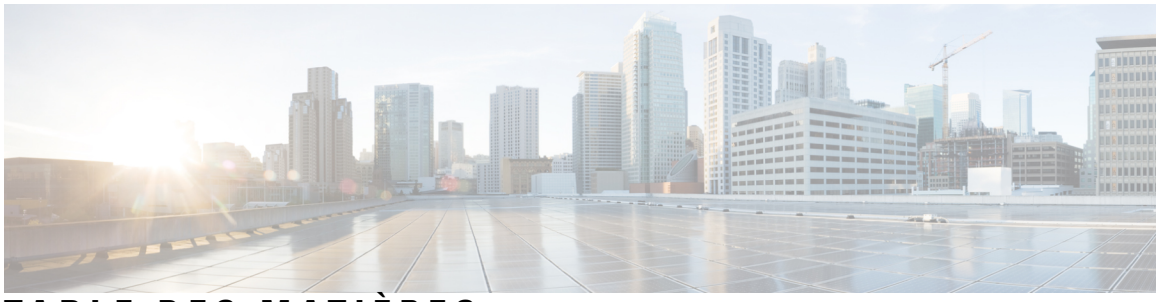
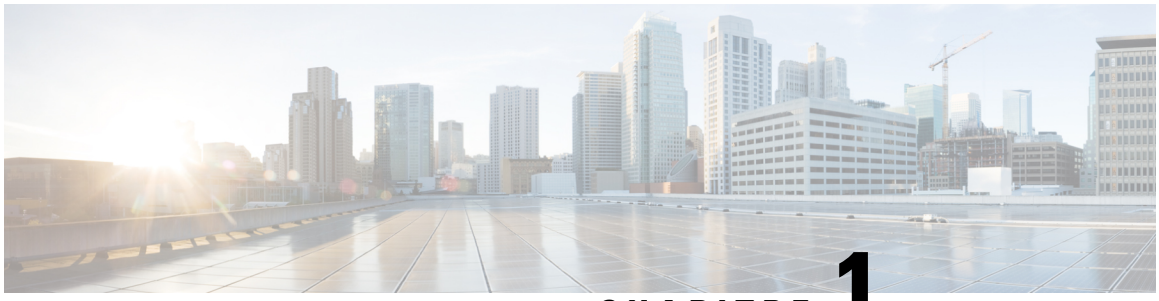


TABLE DES MATIÈRES



CHAPITRE 1

Mise en route de l'outil de migration Secure Firewall

À propos de l'outil de migration Secure Firewall

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

L'exemple de procédure de migration (Exemple de migration : avec dispositif géré par FPS FDM vers Threat Defense 2100) inclus dans ce livre aide à faciliter la compréhension du processus de migration.

L’outil de migration Cisco Secure Firewall convertit les configurations prises en charge de l’appareil géré par FDM en une plateforme Cisco Secure Firewall Threat Defense prise en charge. L’outil de migration Cisco Secure Firewall vous permet de migrer automatiquement les fonctions et les politiques de l’appareil géré par FDM vers défense contre les menaces. Vous devez migrer manuellement toutes les caractéristiques non prises en charge.

L'outil de migration Secure Firewall recueille les informations sur les des dispositifs gérés par FDM, 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 éléments de configuration de dispositif géré par FDM qui sont entièrement migrés, partiellement migrés, non pris en charge pour la migration et ignorés pour la migration.

- Les lignes de configuration de dispositifs gérés par FDM avec erreurs, qui répertorie les composants de dispositif géré par FDM que l'outil de migration Secure Firewall ne peut pas reconnaître, ce qui bloque la migration.

Console

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

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

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

Journaux

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

Vous pouvez trouver les fichiers journaux pour l'outil de migration Secure Firewall à l'endroit suivant : `<migration_tool_folder>\logs`

Ressources

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

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

Fichier non analysé

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

<migration_tool_folder>\resources

Recherche dans l'outil de migration Secure Firewall

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

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

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

Ports

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

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

Cisco Success Network (Réseau de succès Cisco)

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

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

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

Quoi de neuf dans l'outil de migration Secure Firewall

Version	Fonctionnalités prises en charge
6.0	

Version	Fonctionnalités prises en charge
	Cette version comprend les nouvelles caractéristiques et améliorations suivantes : **Migration de Cisco Secure Firewall ASA vers Cisco Secure Firewall Threat Defense** • Vous pouvez maintenant faire la migration des configurations WebVPN de votre Cisco Secure Firewall ASA vers les configurations de Cisco Zero Trust Access Policy sur un appareil de protection contre les menaces. Cochez bien la case **WebVPN** à la page **Select Features** [sélectionner les fonctions] et jetez un œil au nouvel onglet **WebVPN** à la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration]. L'appareil de protection contre les menaces et le centre de gestion cible doit fonctionner sur la version 7.4 ou une version ultérieure et doit exécuter Snort3 comme moteur de détection. • Vous pouvez désormais procéder à la migration des configurations des protocoles SNMP (Simple Network Management Protocol) et DHCP (Dynamic Host Configuration Protocol) vers un appareil de protection contre les menaces. Cochez bien les cases **SNMP** et **DHCP** à la page **Select Features** [sélectionner les fonctions]. Si vous avez configuré le protocole DHCP sur Cisco Secure Firewall ASA, notez que le serveur DHCP, ou l'agent de relais et les configurations du système DDNS, peuvent également être sélectionnés pour la migration. • Vous pouvez désormais effectuer la migration des configurations du routage ECMP (Equal-Cost Multipath) lors de la migration d'un appareil ASA en mode multicontexte vers un contexte unique et fusionné de protection contre les menaces. L'encadré **Routes** [routes] dans le résumé de l'analyse comprend également des zones ECMP, que vous pouvez valider dans l'onglet **Routes** [routes] de la page **Optimize, Review and Validate Configuration** [optimiser, revoir et valider les configurations]. • Vous pouvez désormais effectuer la migration des tunnels dynamiques à partir de l'interface DVTI (Dynamic Virtual Tunnel Interface), de votre Cisco Secure Firewall ASA vers un appareil de protection contre les menaces. Vous pouvez les faire correspondre à la page **Map ASA Interfaces to Security Zones, Interface Groups, and VRFs** [mapper les interfaces ASA aux périmètres de sécurité, aux groupes d'interfaces et aux VRF]. Assurez-vous d'avoir un ASA de version 9.19 (x) ou ultérieure pour que s'applique cette fonctionnalité. **Migration d'un appareil géré par FDM vers Cisco Secure Firewall Threat Defense** • Vous pouvez désormais effectuer la migration des politiques de sécurité de couche 7, y compris les protocoles SNMP et HTTP, ainsi que les configurations des politiques sur les programmes malveillants et les fichiers de votre appareil géré par FDM vers un appareil de protection contre les menaces. Assurez-vous d'avoir un centre de gestion cible de version 7.4 ou ultérieure et vérifiez que les cases des **paramètres de la plateforme** et de la **politique sur les programmes malveillants et les fichiers** à la page **Select Features** [sélectionner les fonctions] sont bien cochées.

Version	Fonctionnalités prises en charge
	Migration du pare-feu Check Point vers Cisco Secure Firewall Threat Defense • Vous pouvez dorénavant effectuer la migration des configurations VPN de site à site (basées sur les politiques) de votre pare-feu Check Point vers un appareil de protection contre les menaces. Notez que cette fonction s'applique aux versions Check Point R80 ou ultérieures, et aux versions 6.7 ou ultérieures du centre de gestion et de Threat Defense. Assurez-vous que la case **Site-to-Site VPN Tunnels** [tunnels VPN de site à site] est bien cochée à la page **Select Features** [sélectionner les fonctions]. Notez qu'étant donné qu'il s'agit d'une configuration propre à l'appareil, l'outil de migration n'affiche pas ces configurations si vous décidez de **poursuivre sans FTD**. **Migration de Fortinet Firewall vers Cisco Secure Firewall Threat Defense** • Vous pouvez dorénavant optimiser vos listes de contrôle d'accès (ACL) lorsque vous procédez à la migration des configurations d'un pare-feu Fortinet à votre appareil de protection contre les menaces. Utilisez le bouton **Optimize ACL** [optimiser l'ACL] à la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration] pour consulter la liste des ACL redondantes et dupliquées et pour télécharger le rapport d'optimisation qui détaille l'ACL.

Version	Fonctionnalités prises en charge
5.0.1	Cette version comprend les nouvelles caractéristiques et améliorations suivantes : • L'outil de migration Cisco Secure Firewall prend maintenant en charge la migration de plusieurs contextes de sécurité transparents en mode pare-feu à partir des appareils Cisco Secure Firewall ASA vers les appareils de protection contre les menaces. Vous pouvez fusionner au moins deux contextes transparents en mode pare-feu qui se trouvent dans votre appareil Cisco Secure Firewall ASA à une instance en mode transparent, et procéder ensuite à leur migration. Là où au moins un de vos contextes dispose d'une configuration VPN, lors d'un déploiement ASA avec VPN configuré, vous pouvez choisir un seul contexte pour lequel vous souhaitez réaliser la migration de la configuration VPN vers l'appareil cible de protection contre les menaces. À partir des contextes que vous n'avez pas sélectionnés, seule la configuration VPN est ignorée, tandis que toutes les autres configurations font l'objet d'une migration. Consultez la rubrique Select the ASA Security Context [sélectionner le contexte de sécurité ASA] pour en savoir plus. • Vous pouvez désormais procéder à la migration des configurations VPN de site à site et avec accès à distance à partir de vos pare-feu Fortinet et Palo Alto Networks vers la protection contre les menaces au moyen de l'outil de migration Cisco Secure Firewall. Depuis le panneau **Select Features** [sélectionner les fonctions], choisissez les fonctions VPN à migrer. Consultez la rubrique Specify Destination Parameters for the Secure Firewall Migration Tool [indiquer les paramètres de destination pour l'outil de migration Cisco Secure Firewall] dans les guides Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool [migration du pare-feu Palo Alto Networks vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration] et Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool [migration du pare-feu Fortinet vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration]. • Vous pouvez désormais sélectionner au moins un contexte de sécurité routé ou transparent en mode pare-feu à partir de vos appareils Cisco Secure Firewall ASA et procéder à la migration à un ou plusieurs contextes au moyen de l'outil de migration Cisco Secure Firewall.

Version	Fonctionnalités prises en charge
5.0	• L'outil de migration Cisco Secure Firewall prend maintenant en charge la migration de plusieurs contextes de sécurité à partir des appareils Cisco Secure Firewall ASA vers les appareils de protection contre les menaces. Vous pouvez choisir d'effectuer la migration de configurations à partir d'un de vos contextes ou fusionner les configurations de tous vos contextes routés en mode pare-feu, et ensuite procéder à leur migration. Un soutien sera bientôt offert pour la fusion des configurations de plusieurs contextes transparents en mode pare-feu. Consultez la rubrique Select the ASA Primary Security Context [sélectionner le contexte de sécurité primaire ASA] pour en savoir plus. • L'outil de migration tire maintenant profit de la fonctionnalité virtuelle de routage et de transfert afin de reproduire le flux de trafic divisé, qui est observé dans un environnement ASA à plusieurs contextes, lequel fera partie de la nouvelle configuration fusionnée. Vous pouvez vérifier le nombre de contextes qu'a détecté l'outil de migration dans un nouvel encadré **Contexts** [contextes] et pareillement après l'analyse, dans un nouvel encadré **VRF** de la page **Parsed Summary** [résumé de l'analyse]. De plus, l'outil de migration affiche les interfaces auxquelles sont mappés ces VRF, à la page **Map Interfaces to Security Zones and Interface Groups** [mapper les interfaces aux périmètres de sécurité et aux groupes d'interfaces]. • Vous pouvez désormais essayer l'intégralité du flux de travail de la migration au moyen du nouveau mode de démonstration de l'outil Cisco Secure Firewall et visualiser à quoi ressemble réellement votre migration. Consultez la rubrique Using the Demo Mode in Firewall Migration Tool [utilisation du mode de démonstration de l'outil de migration du pare-feu] pour en savoir plus. • Grâce aux nouvelles améliorations et à la correction des problèmes, l'outil de migration Cisco Secure Firewall offre maintenant une expérience améliorée et plus rapide lors de la migration du pare-feu Palo Alto Networks vers Threat Defense.
4.0.3	L'outil de migration Secure Firewall 4.0.3 comprend des corrections de bogues et les nouvelles améliorations suivantes : • L'outil de migration offre désormais un écran de **mappage d'application amélioré** pour la migration des configurations de PAN vers la défense contre les menaces. Reportez-vous à la section Mappage des configurations avec les applications lors de la *migration du pare-feu de Palo Alto Networks vers Secure Firewall Threat Defense avec le guide de l'outil de* migration pour plus d'informations.
4.0.2	L'outil de migration Secure Firewall 4.0.2 inclut les nouvelles caractéristiques et améliorations suivantes : • L'outil de migration dispose désormais d'une télémétrie permanente; cependant, vous pouvez désormais choisir d'envoyer des données de télémétrie limitées ou élargies. Les données de télémétrie limitées comprennent peu de points de données, tandis que les données de télémétrie élargies envoient une liste plus détaillée de données de télémétrie. Vous pouvez modifier ce paramètre dans **les Paramètres** > **Envoyer les données de télémétrie à Cisco?**.

Version	Fonctionnalités prises en charge
4.0.1 ou ultérieure	L'outil de migration Secure Firewall 4.0.1 inclut les nouvelles caractéristiques et améliorations suivantes : L'outil de migration Secure Firewall analyse maintenant tous les objets et groupes d'objets selon leur nom et leur configuration et réutilise les objets qui ont le même nom et configuration. Seuls les objets réseaux et les groupes d'objets réseaux sont analysés selon leur nom et configuration antérieure. À noter que les profils XML dans les VPN d'accès à distance sont toujours valides uniquement à l'aide de leur nom.
4.0	L'outil de migration Secure Firewall 4.0 prend en charge : Migration d'un dispositif géré par FDM vers le centre de gestion à condition que la version du centre de gestion de destination soit 7.3 ou ultérieure et que la version du gestionnaire du dispositif source soit 7.2 ou ultérieure. La version du gestionnaire d'appareil doit être égale ou supérieure à la version du centre de gestion destinataire. Les options suivantes sont disponibles pour la migration : 1. **Migrer Firepower Device Manager (Configurations partagées uniquement)** : Cette option vous permet d'effectuer des migrations par étapes. Dans ce cas, vous pourrez d'abord migrer toutes les configurations partagées et migrer les configurations d'appareil plus tard selon vos besoins. Durant le processus de migration, seules les configurations partagées sont migrées au centre de gestion ciblé. Le paquet de configuration obtenu à partir du gestionnaire de périphériques peut être téléchargé ou les informations d'identification du gestionnaire de périphériques peuvent être fournies pour que l'outil récupère les détails de la configuration. L'extraction automatisée des détails de la configuration est la méthode préférée. 2. **Migrer Firepower Device Manager (inclut les configurations d'appareil et partagés)** : Cette option vous permet de migrer à la fois le dispositif et les configurations partagées du gestionnaire de dispositifs vers le centre de gestion ciblé. Une fois le dispositif source et sa configuration migrés vers le centre de gestion cible, le dispositif géré par le FDM devient le dispositif du centre de gestion cible. Pour que l'outil puisse récupérer les détails de la configuration, vous devez fournir les informations d'identification du gestionnaire de périphérique. Seule une récupération automatique des configurations est autorisée pour cette option de migration. 3. **Migrer Firepower Device Manager (y compris le dispositif et les configurations partagées) vers le dispositif FTD (nouveau matériel)** : Cette option permet de migrer le dispositif et la configuration partagée vers un dispositif de défense contre les menaces géré par le centre de gestion ciblé. Dans ce cas, au cours du processus de migration, le dispositif source n'est pas migré et seule la configuration du dispositif est migrée vers le nouveau dispositif de défense contre les menaces. Le paquet de configuration obtenu à partir du gestionnaire de périphériques peut être téléchargé ou les informations d'identification du gestionnaire de périphériques peuvent être fournies pour que l'outil récupère les détails de la configuration. L'extraction automatisée des détails de la configuration est la méthode préférée.

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 de l'appareil géré par FDM

Vous pouvez obtenir un groupe de configurations pour l'appareil géré par FDM, soit manuellement soit en vous connectant à un appareil géré par FDM en direct, à partir de l'outil de migration Cisco Secure Firewall. Un chargement manuel n'est pris en charge que pour les options suivantes :

- Migrer le gestionnaire d'appareil Firepower (y compris les dispositifs et les configurations partagées) vers le dispositif FTD (nouveau matériel)
- Migrer le gestionnaire d'appareil Firepower (Configurations partagées uniquement)

Remarque Un chargement manuel n'est pas pris en charge pour l'option **Migrate Firepower Device Manager (Includes Device & Shared Configurations)** [migrer le gestionnaire d'appareil Firepower (y compris les configurations partagées et celles de l'appareil)].

Le groupe de configurations de l'appareil géré par FDM que vous devez importer manuellement dans l'outil de migration Cisco Secure Firewall doit remplir les exigences suivantes :

- Contient seulement des configurations valides de la CLI du gestionnaire d'appareil.
- Comprend le numéro de version.
- Le groupe de configurations doit être en format .zip.
- Dispose d'une configuration entièrement exportée, à partir du gestionnaire d'appareil, consultez Export the FDM-managed device Configuration File [exporter le fichier de configuration de l'appareil géré par FDM] à la page 28.

- Doit avoir au moins un fichier .txt contenant la configuration.
- Des clés devraient être fournies pour le groupe chiffré. Pour les groupes non chiffrés, la clé de chiffrement peut être laissée vide.
- Ne contient pas d'erreurs de syntaxe.
- N'a pas été codé à la main ou modifié manuellement.

Exigences et conditions préalables pour les appareils Threat Defense

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

- Le matériel de défense contre les menaces doit être supérieur ou égal au modèle de dispositif géré par FDM. Par exemple, si le modèle du dispositif géré par le FDM source est 2100, le modèle de défense contre les menaces de destination peut être 2100 ou 3100 ou 4100 ou 9300, mais pas un modèle inférieur à 2100.
- 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 dispositif géré par le FDM ; 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 l'appareil de protection contre les menaces cible est une instance de contenant, il doit utiliser au minimum un nombre égal d'interfaces et de sous-interfaces physiques et d'interfaces et de sous-interfaces de canal de port (sauf pour la gestion seulement) que celui de l'appareil géré par FDM. Si vous devez ajouter le type nécessaire d'interface sur l'appareil cible de protection contre les menaces.

Remarque

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

Soutien pour la configuration de l'appareil géré par FDM

Configuration des dispositifs gérés par FDM pris en charge

L'outil de migration Cisco Secure Firewall peut totalement migrer les configurations suivantes de l'appareil géré par FDM :

- 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 Cisco Secure Firewall ne migre pas les objets de service étendus (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)
- Politique de contrôle d'accès
- NAT automatique et NAT manuelle
- Routes statiques, routes ECMP
- Interfaces physiques
- VLAN secondaires sur les interfaces de l'appareil géré par FDM qui ne sont pas 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.

- 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 processus de configuration partagée et sera désactivée.
- Objets temporels

- 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 par rapport aux 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 de l'appareil géré par FDM source vers la solution FTD cible.

- Tunnels de réseau privé virtuel (VPN) de site à site
  - VPN de site à site : Lorsque l'outil de migration Cisco Secure Firewall détecte la configuration de la carte cryptographique dans l'appareil géré par FDM source, l'outil de migration Cisco Secure Firewall migre cette carte vers le VPN du centre de gestion en tant que topologie point à point.
  - VPN basé sur une carte cryptographique (statique/dynamique) à partir d'un appareil géré par FDM.
  - VPN FDM basé sur les routes (VTI)
  - Migration VPN basée sur un certificat à partir de l'appareil géré par FDM
  - La migration des certificats ou des points de confiance des appareils gérés par FDM vers le centre de gestion doit être effectuée manuellement et fait partie de l'activité de prémigration.

- 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.
  - Dans le cadre des activités préalables à la migration, effectuez les opérations suivantes:
    - Faites migrer manuellement les points de confiance de l'appareil géré par FDM vers le centre de gestion en tant qu'objets PKI.
    - Récupérez les paquets AnyConnect, les fichiers Hostscan (Dap.xml, Data.xml, paquet Hostscan), le paquet du navigateur externe et les profils AnyConnect à partir de l'appareil géré par FDM source.
    - Chargez tous les packages AnyConnect sur lecentre de gestion.
    - Chargez les profils AnyConnect directement vers centre de gestion ou à partir de l'outil de migration Cisco Secure Firewall.
- Politiques relatives aux fichiers et aux logiciels malveillants
  - L'outil de migration ajoute les politiques des programmes malveillants et des fichiers de votre appareil géré par FDM aux règles respectives dans une politique de contrôle d'accès, qui est transmise au centre de gestion cible.
  - Des politiques de fichiers par défaut, comme Block Malware All et Malware Cloud Look up – No Block, sont créées.
- Politiques de déchiffrement SSL
- SNMP
  - Pour SNMPv1 et SNMPv2, assurez-vous que l'identifiant de communauté est mis à jour manuellement à la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration].
  - Pour SNMPv3, assurez-vous que les mots de passe pour l'authentification et le chiffrement de l'utilisateur soient fournis manuellement à la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration].

Configurations de l'appareil géré par FDM prises en charge partiellement

L'outil de migration Cisco Secure Firewall prend en charge partiellement les configurations suivantes de l'appareil géré par FDM pour la 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 de l'appareil géré par FDM non prises en charge

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

- Règles de politique de contrôle d'accès basées sur SGT
- Objets basés sur SGT
- Règles de politique de contrôle d'accès basées sur l'utilisateur
- Règles NAT configurées avec l'option d'allocation de bloc
- Objets dont le type et le code ICMP ne sont pas pris en charge
- Règles de contrôle d'accès basées sur le protocole de tunnellisation

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

- Règles NAT configurées avec SCTP
- Règles NAT configurées avec l'hôte « 0.0.0.0 »
- Route par défaut obtenue par DHCP ou PPPoE avec suivi SLA
- Calendrier du suivi SLA
- Mode de transport IPsec transform-set
- Migration des points de confiance de l'appareil géré par FDM vers le centre de gestion
- Mode de pare-feu transparent pour BGP
- Groupes d'utilisateurs et groupes d'hôtes SNMPv3

Objets dans l'appareil géré par FDM et la protection contre les menaces

Un fichier de configuration pour l'appareil géré par FDM contient les objets suivants, que vous pouvez migrer vers la protection contre les menaces :

- Objets de réseau
- Les objets de service, appelés objets de port dans Threat Defense
- Objets IP SLA
- Objets temporels
- Objets VPN (politique IKEv1/IKEv2, proposition IKEv1/IKEv2 IPSec)
- Objets de la route dynamique (Policy-List, Prefix-List, Route-Map, Community-List, AS-Path, Access-List et Route-Map)
- BGP et EIGRP pris en charge en mode routé
- Objets VPN RA
- Règle de groupe
- Objets AAA (Radius, SAML, domaine local, domaine AD/LDAP/LDAPS)
- Ensemble des adresses (IPv4 et IPv6)
- Profil de connexion
- Carte d'attributs LDAP
- Politique IKEv2
- Proposition IPSec IKEv2
- Carte de certificat
- DAP
- Politique de prévention des intrusions
- Règles d'intrusion

Lignes directrices et limites relatives à la licence

Lignes directrices pour la migration des appareils gérés par FDM

Voici les lignes directrices pour la migration de l'appareil géré par FDM au moyen de l'outil de migration Cisco Secure Firewall :

- Chaque objet de l'appareil géré par FDM a un nom et une configuration unique – L'outil de migration Cisco Secure Firewall migre les objets avec succès sans changements.
- Le nom d'un objet de l'appareil géré par FDM comprend au moins un caractère spécial qui n'est pas pris en charge par le centre de gestion – L'outil de migration Cisco Secure Firewall renomme les caractères spéciaux dans le nom de l'objet avec le caractère « _ » pour remplir le critère de dénomination d'objets du centre de gestion.

- Un objet de l’appareil géré par FDM a le même nom et configuration qu’un objet existant dans le centre de gestion — L’outil de migration Cisco Secure Firewall réutilise l’objet du centre de gestion pour la configuration de la protection contre les menaces et ne migre pas l’objet de l’appareil géré par FDM.
- Une multitude d’objets de l’appareil géré par FDM ont le même nom, mais dans une casse différente – L’outil de migration Cisco Secure Firewall renomme des objets de ce type afin de remplir le critère de dénomination des objets.

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.

Limites pour la configuration de l’appareil géré par FDM

Voici les limites imposées à votre migration de la configuration source de l’appareil géré par FDM :

- Les objets et règles NAT non supportés ne sont pas migrés.
- Les règles ACL qui ne sont pas prises en charge sont migrées dans le centre de gestion en tant que règles désactivées.
- Toutes les cartes cryptographiques de l’appareil géré par FDM prises en charge seront migrées en tant que topologie point à point du centre de gestion.
- Les topologies VPN cryptographiques non supportées ou incomplètes ne seront pas migrées.
- Vous ne pouvez pas migrer certaines configurations de l’appareil géré par FDM, par exemple, le routage dynamique vers la protection contre les menaces. Migrez manuellement ces configurations.
- Les groupes d’objets de service imbriqués ou les groupes de ports ne sont pas pris en charge par le centre de gestion. Dans le cadre de la conversion, l'outil de migration Secure Firewall étend le contenu du groupe objet imbriqué ou du groupe de port.
- L'outil de migration 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 règles de centre de gestion ayant exactement la même signification.
- Si la configuration source de l’appareil géré par FDM a des règles de contrôle d’accès qui ne renvoient pas à des protocoles de tunnelage en particulier (comme GRE, IP dans IP, et IP6 dans IP), mais que ces règles correspondent à un trafic de tunnelage non chiffré sur l’appareil géré par FDM, alors, en migration vers la protection contre les menaces, les règles correspondantes ne se comporteront pas de la même manière qu’elles le font sur l’appareil géré par FDM. Nous vous conseillons de créer des règles de tunnel précises pour celles-ci dans la politique de préfiltrage, sur la protection contre les menaces.
- Les cartes cryptographiques de l’appareil géré par FDM prises en charge seront migrées en tant que topologie point à point.
- Si un objet AS-Path portant le même nom dans le centre de gestion apparaît, la migration cesse et affiche le message d’erreur suivant :

  « Conflicting AS-Path object name detected in the centre de gestion, please resolve conflict in centre de gestion to proceed further » [conflit de noms d’objets AS-Path détecté dans le centre de gestion, veuillez résoudre le conflit dans le centre de gestion pour continuer]

- L’objet Route-Map est partiellement migré à l’aide de l’outil de migration Cisco Secure Firewall. Les clauses « match » et « set » ne sont pas prises en charge en raison des limites de l’API.
- Les politiques de couche 7, comme la politique d’identité, la politique SSL, les renseignements de sécurité, SGT et les règles basées sur l’utilisateur ne sont pas migrées en raison des limites de l’API.

Limites pour la migration AD VPN

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

- La migration des attributs personnalisés, des paramètres SSL et de l’équilibrage de charges VPN 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 une configuration de l’appareil géré par FDM est trouvée avec un serveur AAA dont l’autorisation dynamique est activée sans interface, l’outil de migration Cisco Secure Firewall ignore l’autorisation dynamique. Vous devez activer manuellement l'autorisation dynamique après avoir choisi une interface dans le centre de gestion.
- 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.

Plateformes prises en charge pour la migration

Le périphérique géré par FDM et les plateformes défense contre les menacessuivantes sont pris en charge pour la migration avec l’outil de migration Cisco Secure Firewall : Pour plus d’informations sur les plateformes défense contre les menaces prises en charge, consultez le Guide de compatibilité de Cisco Secure Firewall.

Plateformes de périphériques sources gérées par FDM

Vous pouvez utiliser l'outil de migration de pare-feu pour migrer la configuration des platesformes de dispositifs gérés par FDM suivantes :

- Firepower de Série 1000
- Série Firepower 2100
- Secure Firewall de Série 3100
- Firepower de série 4100
- Secure Firewall de Série 4200

- Série Firepower 9300
- FDM virtuel sur VMware, AWS, Azure, KVM

Plateformes Défense contre les menaces cibles prises en charge

Vous pouvez utiliser l'outil de migration Secure Firewall pour migrer une source vers l'instance autonome ou conteneur suivante des platesformes défense contre les menaces :

- Firepower de Série 1000
- Série Firepower 2100
- Secure Firewall de Série 3100
- Firepower de série 4100
- Secure Firewall de Série 4200
- Série Firepower 9300 qui comprend :
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- Threat Defense sur VMware, déployé à l'aide de VMware ESXi, VMware vSphere Web Client ou le client autonome vSphere
- Threat Defense Virtual sur Microsoft Azure Cloud ou AWS Cloud

Remarque

- Pour les conditions préalables et la préparation de défense contre les menaces virtuellesl'installation dans Azure, voir la section Prise en main de Secure Firewall Threat Defense Virtual et Azure.
- Pour les prérequis et la mise en place préalable de défense contre les menaces virtuellesdans AWS Cloud, voir les prérequis virtuels de Threat Defense.

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

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

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 21.
- Vous avez obtenu et installé des licences intelligentes défense contre les menacesqui incluent toutes les fonctionnalités que vous prévoyez de migrer depuis ASA , comme décrit ci-dessous :
  - La section Mise en route du compte Smart de Cisco sur Cisco.com
  - Enregistrez le Centre de gestion du pare-feu avec le Cisco Smart Software Manager.
  - Octroi de licences pour le système de pare-feu
  - Vous avez activé l'API REST.centre de gestion

    Sur l'interface Web centre de gestion, allez à **System** > **Configuration [configuration du système]** > **Rest API Preferences [préférences REST API]** > **Enable Rest API [activer REST API]**, puis cochez la case **Enable Rest API [activer REST API]**.

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

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

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

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

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

Régions CDO

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

Tableau 1 : Régions CDO et URL

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

Versions logicielles prises en charge pour la migration

Les outils de migration Secure Firewall, géré par FDM et les versions défense contre les menacespour la migration sont les suivants :

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

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

Versions prises en charge des dispositifs gérés par FDM

L'outil de migration Secure Firewall prend en charge la migration à partir d'un dispositif géré par FDM qui utilise la version 7.2 ou ultérieure du logiciel de défense contre les menaces.

Versions du centre de gestion prises en charge pour la configuration source des dispositifs gérés par FDM

Pour un dispositif géré par FDM, l'outil de migration Secure Firewall prend en charge la migration vers un dispositif de défense contre les menaces géré par un centre de gestion qui exécute la version 7.2+.

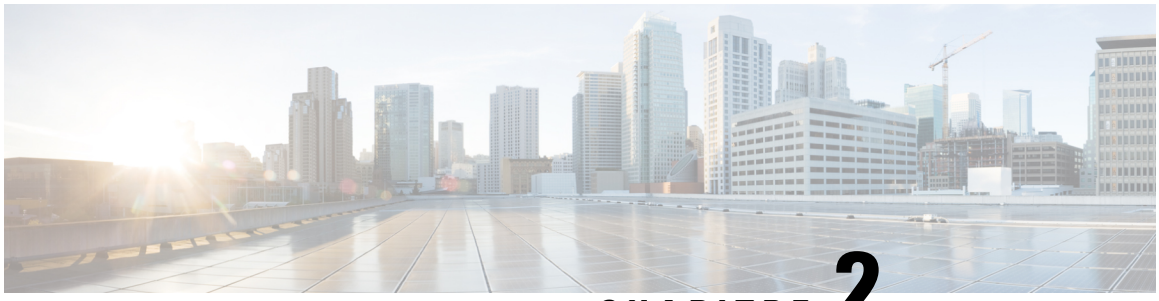
Remarque

- Certaines fonctionnalités ne sont prises en charge que dans la dernière version du centre de gestion et de la défense contre les menaces.
- Pour des temps de migration optimaux, nous vous recommandons de mettre à niveau le centre de gestion vers la version suggérée mentionnée dans le logiciel.cisco.com/downloads.

Versions Défense contre les menaces prises en charge

Pour les dispositifs gérés par FDM, l'outil de migration Secure Firewall prend en charge la migration vers un dispositif qui utilise la version 7.2 ou ultérieure de la défense contre les menaces.

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

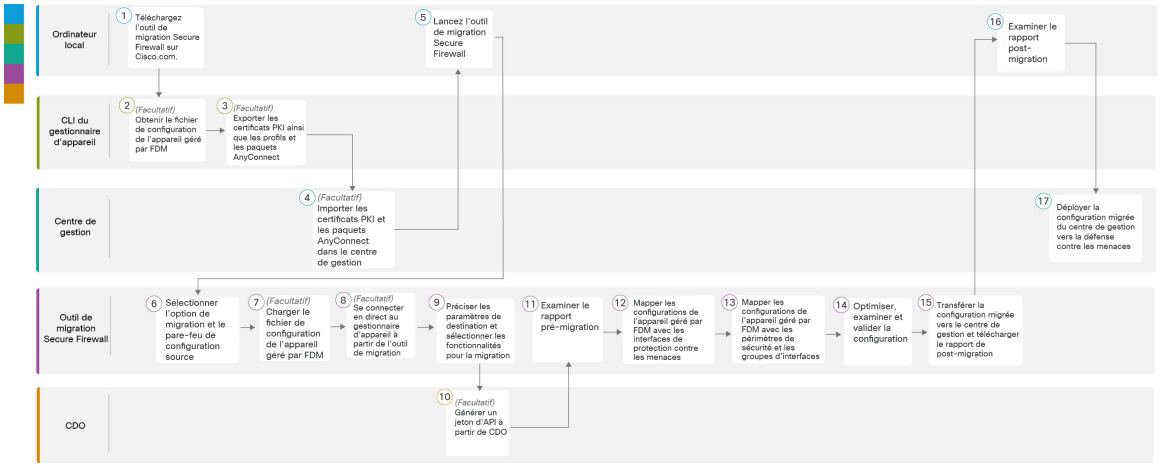


CHAPITRE 2

Flux de travail de l'appareil géré par FDM vers Threat Defense

Procédure de bout en bout

L'organigramme suivant illustre le flux de travail de migration d'un appareil géré par FDM vers la protection contre les menaces à l'aide de l'outil de migration Cisco Secure Firewall.



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

	Espace de travail	Étapes
2	CLI du gestionnaire d'appareil	(Facultatif) Obtenez le fichier de configuration de l'appareil géré par FDM : Pour obtenir le fichier de configuration de l'appareil géré par FDM à partir de la CLI du gestionnaire d'appareil, consultez Obtenir le fichier de configuration du dispositif géré par FDM [obtenir le fichier de configuration de l'appareil géré par FDM]. Si vous avez l'intention de connecter l'appareil géré par FDM à partir de l'outil de migration Cisco Secure Firewall, passez à l'étape 3.
3	CLI du gestionnaire d'appareil	(Facultatif) Exporter les certificats PKI ainsi que les profils et les paquets AnyConnect : Cette étape n'est requise que si vous prévoyez de migrer les fonctions VPN de site à site et les fonctions VPN RA de l'appareil géré par FDM vers la protection contre les menaces. Pour exporter les certificats PKI à partir de la CLI du gestionnaire d'appareil, consultez Exporter le certificat PKI à partir du gestionnaire d'appareil et l'importer dans le Centre de gestion Firepower [exporter un certificat PKI et l'importer dans le centre de gestion du pare-feu, étape 1]. Pour exporter les profils et les paquets AnyConnect à partir de la CLI du gestionnaire d'appareil, consultez Récupérer les paquets et les profils AnyConnect [récupérer les profils et les paquets AnyConnect, étape 1]. Si vous ne prévoyez pas de migrer le VPN site à site et l'AD VPN, passez à l'étape 7.
4	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 à partir du gestionnaire d'appareil et l'importer dans le Centre de gestion Firepower et Récupérer les paquets et les profils AnyConnect.
5	Ordinateur local	Lancez l'outil de migration Secure Firewall sur votre machine locale, voir Lancer l'outil de migration Secure Firewall.
6	Outil de migration Secure Firewall	Pour sélectionner l'option de migration et de pare-feu de la configuration source, consultez Sélectionnez la configuration source et l'option de migration du gestionnaire d'appareil [sélectionner l'option de la migration et du pare-feu de la configuration source].
7	Outil de migration Secure Firewall	(Facultatif) Pour savoir comment charger le fichier de configuration de l'appareil géré par FDM obtenu de la CLI du gestionnaire d'appareil, consultez Téléverser le paquet configuration FDM [charger le fichier de configuration de l'appareil géré par FDM]. Si vous prévoyez de vous connecter à l'appareil géré par FDM en direct, passez à l'étape 8.
8	Outil de migration Secure Firewall	Vous pouvez vous connecter au gestionnaire d'appareil directement à partir de l'outil de migration Cisco Secure Firewall. Pour en savoir plus, consultez Connectez-vous au périphérique géré par FDM à partir de l'outil de migration Secure Firewall [connexion à l'appareil géré par FDM à partir de l'outil de migration Cisco Secure Firewall].
9	Outil de migration Secure Firewall	Durant cette étape, vous pouvez spécifier les paramètres de destination pour la migration. Pour les étapes détaillées, référez-vous à Préciser les paramètres de destination pour l'outil de migration Secure Firewall .

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

Préalables pour la migration

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

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

Avant de commencer

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

Étape 1 Sur votre ordinateur, créez un dossier pour l'outil de migration Secure Firewall

Nous vous recommandons de ne pas stocker d'autres fichiers dans ce dossier. Lorsque vous lancez l'outil de migration Secure Firewall, il place les journaux, ressources et tous les autres fichiers dans ce dossier.

Remarque Peu importe quand vous téléchargez la plus récente version de l'outil de migration Secure Firewall, assurez-vous de créer un nouveau fichier et de ne pas utiliser le dossier actuel.

Étape 2 Naviguez vers https://software.cisco.com/download/home/286306503/type et cliquez sur **Outil de migration Firewall**

Le lien ci-dessus vous amène à l'outil de migration Secure Firewall sous Firewall NGFW Virtual. Vous pouvez également télécharger l'outil de migration Secure Firewall à partir des zones de téléchargement des appareils défense contre les menaces.

Étape 3 Téléchargez la version la plus récente de l'outil de migration Secure Firewall dans le dossier que vous avez créé.

Téléchargez l'exécutable approprié de l'outil de migration Secure Firewall pour les machines Windows ou macOS.

Obtenir le fichier de configuration du dispositif géré par FDM

Vous pouvez utiliser une des méthodes suivantes pour obtenir un fichier de configuration de dispositif géré par FDM :

- Exporter le fichier de configuration du périphérique géré par FDM, à la page 26
- Connectez-vous au périphérique géré par FDM à partir de l'outil de migration Secure Firewall, à la page 38

Exporter le fichier de configuration du périphérique géré par FDM

Cette tâche n'est requise uniquement que si vous voulez téléverser manuellement un fichier de configuration de dispositif géré par FDM. Le fichier de configuration du gestionnaire d'appareil peut être exporté en utilisant l'API de la défense contre les menaces. Lorsque la configuration est exportée, le système crée un fichier ZIP. Le fichier ZIP peut être téléchargé vers l'ordinateur local. La configuration elle-même est représentée sous forme d'objets définis à l'aide de paires attribut-valeur dans un fichier texte au format JSON.

Lorsque vous faites une exportation, vous devez spécifier quelles configurations doivent être incluses dans le fichier d'exportation. Une exportation complète comprend toute la configuration dans le fichier d'exportation zip.

Le fichier d'exportation zip peut comprendre ce qui suit :

- Paires attribut-valeur qui définissent chaque objet configuré. Tous les éléments configurables sont modélisés en tant qu'objets, et pas seulement ceux qui sont appelés « objets » dans le gestionnaire de périphériques.
- VPN d'accès à distance, les paquets AnyConnect et tous les autres fichiers référencés tels que les fichiers XML du profil client, le fichier XML DAP et les paquets Hostscan.
- Liste de nettoyage référencée ou liste de détection personnalisée si vous avez configuré des stratégies de fichiers personnalisées.

Étape 1 Créez le corps de l'objet JSON pour l'exportation.

Exemple :

Ce qui suit est un exemple d'objet JSON.

```
  "diskFileName": "string",
  "encryptionKey": "*********",
  "doNotEncrypt": false,
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": true,
  "entityIds": [
    "string"
  ],
  "jobName": "string",
  "type": "scheduleconfigexport"
}
```

Les attributs sont,

- **diskFileName** - (Facultatif) Le nom du fichier d'exportation zip Si vous ne spécifiez pas de nom, le système génère un nom par défaut. Même si vous spécifiez un nom, le système peut ajouter des caractères au nom pour garantir l'unicité. Le nom a une longueur maximale de 60 caractères.
- **encryptionKey** - Une clé de chiffrement pour le fichier zip. Si vous ne voulez pas chiffrer le fichier, ignorez ce champ et spécifiez plutôt **doNotEncrypt: true**. Si vous spécifiez une clé, utilisez la clé pour ouvrir le fichier zip après l'avoir téléchargé sur votre ordinateur local. Le fichier de configuration exporté expose des clés secrètes, des mots de passe et autres données sensibles en texte clair (sinon ils ne peuvent pas être importés). Dans ce cas vous voudrez peut-être appliquer une clé de chiffrement pour protéger les données sensibles. Le système utilise le chiffrement AES 256.
- **doNotEncrypt**-(Facultatif) Indique si le fichier d'exportation doit être chiffré (false) ou non (true). La valeur par défaut est false, ce qui signifie que vous devez spécifier un attribut de clé de chiffrement non vide. Si vous spécifiez true, l'attribut de clé de chiffrement est ignoré.
- **configExportType** - Vous pouvez sélectionner l'un des types d'exportation suivants pour exporter les fichiers de configuration :
  - FULL EXPORT - Comprend toute la configuration dans le fichier d'exportation. **C'est l'option par défaut et devrait être choisie pour la migration**

- **deployedObjectsOnly**-(Facultatif) Indique si les objets doivent être inclus dans le fichier d'exportation uniquement s'ils ont été déployés. La valeur par défaut est false, ce qui signifie que tout changement en attente est inclus dans l'exportation. Spécifiez true pour exclure les changements en attente.
- **entityIds** - Une liste d'identités séparées par des virgules avec un ensemble d'objets de point de départ entre [crochets]. La liste est nécessaire pour une tâche PARTIAL_EXPORT. Chaque élément de la liste peut être une valeur UUID ou une paire attribut-valeur correspondant à des motifs tels que « id=uuid-value », « type=objet-type » ou « name=objet-name ». Par exemple, « type=networkobject »
  - Le type peut être une entité leaf, telle qu'un objet réseau, ou un alias d'un ensemble de types leaf. Voici quelques alias de types typiques : network (NetworkObject et NetworkObjectGroup), port (tous les types de port, de protocole et de groupe TCP/UDP/ICMP), url (objets et groupes URL), ikepolicy (politiques IKE V1/V2), ikeproposal (propositions Ike V1/V2), identitysource (toutes les sources d'identité), certificate (tous les types de certificats), object (tous les types d'objets/groupes qui seraient répertoriés dans le gestionnaire de périphériques sur la page Objects), interface (toutes les interfaces réseau, s2svpn (tous les types de VPN site à site), ravpn (tous les types de VPN RA), vpn (s2svpn et ravpn).
  - Tous les objets et leurs descendants référentiels sortants seront inclus dans le fichier de sortie PARTIAL_EXPORT. Tous les objets non exportables seront exclus de la sortie même si vous spécifiez leurs identités. Utilisez la méthode GET pour les types de ressources appropriés afin d'obtenir les UUID, les types ou les noms des objets cibles.

  Par exemple, pour exporter tous les objets réseau, ainsi qu'une règle d'accès nommée myaccessrule et deux objets identifiés par UUID, vous pouvez spécifier :

  ```
  "entityIds": [
     "type=networkobject",
     "id=bab3e3cd-8c70-11e9-930a-1f12ee87d473",
     "name=myaccessrule",
     "acc2e3cd-8c70-11e9-930a-1f12ee87b286"
     ]",
  ```

- **jobName** - (Facultatif) Donner un nom à la tâche d'exportation permet de la retrouver plus facilement lorsque vous récupérez le statut de la tâche.
- **type** - Le type de tâche est toujours **scheduleconfigexport**

Étape 2 Postez l'objet.

Exemple :

La commande curl ressemblerait à ce qui suit :

```
  curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{
 \
   "configExportType": "FULL_EXPORT", \
   "type": "scheduleconfigexport" \
}' 'https://10.89.5.38/api/fdm/latest/action/configexport'
```

Étape 3 Vérifiez la réponse.

Vous devriez obtenir un code réponse de 200. Si vous envoyez l'objet JSON minimum, le corps de la réponse ressemblera à ce qui suit :

```
{
  "version": null,
  "scheduleType": "IMMEDIATE",
  "user": "admin",
  "forceOperation": false,
```

```
  "jobHistoryUuid": "c7a8ba61-629a-11e9-8b8d-0fcc3c9d6d0b",
  "ipAddress": "10.24.5.177",
  "diskFileName": "export-config-1",
  "encryptionKey": null,
  "doNotEncrypt": true
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "jobName": "Config Export",
  "id": "c79be920-629a-11e9-8b8d-85231be77de0",
  "type": "scheduleconfigexport",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/action/configexport/c79be920-629a-11e9-8b8d-85231be77de0"
  }
}
```


Étape 4 Vérifiez le statut de l'exportation de configuration.

La réalisation d'une exportation prend un certain temps. Plus la configuration est volumineuse, plus de temps la tâche prendra. Vérifiez le statut de la tâche pour vous assurer qu'elle se réalise complètement avant d'essayer de télécharger le fichier.

La manière la plus simple de récupérer le statut est d'utiliser **GET /jobs/configexportstatus** . Par exemple, la commande curl ressemblerait à ce qui suit :

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/jobs/configexportstatus'
```

Une tâche réalisée avec succès affiche le status suivant :


```
{
  "version": "hdy62yf5xp3vf",
  "jobName": "Config Export",
  "jobDescription": null,
  "user": "admin",
  "startDateTime": "2019-04-19 13:14:54Z",
  "endDateTime": "2019-04-19 13:14:56Z",
  "status": "SUCCESS",
  "statusMessage": "The configuration was exported successfully",
  "scheduleUuid": "1ef502ad-62a5-11e9-8b8d-074ebc750708",
  "diskFileName": "export-config-1.zip",
  "messages": [],
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "id": "1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300",
  "type": "configexportjobstatus",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/jobs/configexportstatus/1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300"
  }
}
```


Étape 5 Téléchargez le fichier d'exportation.

Lorsqu'une tâche d'exportation est terminée, le fichier d'exportation est écrit sur le disque système et est appelé fichier de configuration. Vous pouvez télécharger ce fichier d'exportation sur votre machine locale à l'aide de la commande **GET /action/downloadconfigfile/{objId}** .

Pour obtenir une liste des fichiers disponibles, utilisez la méthode GET /action/configfiles.

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/action/configfiles'
```

La réponse montrerait une liste d'items, chacun étant un fichier de configuration. Par exemple, la liste suivante affiche 2 fichiers. L'identifiant de tous les fichiers est par défaut et, à titre de bonne pratique, vous pouvez ignorer l'identifiant et utiliser le nom du fichier disque à la place.


```
{
  "items": [
    {
      "diskFileName": "export-config-2.zip",
      "dateModified": "2019-04-19 13:32:28Z",
      "sizeBytes": 10182,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    },
    {
      "diskFileName": "export-config-1.zip",
      "dateModified": "2019-04-19 13:14:56Z",
      "sizeBytes": 10083,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    }
  ],
```


Téléchargez le fichier utilisant le diskFileName comme l'identifiant de l'objet.

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.89.5.38/api/fdm/latest/action/downloadconfigfile/export-config-2.zip'
```

Le fichier est téléchargé dans votre dossier de téléchargement par défaut. Si vous utilisez la méthode GET à partir de l'explorateur API et que votre navigateur est configuré pour demander l'emplacement du téléchargement, vous serez invité à enregistrer le fichier.

Remarque Un téléchargement réussi résultera en un code de retour 200 et aucun corps de réponse.

Exporter le certificat PKI à partir du gestionnaire d'appareil et l'importer dans le Centre de gestion Firepower

L'outil de migration Cisco Secure Firewall permet la migration du VPN basé sur le certificat dans le centre de gestion.

Le groupe de configurations de l'appareil géré par FDM importé contient les données utiles du certificat ainsi que les clés. Cela peut être importé dans le centre de gestion.

Dans le centre de gestion de destination, migrez manuellement le point de confiance ou les certificats VPN en tant qu'objets PKI dans le cadre de l'activité prémigration. Cette activité doit être effectuée avant de commencer la migration à l'aide de l'outil de migration Cisco Secure Firewall.

Étape 1 À partir du groupe de configurations, copiez la charge utile du certificat (valeur entre -----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----) et de la clé (valeur entre -----BEGIN RSA PRIVATE KEY----- et -----END RSA PRIVATE KEY-----).

Exemple :


```
   "type":"identitywrapper",
   "action":"CREATE",
   "data":{
      "version":"girr7veykdjvx",
      "name":"RA_VPN_Cert",
      "cert":"-----BEGIN
[redacted]
 CERTIFICATE-----",
      "privateKey":"-----BEGIN RSA PRIVATE
[redacted]
 RSA PRIVATE KEY-----",
      "issuerCommonName":"mojave-rsa-root-2048-sha384.cisco.com, CN =
mojave-rsa-root-2048-sha384.cisco.com",
      "issuerCountry":"US",
      "issuerOrganization":"Cisco",
      "subjectCommonName":"fdm-ra-vpn-cert.cisco.com, CN = 172.16.10.50",
      "subjectCountry":"US",
      "subjectDistinguishedName":" C = US, O = Cisco, CN = fdm-ra-vpn-cert.cisco.com, CN =
172.16.10.50",
      "subjectOrganization":"Cisco",
      "validityStartDate":"Jan  1 12:00:00 2012 GMT",
      "validityEndDate":"Sep  1 12:00:00 2034 GMT",
      "isSystemDefined":false,
      "keyType":"RSA",
      "keySize":2048,
      "allowWeakCert":false,
      "signatureHashType":"SHA1",
      "weakCertificate":true,
      "id":"9d0a8efb-01fa-11ed-8d7b-1f4809c453ac",
      "type":"internalcertificate"
   }
}
```


Étape 2 Importez le certificat PKI dans un centre de gestion (**ObjectManagement** > **PKIObjects**).

Pour plus d'informations, référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements.

Les objets PKI créés manuellement peuvent désormais être utilisés dans l'outil de migration Cisco Secure Firewall à la page **Review and Validate** [examiner et valider], à la section **VPN Tunnels** [tunnels VPN].

Récupérer les paquets et les profils AnyConnect

Avant de commencer

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

- 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 charger 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 au moyen de l'outil de migration Cisco Secure Firewall.

Vérifiez les paquets disponibles sur le gestionnaire d'appareil à télécharger.

Étape 1 Vérifiez les paquets disponibles sur le gestionnaire d'appareil à télécharger.

Vous pouvez utiliser l'API **GET/object/anyconnectpackagefiles** pour afficher les paquets figurant sur l'appareil.

```
curl -X GET --header 'Accept: application/json' '
 https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles'
```

Cette commande récupère les paquets AnyConnect disponibles sur le gestionnaire d'appareil.

```
{
  "items": [
    {
      "version": "gx5yk7xkdsosu",
      "name": "anyconnect-win-4.10.02086-webdeploy-k9.pkg",
      "md5Checksum": "63e4a86fc7c68d7769b6a1b2976ffa73",
      "description": null,
      "diskFileName": "12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg",
      "platformType": "WINDOWS",
      "id": "133f2dbf-01fb-11ed-8d7b-89d64ab04e18",
      "type": "anyconnectpackagefile",
      "links": {
        "self": "
https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles/133f2dbf-01fb-11ed-8d7b-89d64ab04e18"
      }
    }
  ],
}
```

L'identifiant `diskFilename` de la réponse est utilisé pour télécharger le paquet AnyConnect.

Étape 2 Téléchargez le paquet AnyConnect.

Vous pouvez utiliser **GET /action/downloaddiskfile/{objId}** pour télécharger le paquet AnyConnect sur le poste de travail local. L'ID d'objet à utiliser est diskFileName (12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg) de la réponse du paquet AnyConnect.

```
curl -X GET --header 'Accept: application/octet-stream'
' https://10.89.5.38/api/fdm/v6/action/downloaddiskfile/12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg'
```

Étape 3 Vérifiez les profils AnyConnect disponibles sur le gestionnaire d'appareil.

Remarque Les profils AnyConnect sont automatiquement récupérés du gestionnaire d'appareil par l'outil de migration Cisco Secure Firewall. Cette étape n'est requise que si vous souhaitez charger manuellement le profil AnyConnect.

Vous pouvez utiliser **GET /object/anyconnectclientprofiles** pour vérifier les profils disponibles sur le gestionnaire d'appareil.

```
curl -X GET --header 'Accept: application/json'
'https://10.196.155.3:12272/api/fdm/v6/object/anyconnectclientprofiles'
```

La réponse suivante s'affichera :

```
  "items": [

    {
      "version": "jqtwzirf36qke",
      "name": "AnyConnect_VPN_Profile",
```

```
      "md5Checksum": "e4ba581f84daec6f24c209f9f7f9e1fb",
      "description": null,
      "diskFileName": "1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "1754c10b-0384-11ed-8d7b-6b8e36ae1285",
      "type": "anyconnectclientprofile",
    }
  ]
}
```


L'identifiant `diskFilename` de la réponse est utilisé pour télécharger le profil AnyConnect.

Étape 4 Téléchargement du profil AnyConnect.

Vous pouvez utiliser **GET /action/downloaddiskfile/{objId}** pour télécharger le paquet AnyConnect sur le poste de travail local. L'identifiant de l'objet (objId) à utiliser est le diskFileName (1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml) de la réponse des profils AnyConnect.

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.196.155.3:12272/api/fdm/v6/action/downloaddiskfile/1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml'
```

Étape 5 Importer les paquets téléchargés dans le centre de gestion (**ObjectManagement >)** > **VPN** > **AnyConnect File**.

1. Les fichiers Dap.xml et Data.xml doivent être chargés dans le centre de gestion à partir de l'outil de migration Cisco Secure Firewall dans la section **Review and Validate [examiner et valider]** > **Remote Access VPN [VPN à accès à distance]** > **AnyConnect File [fichier AnyConnect]**.
2. Les profils AnyConnect peuvent être chargés directement dans le centre de gestion à partir de l'outil de migration Cisco Secure Firewall dans la section **Review and Validate [examiner et valider]** > **Remote Access VPN [VPN à accès à distance]** > **AnyConnect File [fichier AnyConnect]**.

Les fichiers chargés manuellement peuvent désormais être utilisés dans l'outil de migration Cisco Secure Firewall.

Exécuter la migration

Lancer l'outil de migration Secure Firewall

Cette tâche s'applique uniquement si vous utilisez la version de bureau de l'outil de migration de pare-feu sécurisé. Si vous utilisez la version en nuage de l'outil de migration hébergé sur CDO, passez à Téléverser le paquet de configuration FDM .

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

Avant de commencer

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

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

Étape 1 Sur votre ordinateur, naviguez jusqu'au dossier où vous avez téléchargé l'outil de migration Secure Firewall.

Étape 2 Effectuez l'une des opérations suivantes :

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

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

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

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

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

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

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

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

  Remarque Utilisez la méthode zip du terminal MAC.

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

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

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

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

  Passez à l'étape 8 si vous avez utilisé votre compte Cisco.com pour vous connecter.

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

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

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

Étape 6 Cliquez sur **Réinitialiser**.

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

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

Étape 8 Passez en revue la liste de contrôle de pré-migration et assurez-vous que vous avez rempli tous les points énumérés.

Si vous n'avez pas rempli un ou plusieurs points de la liste de contrôle, ne continuez pas tant que vous ne l'avez pas fait.

Étape 9 Cliquez sur **Nouvelle migration**.

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

Étape 11 Cliquez sur **Procéder**.

Prochaine étape

Vous pouvez procéder à l'étape suivante :

- Si vous avez exporté la configuration du dispositif géré par FDM sur votre ordinateur, passez à la section Téléverser le paquet configuration FDM.

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

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

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

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

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

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

Sélectionnez la configuration source et l'option de migration du gestionnaire d'appareil

Étape 1 Sélectionnez le **fournisseur du pare-feu source** dans la liste déroulante, puis cliquez sur **Start Migration** [commencer la migration].

Étape 2 Sélectionnez l'option de migration que vous souhaitez utiliser pour migrer l'appareil géré par FDM.

Voici les options offertes :

- **Migrate Firepower Device Manager (Shared Configurations only)** [migrer le gestionnaire d'appareil Firepower (configurations partagées seulement)]

  Cette option permet la migration de la configuration partagée du gestionnaire d'appareil vers le centre de gestion de destination. Cette option devrait être utilisée pour les migrations par étapes, de sorte que les configurations partagées soient migrées initialement et que la configuration de l'appareil puisse être migrée ultérieurement. Il n'y a aucun temps d'arrêt dans ce scénario.

- **Migrate Firepower Device Manager (Includes Device and Shared configurations)** [migrer le gestionnaire d'appareil Firepower (y compris l'appareil et les configurations partagées)]

  Cette option permet de migrer la configuration partagée et celle de l'appareil vers le centre de gestion de destination. Dans le cadre de cette migration, la protection contre les menaces sources est déplacée du gestionnaire d'appareil vers le centre de gestion. Après la migration, le centre de gestion continue de gérer l'appareil de protection contre les menaces. Par conséquent, il s'agit, pour la source et la destination, du même appareil de protection contre les menaces dans ce scénario. Ce scénario comporte un temps d'arrêt, car l'appareil de protection contre les menaces est déplacé vers le centre de gestion.

  Pour migrer votre configuration au moyen de cette option, dans le cadre de l'activité prémigration :

1. Connectez-vous au gestionnaire d'appareil et accédez à la section **Objects** [objets].
2. Cliquez sur **Identity Sources** [sources de l'identité] et sélectionnez **AD Realm** [domaine AD] dans **Preset Filters** [filtres prédéfinis].
3. Sous **Actions** [actions], cliquez sur **Modifier** ( ) pour connaître le domaine pour lequel le type de chiffrement est **LDAPS** ou **STARTTLS**.
4. Sous **Directory Server Configuration** [configuration du serveur du répertoire], cliquez sur la flèche de la **liste déroulante** à côté du nom du serveur.
5. Dans la section **Encryption** [chiffrement], modifiez le type de chiffrement pour **NONE** [AUCUN], puis cliquez sur **OK**.
6. Déployez les modifications.

Remarque Une fois la configuration migrée vers le centre de gestion, vous pouvez rétablir le type de chiffrement du domaine AD dans le centre de gestion à LDAPS ou STARTTLS. Pour voir les instructions détaillées, consultez Examiner le rapport de post-migration et terminer la migration [examiner le rapport postmigration et terminer la migration, étape 4 (b)].

- **Migrer le gestionnaire d'appareil Firepower (y compris les configurations partagées et celles de l'appareil) vers l'appareil FTD (nouveau matériel)**

  Cette option permet de migrer la configuration de l'appareil géré par FDM vers la protection contre les menaces déjà enregistrée dans le centre de gestion de destination. La configuration de l'appareil géré par FDM source est migrée vers la protection contre les menaces de destination choisie par l'utilisateur et déjà enregistrée dans le centre de gestion de destination. Il n'y a aucun temps d'arrêt dans ce scénario.

Téléverser le paquet configuration FDM

Avant de commencer

Exportez le paquet configuration comme `.zip` à partir du gestionnaire d'appareil source

Remarque Le téléversement manuel sera pris en charge pour les deux options ci-dessous :

- **Migrer le gestionnaire d'appareil Firepower (y compris les dispositifs et les configurations partagées) vers le dispositif FTD (nouveau matériel)**
- **Migrer le gestionnaire d'appareil Firepower (Configurations partagées uniquement)**

Étape 1 Sur l'écran **Extraire les informations FDM**, dans la section **Téléversement manuel**, cliquez sur **Téléverser** pour téléverser un paquet de configuration géré par FDM. Si le paquet de configuration est crypté, indiquez la clé dans la zone de texte pour que l'outil de migration Secure Firewall puisse décrypter le paquet.

Étape 2 Recherchez l'emplacement du fichier de configuration du dispositif géré par FDM et cliquez sur **Ouvrir**.

L'outil de migration Secure Firewall téléverse le paquet 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 configuration de l'appareil géré par FDM 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

Étape 3 Cliquez sur **Démarrer l'analyse**.

La section **Résumé de l'analyse** affiche le statut de l'analyse.

Étape 4 Passez en revue le récapitulatif des éléments du fichier de configuration chargé que l'outil de migration Secure Firewall a détectés et analysés.

Étape 5 Cliquez sur **Suivant** pour choisir les paramètres cibles.

Prochaine étape

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

Connectez-vous au périphérique géré par FDM à partir de l'outil de migration Secure Firewall

Avant de commencer

L'outil de migration Secure Firewall peut se connecter à un dispositif géré par FDM que vous voulez migrer et en extraire les informations de configuration requises. La connexion en direct à un dispositif géré par FDM est prise en charge pour les trois cas d'utilisation.

- Télécharger et lancer l'outil de migration Secure Firewall.
- Sélectionnez le cas d'utilisation que vous souhaitez exécuter pour la migration des dispositifs gérés par le FDM vers le centre de gestion.
- Obtenez l'adresse IP de gestion et les informations d'identification de l'administrateur du gestionnaire de périphérique.

Étape 1 Sur l'écran **Extraire les informations** FDM, dans la section **Se connecter à FDM**, cliquez sur **Connexion** pour se connecter au dispositif géré par FDM que vous voulez migrer

Étape 2 Sur l'écran **Connexion à FDM**, saisissez les informations suivantes :

1. Dans le champ **Adresse IP FDM/Nom d'hôte**, saisissez l'adresse IP de gestion ou le nom d'hôte du FDM. Cliquez sur **Ouvrir une session**.
2. Dans les champs **Nom d'utilisateur**, **Mot de passe**, saisissez les identifiants de connexion administrateur.
3. Cliquez sur **Ouvrir une session**.

Lorsque l'outil de migration Secure Firewall se connecte au dispositif géré par le FDM, une série de contrôles de conformité est effectuée sur le dispositif géré par le FDM avant de procéder à la migration. Ces vérifications sont abordées dans la section relative aux conditions préalables et aux bonnes pratiques. Si ces vérifications sont réussies, la migration passera à la prochaine étape.

L'outil de migration Secure Firewall se connecte au dispositif géré par FDM et une fois le contrôle de conformité réussi, l'outil commence à extraire les informations de configuration. Lorsque l'extraction se termine avec succès, la page de résumé d'analyse s'affiche.

La section **Résumé de l'analyse** affiche le statut de l'analyse.

Étape 3 Examinez le résumé des éléments que l'outil de migration Secure Firewall a détecté et analysé, à partir du dispositif géré par FDM.

Étape 4 Cliquez sur **Suivant** pour choisir les paramètres cibles.

Prochaine étape

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

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

Avant de commencer

- Obtenez l'adresse IP de centre de gestion pour le centre de gestion du pare-feu sur place
- (Facultatif) Ajoutez le dispositif de défense contre les menaces cible au centre de gestion si le flux sélectionné est **Migrer le gestionnaire d'appareil Firepower (y compris les configurations d'appareil & partagées) vers le dispositif FD (Nouveau matériel)** au centre de centre de gestiongestion. 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 gestionconnecté. 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 : .

- Pour migrer vers un centre de gestion sur place, faites ce qui 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 avez sélectionné **Migrer le gestionnaire d'appareil Firepower (y compris les configurations d'appareils & partagées) vers un dispositif FTD (Nouveau matériel)**, vous ne pouvez migrer que vers les dispositifs de défense contre les menaces disponibles dans le domaine sélectionné.

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

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

a) Cliquez sur le bouton radio **FMC en nuage**.
b) Choisissez la région et collez le jeton API CDO. Pour générer le jeton API du CO, suivez les étapes ci-dessous :

1. Connectez-vous au portail CDO

2. Naviguez vers **Paramètres** > **Paramètres généraux** et copiez le jeton API.

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

Étape 2 Dans la boîte de dialogue Connexion du **Centre de gestion du pare-feu**, entrez le nom d'utilisateur et le mot de passe du compte dédié à l'outil de migration Secure Firewall, puis cliquez sur **Connexion**.

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

Étape 3 Cliquez sur **Procéder**.

Si vous avez sélectionné **Migrer le gestionnaire d'appareil Firepower (y compris les configurations d'appareils & partagées) vers un dispositif FTD (Nouveau matériel)**, vous ne pouvez migrer que vers les dispositifs de défense contre les menaces disponibles dans le domaine sélectionné.

Si vous avez choisi **Migrer le gestionnaire d'appareil Firepower (Configurations partagées uniquement)**

La section de défense contre les menaces du centre de gestion n'est pas remplie dans ce flux de travail, seules les politiques partagées (listes de contrôle d'accès, NAT et objets) sont transmises à la FMC. Vous pouvez choisir d'inclure ou d'ignorer les stratégies partagées qui doivent être transférées au centre de gestion.

Si vous avez choisi **Migrer le gestionnaire d'appareil Firepower (y compris l'appareil & les configurations partagées)**

Le dispositif de défense contre les menaces qui est déplacé vers le centre de gestion est le même que celui qui est géré par le gestionnaire de dispositifs. Le dispositif de défense contre les menaces faisant partie du centre de gestion n'est pas comptabilisé dans ce cas.

Étape 4 Dans la section **Choisir la défense contre les menaces**, faites l'une de ces choses :

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

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

  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.

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

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

Étape 5 Cliquez sur **Procéder**.

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

Étape 6 Cliquez sur la section **Sélectionner les fonctionnalités**pour examiner et sélectionner les fonctionnalités que vous souhaitez migrer vers la destination.

- Si vous effectuez une migration vers un dispositif de destinationdéfense contre les menaces, l'outil de migration Secure Firewall sélectionne automatiquement les fonctionnalités disponibles pour la migration à partir de la configuration de du dispositif géré par FDM dans les sections **Configuration du dispositif** et **Configuration partagée**. Vous pouvez modifier la sélection par défaut, selon vos besoins.
- Si vous effectuez une migration vers un centre de gestion, l'outil de migration Cisco Secure Firewall sélectionnera automatiquement les fonctions disponibles pour la migration à partir de l'appareil géré par FDM dans les sections **Device Configuration** [configuration de l'appareil], **Shared Configuration** [configuration partagée] et **Optimization** [optimisation]. Vous pouvez modifier la sélection par défaut, selon vos besoins.

  Remarque La section **Device Configuration** [configuration de l'appareil] n'est pas disponible si vous avez choisi **Migrate Firepower Device Manager (Shared Configurations Only)** [migrer le gestionnaire d'appareil Firepower (configurations partagées seulement)].

- 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, alors que 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.

  -
    - 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 traffic tunnelisé seront migrées comme des règles non prises en charge.

    Les règles de tunnel ACL (GRE et IPnIP) dans la configuration de l' de dispositif géré par FDM 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 les menaces cible est la version 6.6 ou plus récente.
  - Basée sur l'itinéraire (VTI) - Si le centre de gestionet défense contre les menacescible 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' de l'appareil géré par FDM 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 les menaces .
- Si votre appareil géré par FDM dispose de paramètres pour la plateforme, et de fichiers et politiques concernant les programmes malveillants, l'outil de migration les affiche alors à la page **Select Features** [sélectionner des fonctions] en tant que **paramètres de plateforme** sous la configuration partagée et que **stratégie de fichiers et de programmes malveillants** sous la configuration de l'appareil. Notez que ces cases sont cochées par défaut.

Étape 7 Cliquez sur **Procéder**.

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

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

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

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

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

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

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 examiner 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 du dispositif géré par le FDM ou pour se connecter à une configuration dispositif géré par l'ASAFDM.

  Un résumé des éléments de configuration des dispositifs gérés par FDM qui peuvent être migrés avec succès et des défense contre les menacesfonctionnalités spécifiques ASA sélectionnées pour la migration.

  Lors de la connexion à un dispositif ASA géré par , le résumé comprend des informations sur le nombre d'occurrences - le nombre de fois où une règle de dispositif géré par FDM a été rencontrée et les informations sur l'horodatage.

- **Lignes de configuration avec des erreurs** - Détails des éléments de configuration ASA avec 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 la de ASA , 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 gérés par FDM 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 dispositifs ASA avec gérés par FDM 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 dispositifsASA gérés par FDM qui sont ignorés parce qu'ils ne sont pas pris en charge par centre de gestionl'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 les 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, exportez à nouveau le fichier de configuration du dispositif ASA géré par FDM et téléchargez le fichier de configuration mis à jour avant de poursuivre.

Étape 4 Une fois que le fichier de configuration de votre ASA dispositif avec FPS 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

Mappez les configurations de de l'appareil géré par FDM avec les interfaces de Défense contre les menaces.

Mappez les configurations de de l'appareil géré par FDM avec les interfaces de Défense contre les menaces.

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

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

Le mappage de l'interface de l' avec l'appareil géré par FDM à l'interface défense contre les menaces diffère en fonction du type de périphérique défense contre les menaces :

- Si la cible défense contre les menaces est de type natif :
  - Le défense contre les menacesdoit avoir un nombre égal ou supérieur d'interfaces d'appareils gérés par FDM 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 d'appareils gérés par FDM). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre les menaces cible.
  - Les sous-interfaces sont créées par l'outil de migration du pare-feu sécurisé sur la base de l'interface physique ou du mappage du canal de port.
- Si la cible défense contre les menaces est de type contenant :
  - Le défense contre les menacesdoit avoir un nombre égal ou supérieur d'interfaces 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 ASA). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre les menaces cible. Par exemple, si le nombre d'interfaces physiques et de sous-interfaces physiques sur la cible défense contre les menaces est inférieur de 100 à celui de l' d'appareil géré par FDM, vous pouvez créer des interfaces physiques ou des sous-interfaces physiques supplémentaires sur la cible défense contre les menaces.
  - Les sous-interfaces ne sont pas créés par l'outil de migration Secure Firewall Seul le mappage d'interface est autorisé entre les interfaces physiques, les canaux de port ou les sous-interfaces.

Avant de commencer

Assurez-vous de vous être connecté au centre de gestion et choisi la destination comme défense contre les menaces Pour en savoir plus, consultez Préciser les paramètres de destination pour l'outil de migration Secure Firewall, à la page 39.

Remarque Cette étape n'est pas applicable si vous migrez en utilisant le **gestionnaire d'appareil Migrate Firepower (Configurations partagées uniquement)**

Cette étape est une étape d'information seulement qui sert à la **migration du gestionnaire de l'appareil Firepower (y compris les configurations de l'appareil et les configurations partagées)**.

Étape 1 Si vous souhaitez modifier le mappage d'une interface, cliquez sur la liste déroulante du **nom de l'interface FTD** et choisissez l'interface que vous souhaitez mapper à l'interface .

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

Vous n'avez pas besoin de mapper les sous-interfaces. L'outil de migration Secure Firewall fait correspondre les sous-interfaces du dispositif défense contre les menacesà toutes les sous-interfaces de la configuration de du dispositif géré par FDM.

Étape 2 Lorsque vous avez mappé chaque interface de périphérique d'appareil géré par FDM à une interfacedéfense contre les menaces, cliquez sur **Suivant**.

Associez les interfaces de l'appareil géré par FDM à des périmètres de sécurité, à groupes d'interfaces .

Remarque Si la configuration de votre de l'appareil géré par FDM 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 .Optimisez, examinez et validez la configuration à être migrée, à la page 46

Pour que la configuration de l'appareil géré par FDM soit migrée correctement, mappez les interfaces de l'appareil géré par FDM aux objets d'interface défense contre les menaces, aux périmètres de sécurité, appropriés. Dans une configuration de dispositif géré par FDM, 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 Cisco Secure Firewall permet le mappage individuel des interfaces avec les périmètres de sécurité les groupes d'interfaces. Lorsqu'un périmètre de sécurité ou un groupe d'interfaces est mappé à une interface, il n'est pas disponible pour le mappage à d'autres interfaces, bien que le centre de gestion le

permette. Pour en savoir plus sur les périmètres de sécurité et les groupes d'interfaces dans le centre de gestion, consultez la section Security Zones and Interface Groups [périmètres de sécurité et groupes d'interfaces] du *guide de configuration d'appareil de Cisco Secure Firewall Management Center*.

Étape 1 Sur l'écran **Mapper les zones de sécurité et les groupes d'interfaces**, passez en revue les interfaces, les zones de sécurité et les groupes d'interfaces disponibles.

Étape 2 Pour mapper des interfaces à des zones de sécurité et à des groupes d'interfaces qui existent dans centre de gestion, ou qui sont disponibles dans les fichiers de configuration de des dispositifs gérés par FDM en tant qu'objets de type zone de sécurité et qui sont disponibles dans la liste déroulante, procédez comme suit :

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

Étape 3 Vous pouvez mapper manuellement ou auto-créer 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 :

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

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

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

L'outil de migration Secure Firewall donne à ces zones de sécurité le même nom que l'interface du dispositif géré par FDM, 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 du dispositif géré par FDM. Par exemple, si l'interface logique du dispositif géré par FDM 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**.

Optimisez, examinez et validez la configuration à être migrée

Pour la configuration des dispositifs gérés par FDM, la configuration est validée de différentes manières et dépend du flux de migration sélectionné. La validation de la configuration pour les différentes options va comme suit :

- **Migration du gestionnaire d'appareil Firepower (y compris le dispositif et les configurations partagées) vers le dispositif FTD (nouveau matériel)** - Le dispositif et la configuration partagée sont examinés et validés en un seul flux.
- **Migration du gestionnaire d'appareil Firepower (Configurations partagées uniquement)** - Seule la configuration partagée est examinée et validé

- **Migration du gestionnaire d'appareil Firepower (y compris les configurations des appareils et les configurations partagées)** - Les configurations partagées et des appareils sont validées dans un flux séparé.

Optimisez, examinez et validez la configuration partagée

Avant de transmettre la configuration du FDM migré vers le centre de gestion, optimisez et examinez soigneusement la configuration, puis vérifiez qu'elle est correcte et qu'elle correspond à la façon dont vous souhaitez configurer l'appareil de protection contre les menaces. Un onglet clignotant indique que vous devez passer à l'action suivante.

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

Ici, l'outil de migration Secure Firewall récupère les règles du système de prévention des intrusions (IPS) et les règles de fichiers déjà présentes dans le centre de gestionet vous permet de les associer aux règles de contrôle d'accès que vous migrez.

Une stratégie de fichiers est un ensemble de configurations que le système utilise pour effectuer une protection avancée contre les logiciels malveillants pour les réseaux et le contrôle des fichiers, dans le cadre de votre configuration globale de contrôle d'accès. Cette association fait en sorte qu'avant que le système passe un fichier dans le trafic correspondant aux conditions de la règle de contrôle d'accès, le fichier est d'abord inspecté.

De même, vous pouvez utiliser une politique IPS comme dernière ligne de défense du système avant que le trafic ne soit autorisé à se rendre à destination. Les politiques d'intrusion régissent la manière dont le système inspecte le trafic à la recherche de violations de la sécurité et, dans les déploiements en ligne, peuvent bloquer ou modifier le trafic malveillant. Chaque fois que le système utilise une politique d'intrusion pour évaluer le trafic, il utilise un ensemble de variables associé. La plupart des variables d'un ensemble représentent des valeurs couramment utilisées dans les règles d'intrusion pour identifier les adresses IP et les ports source et destination. Vous pouvez également utiliser des variables dans les politiques d'intrusion pour représenter les adresses IP dans les états de suppression de règles et de règles dynamiques.

Pour rechercher des éléments de configuration spécifiques dans un onglet, saisissez le nom de l'élément dans le champ situé en haut de la colonne. Les rangées du tableau sont filtrées pour afficher seulement les éléments correspondant au terme de recherche.

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

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

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

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

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

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

Remarque L'optimisation est possible pour l'appareil géré par FDM seulement pour une action découlant d'une règle ACP.

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

Optimisation de l'objet

Les objets suivants sont considérés pour l'optimisation d'objet durant le procédé de migration :

- Objets non référencés - Vous pouvez choisir de ne pas migrer les objets non référencés au début de la migration.
- Objets en double - Si un objet existe déjà sur centre de gestion, au lieu de créer un objet en double, la politique est réutilisée.

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

a) Pour télécharger les règles d'optimisation d'ACL, cliquez sur **Télécharger**.
b) Sélectionnez les règles et choisissez **Actions** > **Migrer comme désactivé** ou **Ne pas migrer** et appliquez l'une des actions.
c) 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 optimiser,l'écran **Examiner et valider la configuration**, cliquez sur **Règles de contrôle d'accès** et faites ceci :

a) 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 de l'appareil géré par FDM. Par exemple, si une ACL pour un appareil géré par FDM 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 gestionà 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 gestionà 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. Cette liste comprend également les politiques de fichiers et de programmes malveillants associées aux ACL, que vous pouvez choisir de ne pas migrer, appliquer ou modifier.

- 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.

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 triez 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.

g) Dans la **politique de prévention des intrusions**, toutes les politiques de prévention des intrusions, la politique de base correspondante, les règles personnalisées ou remplacées présentes, le mode d'intrusion et la référence figurant dans l'ACP sont affichés. Le moteur du renifleur et la politique NAP pour Snort 3 sont également présentés.

Les politiques Snort 2 avec des règles remplacées sont ignorées compte tenu de la limitation d'API dans le centre de gestion.

Une politique de prévention des intrusions avec un paramètre par défaut est réutilisée dans le centre de gestion.

Une nouvelle politique est créée avec le nom de politique _<FDM Hostname> pour une politique de prévention des intrusions avec des règles remplacées ou personnalisées pour Snort 3 ou un mode de détection des intrusions pour Snort3/Snort2.

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 examinant 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 **Remote Access VPN** [VPN d'accès à distance], tous les objets correspondant au VPN d'accès à distance sont migrés de l'appareil géré par FDM 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 devraient être récupérés à partir de l'appareil géré par FDM source 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'appareil géré par FDM. 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 Cisco Secure Firewall 3.0, les clés prépartagées sont récupérées automatiquement pour un appareil géré par FDM 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'appareil géré par FDM au moyen de 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.

     ```
     ciscoFDM#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 <Password in clear text> <-----TheLDAP/AD/LDAPS password is now displayed
      in clear text format.
     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, l'appareil géré par FDM prend en charge 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 de l'appareil géré par FDM contient le nom d'hôte ou le domaine, celui-ci est récupéré et affiché. Si la configuration de l'appareil géré par FDM contient l'adresse IP pour LDAPS, entrez un domaine dans la section **AAA** sous **Remote Access VPN** [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'appareil géré par FDM), le **AD Primary Domain** [domaine primaire AD] est un champ obligatoire qui doit être configuré dans un centre de gestion. Ce champ n'est pas configuré séparément sur l'appareil géré par FDM et est extrait de la configuration LDAP-base-dn sur l'appareil géré par FDM.

  ```
  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=FDM,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. Au cas où un conflit serait détecté ou si l'outil de migration Cisco Secure Firewall est incapable de trouver la valeur dans la configuration de l'appareil géré par FDM, vous devez saisir un domaine primaire AD pour le serveur. 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 connections/groupes tunnels sont affichés ici.
- **Point de confiance** – La migration des points de confiance ou des objets PKI de l'appareil géré par FDM vers le centre de gestion fait partie de l'activité de prémigration et est nécessaire à la réussite de la migration de RA VPN. 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 remplacé est disponible dans l'appareil géré par FDM, elle peut être sélectionnée dans l'option **Override SAML** [remplacer SAML].

Pour en savoir plus sur l'exportation de certificats PKI à partir de l'appareil géré par FDM, consultez Exporter le fichier de configuration du périphérique géré par FDM [exporter le certificat du gestionnaire d'appareil et l'importer dans le centre de gestion].

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

Étape 6 Sous l'onglet **SNMP** [SNMP], vous pouvez examiner les onglets suivants, les valider et les utiliser pour travailler :

Selon la configuration de votre appareil ASA, soit SNMPV1/V2 ou SNMPV3, les configurations s'afficheront à l'onglet **SNMPV1/V2** ou **SNMPV3**.

SNMPV1/V2 :

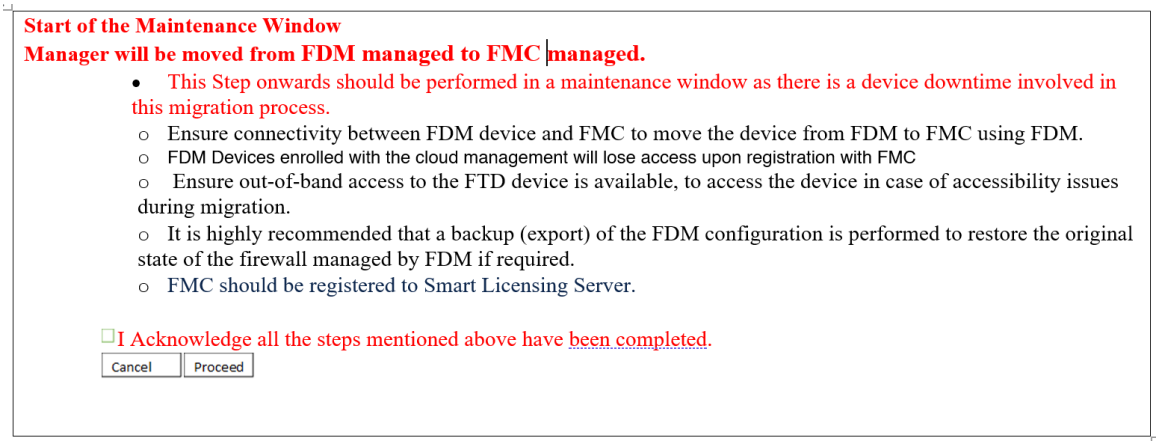
- **Nom du serveur hôte** : Le nom de domaine de l'hôte SNMP.
- **Adresse IP** : L'adresse IP de l'hôte SNMP.
- **Identifiant de communauté** : L'identifiant de communauté à fournir manuellement. Sélectionnez l'hôte et allez à **Actions [action]** > **Update Community String [mettre à jour l'identifiant de communauté]** pour fournir l'identifiant de communauté. Il doit être le même que celui de la communauté ou que le nom d'utilisateur configuré pour le service SNMP.
- **État de validation** : L'état de validation du serveur hôte qui sera créé dans le centre de gestion cible.

SNMPV3 :

- **Nom d'utilisateur** : Le nom d'utilisateur de l'hôte SNMP.
- **Mot de passe de l'authentification** : Cliquez sur **Actions** [actions] pour fournir à l'utilisateur son mot de passe d'authentification.
- **Mot de passe du chiffrement** : Cliquez sur **Actions** [actions] pour fournir à l'utilisateur son mot de passe de confidentialité.
- **État de validation** : L'état de validation de l'utilisateur qui sera créé dans le centre de gestion cible.

Démarrez la maintenance et déplacez le gestionnaire

Une fois la configuration partagée transmise, vous devez accepter une fenêtre contextuelle pour accéder à la fenêtre de maintenance.



Dans la page **Move Manager** [déplacer le gestionnaire], les détails suivants devraient idéalement être mentionnés :

- Choisissez entre : **FTD is behind NAT Device [FTD est derrière l'appareil NAT], FMC is behind NAT Device [FMC est derrière l'appareil NAT], No Device is behind NAT [aucun appareil n'est derrière la NAT] (paramètre par défaut)**
- **Nom d'hôte ou adresse IP du centre de gestion ou de CDO** : Tous les détails seront extraits du gestionnaire cible. Vous pouvez modifier l'adresse IP, s'il y a lieu.

Remarque Les champs seront ignorés si **FMC est derrière l'appareil NAT**.

- **Clé d'enregistrement du centre de gestion ou de CDO** : Une clé d'enregistrement unique doit être fournie et sera utilisée pendant le déplacement du gestionnaire.
- **ID de la NAT** : (facultatif). Requis lorsque le centre de gestion ou la protection contre les menaces se trouve derrière l'appareil NAT.
- **Nom d'hôte de Threat Defense (FTD)** : L'adresse IP ou le nom d'hôte de Threat Defense est récupéré à partir de la configuration de l'appareil géré par FDM. L'utilisateur peut modifier l'adresse IP au besoin. Le champ sera ignoré si **FTD est derrière un appareil NAT**.
- **Groupe de serveurs DNS** : Groupe de serveurs DNS utilisé pour la connectivité entre le gestionnaire d'appareil et le centre de gestion.
- **Interface d'accès du centre de gestion/CDO (données/gestion)** : Choisissez entre l'interface de données/gestion pour déplacer le gestionnaire. L'interface de données est prise en charge seulement si les routes appropriées sont configurées au moyen de l'interface de données.

Une fois que vous avez sélectionné **Move Manager** [déplacer le gestionnaire], l'outil de migration Cisco Secure Firewall déclenche le déplacement du gestionnaire d'appareil vers le centre de gestion. Par la suite, l'appareil devient inaccessible à partir du gestionnaire d'appareil.

Optimisez, examinez et validez la configuration de l'appareil visé par la migration

Étape 1 Cliquez sur les onglets suivants pour examiner les éléments de configuration

- **Interfaces**
- **Routs**
- **Tunnels de réseau privé virtuel (VPN) de site à site**

Dans la section **Dynamic-Route-Objects** [objets de routage dynamique], tous les objets pris en charge qui sont migrés sont affichés :

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

Étape 2 Dans la section **Routes** [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.

Étape 3 Après avoir complété votre examen, cliquez sur **Valider**.

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

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

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

Étape 4 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 Cisco Secure Firewall affiche une icône d'avertissement dans l'onglet **Network Objects** [objets réseau] ou **Port Objects** [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 5 Lorsque la validation est terminée et que la boîte de dialogue **Validation Status** [état de la validation] affiche le message **Successfully Validated** [validé avec succès], amorcez le transfert de la configuration migrée vers le centre de gestion.

Transférer la configuration migrée vers Centre de gestion

Vous ne pouvez pas pousser la configuration de migré avec un dispositif géré par FDM vers centre de gestionsi 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 géré par FDM 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 Optimisez, examinez et validez la configuration à être migrée, à la page 46

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

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 d'appareil géré par FDM a été migrée :

- **Résumé de la migration** - Résumé de la configuration qui a été migrée avec succès de de l'appareil géré par FDM vers Défense contre les menaces, y compris des informations sur l'interface du dispositif géré par FDM, 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.
- **Chemin de migration FDM** - Indique l'option qui a été sélectionnée parmi les trois flux de migration :
  - **Migrer le gestionnaire d'appareil Firepower (Configurations partagées uniquement)**
  - **Migrer le gestionnaire d'appareil Firepower (y compris l'appareil & les configurations partagées)**
  - **Migrer le gestionnaire d'appareil Firepower (y compris les dispositifs et les configurations partagées) vers le dispositif FTD (nouveau matériel)**
- **Migration sélective des règles** : les détails de la fonction spécifique de de l'appareil géré par FDM 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 du dispositif géré par FDM 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 du dispositif géré par FDM vers les Défense contre les menacesinterfaces 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 du dispositif géré par FDM 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 des objets de dispositifs gérés par FPS FDM 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 de l'appareil géré par FDM 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 de l'appareil géré par FDM 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 caractéristiques 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 de l'appareil géré par FDM qui ont été étendues d'une seule règle de point d'appareil géré par FDM en plusieurs règles Défense contre les menacesau 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 de l'appareil géré par FDM 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 de dispositif géré par FDM 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' de l'appareil géré par FDM 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 d'appareil géré par FDM 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.

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 desd'appareils gérés par FDM que vous devez migrer manuellement sur le Défense contre les menacesdispositif.

Étape 4 Dans centre de gestion, faites ceci :

a) 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
- 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 défensecontre 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

Si vous avez modifié le cryptage de la zone AD avant la migration, suivez les étapes ci-dessous pour rétablir le type de cryptage à LDAPS ou STARTTLS :

1. Naviguez vers la section **Intégration**et cliquez sur **Autres intégrations**
2. Sélectionnez **Domaines**et cliquez **Modifier** ( )à côté du domaine spécifique pour modifier le type de cryptage.
3. Cliquez sur **Répertoire**et changer le type de chiffrement à **LDAPS** ou **STARTTLS**.
4. Sauvegardez et déployez les changements.

Étape 5 Après avoir complété votre examination, déployez la configuration migrée de centre de gestionvers 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 de l'appareil géré par FDM.

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 coller le dossier `journal` vers un endroit différent.

Étape 3 Si vous voulez sauvegarder les rapports pré-migration et les rapports post-migration, coupez ou copiez et collez le dossier `ressources`vers un endroit différent.

Étape 4 Supprimez le dossier où vous avez placé l'outil de migration Secure Firewall.

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

Exemple de migration : avec dispositif géré par FPS FDM 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 Obtenez la configuration gérée par le FDM ou connectez-vous au dispositif géré par le FDM pour récupérer la configuration.

Étape 2 Examinez le fichier de configuration du dispositif géré par FDM.

Étape 3 Déployez l'appareil Série Firepower 2100 dans votre réseau, connectez les interfaces et mettez l'appareil sous tension.

Pour plus d'informations, consultez le Guide de démarrage rapide Cisco Threat Defense pour la série 2100 en utilisant le centre de gestion.

Étape 4 Inscrivez l'appareil Série Firepower 2100 qui sera géré par le centre de gestion.

Pour plus d'informations, consultez Ajouter des appareils au centre de gestion.

Étape 5 (Facultatif) Si la configuration du dispositif géré par le FDM source comportedes canaux de port, créez des canaux de port (EtherChannels) sur le dispositif cibleSérie Firepower 2100.

Pour plus d'informations, consultez Configurez des EtherChannels et les interfaces redondantes.

Étape 6 Téléchargez et exécutez la version la plus récente de l'outil de migration Secure Firewall de https://software.cisco.com/download/home/286306503/type.

Pour en savoir plus, consultez Télécharger l'outil de migration de pare-feu sécurisé sur Cisco.com, à la page 26.

Étape 7 Lorsque vous lancez l'outil de migration Secure Firewall et que vous spécifiez les paramètres de destination, assurez-vous de sélectionner l'appareil Série Firepower 2100que vous avez enregistré vers le centre de gestion.

Pour en savoir plus, consultez Préciser les paramètres de destination pour l'outil de migration Secure Firewall, à la page 39.

Étape 8 Mappez les ASA les interfaces d'appareil géré par FDM avec les interfaces Défense contre les menaces.

Remarque L'outil de migration Secure Firewall vous permet de mapper un d'interface avec des appareils gérés par FDM au type Défense contre les menacesd'interface.

Par exemple, vous pouvez mapper un canal de port dans un dispositif géré par FDM à une interface physique dans Défense contre les menaces.

Pour plus d'informations, voir Mappez les configurations de de l'appareil géré par FDM avec les interfaces de Défense contre les menaces..

Étape 9 Lors du mappage des interfaces logiques aux zones de sécurité, cliquez sur **Création automatique** pour permettre à l'outil de migration Secure Firewall de créer de nouvelles zones de sécurité. Pour utiliser les zones de sécurité existantes, mappez manuellement les interfaces logiques de géré par FDM aux zones de sécurité.

Pour plus d'informations, voir Associez les interfaces de l'appareil géré par FDM à des périmètres de sécurité, à 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 leDéfense contre les menaces et complétez la migration.

Pour plus de renseignements, consultez la section Optimisez, examinez et validez la configuration à être migrée, à la page 46.

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 61.

Étape 1 Connectez-vous au dispositif géré par FDMvia la console SSH et changez pour le mode de configuration d'interface.

Étape 2 Arrêtez les interfaces du dispositif géré par FDM 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

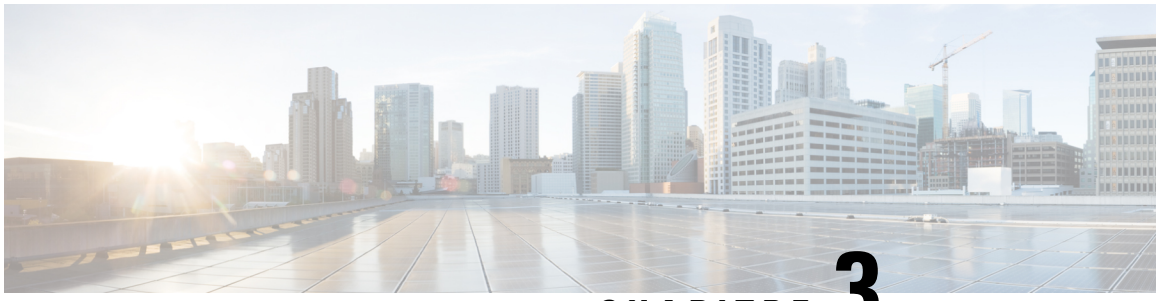
Étape 5 Effectuez des tests ping de base depuis l'infrastructure de commutation environnante jusqu'aux adresses IP de l'interface de l'appareil Série Firepower 2100, afin de vous assurer qu'elles sont accessibles.

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 FDM, 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

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 de l'appareil géré par FDM migré vers centre de gestion, le service de transfert lit le fichier de données de télémétrie à partir de l'emplacement et le supprime une fois les données téléchargées avec succès dans le nuage.

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

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

Tableau 2 : Télémétrie limitée

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

Cisco Success Network - Données de télémétrie

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

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

Tableau 3 : Données système

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 : Information sur l'appareil géré par FDM source

Point de données	Description	Exemple de valeur
Type de source	Le type de périphérique source	FDM
Numéro de série du périphérique source	Numéro de série de l'appareil géré par FDM	Cisco Firepower Threat Defense pour VMware
Version du périphérique source	Version de l'appareil géré par FDM	7.2.0-8.0
Mode pare-feu	Le mode du pare-feu configuré sur l'appareil géré par FDM, routé ou transparent	ROUTAGE
Mode contextuel	Le mode de contexte de l'appareil géré par FDM. Il peut s'agir d'un contexte unique ou multiple.	UNIQUE
Statistiques de la configuration de l'appareil géré par FDM :		
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

Cisco Success Network - Données de télémétrie

Point de données	Description	Exemple de valeur
Nombre de règles NAT	Le nombre total de règles NAT	17
Compte d'objets réseau	Le nombre d'objets réseau configurés dans l'appareil géré par FDM	34
Nombre de groupes d'objets réseau	Le nombre de groupes d'objets réseau dans l'appareil géré par FDM	6
Compte d'objets de port	Le nombre d'objets de port	85
Compte de groupes d'objets de port	Le nombre de groupes d'objets de port	37
Nombre de règles d'accès non prises en charge	Le nombre total de règles d'accès non prises en charge	3
Nombre de règles NAT non prises en charge	Le nombre total de règles d'accès NAT non prises en charge	0
Nombre de règles d'accès basées sur FQDN	Le nombre de règles d'accès basées sur le nom de domaine complet (FQDN)	7
Nombre de règles d'accès basées sur une plage de temps	Le nombre de règles d'accès basées sur une plage de temps	1
Nombre de règles d'accès basées sur SGT	Le nombre de règles d'accès basées sur SGT	0
Résumé des lignes de configuration que l'outil n'est pas en mesure d'analyser		
Nombre de configurations non analysées	Le nombre de lignes de configuration non reconnues par l'analyseur syntaxique	68
Nombre total de règles d'accès non analysées	Le nombre total de règles d'accès non analysées	3
Plus de détails sur la configuration de l'appareil géré par FDM...		
Le VPN d'accès à distance est-il configuré	Le VPN avec accès à distance est-il configuré sur l'appareil géré par FDM	faux
Le VPN S2S est-il configuré	Le VPN de site à site est-il configuré sur l'appareil géré par FDM	faux
Le BGP est-il configuré	Le BGP est-il configuré sur l'appareil géré par FDM	faux
L'EIGRP est-il configuré	Le protocole EIGRP est-il configuré sur l'appareil géré par FDM	faux
Le protocole OSPF est-il configuré	OSPF est-il configuré sur l'appareil géré par FDM	faux
Comptes d'utilisateurs locaux	Le nombre d'utilisateurs locaux configurés	0

Cisco Success Network - Données de télémétrie

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

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

Tableau 6 : Résumé de la migration

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

Cisco Success Network - Données de télémétrie

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

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

Point de données	Description	Exemple de valeur
Temps de conversation	Le temps nécessaire pour analyser les lignes de configuration de l'appareil géré par FDM (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 de l'appareil géré par FDM 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	nulle

Fichier d'exemple de télémétrie de l'appareil géré par FDM

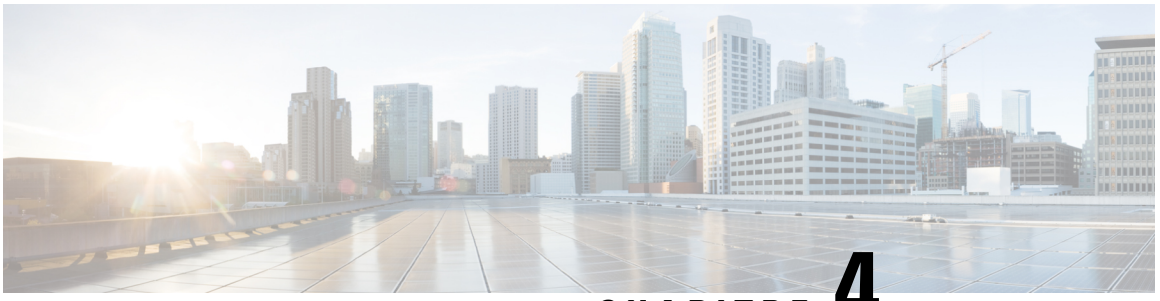
Voici un exemple de fichier de données de télémétrie sur la migration de la configuration de l'appareil géré par FDM vers la protection contre les menaces :


```
{
"metadata": {
"contentType": "application/json", "topic": "migrationtool.telemetry"
},
"payload": { "FDM_config_stats": {
"access_rules_counts": 46,
"acl_counts": 46,
"fqdn_based_access_rule_counts": 7, "is_bgp_configured": false, "is_eigrp_configured":
false, "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, "local_users_counts": 0,
"nat_rule_counts": 17,
"network_object_counts": 34,
"network_object_group_counts": 6,
"port_object_counts": 85,
"port_object_group_counts": 37,
"sgt_based_access_rules_count": 0,
"timerange_based_access_rule_counts": 1,
"total_unparsed_access_rule_counts": 3,
"unparsed_config_count": 68,

"unsupported_access_rules_count": 3,
"unsupported_nat_rule_count": 0
},
"context_mode": "SINGLE", "error_description": null, "error_message": null, "firewall_mode":
```

Cisco Success Network - Données de télémétrie


```
 "ROUTED", "migration_status": "SUCCESS", "migration_summary": {
"access_control_policy": [ [
{
"access_rule_counts": 0,
"expanded_acp_rule_counts": 0, "name": "Doesn't Exist",
"partially_migrated_acl_rule_counts": 3
}
]
],
"interface_counts": 0,
"interface_group_counts": 0, "nat_Policy": [
[
{
"NAT_rule_counts": 0, "name": "Doesn't Exist",
"partially_migrated_nat_rule_counts": 0
}
]
],
"network_object_rename_counts": 1,
"network_object_reused_counts": 21,
"object_group_counts": 6,
"objects_counts": 34,
"port_object_rename_counts": 0,
"port_object_reused_counts": 0,
"security_zone_counts": 3,
"static_routes_counts": 0,
"sub_interface_counts": 0
},
"migration_tool_version": "1.1.0.1912",
"source_config_counts": 504,
"source_device_model_number": " FDM5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 series 2000 MHz,
 1 CPU (4 cores)",
"source_device_serial_number": "JAF1528ACAD", "source_device_version": "9.6(2)",
"source_type": "FDM",
"system_information": {
"browser": "Chrome/69.0.3497.100", "operating_system": "Windows NT 10.0; Win64; x64"
},
"target_device_model": "Cisco Firepower Threat Defense for VMWare", "target_device_version":
 "75",
"target_management_type": "Management Center", "target_management_version": "6.2.3.3 (build
 76)",
"time": "2018-09-28 18:17:56",
"tool_performance": { "config_push_time": 7,
"conversion_time": 14,
"migration_time": 592
}
},
"version": "1.0"
```



CHAPITRE 4

Dépannage des problèmes de migration

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

Une migration échoue généralement lors du chargement du fichier de configuration de l'appareil géré par FDM ou lors du transfert de la configuration migrée vers centre de gestion.

Voici certains des scénarios courants où le processus de migration échoue :

- Fichiers manquants dans le fichier compressé config.zip de l'appareil géré par FDM.
- Les fichiers non valides sont détectés par l'outil de migration du pare-feu dans le fichier Cofig.zip de l'appareil géré par FDM.
- Si le fichier de configuration de l'appareil géré par FDM est d'un autre type de fichier compressé que le type .zip.
- Caractères inconnus ou non valides dans le fichier de configuration de l'appareil géré par FDM
- Éléments incomplets ou manquants dans le fichier de configuration de l'appareil géré par FDM.
- Perte de connectivité réseau ou latence

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

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

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

   La page de soutien technique apparaît.

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

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

3. Cliquez sur **Télécharger**.

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

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

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

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

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

Journaux et autres fichiers utilisés pour le dépannage

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

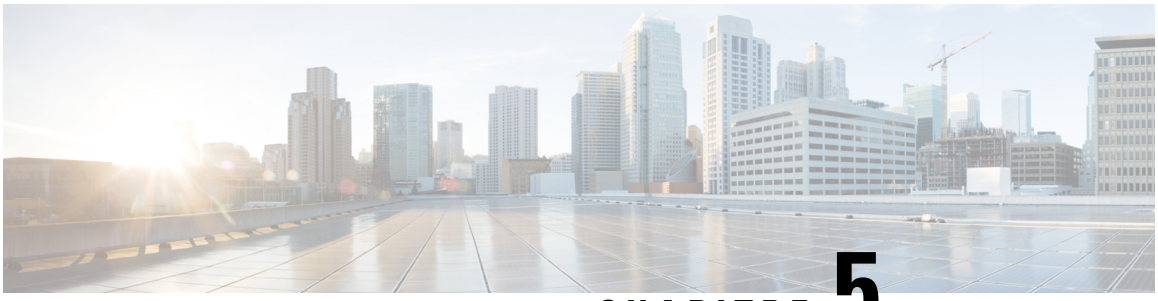
Fichier	Emplacement
Fichier de journalisation	<migration_tool_folder>\journaux
Rapport pré-migration	<migration_tool_folder>\ressources
Rapport post-migration	<migration_tool_folder>\ressources
fichier non analysé	<migration_tool_folder>\ressources

Résolution de problèmes des échecs du chargement de fichiers

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

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

- Message d'erreur affiché par l'outil de migration de pare-feu sécurisé : fournit un résumé de haut niveau de la cause de l'échec.
- Fichier journal : recherchez le mot « erreur » pour afficher la raison de l'échec.



CHAPITRE 5

Foire aux questions

Foire aux questions

Q. Quelles sont les nouvelles fonctionnalités prises en charge par la version 4.0 de l'outil de migration Secure Firewall ?

A. Les fonctionnalités suivantes sont prises en charge avec la version 4.0 :

- Migration d'un appareil géré par FDM vers un appareil de défense contre les menaces géré par le centre de gestion ou le centre de gestion de pare-feu fourni dans le nuage.
- Migration des routes ECMP (Equal Cost Multi-Path) à partir d'ASA.
- Migration du routage basé sur les politiques (PBR) à partir d'ASA.
- Migration des attributs personnalisés du VPN à accès à distance et de l'équilibrage de charge du VPN à partir d'ASA.

Foire aux questions

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.