Mise en route de l'outil de migration Secure Firewall

À propos de l'outil de migration Secure Firewall

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

L'exemple de procédure de migration (Exemple de migration : du dispositif géré par 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.

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.