Migration du pare-feu Palo Alto Networks vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration

Première publication : 2022-11-21

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

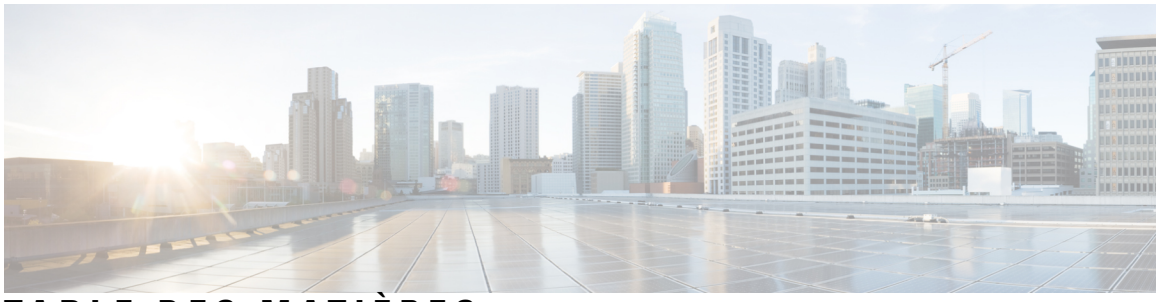
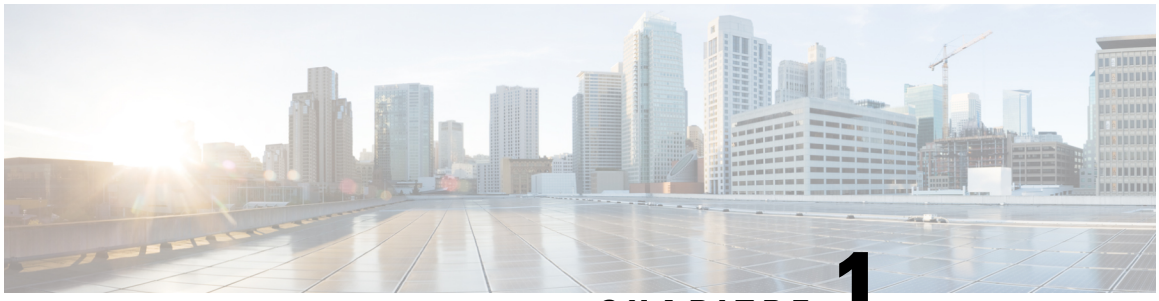


TABLE DES MATIÈRES



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 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 PAN 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 PAN 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 PAN des , les analyse et les transmet au Cisco Secure Firewall Management Center. Pendant la phase d'analyse, l'outil de migration Secure Firewall génère un **rapport de pré-migration** qui identifie les éléments suivants :

- Lignes XML de configuration du PAN contenant des erreurs
- PAN dresse la liste des lignes PAN XML que l'outil de migration Secure Firewall ne peut pas reconnaître. Signalez les lignes de configuration XML sous la rubrique erreur dans le **rapport de pré-migration** et dans les journaux de la console ; cela bloque la migration.

S'il y a des erreurs d'analyse, vous pouvez les corriger, télécharger à nouveau une nouvelle configuration, vous connecter à l'appareil de destination, mapper les interfaces aux interfaces défense contre les menaces, mapper les applications, mapper les zones de sécurité et procéder à l'examen et à la validation de votre configuration. Vous pouvez ensuite faire migrer la configuration vers le périphérique de destination.

Console

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

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

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

Journaux

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

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

Ressources

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

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

Fichier non analysé

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

<migration_tool_folder>\resources

Recherche dans l'outil de migration Secure Firewall

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

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

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

Ports

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

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

Cisco Success Network (Réseau de succès Cisco)

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

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

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

Quoi de neuf dans l'outil de migration Secure Firewall

Version	Fonctionnalités prises en charge
6.0	

Version	Fonctionnalités prises en charge
	Cette version comprend les nouvelles caractéristiques et améliorations suivantes : **Migration de Cisco Secure Firewall ASA vers Secure Firewall Threat Defense** • Vous pouvez maintenant faire la migration des configurations WebVPN de votre Cisco Secure Firewall ASA vers les configurations de Cisco Zero Trust Access Policy sur un appareil de protection contre les menaces. Cochez bien la case **WebVPN** à la page **Select Features** [sélectionner les fonctions] et jetez un œil au nouvel onglet **WebVPN** à la page **Optimize, Review and Validate Configuration** [optimiser, revoir 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. **Migration du pare-feu Check Point vers Cisco Secure Firewall Threat Defense**

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

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

Version	Fonctionnalités prises en charge
5.0	• L'outil de migration Cisco Secure Firewall prend maintenant en charge la migration de plusieurs contextes de sécurité à partir des appareils Cisco Secure Firewall ASA vers les appareils de protection contre les menaces. Vous pouvez choisir d'effectuer la migration de configurations à partir d'un de vos contextes ou fusionner les configurations de tous vos contextes routés en mode pare-feu, et ensuite procéder à leur migration. Un soutien sera bientôt offert pour la fusion des configurations de plusieurs contextes transparents en mode pare-feu. Consultez la rubrique Select the ASA Primary Security Context [sélectionner le contexte de sécurité primaire ASA] pour en savoir plus. • L'outil de migration tire maintenant profit de la fonctionnalité de routage et de transfert virtuels afin de reproduire le flux de trafic divisé 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.

Version	Fonctionnalités prises en charge
4.0.2	L'outil de migration Secure Firewall 4.0.2 inclut les nouvelles caractéristiques et améliorations suivantes : • Outil de migration Cisco Secure Firewall prend désormais en charge le fractionnement des listes de contrôle d'accès (ACL) avec des applications par règle. Lorsque votre configuration de pare-feu Palo Alto Networks contient des listes de contrôle d'accès (ACL) avec une règle configurée pour plusieurs applications, vous pouvez utiliser l'option **Fractionner les listes de contrôle d'accès (ACL) avec les applications par règle** pour diviser la règle en plusieurs règles avec une application par règle. L'outil de migration crée de nouvelles règles de sorte qu'une règle soit configurée pour une application, ce qui garantit plus de clarté dans l'examen et la validation de la configuration. • L'outil de migration valide désormais la configuration NAT dans votre pare-feu source pour les adresses IP dynamiques ou les adresses de secours de port et migre les configurations uniquement si l'adresse de repli est la même que l'adresse de la zone de destination. En effet, Secure Firewall Management Center ne peut avoir que l'adresse de destination en tant qu'interface IP dynamique ou interface de repli de port. • 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?**.
4.0.1 ou ultérieure	L'outil de migration Secure Firewall 4.0.1 inclut les nouvelles caractéristiques et améliorations suivantes : • Le Outil de migration Cisco Secure Firewall prend désormais en charge les règles de traduction d'adresses réseau (NAT) avec des objets de type nom de domaine entièrement qualifié (FQDN) dans la destination traduite lors de la migration vers unecentre de gestion version 7.1 ou supérieure. **Important** Les règles NAT avec des objets FQDN ou des groupes d'objets FQDN dans la source traduite, les règles NAT avec des objets FQDN et des groupes d'objets FQDN à la fois dans la source d'origine et la destination, et les règles NAT avec des groupes d'objets FQDN dans la destination traduite ne sont pas prises en charge. • L'optimisation de l'ACL est désormais améliorée pour inclure une nouvelle colonne **Application** dans le rapport post-migration, qui répertorie les applications optimisées.
3.0.1	• Pour ASA avec FirePOWER Services, Check Point, Palo Alto Networks et Fortinet, Secure Firewall Série 3100 n'est pris en charge qu'en tant que dispositif de destination.

Version	Fonctionnalités prises en charge
3.0	L'outil de migration Secure Firewall 3.0 permet de migrer vers le centre de gestion de pare-feu de Palo Alto Networks fourni dans le nuage si le centre de gestion de destination est 7.2 ou plus récent.

2,1	• Offre le support pour les versions 6.1 x et ultérieures du système d'exploitation PAN
	• L'outil de migration Secure Firewall vous permet de migrer les éléments de configuration PAN suivants vers défense contre les menaces :
	  • Interfaces
	  • Routes statiques
	  • Objets et groupes de réseau
	  • Objets de port et groupes de port
	  • Listes de contrôle d'accès (Politiques)
	  • Zones
	  • Applications
	  • Règles NAT
	• Capacité de recherche basée sur le contenu qui est activée sur la page **Examen et validation**
	• Une barre de progression est fournie dans le cadre de l'amélioration de l'interface utilisateur

Licence pour l'outil de migration Secure Firewall

L'application outil de migration Secure Firewall est gratuite et ne requiert pas de licence. Cependant, le centre de gestion doit avoir les licences requises pour les caractéristiques défense contre les menaces correspondantes afin d'enregistrer les appareils défense contre les menaces et d'y déployer les politiques.

Configuration requise pour l'outil de migration Cisco Secure Firewall

L'outil de migration Cisco Secure Firewall a les exigences en matière d'infrastructure et de plateforme suivantes:

- Fonctionne sur un système d'exploitation Microsoft Windows 10 64-bit ou sur une version macOS 10.13 ou une version récente
- Google Chrome comme navigateur par défaut du système

- (Windows) Comporte des paramètres de veille configurés dans la consommation et la veille pour ne jamais mettre l'ordinateur en veille, de sorte que le système ne se met pas en veille lors d'une migration importante
- (macOS) Comporte des paramètres d'économie d'énergie 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 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 PAN vers la protection contre les menaces, prenez en compte les conditions préalables et les exigences qui suivent :

- Le dispositif de défense contre les menaces cible doit être enregistré auprès du centre de gestion.
- Le dispositif de défense contre les menaces peut être un dispositif autonome ou une instance de conteneur. Il ne doit **pas** faire partie d'un cluster ou d'une configuration de haute disponibilité.
  - 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 PAN. 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.

Lignes directrices et limites relatives à la licence

L'outil de migration Cisco Secure Firewall crée un mappage individuel pour l'ensemble des objets et des règles pris en charge, qu'ils soient utilisés dans une règle ou une politique.L'outil de migration Cisco Secure Firewall offre une caractéristique d'optimisation qui vous permet d'exclure la migration d'objets inutilisés (des objets qui ne sont cités en référence dans aucune ACL ou NAT).

L'outil de migration Cisco Secure Firewall ne migre pas les objets, les règles NAT et les routes qui ne sont pas pris en charge.

Limites de configuration PAN

Voici les limites imposées à la migration de la configuration PAN source :

- L’outil de migration Cisco Secure Firewall permet la migration des systèmes multi-vsys.
- La configuration système n'est pas migrée.
- Les groupes d’objets de service imbriqués ou le groupe de ports ne sont pas pris en charge par le centre de gestion. Dans le cadre de la conversion, l’outil de migration Cisco Secure Firewall étend le contenu du groupe d’objets imbriqués ou du groupe de ports.
- L’outil de migration Cisco Secure Firewall divise les groupes ou les objets de service étendus aux ports sources et 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 centre de gestion dont la signification est la même.

Lignes directrices pour la migration de PAN

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

- La migration de l'option de journalisation ACL suit les meilleures pratiques pour défense contre les menaces. L’option de journalisation pour une règle est activée ou désactivée selon la configuration du PAN source. Pour les règles dont l'action est le **refus**, l'outil de migration Secure Firewall configure la journalisation au début de la connexion. Si l'action est la **permission**, l'outil de migration Secure Firewall configure la journalisation à la fin de la connexion.

Configurations de PAN prises en charge

L’outil de migration Cisco Secure Firewall peut totalement migrer les configurations PAN suivantes :

- Objets et des groupes de réseau
- Zones (couche 2, couche 3, fil virtuel)
- Objets de service
- 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, toutefois, sont migrées avec toutes les fonctionnalités.

- Objets et groupes FQDN IPv4 et IPv6
- Prise en charge de la conversion IPv6 (interface, routes statiques, objets, ACL)
- Règles d’accès
- Règles NAT

Remarque Toutes les politiques avec le service comme « application-default » seront migrées comme « any », car défense contre les menaces n'a pas de fonctions équivalentes.

La source traduite et la destination originale n'ont pas d'objet « any » prédéfini sur centre de gestion. Par conséquent, un objet avec 0.0.0.0/0 nommé Obj_0.0.0.0 sera créé et envoyé.

- Règles NAT avec un objet FQDN dans la destination traduite, lors de la migration vers Cisco Secure Firewall Threat Defense exécutant la version 7.1 ou une version ultérieure
- Interfaces physiques
- Sous-interfaces (l'ID de sous-interface est toujours défini sur le même numéro que l'ID de VLAN lors de la migration)
- Agrégation des interfaces (canaux de port)
- Routes statiques, à l'exception de celles configurées avec Next Hop [saut suivant] en tant que routes Next VR [VR suivant] et ECMP qui ne sont pas migrées

Remarque Si le pare-feu source (PAN) a des routes connectées qui sont configurées comme des routes statiques, la transmission échoue. centre de gestion ne vous permet pas de créer des routes statiques pour les routes connectées. Supprimez ces routes et poursuivez la migration.

Remarque L'interface filaire virtuelle ne sera pas migrée, alors que la zone filaire virtuelle le sera. Vous devez créer manuellement l'interface BVI sur défense contre les menaces après la migration.

Configurations de PAN prises en charge partiellement

L'outil de migration Cisco Secure Firewall prend partiellement en charge les configurations suivantes de PAN pour la migration. Certaines de ces configurations comprennent des règles avec des options avancées qui sont migrées sans ces options. Si centre de gestion prend en charge ces options avancées, vous pouvez les configurer manuellement lorsque la migration sera terminée.

- Règles des stratégies de contrôle d'accès au moyen des profils
- Groupe de services qui contient des objets de service avec des protocoles contenant TCP, UDP et SCTP.

Remarque Le type SCTP sera supprimé, et le groupe de services sera migré partiellement.

- Le groupe d'objets qui contient des objets pris en charge et non pris en charge sera migré, et les objets non pris en charge seront supprimés.

Configurations PAN non prises en charge

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

- Règles des stratégies de contrôle d'accès basées sur le temps
- Règles de politique de contrôle d'accès basées sur l'utilisateur
- Objet de service utilisant le protocole SCTP
- Objets FQDN commençant par un caractère spécial ou contenant un caractère spécial
- Noms de domaine complets (FQDN) génériques
- Règles NAT configurées avec SCTP
- Règle NAT avec un objet FQDN et un groupe d'objets FQDN dans la source traduite
- Règle NAT avec un objet FQDN et un groupe d'objets FQDN dans la source et la destination d'origine
- Règle NAT avec un groupe d'objets FQDN dans la destination traduite
- NAT IPv6
- Politiques qui utilisent le filtrage d'URL

Pour configurer les fonctions non prises en charge par défense contre les menaces, consultez le guide de configuration de Threat Defense.

Remarque Toutes les politiques, prises en charge ou non, sont migrées vers centre de gestion. Les politiques non prises en charge sont migrées comme des politiques désactivées. Vous pouvez activer ces politiques après la solution de contournement ou les configurer selon centre de gestion.

La politique dont le filtrage d'URL des profils, l'identifiant de l'utilisateur, la source et la destination sont rejetés n'est **pas prise en charge**.

Lignes directrices et limites relatives aux appareils Défense contre les menaces

Si vous prévoyez de migrer votre configuration PAN vers défense contre les menaces, s'il existe des configurations propres à l'appareil sur défense contre les menaces, comme des routes et des interfaces, lors de la migration poussée, l'outil de migration Cisco Secure Firewall nettoie automatiquement l'appareil et remplace la configuration PAN.

Remarque Afin de prévenir toute perte indésirable de données de l'appareil (cible défense contre les menaces), nous vous recommandons de nettoyer manuellement l'appareil avant la migration.

Plateformes prises en charge pour la migration

Le 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 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 platesdéfense contre les menaces-formes :

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

Remarque

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

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

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

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 17.
- La version du logiciel centre de gestion qui est prise en charge pour la migration pour PAN est 6.1.x et les versions ultérieures.
- Vous avez obtenu et installé des licences intelligentes défense contre les menacesqui incluent toutes les fonctionnalités que vous prévoyez de migrer depuis ASA PAN, comme décrit ci-dessous :
  - La section Mise en route du compte Smart de Cisco sur Cisco.com
  - Enregistrez le Centre de gestion du pare-feu avec le Cisco Smart Software Manager.
  - Octroi de licences pour le système de pare-feu
  - Vous avez activé l'API REST.centre de gestion

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

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

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

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

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

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

Régions CDO

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

Tableau 1 : Régions CDO et URL

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

Versions logicielles prises en charge pour la migration

Les outils de migration Secure Firewall, et les versions défense contre les 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 de pare-feu de Palo Alto Networks prises en charge

L'outil de migration Cisco Secure Firewall prend en charge la migration vers défense contre les menaces le système d'exploitation du pare-feu PAN version 6.1.x et version plus récente.

Versions Centre de gestion prises en charge pour la configuration source du pare-feu PAN

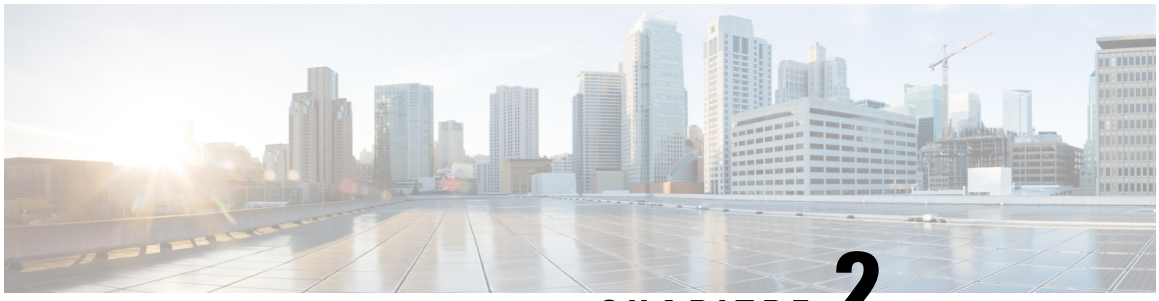
Pour le pare-feu PAN, l'outil de migration Cisco Secure Firewall prend en charge la migration vers un périphérique centre de gestion géré par uncentre de gestion qui exécute la version 6.2.3.3 ou une version récente.

Remarque La migration vers l'appareil défense contre les menaces6.7 n'est pas actuellement prise en charge. Par conséquent, la migration peut échouer si le périphérique est configuré avec une interface de données pour l'accès centre de gestion.

Versions Défense contre les menaces prises en charge

L'outil de migration Secure Firewall recommande de migrer vers un appareil fonctionnant défense contre les menaces avec la version 6.5 ou une version ultérieure.

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

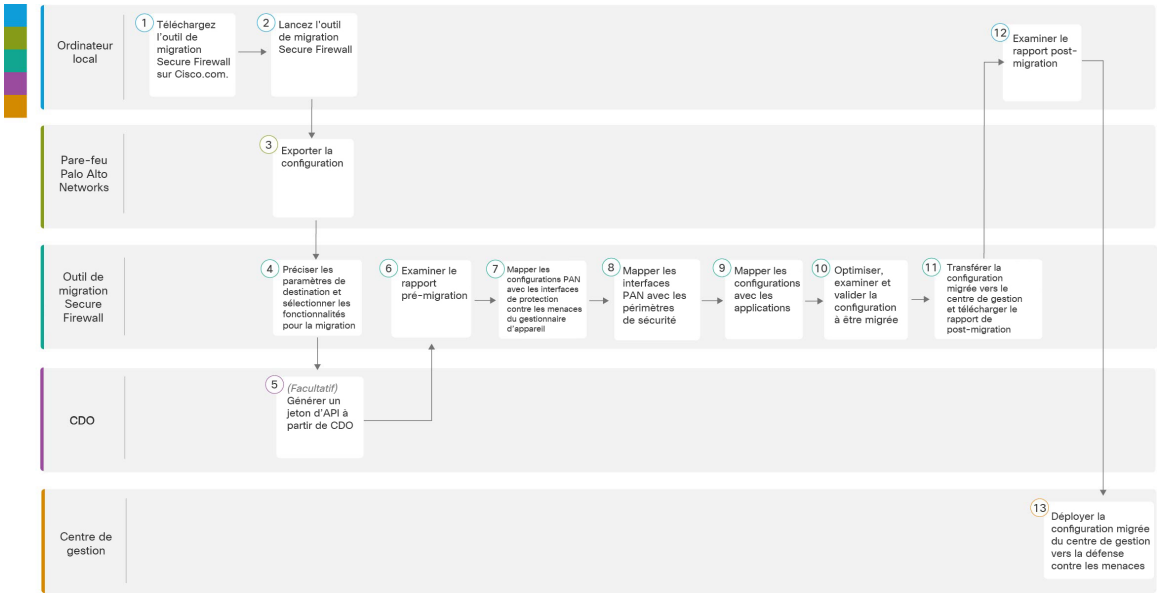


CHAPITRE 2

Flux de travail de la migration du pare-feu Palo Alto Networks vers Threat Defense

Procédure de bout en bout

L'organigramme suivant illustre le flux de travail de migration d'un pare-feu Palo Alto Networks 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
2	Ordinateur local	Lancez l'outil de migration Secure Firewall sur votre machine locale, voir Lancer l'outil de migration Secure Firewall.
3	Pare-feu Palo Alto Networks	Exportation du fichier de configuration : Pour exporter la configuration du pare-feu Palo Alto Networks, consultez Exporter la configuration du pare-feu de Palo Alto Networks [exporter la configuration de Palo Alto Networks].
4	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 .
5	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, reportez-vous à la section Préciser les paramètres de destination pour l'outil de migration Secure Firewall
6	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
7	Outil de migration Secure Firewall	Pour vous assurer que la configuration PAN est correctement migrée, mappez les interfaces PAN aux objets d'interface de protection contre les menaces, aux périmètres de sécurité et aux groupes d'interfaces appropriés. Pour connaître les étapes détaillées, consultez la section Mappez les configurations de de PAN du pare-feu avec les interfaces de Défense contre les menaces. [mappage des configurations du pare-feu Fortinet avec les interfaces de protection contre les menaces du gestionnaire de l'appareil Cisco Secure Firewall].
8	Outil de migration Secure Firewall	Pour mapper les interfaces PAN aux périmètres de sécurité appropriés, consultez Associez les interfaces PAN à des périmètres de sécurité, à groupes d'interfaces . [mappage des interfaces PAN aux périmètres de sécurité] pour obtenir des instructions détaillées.
9	Outil de migration Secure Firewall	Vous pouvez mapper la configuration PAN aux applications cibles correspondantes. Consultez à cet effet la section Mappez les configurations avec les applications [mappage des configurations avec les applications] pour obtenir les instructions détaillées.
10	Outil de migration Secure Firewall	Optimisez et examinez soigneusement la configuration et vérifiez qu'elle est correcte et qu'elle correspond à la façon dont vous souhaitez configurer le dispositif de défense contre les menaces. Pour les étapes détaillées, référez-vous à Optimiser, examiner Examiner et valider la configuration.

	Espace de travail	Étapes
11	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 .
12	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.
13	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 PAN, 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.

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 Exporter la configuration du pare-feu de Palo Alto Networks .

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 16.
- 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 devez extraire des informations d'un pare-feu PAN à l'aide de l'outil de migration Secure Firewall, passez à la section Fichier de configuration du pare-feu Palo Alto (pas géré par Panorama).

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.

Exporter la configuration du pare-feu de Palo Alto Networks

Vous pouvez exporter le fichier de configuration comme suit :

Fichier de configuration du pare-feu Palo Alto (pas géré par Panorama)

Suivez ces étapes pour extraire la configuration de la passerelle :

Étape 1 Naviguer vers **Appareil** > **Mise** en place > **Opérations**, et sélectionner **Sauvegarder la configuration** nommée *<file_name.xml>*.

Étape 2 Cliquez sur **Ok**.

Étape 3 Naviguer vers **Appareil** > **Mise** en place > **Opérations**, et sélectionner **Exporter la configuration** nommée

Étape 4 Choisissez le fichier <*file_name.xml*>

Étape 5 Cliquez sur **Ok**.

Étape 6 Choisissez le fichier XML qui contient votre configuration en cours d'exécution <*file_name.xml*>et cliquez sur **OK** pour exporter le fichier de configuration

Étape 7 Sauvegardez le fichier exporté à un endroit, à l'extérieur du pare-feu. Vous pouvez utiliser cette copie pour téléverser vers l'outil de migration Secure Firewall pour faire migrer la configuration vers défense contre les menaces.

Étape 8 (Facultatif) Si vous avez une stratégie NAT dans laquelle le NAT de destination a les mêmes zones de source et de destination, procédez comme suit :

a) Exécutez la **commande d'affichage** d'itinéraire à partir de l'interface utilisateur du pare-feu.

b) Copiez le tableau de routage vers un fichier *.txt.*

c) Ajoutez le fichier *.txt* au dossier où vous compresserez les fichiers .txt et .xml avec le *panconfig.xml*.

Ces étapes sont obligatoires pour la migration. Si vous n'effectuez pas ces étapes, les zones de destination ne seront pas mappées pendant la migration de l'outil de migration Secure Firewall et seront incluses dans les rapports de migration.

Remarque Utilisez la **commande d'affichage d'itinéraire** pour extraire les détails du tableau de routage. Collez la sortie extraite dans un bloc-notes.

Fichier de configuration du pare-feu Palo Alto (géré par Panorama)

La configuration doit être extraite de la passerelle si votre appareil est géré par Panorama. Il suffit de fusionner la configuration de Panorama avec la passerelle et d'extraire la configuration.

Dans l'interface utilisateur de l'outil de migration Cisco Secure Firewall :

Avant de commencer

Connectez-vous à l'interface utilisateur Web du pare-feu Palo Alto en utilisant le compte de super utilisateur.

Étape 1 Allez à **Device [appareil]** > **Support [soutien]** > **Tech Support File [fichier de soutien technique]**.

Étape 2 Cliquez sur **Generate Tech Support File** [générer un fichier de soutien technique].

Étape 3 Cliquez sur **Download Tech Support File** [télécharger le fichier de soutien technique] une fois le fichier généré.

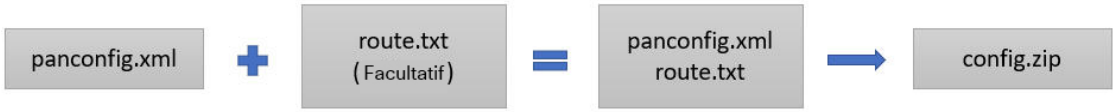
Étape 4 Décompressez le fichier (.zip ou .tar), puis suivez le chemin *\opt\pancfg\mgmt\saved-configs* pour récupérer le fichier *merged-running-config.xml*.

Prochaine étape

Compresser les fichiers exportés

Compresser les fichiers exportés

Exportez le fichier *panconfig.xml* pour le pare-feu de la passerelle Palo Alto et le fichier *route.txt* (si les règles NAT ont les mêmes zones sources et de destination).



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
- À partir de l'outil de migration Secure Firewall 3.0, vous pouvez choisir entre le centre de gestion des pare-feux sur site et le centre de gestion des pare-feux en nuage.
- Pour le centre de gestion de pare-feu en nuage, la région et le jeton API doivent être fournis. Pour en savoir plus, consultez le Centre de gestion cible pour la migration pris en charge.
- (Facultatif) Si vous souhaitez faire migrer des configurations spécifiques à un dispositif, comme des interfaces et des itinéraires, ajoutez le défense contre les menaces cible 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 : vous pouvez choisir de migrer vers un centre de gestion de pare-feu sur site ou un centre de gestion de pare-feu en nuage .

- 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 voulez migrer vers un appareil défense contre les menaces, vous pouvez seulement migrer vers les appareils défense contre les menaces offerts 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**.

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 .

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

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

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

  L'outil de migration Secure Firewall prend en charge la migration du pare-feu Palo Alto Networks vers la version 6.7 centre de gestion oudéfense contre les menaces ou ultérieure avec l'option de déploiement à distance activée. La migration des interfaces et des itinéraires doit être faite manuellement.

- 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.

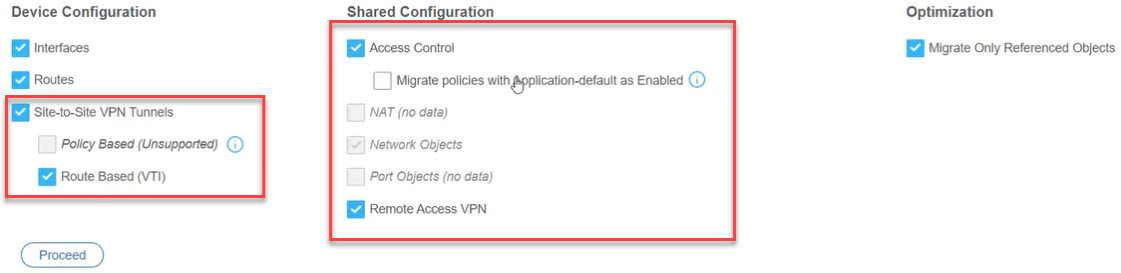
- Si vous effectuez une migration vers un dispositif de destinationdéfense contre les menaces, l'outil de migration Secure Firewall sélectionne automatiquement les fonctionnalités disponibles pour la migration à partir de la

configuration de du 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 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.
- Pour PAN, sous **Configuration partagée**, sélectionnez l'option **Contrôle d'accès** appropriée :

  Migrer les politiques avec l'application - activé par défaut - Lorsque vous sélectionnez cette option, l'application PAN sera migrée. Vous ne pouvez afficher l'option **Migrer les politiques avec l'application par défaut** que si vous cochez cette case.

Remarque **Le mappage d'applications** n'est activé que lorsque des stratégies sont sélectionnées pour la migration.



Si vous migrez la configuration d'un pare-feu Palo Alto Networks avec configuration VPN, vous pouvez choisir de sélectionner ou de désélectionner les **tunnels VPN de site à site** dans le panneau **Device Configuration** [configuration de l'appareil] et **Remote Access VPN** [VPN avec accès à distance] dans le panneau **Shared Configuration** [configuration partagée]. Notez que la configuration VPN de site à site basée sur les politiques n'est pas prise en charge, car le pare-feu Palo Alto Networks n'est pas compatible.

Politiques dont le service est « Application par défaut »

Les politiques dont le service est **« application par défaut »**et dont l'application a un membre ou un groupe qui est référencé, sont migrées selon les choix que vous avez faits sur la page de **sélection des fonctionnalités**. centre de gestion n'a pas l'équivalent de « **application par défaut** », donc ces politiques sont poussées avec le service « any ». Si vous reproduisez la même fonctionnalité que **l'application par défaut**, déterminez les ports utilisés par l'application à partir du pare-feu de Palo Alto Networks et configurez les ports dans la section des ports de la politique dans centre de gestion.

Par exemple, une politique ayant pour nom « **navigation web** » et pour service « **application par défaut** » est migrée en tant qu'application HTTP (l'équivalent de navigation web) et en tant que port « **any** ». Pour reproduire la même fonctionnalité que « **application par défaut** », configurez le port comme TCP/80 et TCP/8080. La navigation web utilise les ports TCP 80 et TCP 8080 Si une politique a de multiples applications, configurez les ports qui sont utilisés pour chaque application.

En cas de multiples applications à une politique, nous vous recommandons de diviser la politique avant de configurer les ports, puisque cela pourrait permettre un accès supplémentaire à d'autres applications.

Les politiques dont l'application est configurée comme « **any** » et le service comme « **application par défaut** » sont migrées comme désactivées, indépendamment des choix disponibles sur la page de **sélection des fonctionnalités** (l'application comme « **any** » et le service comme « **any** ».) Si ceci est un comportement acceptable, activez l'application et acceptez les changements. Autrement, choisissez l'application ou le service requis et activez la politique.

Diviser les listes de contrôle d'accès avec des applications par règle

Lors de la migration de listes de contrôle d'accès contenant une règle configurée pour plusieurs applications, vous pouvez choisir de diviser les listes de contrôle d'accès, ce qui divise la règle en plusieurs règles avec une application par règle. Pour ce faire, cochez la case **Diviser les ACL avec les applications par règle**. Par contre, la case n'apparait pas si la configuration que vous tentez de migrer ne contient pas d'applications multiples configurées par règle d'accès.

Chaque règle est convertie en de multiples règles avec une application par règle, ce que vous pouvez examiner dans la page **Optimiser, examiner et valider**.

- 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 ne seront pas migrés. Cela optimise le temps de migration et nettoie les objets inutilisés de la configuration.

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 :

- Un résumé des éléments de configuration des dispositifs qui peuvent être migrés avec succès et des défense contre les menacesfonctionnalités spécifiques ASA sélectionnées pour la migration.
- **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 qui ne peuvent être que partiellement migrés. Ces éléments de configuration comprennent des règles et des objets avec des options avancées, alors que la règle ou l'objet peut être migré sans les options avancées. Examinez ces lignes, vérifiez si les options avancées sont prises en charge dans centre de gestion, et si c'est le cas, prévoyez de configurer ces options manuellement après avoir terminé la migration à l'aide de l'outil de migration Secure Firewall.
- **Configuration** non prise en charge - Détails des éléments de configuration des qui ne peuvent pas être migrés car l'outil de migration Secure Firewall ne prend pas en charge la migration de ces fonctionnalités. Examinez ces lignes, vérifiez si chaque fonctionnalité est prise en charge dans centre de gestion, et si c'est le cas, prévoyez de configurer les fonctionnalités manuellement après avoir terminé la migration à l'aide de l'outil de migration Secure Firewall.
- **Configuration ignorée** - Détails des éléments de configuration des dispositifsASA 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 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 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 PAN du pare-feu avec les interfaces de Défense contre les menaces.

Mappez les configurations de de PAN du pare-feu 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 ASA. Ces interfaces ne doivent pas avoir les mêmes noms sur les deux appareils. Vous pouvez choisir comment associer les interfaces.

Le mappage de l'interface de l' avec 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 menaces doit avoir un nombre égal ou supérieur d'interfaces PAN ou d'interfaces de données de canal de port (PC) ou de sous-interfaces utilisées (à l'exception de la gestion seule dans la configuration PAN). 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 d'appareils gérés par FDMou de sous-interfaces physiques utilisées, de canal de port ou de sous-interfaces de canal de port (à l'exclusion des interfaces de gestion uniquement et des sous-interfaces dans la configuration de dispositifs gérés par un). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre 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'PAN , vous pouvez créer des interfaces physiques ou des sous-interfaces physiques supplémentaires sur la cible défense contre les menaces.

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 26.

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

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 , 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.

Remarque Si le nombre d'interfaces sur le pare-feu source est plus que celui du pare-feu cible, créez alors des sous-interfaces sur le pare-feu cible et réessayez la migration.

Étape 2 Lorsque vous avez mappé chaque interface de périphérique à une interfacedéfense contre les menaces, cliquez sur **Suivant**.

Prochaine étape

Mappez les interfaces PAN aux objets d'interface et zones de sécurité défense contre les menacesappropriés Pour plus d'informations, référez-vous Associez les interfaces PAN à des périmètres de sécurité, à groupes d'interfaces .

Associez les interfaces PAN à des périmètres de sécurité, à groupes d'interfaces .

Pour que la configuration soit migrée correctement, mappez les interfaces de aux objets d'interface défense contre les menaces, aux périmètres de sécurité, appropriés. Dans une configuration de , les politiques de contrôle d'accès et les politiques NAT utilisent des noms d'interface (nameif). Dans centre de gestion, ces politiques utilisent des objets d'interface. De plus, les politiques centre de gestion regroupent les objets d'interface ainsi :

- Zones de sécurité - Une interface ne peut appartenir qu'à une seule zone de sécurité.

L'outil de migration Secure Firewall permet le mappage un à un des interfaces avec les zones de sécurité ; lorsqu'une zone de sécurité est mappé à une interface, il n'est pas disponible pour le mappage à d'autres interfaces, bien que centre de gestion le permette. Pour en savoir plus sur les périmètres de sécurité 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**, examinez les interfaces disponibles et les zones de sécurité.

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 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 Pour mapper les interfaces aux zones de sécurité qui existent dans centre de gestion, dans la colonne **Zones de sécurité**, choisissez la zone de sécurité pour cette interface.

Étape 4 Vous pouvez mapper manuellement ou auto-créer les zones de sécurité.

Pour mapper manuellement les zones de sécurité, 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.
c) Saisissez le nom de la zone de sécurité dans la colonne **Zone de sécurité**. Le nombre maximal de caractères est de 48.
d) Cliquez sur **Close** (Fermer).

Pour mapper les zones de sécurité par auto-création, faites ce qui suit :

a) Cliquez sur **Auto-créer**.
b) Dans la boîte de dialogue **Auto-créer**, cochez **Mappage de zone**.
c) Cliquez sur **Auto-créer**.

Une fois que vous avez cliqué sur **Auto-créer**, les zones de pare-feu source sont mappés automatiquement. Si les mêmes zones de nom existent déjà dans centre de gestion, alors la zone sera réutilisée. La page de mappage affichera « (A) » contre la zone réutilisée. Par exemple, « (A) » **à l'intérieur**.

Étape 5 Lorsque vous avez mappé toutes les interfaces aux zones de sécurité appropriées, cliquez sur **Suivant**.

Mappez les configurations avec les applications

Vous pouvez mapper les applications aux applications cibles correspondantes. Vous pouvez migrer les règles basées sur l'application.

Une liste d'applications prédéfinies issue du centre de gestion et certaines applications des fichiers de configuration sont répertoriées dans cet onglet. Certains mappages prédéfinis qui existent dans le centre de gestion sont mappés.

Remarque Vous ne pourrez pas modifier un mappage prédéfini.

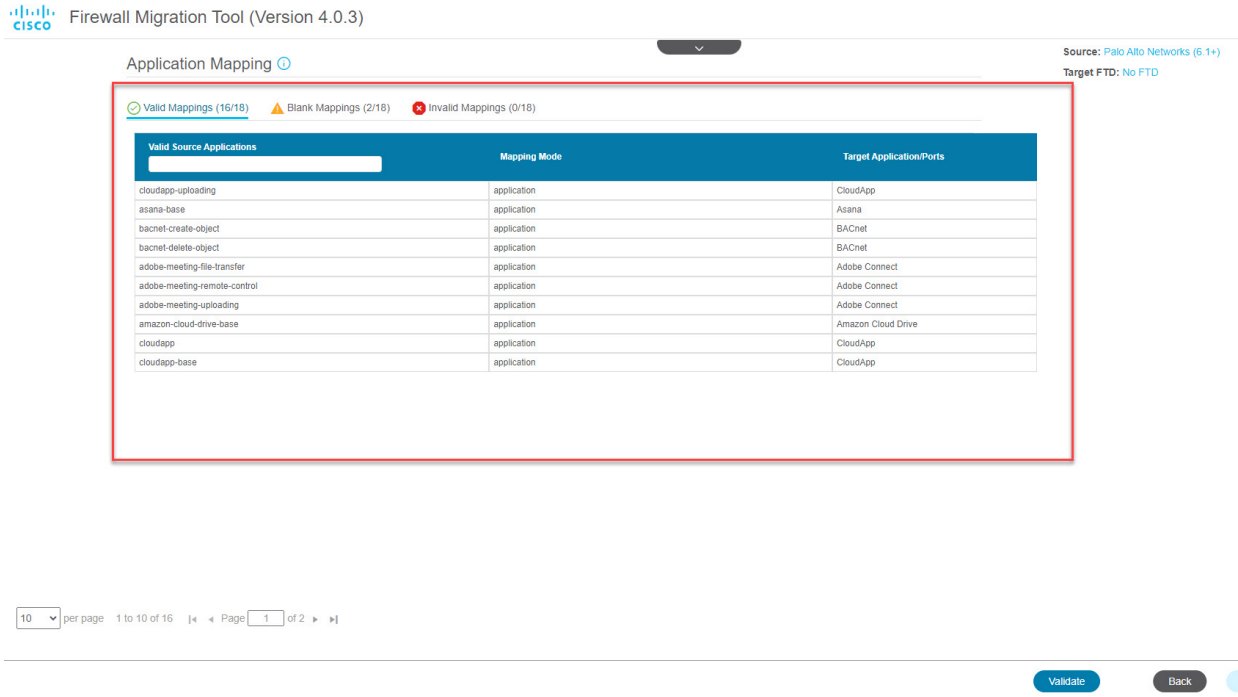
La page **Application Mapping** [mappage des applications] affiche les onglets suivants :

- Mappages non valides : Pour afficher la liste des mappages non valides pour la migration.

  Un mappage est dit **non valide** dans les scénarios suivants :

  - Lorsque le **mode de mappage** est réglé sur **Application** ou **Port**, mais que la **cible** est vide.
  - Lorsque le **mode de mappage** est réglé sur **Port** et que la syntaxe du port est incorrecte. Pour procéder à la migration, la valeur du **mappage non valide** doit être de zéro.

Remarque Le bouton **Next** [suivant] est désactivé jusqu'à ce que la validation soit correcte.



Lorsque vous obtenez la liste prédéfinie des mappages de la source, certaines applications prédéfinies seront mappées automatiquement. Si certaines applications ne sont pas mappées, vous devez le faire manuellement pour le port ou l'application.

- Mappages vides : Pour afficher l'application non mappée. Pour ce faire, l'utilisateur doit entreprendre une action. L'**application** doit être mappée à **Application** ou à **Port**.

Remarque Nous vous recommandons de mapper toutes les entrées **Application**, mais ce n'est pas obligatoire.

Lorsque le mode de mappage est sélectionné et que l'application cible dispose de données valides, il s'agit d'un mappage valide.

Remarque Par défaut, tous les mappages prédéfinis sont disponibles dans l'onglet **Valid Mappings** [mappages valides].

- Mappages valides : Pour afficher le bon mappage. L'outil de migration Cisco Secure Firewall possède sa propre base de données de mappage prédéfini avec PAN et l'application défense contre les menaces pour les applications couramment utilisées. Si l'application de PAN correspond à la base de données du mappage prédéfini, ces applications seront mappées automatiquement et s'afficheront sous un mappage valide.

  Une fois qu'une **application** est mappée à une **application** ou à un **port** dans le **mappage vide**, elle est déplacée vers un **mappage valide** après validation.

Remarque Le mappage prédéfini n'est pas modifiable.

Le nombre de mappages non valides, valides et vides continue de changer selon la migration.

Le tableau suivant affiche les propriétés de mappage d'application.

Tableau 2 : Propriétés du tableau de mappage d'applications

Champ	Description
Application source	Affiche la liste des applications utilisées sur votre pare-feu Palo Alto Networks.
Mode de mappage	Choisissez le mode de mappage qui est soit Application soit Ports. • Application : Choisissez dans la liste des applications cibles pour le mappage. Vous ne pouvez mapper qu'une seule application. • Ports : Choisissez un port disponible pour le mappage. Lorsque vous sélectionnez Ports, saisissez les renseignements sur le port pertinent dans le format indiqué. Par exemple, tcp/80 et udp/80. **Remarque** Les espaces ne sont pas autorisées.
Application cible	Affiche une liste des applications cibles ou des ports cibles selon le mode de mappage.

Les applications ICMP et Ping seront migrées en tant que services **ICMP** et **Ping**. La migration se fait automatiquement par l'outil de migration Cisco Secure Firewall et ne s'affichera pas dans la page de **mappage des applications**.

Étape 1 Cliquez sur l'onglet **Valid Mappings** [mappages valides] pour afficher le nombre de mappages valides pour cette migration. Mappez l'**application source valide** avec le **mode de mappage** valide et l'**application cible**.

Lorsqu'un mappage devient valide, vous pouvez afficher l'augmentation du nombre de mappages valides.

Étape 2 Cliquez sur **Blank Mappings** [mappages vides] pour afficher la liste des mappages vides pour cette migration. Mappez l'**application source vide** avec le **mode de mappage** valide et l'**application cible**.

Par exemple, si vous sélectionnez le mode de mappage et l'enregistrez sans saisir la destination cible, le nombre de mappages vides augmente. Passez en revue l'onglet, mappez-le correctement, puis procédez à la migration.

Remarque Même en présence d'un mappage vide, vous pouvez toujours procéder à la migration.

Étape 3 Cliquez sur l'onglet **Invalid Mappings** [mappages non valides] pour afficher la liste des mappages non valides. Procédez comme suit:

a) Invalid Application [application non valide] : Affiche le mappage non valide pendant la migration.
b) Mapping Mode [mode de mappage] : Choisissez le mode de mappage, soit Application soit Port.

c) Target Application [application cible] : Choisissez l'application cible pour le mappage de l'application.

Par exemple, si vous avez sélectionné le mode de mappage, mais que vous l'avez mappé avec une destination cible différente, vous ne pouvez pas passer aux autres onglets. Passez en revue l'onglet **Invalid Mappings** [mappages non valides], saisissez la bonne application cible, puis procédez au mappage de l'application.

Étape 4 Cliquez sur **Validate** [valider] dans chaque onglet pour valider les mappages non valides, vides ou valides pour cette migration.

Étape 5 Cliquez sur **Next** [suivant] pour continuer.

Étape 6 Cliquez sur **Clear Mapped Data** [effacer les données mappées] pour effacer les mappages que vous avez effectués manuellement avant de valider. Il est recommandé de cliquer sur **Validate** [valider] seulement lorsque vous êtes convaincu des mappages que vous effectuez, car vous ne pourrez pas annuler le mappage après avoir cliqué sur valider, car le mappage deviendra valide.

Prochaine étape

Optimiser, examiner Examiner et valider la configuration

Optimiser, examiner Examiner et valider la configuration

Avant de transférer la configuration de verscentre de gestion, optimisez et examinez soigneusement la configuration et vérifiez qu'elle est correcte et qu'elle correspond à la façon dont vous souhaitez configurer l'appareil défense 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 Cisco Secure Firewall récupère les politiques du système de prévention des intrusions (IPS) et les politiques des fichiers, qui sont déjà présentes dans le centre de gestion, et 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.

Remarque Par défaut, l'option du Groupement en ligne est activée.

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 disponible pour le PANuniquement 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

Cliquez sur **Download Report** [télécharger le rapport] pour revoir le nom de l'ACL et les ACL redondantes et dupliquées correspondantes figurant dans un fichier Excel. Utilisez la feuille **Detailed ACL Information** [information détaillée sur les ACL] pour afficher plus de détails sur les ACL.

Interface de repli dynamique IP/Port

Lorsque vous examinez les configurations NAT sur la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration] pour une migration de Palo Alto Networks vers la protection contre les menaces, vous pouvez vérifier si la règle NAT a une configuration **interface de repli dynamique IP/Port** et si la règle est migrée ou abandonnée.

L'outil de migration Secure Firewall migre la règle NAT si l'adresse IP dynamique configurée ou l'adresse de l'interface de repli du port est identique à l'adresse de la zone de destination. Si elle est différente, la règle n'est pas migrée et est répertoriée comme non prise en charge, car le Secure Firewall Management Center ne peut avoir que l'adresse de destination comme interface de repli de l'IP dynamique ou du port. Si la règle NAT n'a pas de configuration de repli, la migration s'effectue sans aucune validation et est répertoriée comme **Non applicable**dans la colonne **Repli dynamique de l'IP/du port**.

Étape 1 À la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration], cliquez sur **Access Control Rules** [règles de contrôle d’accès] et faites comme suit :

a) Pour chaque entrée dans le tableau, examinez les mappages et vérifiez s’ils sont corrects.

b) Si vous ne souhaitez pas migrer une ou plusieurs politiques de liste de contrôle d’accès, cochez la case des lignes concernées, choisissez**Actions [actions]** > **Do not migrate**[ne pas migrer], puis **Save** [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**.

Astuces Les politiques IPS et les politiques de fichiers joints à une règle de contrôle d’accès seront automatiquement supprimées pour les actions découlant d’une règle, à l’exception de l’option **Allow** [autoriser].

Vous pouvez filtrer le nombre d’ACE dans l’ordre croissant ou décroissant, ou pour voir les résultats égaux, supérieurs et inférieurs.

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.

Étape 2 Cliquez sur les onglets suivants et examinez les éléments de configuration :

- **Contrôle d'accès**
- **Objets (objets de réseau, objets de port)**
- **NAT**
- **Interfaces**
- **Routs**
- **Tunnels de réseau privé virtuel (VPN) de site à site**
- **VPN d'accès à distance**

Remarque Pour les configurations VPN de site à site et d'accès à distance, les configurations de filtre VPN et les objets de liste d'accès étendue qui s'y rapportent sont migrés et peuvent être examinés sous les onglets respectifs.

Si vous ne souhaitez pas migrer une ou plusieurs règles NAT ou interfaces de routes, cochez la case des lignes concernées, choisissez **Actions [actions]** > **Do not migrate**[ne pas migrer], puis **Save** [enregistrer].

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

Étape 3 (Facultatif) Tout en examinant votre configuration, vous pouvez renommer un ou plusieurs objets réseau ou port dans l'onglet **Network Objects** [objets réseau] ou **Port Objects** [objets port] en sélectionnant l'objet et en choisissant **Actions [actions]** > **Rename**[renommer] .

Les critères d'accès et les politiques NAT qui renvoient aux objets renommés sont aussi mis à jour, en leur attribuant de nouveaux noms d'objet.

Étape 4 Vous pouvez afficher les routes à partir de la zone **Routes** [routes] et sélectionner les routes que vous ne souhaitez pas migrer, en sélectionnant une entrée et en choisissant **Actions [actions]** > **Do not migrate** [ne pas migrer].

Étape 5 À la section **Site-to-Site VPN Tunnels** [tunnels VPN de site à site], les tunnels VPN des configurations du pare-feu source sont indiqués. Passez en revue les données du tunnel VPN, comme les configurations de **l'interface source**, du **type VPN**, **IKEv1** et **IKEv2** pour chaque ligne, et assurez-vous de fournir les valeurs des clés prépartagées pour toutes les lignes.

Étape 6 À la section **Remote Access VPN** [VPN à accès à distance], tous les objets correspondants au VPN à l'accès à distance sont migrés du pare-feu Palo Alto Networks vers le centre de gestion, et sont affichés ainsi :

- **Affectation des politiques** : Passez en revue vos profils de connexion et validez vos connexions, les protocoles VPN, les appareils ciblés, et le nom des interfaces VPN. Pour renommer un profil de connexion, sélectionnez l'entrée correspondante, puis choisissez **Actions [actions]** > **Rename**[renommer].
- **IKEV2** : Passez en revue et validez vos configurations du protocole IKEv2, le cas échéant, ainsi que les interfaces sources qui leur sont associées.
- **Paquets Anyconnect** – Récupérez les paquets AnyConnect et les profils AnyConnect à partir de l'appareil source pour la migration.

  Dans le cadre de l'activité préparatoire à la migration, chargez tous les paquets AnyConnect dans le centre de gestion. Vous pouvez charger les profils AnyConnect soit dans le centre de gestion directement, soit à partir de l'outil de migration Cisco Secure Firewall.

  Sélectionnez les paquets déjà existants AnyConnect ou Hostscan ou ceux du navigateur externe récupérés à partir du centre de gestion. Vous devez sélectionner au moins un paquet AnyConnect. Vous devez également

sélectionner Hostscan, dap.xml, data.xml ou le navigateur externe, si ceux-ci sont disponibles dans la configuration source. Les profils AnyConnect sont facultatifs.

Assurez-vous que le bon fichier Dap.xml est récupéré à partir du pare-feu source. Les validations sont effectuées sur le fichier dap.xml figurant dans le fichier de configuration. Vous devez sélectionner et charger tous les fichiers nécessaires pour la validation. Si la mise à jour n'est pas effectuée, elle sera indiquée comme incomplète, et l'outil de migration Cisco Secure Firewall ne procédera pas à la validation.

- **Ensemble d'adresses** — Passez en revue toutes les adresses IPv4 et IPv6 affichées ici.
- **Stratégies de groupe** — Sélectionnez ou supprimez le profil de l'utilisateur, le profil de gestion, et le profil du module client de cette zone, affichant les stratégies de groupe assorties de profils client, de profils de gestion et de modules client, ainsi que les stratégies de groupe sans profil. Si un profil a été ajouté dans la zone du fichier AnyConnect, il est affiché comme présélectionné. Vous pouvez choisir ou enlever le profil d'utilisateur, le profil de gestion et le profil de module de client.
- **Profil de connexion** – Passez en revue tous les profils de connexions et les groupes de tunnels qui sont affichés ici.
- **Points de confiance** – La migration des points de confiance ou des objets PKI du pare-feu PAN vers le centre de gestion fait partie de l'activité préalable à la migration et est nécessaire à la réussite de la migration du VPN avec accès à distance. Mappez le point de confiance pour Global SSL, IKEv2 et les interfaces dans la section **Remote Access Interface** [interface d'accès à distance] pour aller de l'avant avec la migration.

  Si un objet SAML (Security Assertion Markup Language) existe, les points de confiance pour SAML IDP et SP peuvent être mappés dans la section SAML. Le chargement du certificat SP est facultatif. Les points de confiance peuvent également être modifiés pour un groupe de tunnels donné. Si la configuration du point de confiance SAML remplacé figure dans l' ou le source, elle peut être sélectionnée dans l'option **Override SAML** [remplacer SAML].

Étape 7 (Facultatif) Pour télécharger les détails pour chaque élément de configuration dans la grille, cliquez sur **Télécharger**.

Étape 8 Après avoir complété votre examen, cliquez sur **Valider**. Prenez note que les champs obligatoires qui requièrent votre attention clignoteront jusqu'à ce que vous les remplissiez. Vous pourrez cliquer sur le bouton **Validate** [valider] seulement après que vous aurez rempli tous les champs obligatoires.

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

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

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

Étape 9 Lorsque la validation est terminée, si la boîte de dialogue **Statut de la validation** montre un ou plusieurs conflits d'objets, faites ce qui suit :

a) Cliquez sur **Résoudre les conflits**

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

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

c) Vérifiez l'entrée pour chaque objet qui présente un conflit et sélectionnez **Actions** > **Résoudre les conflits**.
d) Dans la fenêtre **Résoudre les conflits**, complétez l'action recommandée.

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

e) Cliquez sur **Résoudre**
f) Lorsque vous avez résolu tous les conflits d'objet sur un onglet, cliquez sur **Sauvegarder**
g) Cliquez sur **Valider** pour revalider la confirmation et confirmer que vous avez résolu tous les conflits d'objet.

Étape 10 Lorsque la validation est terminée et que la boîte de dialogue **Statut de la validation** affiche le message **Validé avec succès**, continuez avec Transférer la configuration migrée vers Centre de gestion , à la page 41

Transférer la configuration migrée vers Centre de gestion

Vous ne pouvez pas pousser la configuration de migré avec un 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 à centre de gestion.

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

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

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

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

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

Assistance à l'échec de migration

Si votre migration a échoué, contactez le soutien technique.

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

   La page de soutien technique apparaît.

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

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

3. Cliquez sur **Télécharger**.

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

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

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

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

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

Examiner le rapport de post-migration et terminer la migration

Le rapport de post-migration fournit des détails sur le nombre d'ACL dans différentes catégories, l'optimisation des ACL et la vue d'ensemble de l'optimisation effectuée sur le fichier de configuration. Pour plus de renseignements, consultez Optimiser, examiner Examiner et valider la configuration, à la page 36

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 a été migrée :

- **Résumé de la migration** - Résumé de la configuration qui a été migrée avec succès de de vers Défense contre les menaces, y compris des informations sur , centre de gestion le nom d'hôte et le domaine, le dispositif Défense contre les menaces cible (le cas échéant) et les éléments de configuration qui ont été migrés avec succès.

- **Migration sélective des règles** : les détails de la fonction spécifique de de sélectionné pour la migration sont disponibles dans trois catégories : Fonctions de configuration du dispositif, Fonctions de configuration partagées et Optimisation.
- **Mappage de l'interface de du dispositif géré par vers l'interface de défense contre les menaces** - Détails des interfaces migrées avec succès et de la manière dont vous avez mappé les l'ASA du 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 des interfaces sources vers les zones de sécurité de la défense contre les menaces** - Détails des interfaces logiques migrées PAN avec succès et de leur nom, ainsi que de la façon dont vous les avez mappées vers les zones de sécurité 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 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 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 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 qui ont été étendues d'une seule règle de point 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 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 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' 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 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 desque 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 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

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 .

Analysez le résumé

Le résumé de l’analyse indique le nombre d’objets, les interfaces, la NAT, la politique et l’application. Le résumé comporte trois composants : le résumé préanalyse, le résumé de l’analyse et le résumé prétransmission.

- **Résumé préanalyse** : S’affiche après le chargement de la configuration. À ce stade, l’outil de migration Cisco Secure Firewall affiche le nombre des divers composants. Seules les applications personnalisées ou celles utilisées dans le groupe s’affichent. Si une configuration est multi-vsys, le nombre d’interfaces sera affiché pour le *vsys* au complet. Le résumé préanalyse n’affiche pas toutes les applications, car l’application qui est appelée directement dans la politique n’est pas prise en compte. Par conséquent, le nombre d’applications est différent de celui du résumé de l’analyse. Un comportement semblable est applicable à la NAT. Peu de composants du résumé préanalyse peuvent afficher un compte de zéro, mais cela ne signifie pas que les configurations n’ont aucun élément de configuration.
- **Résumé de l’analyse** : S’affiche après avoir cliqué sur l’option du lancement de la conversion. À ce stade, l’outil de migration Cisco Secure Firewall a agi sur la configuration, et toutes les configurations qui ne sont pas prises en charge sont supprimées du compte du résumé. Les politiques qui ne sont pas prises en charge font partie du compte, car elles sont migrées vers centre de gestion comme désactivées. Chaque composant de la configuration est analysé. Le nombre figurant dans le résumé de l’analyse est le nombre exact de configurations à être migrées.
- **Résumé prétransmission** : S’affiche avant que vous soyez invité à transmettre la configuration vers le centre de gestion. Le nombre du résumé préanalyse peut être différent de celui du résumé de l’analyse, conformément à l’action entreprise par l’outil de migration Cisco Secure Firewall. Les adresses IP référencées directement dans la NAT seront transmises en tant qu’objets. Si les applications sont mappées aux ports, le nombre de services augmente et l’application tombera en panne. Si le mappage des applications est laissé vide, le nombre d’applications diminue. Si la route statique comprend une entrée en double, celle-ci sera supprimée et le nombre diminuera.

Échecs de la migration

Voici les échecs de l’analyse qui surviennent pendant la migration :

- **Échec de l'analyse** : Se produit après le chargement de la configuration dans l'outil de migration Cisco Secure Firewall. En raison d'une mauvaise configuration de l'interface. Si plusieurs adresses IP sont configurées ou si une adresse IP /32 ou /128 est attribuée à l'interface, l'analyse échoue.

  Si plusieurs adresses IP sont attribuées à une interface ou si une interface en tunnel, boucle avec retour ou VLAN fait partie du routage, la transmission échoue.

  Solution de contournement : Téléchargez le **rapport prémigration** et consultez la section sur les **lignes de configuration contenant des erreurs** du rapport de migration. Cette section présente les détails de la configuration qui est à l'origine du problème. Vous devez corriger la situation et charger de nouveau la configuration dans l'outil de migration Cisco Secure Firewall.

  Si l'échec de la transmission est causé par une interface tunnel, boucle avec retour ou VLAN dans les routes, vous devez supprimer ces routes et retenter la migration, car ces interfaces ne sont pas prises en charge par centre de gestion.

- **Échec de la transmission** : Se produit lorsque l'outil de migration Cisco Secure Firewall a migré la configuration et lorsque la transmission est en cours vers centre de gestion. Ce type d'échecs est consigné dans le **rapport postmigration**.

  Solution de contournement : Téléchargez le **rapport postmigration** et consultez la section sur les **erreurs** du rapport de migration. Cette section présente les détails de la configuration qui est à l'origine du problème. Vous devez corriger le problème à la page **Review and Validation** [examen et validation] en choisissant l'option **Do not migrate** [ne pas migrer] dans la section où est indiqué l'échec. Vous pouvez aussi résoudre le problème dans la configuration source et charger de nouveau la configuration dans l'outil de migration Cisco Secure Firewall.

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 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 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 2 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 3 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 21.

Étape 4 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 26.

Étape 5 Mappez les ASA les interfaces avec les interfaces Défense contre les menaces.

Remarque L'outil de migration Secure Firewall vous permet de mapper un d'interface au type Défense contre les menacesd'interface.

Pour plus d'informations, voir Mappez les configurations de de PAN du pare-feu avec les interfaces de Défense contre les menaces..

Étape 6 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 aux zones de sécurité.

Pour plus d'informations, voir Associez les interfaces PAN à des périmètres de sécurité, à groupes d’interfaces ..

Étape 7 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 8 Examinez le rapport post-migration, installez manuellement et déployez les autres configurations vers le Défense contre les menaces et complétez la migration.

Pour plus de renseignements, consultez la section .

Étape 9 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 47.

Étape 1 Effacez le cache du protocole de résolution d'adresses (ARP) sur l'infrastructure de commutation environnante

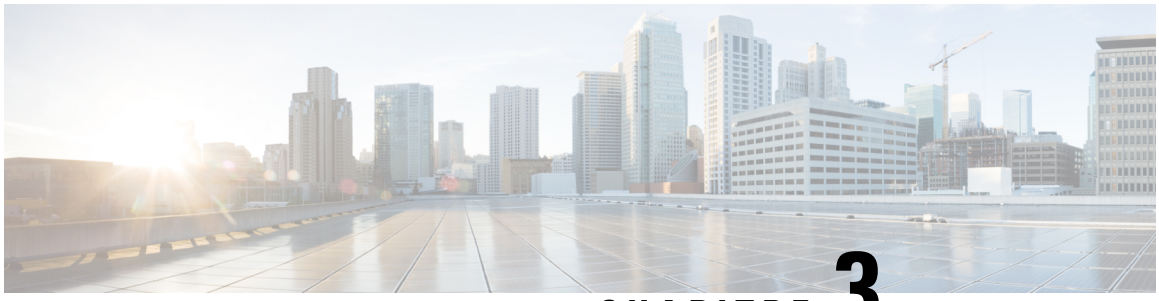
Étape 2 Effectuez des tests ping de base depuis l'infrastructure de commutation environnante jusqu'aux adresses IP de l'interface de l'appareil Série Firepower 2100, afin de vous assurer qu'elles sont accessibles.

Étape 3 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 4 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 , 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 5 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 migrée avec FPS vers centre de gestion, le service de transfert lit le fichier de données de télémétrie à partir de l'emplacement et le supprime une fois les données téléchargées avec succès dans le nuage.

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

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

Tableau 3 : 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

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 4 : Télémétrie étendue

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

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

Point de données	Description	Exemple de valeur
Version de gestion des cibles	La version cible de centre de gestion	6.2.3.3 (build 76)
Type de gestion cible	Le type de périphérique de gestion cible, à savoir, centre de gestion	Centre de gestion
Version du périphérique cible	La version du périphérique cible	75
Modèle de l'appareil cible	Le modèle du périphérique cible	Cisco Secure Firewall Threat Defense pour VMware
Version de l'outil de migration	La version de la migration aussi1	1.1.0.1912

Tableau 6 : Résumé de la migration

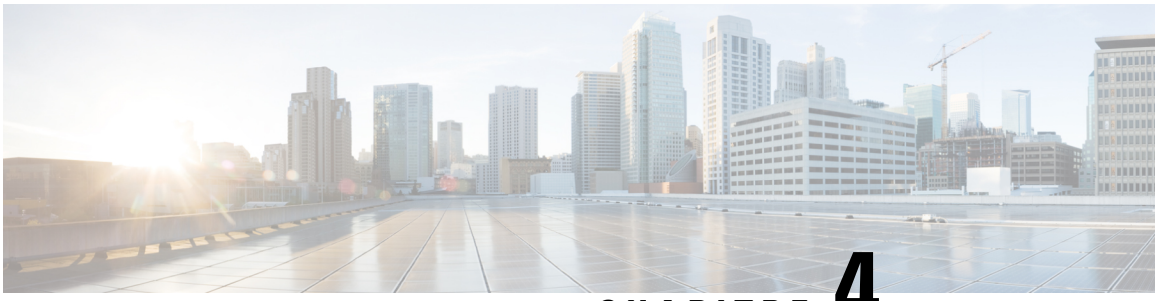
Point de données	Description	Exemple de valeur
Stratégie de contrôle d'accès		

Point de données	Description	Exemple de valeur
Nom	Le nom de la stratégie de contrôle d'accès	N'existe pas
Nombre de règles d'accès	Le nombre total de règles d'ACL migrées	0
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
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 (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

Point de données	Description	Exemple de valeur
État de la migration	L'état de la migration de la configuration vers centre de gestion	SUCCÈS
Message d'erreur	Le message d'erreur affiché par l'outil de migration de pare-feu sécurisé	null (nul)
Description de l'erreur	La description de l'étape où l'erreur s'est produite et la cause première possible	null (nul)



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 PAN ou lors du transfert de la configuration migrée verscentre de gestion.

Fichier inattendu : fichiers non valides détectés pour le PAN. Par exemple, lors de la compression à l'aide de Mac OS, les fichiers système Mac sont créés. Supprimez les fichiers Mac.

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
telemetry_sessionid_timestamp.json	<migration_tool_folder>\resources\telemetry_data

Exemple de résolution de problèmes pour PAN : Impossible de trouver le membre du groupe d'objets

Dans cet exemple, le chargement et l'analyse du fichier de configuration PAN ont échoué en raison d'une erreur dans la configuration d'un élément.

Étape 1 Consultez les messages d'erreur pour identifier le problème.

Cet échec a généré les messages d'erreur suivants :

Emplacement	Message d'erreur
Message de l'outil de migration Cisco Secure Firewall	Les fichiers de configuration Check Point ont été analysés et comportent des erreurs.
Fichier de journalisation	[ERROR | objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;" [INFO | objectGroupRules] > "Parsing object-group service:[services_gvxs06]" [INFO | objectGroupRules] > "Parsing object-group service:[services_iphigenia]" [INFO | objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

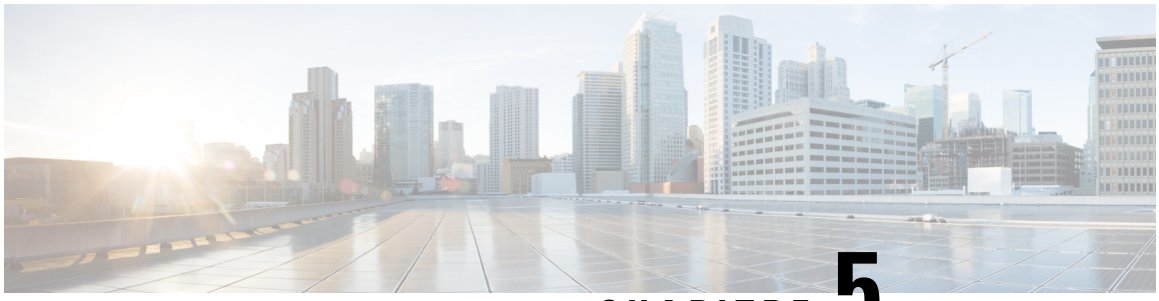
Étape 2 Ouvrez le fichier PAN `services.xml`.

Étape 3 Cherchez le groupe d'objets dont le nom est services_gvxs06.

Étape 4 Créez le membre manquant pour le groupe d'objets au moyen du tableau de bord intelligent.

Étape 5 Exporter de nouveau le fichier de configuration. Pour obtenir plus de renseignements, consultez .

Étape 6 S'il n'y a plus d'erreurs, chargez le nouveau fichier de configuration PAN compressé dans l'outil de migration Cisco Secure Firewall pour poursuivre la migration.



CHAPITRE 5

FAQ de l'outil de migration Secure Firewall

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

Q. Quelles sont les nouvelles fonctionnalités prises en charge sur l'outil de migration Secure Firewall pour la version 3.0.1?

A. L'outil de migration Cisco Secure Firewall 3.0.1 prend désormais en charge Cisco Secure Firewall 3100 uniquement en tant qu'appareil de destination pour les migrations à partir de Palo Alto Networks.

Q. Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration de pare-feu sécurisé pour la version 3.0 ?

A. Les caractéristiques suivantes sont prises en charge avec la version 3.0 :

- Migration vers le Centre de gestion du pare-feu en nuage.

Q. Quelles sont les plateformes source et cible qu'utilise l'outil de migration Cisco Secure Firewall pour la migration de la politique?

A. L'outil de migration Cisco Secure Firewall peut migrer les politiques de la plateforme du pare-feu PAN prise en charge vers la plateforme défense contre les menaces virtuelles. Pour en savoir plus, consultez Plateformes prises en charge pour la migration [plateformes PAN sources prises en charge].

Q. Quelles sont les limites matérielles pour la conversion de PAN en Threat Defense Virtual?

A. L'outil de migration Cisco Secure Firewall migrera la configuration si la version du système d'exploitation PAN est 6.1.x ou ultérieure.

Q. Le pare-feu PAN prend-il en charge les groupes d'interfaces?

A. Non. Le pare-feu PAN ne prend pas en charge les groupes d'interfaces pour la conversion en défense contre les menaces virtuelles.

Q. La NAT utilise le FQDN qui n'est pas pris en charge par Centre de gestion. Que dois-je faire?

A. Tout comme le FQDN dans la NAT qui n'est pas pris en charge par centre de gestion, dans la ligne semblable, le FQDN n'est pas pris en charge par l'outil de migration Cisco Secure Firewall. Pour

reproduire la même configuration que la source, vous devez configurer l'ensemble complet des adresses IP qui sont mappées manuellement avec le FQDN après la migration.

Q. Que faire si le pare-feu source a un plus grand nombre d'interfaces que la cible?
A. Si le pare-feu source a plus d'interfaces que la cible, créez alors des sous-interfaces sur défense contre les menaces virtuelles avant de lancer la migration.

Q. L'outil de migration de Cisco Secure Firewall migrera-t-il les interfaces agrégées (canaux de port)?
A. L'outil de migration de Cisco Secure Firewall ne migrera pas les interfaces agrégées (canaux de port). Vous devez configurer l'interface du canal de port sur centre de gestion avant de lancer la migration.

Q. Le routage Inter VR est-il pris en charge par Centre de gestion?
A. Toute route qui a Next Hop [saut suivant] en tant que route Next VR [VR suivante] n'est pas prise en charge.
Q. Quelle est la commande pour extraire le tableau des routes du PAN?
A. Utilisez la commande **Show routing route** [afficher la route de routage]. Une fois que vous avez collé la route dans le fichier *.txt*, assurez-vous que la mise en forme est correcte. En cas de systèmes multi-vsys, collez uniquement la route pour le *vsys* pertinent. Nous vous recommandons de supprimer les routes de tunnel, de boucle avec retour et VLAN du tableau des routes, car ces interfaces ne sont pas prises en charge par centre de gestion.
Q. Que devrais-je faire des fichiers de la configuration ignorée?
A. La configuration ignorée contient des balises XML qui sont propres à PAN seulement et qui ne sont pas pertinentes pour centre de gestion. Par conséquent, elles sont ignorées. Vous devez examiner attentivement la configuration ignorée. Les éléments imprévus qui sont indiqués dans la section ignorée devraient être configurés manuellement sur centre de gestion.
Q. J'obtiens un message d'erreur dans le rapport prémigration. Puis-je ignorer les interfaces et continuer?
A. Si vous choisissez de continuer sans les interfaces, les routes ne seront pas non plus migrées.
Q. Quelle est la cause courante de l'échec de l'analyse?
A. L'échec de l'analyse se produit si les interfaces ont plusieurs adresses IP ou des adresses IP attribuées à des sous-réseaux, par exemple /32 ou /128. Pour continuer, vous devez corriger l'adresse IP et relancer la migration.
Q. Pourquoi la NAT dans le résumé de préanalyse correspond-elle à zéro?
A. Consultez la section Analysez le résumé [analyse du résumé] pour en savoir plus.

Q. Comment peut-on exporter la configuration PAN?
A. La configuration doit être extraite de la passerelle si votre appareil est géré par Panorama. Il suffit de fusionner la configuration de Panorama avec la passerelle et d'extraire la configuration.

Pour en savoir plus, consultez la section Fichier de configuration du pare-feu Palo Alto (pas géré par Panorama) [exporter la configuration du pare-feu de Palo Alto Networks].

Q. En quoi le mappage d'applications consiste-t-il?
A. Le mappage d'applications vous permet de mapper des applications aux applications cibles correspondantes, comme HTTP ou SSH. Vous pouvez également migrer les règles basées sur l'application.

Pour en savoir plus, consultez la section Map Configurations with Applications [mapper des configurations avec les applications].

Q. Qu'advient-il des politiques affichant « application-default »?
A. Procédez comme suit:

- Si l'application est sélectionnée comme « any » et que le port est réglé sur « application-default », la politique n'est pas prise en charge et est migrée comme désactivée.

- Si l'application est sélectionnée comme « xyz » et que le port est réglé sur « application-default », la politique est migrée avec l'application « xyz » et le service « any ».

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.