Notes de mise à jour de l'outil de migration Cisco Secure Firewall

Première publication : 2023-03-14

Dernière modification : 2023-06-14

À propos de l'outil de migration Cisco Secure Firewall

L'outil de migration Cisco Secure Firewall vous permet de migrer vos configurations de pare-feu vers un Cisco Secure Firewall Threat Defense pris en charge géré par un centre de gestion. L'outil de migration prend en charge la migration à partir de Secure Firewall ASA, ASA avec FirePOWER Services (FPS), des périphériques gérés par FDM, ainsi que des pare-feu tiers de Check Point, de Palo Alto Networks et de Fortinet.

Ce document fournit des renseignements essentiels et spécifiques sur les versions de l'outil de migration Cisco Secure Firewall. Même si vous êtes familiarisé avec les versions de Cisco Secure Firewall et que vous avez de l'expérience avec le processus de migration, nous vous recommandons de lire et de comprendre parfaitement ce document.

Nouvelles fonctionnalités

Versions	Nouvelles fonctionnalités
4.0.3	Cette version comprend des corrections de bogues et les nouvelles améliorations suivantes : **Migration de pare-feu avec l'outil de migration Cisco Secure Firewall dans Cisco Defense Orchestrator** Cisco Defense Orchestrator (CDO) est un gestionnaire multipériphérique basé sur le nuage qui facilite la gestion des politiques de sécurité dans les environnements hautement distribués. CDO héberge désormais une version en nuage du Outil de migration Cisco Secure Firewall. Pour en savoir plus sur l'utilisation de l'outil de migration dans CDO, consultez Migration de pare-feu avec l'outil de migration de pare-feu dans Cisco Defense Orchestrator. **Migration du pare-feu de Palo Alto Networks vers Threat Defense** • L'outil de migration Cisco Secure Firewall 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.

Versions	Nouvelles fonctionnalités
4.0.2	Cette version comprend les améliorations et fonctionnalités suivantes : **Migration Cisco ASA vers Threat Defense** • Outil de migration Cisco Secure Firewall prend désormais en charge la migration des configurations de filtre VPN de site à site et les objets de la liste d'accès étendu se rapportant à ces configurations lorsque le centre de gestion de destination et les versions de défense contre les menaces sont 7.1 ou ultérieures. Auparavant, les configurations de filtre VPN de site à site n'étaient pas migrées et devaient être configurées manuellement après la migration. **Migration du pare-feu de Palo Alto Networks vers Threat Defense** • 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. • 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. **Migration du pare-feu Check Point vers Threat Defense** • Outil de migration Cisco Secure Firewall La version 4.0.2 présente l'outil d'extraction de configuration intégré, qui s'affiche désormais sur la page **Extract Config Information (Extraire les informations de configuration)**. Cela facilite l'extraction de la configuration et élimine la tâche de téléchargement de l'outil d'extraction. Notez que l'outil FMT-CP-Config-Extractor n'est plus disponible en tant qu'application autonome à télécharger. Consultez la section Exporter la configuration du périphérique à l'aide de l'extracteur de configuration pour plus de renseignements. **Amélioration de Cisco Success Network (Réseau de succès Cisco)** • 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 **Paramètres** > **Envoyer les données de télémétrie à Cisco?** .

Pour plus de renseignements sur l'historique de l'outil de migration Secure Firewall, consultez :

- Historique de l'outil de migration de pare-feu ASA

- Historique du pare-feu ASA avec FirePOWER Services vers Threat Defense avec l'outil de migration de pare-feu
- Historique de l'outil de migration de pare-feu Check Point
- Historique de l'outil de migration de pare-feu de Palo Alto Networks
- Historique de l'outil de migration de pare-feu Fortinet
- Historique de l'outil de migration de périphérique géré par FDM

Configurations prises en charge

Les éléments de configuration suivants sont pris en charge pour la migration :

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

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

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

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

- Objets et groupes FQDN IPv4 et IPv6
- Prise en charge de la conversion IPv6 (interface, routes statiques, objets, ACL et NAT)
- Règles d'accès appliquées aux interfaces dans la direction entrante et ACL globales
- NAT automatique, NAT manuel et NAT d'objet (conditionnel)
- Routes statiques, routes ECMP et PBR
- Interfaces physiques
- Les VLAN secondaires sur ASA ou ASA avec des interfaces de services FirePOWER ne migreront pas vers Défense contre les menance.
- Sous-interfaces (l'ID de sous-interface sera toujours défini sur le même numéro que l'ID de VLAN lors de la migration)
- Canaux de port
- Virtual tunnel interface (VTI)
- Groupes de ponts (mode transparent uniquement)

- IP SLA Monitor

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

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

- Recherche groupée d'objets

Remarque

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

- Objets temporels

Remarque

- Vous devez faire migrer manuellement la configuration de fuseau horaire de l'ASA source, de l'ASA avec les services FirePOWER et du périphérique géré par FDM vers la cibleDéfense contre les menance.
- L'objet temporel n'est pas pris en charge pour les non-Défense contre les menanceflux et sera désactivé.
- Les objets temporels sont pris en charge sur les centre de gestionversions 6.6 et ultérieures.

- Tunnels de réseau privé virtuel (VPN) de site à site
  - VPN de site à site : lorsque l'outil de migration Cisco Secure Firewall détecte la configuration de la carte de chiffrement dans l'ASA source et le périphérique géré par FDM, l'outil de migration Cisco Secure Firewall migre la carte de chiffrement vers le VPN en tant que topologie point à point.centre de gestion
  - VPN basé sur une carte de chiffrement (statique/dynamique) à partir d'un périphérique géré par ASA et FDM.
  - VPN ASA et FDM basé sur les routes (VTI)
  - Migration VPN basée sur certificat à partir d'un appareil géré par ASA et FDM.
  - La migration des certificats ou des points de confiance des périphériques gérés par ASA et FDM vers centre de gestiondoit être effectuée manuellement et fait partie de l'activité de prémigration.
- Objets de routage dynamique, BGP et EIGRP
  - Liste de politiques

- Liste des préfixes
- Liste des communautés
- Chemin du système autonome (AS)
- Route-Carte

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

- Optimisation ACL

  L’optimisation ACL prend en charge 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.
  - ACL dupliquée : la première ACL masque complètement les configurations de la deuxième ACL.

Remarque L’optimisation d’ACL n’est actuellement pas disponible pour Palo Alto Networks et ASA avec FirePower Services (FPS).

Pour des renseignements sur les configurations prises en charge de l’outil de migration Cisco Secure Firewall, consultez :

- Configurations ASA prises en charge
- ASA pris en charge avec les configurations de services FirePOWER
- Configurations de Check Point prises en charge
- Configurations de PAN prises en charge
- Configuration Fortinet prise en charge
- Configuration des dispositifs gérés par FDM pris en charge

Processus de migration

Pour plus de renseignements sur le processus de migration de l'outil de migration Cisco Secure Firewall, consultez :

- Exporter le fichier de configuration ASA
- Exporter l'ASA avec le fichier de configuration des services FirePOWER
- Exporter les fichiers de configuration de Check Point
- Exporter la configuration du pare-feu de Palo Alto Networks
- Exporter la configuration du pare-feu Fortinet
- Exporter le fichier de configuration du périphérique géré par FDM

Rapports sur la migration

L'outil de migration Cisco Secure Firewall fournit les rapports suivants au format HTML avec les détails de la migration :

- Rapport préalable à la migration
- Rapport après la migration

Fonctionnalités de l'outil de migration Cisco Secure Firewall

L'outil de migration Cisco Secure Firewall offre les fonctionnalités suivantes :

- Validation tout au long de la migration, y compris les opérations d'analyse et de poussée
- Possibilité de réutilisation des objets
- Résolution des conflits d'objets
- Mappage d'interface
- Vérification des limites de la sous-interface pour le dispositif de défense contre les menaces cible
- Plateformes prises en charge :

-
- FDM virtuel vers Threat Defense Virtual
- Migration du même matériel (migration de périphérique X vers X)
- Migration de périphérique de X vers Y (Y ayant un plus grand nombre d'interfaces)

- Optimisation des ACL pour l'ASA source, le dispositif géré par FDM, Fortinet et Checkpoint pour l'action de la règle ACP.

Exigences en matière d'infrastructure et de plateforme

L'outil de migration Cisco Secure Firewall nécessite l'infrastructure et la plateforme suivantes :

- Système d'exploitation Windows 10 64-bits ou sur une version macOS 10.13 ou plus récente
- Google Chrome comme navigateur par défaut du système

Astuces Nous vous recommandons d'utiliser le mode plein écran dans le navigateur lorsque vous utilisez l'outil de migration.

- Une seule instance de l'outil de migration Cisco Secure Firewall par système
- Management Center et Threat Defense doivent être en version 6.2.3.3 ou plus récente

Remarque Supprimez la version précédente avant de télécharger la nouvelle version.

Problèmes ouverts et résolus

Problèmes ouverts

ID du bogue	Description
CSCwf27912	ASA – La logique est requise pour le mappage du groupe d'interfaces
CSCwf23756	ASA – Le nom logique correspondant génère une erreur `d'entrée en double`
CSCwf39186	ASA avec FPS – Erreur lors de l'analyse de la configuration ASA avec FPS pour ACL

Problèmes résolus

ID du bogue	Description
CSCwf17219	PAN – Erreur de page qui ne répond pas sur la page de mappage de l'application
CSCwf17180	PAN – L'application cible n'est pas en mesure de conserver son état précédent sous un mappage valide
CSCwf17175	ASA : le bouton Valider apparaît même lorsque des conflits sont détectés
CSCwf17148	PAN – Le bouton de sélection ne doit pas apparaître dans le menu déroulant en tant qu'application cible.
CSCwf17146	ASA – Un espace supplémentaire apparaît dans les vignettes des objets de la liste d'accès pour les filtres VPN
CSCwf13810	ASA - RAVPN DAP est migré sans ACL réseau à mapper
CSCwf12370	ASA – Le lien **Aide supplémentaire** de RAVPN est rompu
CSCwf09361	ASA – Les politiques d'accès dynamiques ne sont pas migrées d'ASA 9.12 vers FTD 7.0.4
CSCwe82642	Optimisation ACL lance `un littéral non valide pour int () avec base 10 : erreur « 8/0 »` lors de la collecte des informations d'ACL
CSCvt48216	PAN - Translated-Destination-Range-Group n'est pas créé
CSCwf23748	ASA – Les listes de contrôle d'accès (ACL) élargies ne sont pas migrées vers Cisco Secure Firewall Management Center
CSCwf23756	ASA – Traitement des `entrées en double pour la validation des erreurs de nom logiques` correspondants
CSCwf23734	Les noms de domaine complets ne sont pas pris en charge lors de la saisie des informations de connexion au FMC
CSCwf23771	ASA : l'option permettant d'annuler la reprise de la migration et de démarrer une nouvelle migration n'est pas disponible
CSCwf24988	ASA - Les messages d'erreur affichés lors de la validation ne sont pas très intuitifs
CSCwf27907	ASA - La valeur de l'objet n'est pas vérifiée `/`

Mises en garde ouvertes et résolues

Les mises en garde ouvertes pour cette version sont accessibles via l'outil de recherche de bogues de Cisco. Cet outil Web vous permet d'accéder au système de suivi des bogues de Cisco, qui conserve les informations sur les bogues et les vulnérabilités de ce produit et d'autres produits matériels et logiciels de Cisco.

Remarque Vous devez avoir un compte Cisco.com pour vous connecter et accéder à l'outil de recherche de bogues de Cisco. Si vous n'en avez pas, vous pouvez créer un compte sur Cisco.com. Pour plus d'informations sur l'outil de recherche de bogues, consultez l'aide de l'outil de recherche de bogues.

Utilisez la requête dynamique des Mises en garde ouverts et résolus pour obtenir une liste à jour des avertissements ouverts et résolus dans l'outil de migration Cisco Secure Firewall.

Documentation associée

- Migration de pare-feu ASA vers Firewall Threat Defense avec l'outil de migration Cisco Secure Firewall
- Migration de pare-feu ASA avec les services FirePOWER vers Firewall Threat Defense avec l'outil de migration de Cisco Secure Firewall
- Mise en correspondance des fonctionnalités de Cisco Secure Firewall ASA et Threat Defense
- Migration d'un dispositif géré par FDM vers Secure Firewall Threat Defense avec l'outil de migration
- Migration de Check Point Firewall vers Firewall Threat Defense avec l'outil de migration Cisco Secure Firewall
- Migration de Palo Alto Networks Firewall vers Firewall Threat Defense avec l'outil de migration Cisco Firewall Threat Defense
- Migration de Fortinet Firewall vers Firewall Threat Defense avec l'outil de migration Cisco Secure Firewall
- Migration d'une ASA vers un dispositif géré par FDM à l'aide de Cisco Defense Orchestrator
- Navigation dans la documentation de l'outil de migration Cisco Secure Firewall
- Guide de compatibilité de l'outil de migration Cisco Secure Firewall
- Messages d'erreur de l'outil de migration Cisco Secure Firewall
- Open Source utilisée dans l'outil de migration Cisco Secure Firewall

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

Les adresses IP (Internet Protocol) et les numéros de téléphone utilisés dans ce document ne sont pas censés correspondre à des adresses ni à des numéros de téléphone réels. Tous les exemples, résultats d'affichage de commandes, schémas de topologie de réseau et autres illustrations inclus dans ce document sont donnés à titre indicatif uniquement. L'utilisation d'adresses IP ou de numéros de téléphone réels à titre d'exemple est non intentionnelle et fortuite.

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.