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

- Les éléments de configuration Fortinet qui sont entièrement migrés, partiellement migrés, non pris en charge pour la migration et ignorés pour la migration.
- Les lignes de configuration Fortinet avec erreurs, qui répertorie les CLI Fortinet que l'outil de migration Secure Firewall ne peut pas reconnaître, ce qui bloque la migration.

S'il y a des erreurs d'analyse, vous pouvez 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 Fortinet, et les consigne dans le dossier des **ressources**.

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

Fichier non analysé

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

<migration_tool_folder>\resources

Recherche dans l'outil de migration Secure Firewall

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

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

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

Ports

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

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

Cisco Success Network (Réseau de succès Cisco)

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

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

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

Quoi de neuf dans l'outil de migration Secure Firewall

Version	Fonctionnalités prises en charge
6.0	

Version	Fonctionnalités prises en charge
	Cette version comprend les nouvelles caractéristiques et améliorations suivantes : **Migration de Cisco Secure Firewall ASA vers Cisco Secure Firewall Threat Defense** • Vous pouvez maintenant migrer des configurations WebVPN de votre Cisco Secure Firewall ASA vers les configurations de Cisco Zero Trust Access Policy sur un appareil de protection contre les menaces. Cochez bien la case **WebVPN** à la page **Select Features** [sélectionner les fonctions] et jetez un œil au nouvel onglet **WebVPN** à la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration]. L'appareil de protection contre les menaces et le centre de gestion cible doit fonctionner sur la version 7.4 ou une version ultérieure et doit exécuter Snort3 comme moteur de détection. • Vous pouvez désormais procéder à la migration des configurations des protocoles SNMP (Simple Network Management Protocol) et DHCP (Dynamic Host Configuration Protocol) vers un appareil de protection contre les menaces. Cochez bien les cases **SNMP** et **DHCP** à la page **Select Features** [sélectionner les fonctions]. Si vous avez configuré le protocole DHCP sur Cisco Secure Firewall ASA, notez que le serveur DHCP, ou l'agent de relais et les configurations du système DDNS, peuvent également être sélectionnés pour la migration. • Vous pouvez désormais migrer les 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, examiner 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 mapper 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 migrer les politiques de sécurité de couche 7, y compris les protocoles SNMP et HTTP, ainsi que les configurations des politiques sur les programmes malveillants et les fichiers de votre appareil géré par FDM vers un appareil de protection contre les menaces. Assurez-vous d'avoir un centre de gestion cible de version 7.4 ou ultérieure et vérifiez que les cases des **paramètres de la plateforme** et de la **politique sur les programmes malveillants et les fichiers** à la page **Select Features** [sélectionner les fonctions] sont bien cochées.

Version	Fonctionnalités prises en charge
	Migration du pare-feu Check Point vers Cisco Secure Firewall Threat Defense • Vous pouvez dorénavant effectuer la migration des configurations VPN de site à site (basées sur les politiques) de votre pare-feu Check Point vers un appareil de protection contre les menaces. Notez que cette fonction s'applique aux versions Check Point R80 ou ultérieures, et aux versions 6.7 ou ultérieures du centre de gestion et de la protection contre les menaces. 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 migrez les configurations d'un pare-feu Fortinet à votre appareil de protection contre les menaces. Utilisez le bouton **Optimize ACL** [optimiser l'ACL] à la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration] pour consulter la liste des ACL redondantes et dupliquées et pour télécharger le rapport d'optimisation qui détaille l'ACL.

Version	Fonctionnalités prises en charge
5.0.1	Cette version comprend les nouvelles caractéristiques et améliorations suivantes : • L'outil de migration Cisco Secure Firewall prend maintenant en charge la migration de plusieurs contextes de sécurité transparents en mode pare-feu à partir des appareils Cisco Secure Firewall ASA vers les appareils de protection contre les menaces. Vous pouvez fusionner au moins deux contextes transparents en mode pare-feu qui se trouvent dans votre appareil Cisco Secure Firewall ASA à une instance en mode transparent, et pouvez ensuite procéder 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 migrer les configurations VPN de site à site et VPN à accès à distance à partir de vos pare-feu Fortinet et Palo Alto Networks vers la protection contre les menaces au moyen de l'outil de migration Cisco Secure Firewall. Depuis le panneau **Select Features** [sélectionner les fonctions], choisissez les fonctions VPN à migrer. Consultez la rubrique Specify Destination Parameters for the Secure Firewall Migration Tool [indiquer les paramètres de destination pour l'outil de migration Cisco Secure Firewall] dans les guides Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool [migration du pare-feu Palo Alto Networks vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration] et Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool [migration du pare-feu Fortinet vers Cisco Secure Firewall Threat Defense au moyen de l'outil de migration]. • Vous pouvez désormais sélectionner au moins un contexte de sécurité routé ou transparent en mode pare-feu à partir de vos appareils Cisco Secure Firewall ASA et migrer 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 de migrer les configurations à partir d'un de vos contextes ou de fusionner les configurations de tous vos contextes routés en mode pare-feu et de procéder ensuite 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, qui est observé dans un environnement ASA à plusieurs contextes, lequel fera partie de la nouvelle configuration fusionnée. Vous pouvez vérifier le nombre de contextes qu'a détectés 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 Cisco Secure Firewall] 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 : • 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?**.
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.
3.0	L'outil de migration Secure Firewall 3.0 permet de migrer vers le centre de gestion de pare-feu de Fortinet fourni dans le nuage si le centre de gestion de destination est 7.2 ou plus récent.
2.5.2	L'outil de migration Secure Firewall 2.5.2 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 réseau des pare-feu Fortinet 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. • ACL dupliquée: la première ACL masque complètement les configurations de la deuxième ACL. **Remarque** L'optimisation est disponible pour le Fortinet uniquement pour une action découlant d'une règle ACP. L'outil de migration Secure Firewall 2.5.2 supporte le protocole de passerelle frontière (BGP) et les objets de routage dynamique si la destination centre de gestionest 7.1 ou ultérieure.

Version	Fonctionnalités prises en charge
2,3	• Prend en charge les versions OS des pare-feux Fortinet : 5.0 et ultérieures • L'outil de migration Secure Firewall vous permet de migrer les éléments de configuration Fortinet suivants vers défense contre les menaces : • Interfaces • Zones • Routes statiques • Objets et groupes de réseau • Objets de service et groupes • Listes de contrôle d'accès • Objets dépendant de la NAT (pool d'IP, IP virtuelle) • Règles NAT • VDOM • Objets temporels : lorsque l'outil de migration Secure Firewall détecte des objets temporels référencés par des règles d'accès, il migre les objets temporels et les associe aux règles d'accès correspondantes. Vérifier les objets contre les règles dans la page Examiner et valider la configuration. **Remarque** Les objets temporels sont pris en charge sur les versions 6.6 et ultérieures.centre de gestion

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

Conditions préalables et exigences pour le fichier de configuration du pare-feu Fortinet

Vous pouvez obtenir manuellement un fichier de configuration de pare-feu Fortinet.

Le fichier de configuration du pare-feu Fortinet que vous importez manuellement dans l'outil de migration Cisco Secure Firewall doit remplir les exigences suivantes :

- Possède une configuration en cours d'exécution qui est exportée d'un appareil Fortinet. La sauvegarde de la configuration à partir de l'exportation globale et par VDOM est prise en charge par l'outil de migration du pare-feu. Pour plus d'informations, référez-vous à Exporter le fichier de configuration Fortinet .
- Contient uniquement les configurations CLI valides du pare-feu Fortinet.
- Ne contient pas d'erreurs de syntaxe.
- Possède une extension de fichier de `.cfg` ou `.txt`.
- Utilise un encodage de fichier UTF-8
- N'a pas été codé à la main ou modifié manuellement. Si vous modifiez la configuration du pare-feu Fortinet, nous vous recommandons de tester le fichier de configuration modifié sur l'appareil équipé du pare-feu Fortinet pour vérifier si la configuration est valide.

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 du pare-feu Fortinet 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 du pare-feu Fortinet. Si

vous devez ajouter le type nécessaire de l'interface sur l'appareil cible de protection contre les menaces.

Remarque

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

Soutien pour la configuration de Fortinet

Configurations du pare-feu Fortinet prises en charge

L'outil de migration Cisco Secure Firewall peut totalement migrer les configurations suivantes du pare-feu Fortinet :

- Objets et groupes de réseau, à l'exception du nom de domaine complet (FQDN) générique, du masque générique et des objets dynamiques Fortinet
- 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 et NAT)
- Règles d'accès
- Règles NAT
- Les routes statiques et les routes ECMP non migrées
- Interfaces physiques
- Sous-interfaces (l'ID de sous-interface sera toujours défini sur le même numéro que l'ID de VLAN lors de la migration)
- Agrégation des interfaces (canaux de port)
- L'outil de migration Cisco Secure Firewall prend en charge la migration des VDOM individuellement à partir du pare-feu Fortinet en tant qu'appareils Threat Defense distincts.
- Objets temporels : Lorsque l'outil de migration Cisco Secure Firewall détecte des objets temporels référencés par des règles d'accès, il migre les objets temporels et les associe aux règles d'accès

correspondantes. Vérifiez les objets par rapport aux règles à la page **Optimize, Review and Validate Configuration** [optimiser, examiner et valider la configuration].

Les objets temporels sont des types de listes d'accès qui autorisent l'accès au réseau sur une période donnée. Ces objets sont utiles lorsque vous devez imposer des restrictions au trafic sortant ou entrant en fonction d'une heure particulière de la journée ou de certains jours de la semaine.

Remarque

- Vous devez migrer manuellement la configuration du fuseau horaire du pare-feu Fortinet source vers la protection contre les menaces cible.
- Les objets temporels ne sont pas pris en charge pour les flux qui ne sont pas liés aux menaces. Ces objets seront alors désactivés.
- Les objets temporels sont pris en charge par le centre de gestion cible 6.6 et les versions ultérieures.

Configurations du pare-feu Fortinet prises en charge partiellement

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

- Groupe d'adresses qui contient des objets d'adresse qui ne sont pas pris en charge.
- Groupe de services qui comporte des objets de service avec des protocoles contenant TCP ou UDP et SCTP.

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

Configurations du pare-feu Fortinet non prises en charge

L'outil de migration Cisco Secure Firewall ne prend pas en charge les configurations suivantes du pare-feu Fortinet pour la migration. Si ces configurations sont prises en charge dans le centre de gestion, vous pouvez les configurer manuellement après la migration.

- Règles de la stratégie de contrôle d'accès basées sur l'utilisateur, l'appareil et l'identifiant de service Internet
- Objets de service dont le type et le code ICMP ne sont pas pris en charge
- Règles de contrôle d'accès basées sur le protocole de tunnellisation
- Règles NAT configurées avec l'option d'allocation de bloc
- Règles NAT configurées avec SCTP
- Règles NAT configurées avec l'hôte « 0.0.0.0 »

- Règle NAT avec un objet FQDN dans la source ou la destination
- Objets FQDN qui commencent par un caractère spécial ou qui en contiennent un
- FQDN avec caractère générique
- Fortinet permet la configuration de politiques qui combinent IPv4 et IPv6 (regroupement de politiques).

Remarque Cette politique n’est pas prise en charge par l’outil de migration de Cisco Secure Firewall.

Lignes directrices et limites pour les configurations du pare-feu Fortinet

Pendant la conversion, l’outil de migration Cisco Secure Firewall crée un mappage individuel pour l’ensemble des objets et des règles pris en charge, peu importe 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 Secure Firewall traite les objets et règles non supportés comme suit :

- Les interfaces, les objets, les règles NAT et les routes qui ne sont pas pris en charge ne sont pas migrés.
- Les règles ACL qui ne sont pas prises en charge sont migrées dans le centre de gestion en tant que règles désactivées.

Limites d’une configuration du pare-feu Fortinet

Voici les limites imposées à la migration de la configuration source du pare-feu Fortinet :

- La configuration système n'est pas migrée.
- L’outil de migration Cisco Secure Firewall ne prend pas en charge la migration d’une politique ACL unique qui s’applique à plus de 50 interfaces. Effectuez manuellement la migration des politiques ACL qui sont appliquées à 50 interfaces ou plus.
- Les interfaces du pare-feu Fortinet de type câble virtuel, interface redondante, interface de tunnel, vdom-link et SDwan-interface ou zone ne sont ni prises en charge ni migrées.

  L’interface logique du commutateur matériel ou logiciel Fortinet sera migrée en tant qu’interfaces L3 de la protection contre les menaces. Les interfaces qui sont un membre du commutateur matériel ou logiciel ne seront pas migrées à l’aide de l’outil de migration Cisco Secure Firewall.
- La migration d’objets tels que le nom de domaine complet (FQDN) générique, l’adresse IP générique, les objets dynamiques et les groupes d’exclusion ne sont pas pris en charge.
- Les appareils du pare-feu Fortinet en mode transparent ou le VDOM transparent ne peuvent pas être migrés.

- Les groupes d'objets de service imbriqués et les groupes de ports ne sont pas pris en charge par le centre de gestion. Dans le cadre de la conversion, l'outil de migration 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 pour le centre de gestion dont la signification est exactement la même.

Lignes directrices de la migration du pare-feu Fortinet

L'outil de migration Cisco Secure Firewall utilise les meilleures pratiques pour les configurations de la protection contre les menaces.

La migration de l'option de journalisation de l'ACL suit les meilleures pratiques pour la protection contre les menaces. L'option de journalisation pour une règle est activée ou désactivée selon la configuration du pare-feu Fortinet 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.

Lignes directrices et limites des appareils de protection contre les menaces

Lorsque vous prévoyez de migrer votre configuration vers la protection contre les menaces, tenez compte des lignes directrices et des limites qui suivent :

- S'il existe des configurations propres à l'appareil sur la protection 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.

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

- L'interface logique du commutateur matériel ou logiciel Fortinet sera migrée en tant qu'interfaces L3 de la protection contre les menaces. Les interfaces qui font partie du commutateur matériel ou logiciel ne seront pas migrées à l'aide de l'outil de migration Cisco Secure Firewall.

  Durant la migration, l'outil de migration Secure Firewall réinitialise la configuration de l'interface. Si vous utilisez ces interfaces dans des politiques, l'outil de migration Cisco Secure Firewall ne peut pas les réinitialiser. Or, la migration échoue.

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 18.
- Vous avez obtenu et installé des licences intelligentes défense contre les menacesqui incluent toutes les fonctionnalités que vous prévoyez de migrer depuis ASA Fortinet, 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 le 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 Fortinet prises en charge

L'outil de migration Cisco Secure Firewall prend en charge la migration vers défense contre les menaces la version 5.0 ou ultérieure du système d'exploitation du pare-feu Fortinet et la version plus récente.

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

Pour le pare-feu défense contre les menaces Fortinet , l'outil de migration Cisco Secure Firewall prend en charge la migration vers un périphérique centre de gestion qui exécute la version 6.2.3.3 ou une version récente.

Remarque La migration vers l'appareil défense contre les menaces 6.7 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 menacesavec 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.

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.