Importer/Exporter

Les rubriques suivantes expliquent comment utiliser la fonction d'importation/exportation :

À propos de l'importation et de l'exportation de la configuration

Vous pouvez utiliser la fonction d'importation/exportation pour copier des configurations entre des périphériques. L'importation/exportation n'est pas un outil de sauvegarde, mais peut simplifier le processus d'ajout de nouveaux périphériques à votre déploiement.

Vous pouvez exporter une seule configuration, ou vous pouvez exporter un ensemble de configurations (du même type ou de types différents) en une seule action. Lorsque vous importez ultérieurement le paquet sur un autre appareil, vous pouvez choisir les configurations du paquet à importer.

Un paquet exporté contient des informations de révision pour cette configuration, qui déterminent si vous pouvez importer cette configuration sur un autre appareil. Lorsque les périphériques sont compatibles, mais que l'ensemble comprend une configuration en double, le système propose des options de résolution.

Remarque Les appareils d'importation et d'exportation doivent exécuter la même version du système Firepower. Pour le contrôle d'accès et ses sous-politiques (y compris les politiques de prévention des intrusions), la version de mise à jour de la règle de prévention des intrusions doit également correspondre. Si les versions ne correspondent pas, l'importation échoue. Vous ne pouvez pas utiliser la fonction d'importation/exportation pour mettre à jour les règles de prévention des intrusions. Téléchargez et appliquez plutôt la dernière version de mise à jour des règles.

Configurations qui prennent en charge l'importation et l'exportation

L'importation/exportation est prise en charge pour les configurations suivantes :

- les politiques de contrôle d'accès et les politiques qu'elles utilisent : préfiltre, analyse de réseau, intrusion, SSL, fichier, politique de service de défense contre les menaces

- Politiques de prévention des intrusions, indépendamment du contrôle d'accès
- Politiques NAT (Cisco Secure Firewall Threat Defense uniquement)
- Politiques FlexConfig Cependant, le contenu de toutes les variables de clé secrète est effacé lorsque vous exportez la politique. Vous devez modifier manuellement les valeurs de toutes les clés secrètes après avoir importé une politique FlexConfig qui utilise des clés secrètes.
- Paramètres de la plateforme
- Politiques d'intégrité
- Réponses aux alertes
- Détecteurs d'applications (définis par l'utilisateur et fournis par les services professionnels de Cisco)
- Tableaux de bord
- Tableaux personnalisés
- Flux de travail personnalisés
- Recherches enregistrées
- Rôles d'utilisateur personnalisés
- Modèles de rapports
- Mappages de produits et de vulnérabilités de tiers
- Utilisateurs et groupes pour le contrôle de l'utilisateur

Considérations spéciales pour l'importation et l'exportation de la configuration

Lorsque vous exportez une configuration, le système exporte également les autres configurations requises. Par exemple, l'exportation d'une politique de contrôle d'accès exporte également toutes les sous-politiques appelées, les objets et les groupes d'objets qu'elle utilise, les politiques ancêtres (dans un déploiement multidomaine), etc. Par ailleurs, si vous exportez une politique de paramètres de plateforme avec l'authentification externe activée, l'objet d'authentification est également exporté. Il existe cependant quelques exceptions :

- Bases de données et flux fournis par le système : le système n'exporte pas les données de catégorie de filtrage d'URL et de réputation, les données du flux de renseignements Cisco ou la base de données de géolocalisation (GeoDB). Assurez-vous que tous les périphériques de votre déploiement obtiennent des informations à jour de Cisco.
- Listes globales de renseignement de sécurité : le système exporte le blocage global de renseignement de sécurité et les listes Ne pas bloquer associées aux configurations exportées. (Dans un déploiement multidomaine, cela se produit quel que soit votre domaine actuel. Le système n'exporte **pas** les listes de domaines descendants.) Le processus d'importation convertit ces listes en listes créées par les utilisateurs, puis utilise ces nouvelles listes dans les configurations importées. Cela garantit que les listes importées n'entrent pas en conflit avec les listes de blocage globales et Ne pas bloquer. Pour utiliser des listes globales sur centre de gestion, ajoutez manuellement les listes à vos configurations importées.
- Couches partagées de la politique de prévention des intrusions : le processus d'exportation interrompt les couches partagées de la politique de prévention des intrusions. La couche précédemment partagée

est incluse dans l'ensemble, et les politiques de prévention des intrusions importées ne contiennent pas de couches partagées.

- Ensemble de variables par défaut de la politique de prévention des intrusions : le paquet d'exportation comprend un ensemble de variables par défaut avec des variables personnalisées et des variables fournies par le système avec des valeurs définies par l'utilisateur. Le processus d'importation met à jour la variable par défaut définie sur le centre de gestion d'importation avec les valeurs importées. Cependant, le processus d'importation ne supprime **pas** les variables personnalisées non présentes dans le paquet d'exportation. Le processus d'importation ne rétablit pas non plus les valeurs définies par l'utilisateur sur le centre de gestion d'importation, pour les valeurs qui ne sont pas définies dans le paquet d'exportation. Par conséquent, une politique de prévention des intrusions importée peut se comporter différemment que prévu si le centre de gestion d'importation comporte des variables par défaut configurées différemment.
- Objets utilisateur personnalisés : si vous avez créé des groupes d'utilisateurs ou des objets personnalisés dans votre centre de gestion et si un tel objet utilisateur personnalisé fait partie d'une règle de votre politique de contrôle d'accès, notez que le fichier d'exportation (.sfo) ne transporte pas le nom d'utilisateur informations sur l'utilisateur personnalisé et, par conséquent, lors de l'importation d'une telle politique, toute référence à ces objets utilisateur personnalisés sera supprimée et ne sera pas importée dans le centre de gestion de destination. Pour éviter les problèmes de détection en raison d'un groupe d'utilisateurs manquant, ajoutez manuellement les objets utilisateur personnalisés au nouveau centre de gestion et reconfigurez la politique de contrôle d'accès après l'importation.

Lorsque vous importez des objets et des groupes d'objets :

- En général, le processus d'importation importe les objets et les groupes comme nouveaux et vous ne pouvez pas remplacer les objets et les groupes existants. Toutefois, si des objets ou des groupes de réseau et de port d'une configuration importée correspondent à des objets ou des groupes existants, la configuration importée réutilise les objets ou les groupes existants plutôt que de créer de nouveaux objets ou de nouveaux groupes. Le système détermine une correspondance en comparant le nom (à l'exception de tout numéro généré automatiquement) et le contenu de chaque objet ou groupe de réseau et de ports.
- Si les noms des objets importés correspondent à des objets existants sur centre de gestion, le système ajoute des numéros générés automatiquement aux noms d'objets et de groupes importés pour les rendre uniques.
- Vous devez mapper les zones de sécurité et les groupes d'interface utilisés dans les configurations importées avec les zones et les groupes de type correspondant gérés par la méthode d'importation centre de gestion.
- Si vous exportez une configuration qui utilise des objets PKI contenant des clés privées, le système déchiffre les clés privées avant l'exportation. Lors de l'importation, le système chiffre les clés à l'aide d'une clé générée aléatoirement.

Exigences et conditions préalables à l'importation et à l'exportation de la configuration

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin

Exportation des configurations

Selon le nombre de configurations exportées et le nombre d'objets auxquels ces configurations font référence, le processus d'exportation peut prendre plusieurs minutes.

Astuces De nombreuses pages de listes du système Firepower comprennent un **YouTube EDU** ( ) à côté des éléments de liste. Cette icône signifie qu'elle peut remplacer rapidement la procédure d'exportation qui suit.

Avant de commencer

- Confirmez que les périphériques d'importation et d'exportation exécutent la même version du système Firepower. Pour le contrôle d'accès et ses sous-politiques (y compris les politiques de prévention des intrusions), la version de mise à jour de la règle de prévention des intrusions doit également correspondre.

Procédure

Étape 1 Choisissez **System** ( ) > **Tools (outils)** > **Import/Export (importation/exportation)**.

Étape 2 Cliquez sur **Réduire** ( ) et **Développer** ( ) pour réduire et développer la liste des configurations disponibles.

Étape 3 Cochez les configurations que vous souhaitez exporter et cliquez sur **Exporter**.

Étape 4 Suivez les instructions de votre navigateur Web pour enregistrer le paquet exporté sur votre ordinateur.

Importation des configurations

Selon le nombre de configurations importées et le nombre d'objets auxquels ces configurations font référence, le processus d'importation peut prendre plusieurs minutes.

Remarque Si vous vous déconnectez du système ou si votre session utilisateur expire après que vous ayez cliqué sur **Importer**, le processus d'importation se poursuit en arrière-plan jusqu'à la fin. Nous vous recommandons d'attendre la fin du processus d'importation avant de créer de nouveaux objets ou de nouvelles politiques. Toute tentative de création alors que le processus d'importation est toujours en cours peut entraîner des échecs.

Avant de commencer

- Confirmez que les périphériques d'importation et d'exportation exécutent la même version de logiciel. Pour le contrôle d'accès et ses sous-politiques (y compris les politiques de prévention des intrusions), la version de mise à jour de la règle de prévention des intrusions doit également correspondre.

Procédure

Étape 1 Sur l'appareil d'importation, choisissez **System** (⚙) > **Tools (outils)** > **Import/Export (importation/exportation)**.

Étape 2 Cliquez sur **Upload packet** (Téléverser le paquet).

Étape 3 Saisissez le chemin d'accès au paquet exporté ou recherchez son emplacement, puis cliquez sur **Upload** (Téléverser).

Étape 4 S'il n'y a aucune incompatibilité de versions ou autres problèmes, choisissez les configurations que vous souhaitez importer, puis cliquez sur **Import** (Importer).
Si vous n'avez pas besoin d'effectuer la résolution de conflits ou le mappage d'objets d'interface , l'importation se termine et un message de réussite s'affiche. Sautez le reste de cette procédure.

Étape 5 Si vous y êtes invité, dans la page de résolution des conflits d', mappez les objets d'interface utilisés dans les configurations importées aux zones et aux groupes ayant les types d'interface correspondants gérés par l'importation centre de gestion.

Le type d'objet d'interface (zone de sécurité ou groupe d'interfaces) et le type d'interface (passive, en ligne, routée, etc.) des objets de source et de destination doivent correspondre. Pour en savoir plus, consultez Interface.

Si les configurations que vous importez font référence à des zones de sécurité ou à des groupes d'interfaces qui n'existent pas encore, vous pouvez les mapper avec des objets d'interface existants ou en créer de nouveaux.

Remarque Pour les politiques de contrôle d'accès individuelles, vous avez la possibilité de remplacer une politique existante par des politiques importées. Cependant, pour les politiques de contrôle d'accès imbriquées, vous pouvez uniquement les importer en tant que nouvelles politiques.

Étape 6 Cliquez sur **Import (Importer)**.

Étape 7 Si vous y êtes invité, sur la page Import Resolution (Résolution de l'importation) , développez chaque configuration et choisissez l'option appropriée, comme décrit dans Résolution des conflits d'importation, à la page 6.

Étape 8 Cliquez sur **Import (Importer)**.

Étape 9 Mettre à jour tous les flux

Par exemple, accédez à **Objets > Gestion d'objets > Security Intelligence** et cliquez sur le bouton **Mettre à jour les flux** dans les pages Listes et flux d'URL, de réseau et DNS.

Les politiques importées n'incluent pas le contenu du flux.

Étape 10 Attendez que toutes les mises à jour de flux soient terminées avant de déployer les politiques sur les périphériques.

Prochaine étape

Remarque Si vous importez une configuration qui contient des utilisateurs et des groupes Microsoft Active Directorynous vous recommandons de télécharger tous les utilisateurs et groupes après l'importation pour éviter des problèmes dans Politiques de déchiffrement, les politiques de contrôle d'accès, et éventuellement d'autres politiques. (**Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**, puis cliquez sur (**Télécharger maintenant**).

- Il est possible d'afficher un rapport résumant les configurations importées, consultez Affichage des messages en lien avec les tâches.

Résolution des conflits d'importation

Lorsque vous tentez d'importer une configuration, le système détermine si une configuration du même nom et du même type existe déjà sur le périphérique. Dans un déploiement multidomaine, le système détermine également si une configuration est la copie d'une configuration définie dans le domaine actuel ou dans l'un de ses domaines ascendants ou descendants. (Vous ne pouvez pas afficher les configurations dans les domaines descendants, mais si une configuration avec un nom en double existe dans un domaine descendant, le système vous avertit du conflit.) Lorsqu'une importation comporte une configuration en double, le système propose des options de résolution adaptées à votre déploiement parmi les suivantes :

- **Garder celui qui existe**

  Le système n'importe pas cette configuration.

- **Remplacer celui qui existe**

  Le système remplace la configuration actuelle par la configuration sélectionnée pour l'importation.

- **Garder le plus récent**

  Le système importe la configuration sélectionnée uniquement si son horodatage est plus récent que l'horodatage de la configuration actuelle sur le périphérique.

Remarque Si vous importez une configuration qui contient des utilisateurs et des groupes Microsoft Active Directorynous vous recommandons de télécharger tous les utilisateurs et groupes après l'importation pour éviter des problèmes dans Politiques de déchiffrement, les politiques de contrôle d'accès, et éventuellement d'autres politiques. (**Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)**, puis cliquez sur (**Télécharger maintenant**).

- **Importer comme nouveau**

  Le système importe la configuration en double sélectionnée, en ajoutant un numéro généré par le système au nom pour la rendre unique. (Vous pouvez modifier ce nom avant de terminer le processus d'importation.) La configuration d'origine sur le périphérique reste inchangée.

Les options de résolution offertes par le système varient selon que votre déploiement utilise des domaines et si la configuration importée est la copie d'une configuration définie dans le domaine actuel, ou une configuration définie dans un ancêtre ou un descendant du domaine actuel. Le tableau suivant indique dans quelles circonstances le système présente ou non une option de résolution.

Option de résolution	Cisco Secure Firewall Management Center		Périphérique géré
	En double dans le domaine actuel	En double dans le domaine ancêtre ou descendant	
Garder celui qui existe	Oui	Oui	Oui
Remplacer celui qui existe	Oui	Non	Oui
Garder le plus récent	Oui	Non	Oui
Importer comme nouveau	Oui	Oui	Oui

Lorsque vous importez une politique de contrôle d'accès avec une politique de fichiers qui utilise des listes de fichiers de détection propres ou personnalisées et qu'une liste de fichiers présente un conflit de noms en double, le système propose des options de résolution de conflit comme décrit dans le tableau ci-dessus, mais l'action que le système effectue sur les politiques et les listes de fichiers varie comme décrit dans le tableau ci-dessous :

Option de résolution	Action du système	
	La politique de contrôle d'accès et la politique de fichiers associée sont importées comme nouvelles, et les listes de fichiers sont fusionnées.	La politique de contrôle d'accès existante, sa politique de fichiers et les listes de fichiers associées demeurent inchangés.
Garder celui qui existe	Non	Oui
Remplacer celui qui existe	Oui	Non
Importer comme nouveau	Oui	Non
Conserver la plus récente et la politique de contrôle d'accès importée est la plus récente	Oui	Non
Garder la plus récente et la politique de contrôle d'accès existante est la plus récente	Non	Oui

Si vous modifiez une configuration importée sur un appareil, puis réimportez cette configuration sur le même appareil, vous devez choisir la version de la configuration à conserver.

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.