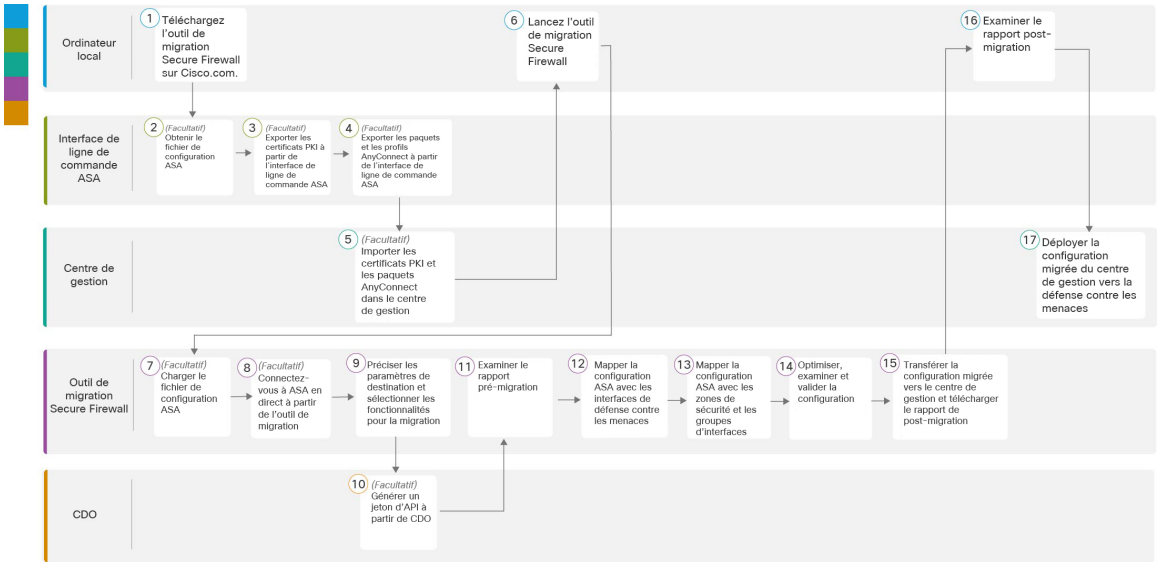
Flux de travail de migration ASA vers Threat Defense

Procédure de bout en bout

L'organigramme suivant illustre le flux de travail de migration d'un ASA vers la protection contre les menaces à l'aide de l'outil de migration de pare-feu sécurisé.



	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

	Espace de travail	Étapes
2	Interface de ligne de commande ASA	(Facultatif) Obtenir le fichier de configuration ASA : Pour obtenir le fichier de configuration ASA de ASA CLI, voir Obtenir le fichier de configuration d'ASA. Si vous avez l'intention de connecter l'ASA à partir de l'outil de migration Secure Firewall, sautez à l'étape 3.
3	Interface de ligne de commande ASA	(Facultatif) Exporter les certificats PKI à partir du CLI ASA : cette étape n'est requise que si vous prévoyez de migrer les fonctions VPN site à site et VPN RA de l'ASA vers la défense contre les menaces. Pour exporter les certificats PKI à partir de l'ASA CLI, voir Exporter le certificat PKI à partir d'ASA et l'importer dans le centre de gestion. Si vous ne prévoyez pas de migrer le VPN site à site et l'AD VPN, passez à l'étape 7.
4	Interface de ligne de commande ASA	(Facultatif) Exportez les paquets et les profils AnyConnect à partir de l'interface de ligne de commande ASA : cette étape n'est requise que si vous envisagez de migrer les fonctionnalités AD VPN d'ASA avec FPS vers la défense contre les menaces. Pour exporter les paquets et profils AnyConnect à partir de l'ASA CLI, voir Récupérer les paquets et les profils AnyConnect. Si vous ne prévoyez pas de migrer le VPN site à site et l'AD VPN, passez à l'étape 7.
5	Centre de gestion	(Facultatif) Importez les certificats PKI et les paquets Anyconnect dans le centre de gestion : pour importer les certificats PKI dans le centre de gestion, reportez-vous aux sections Exporter le certificat PKI à partir d'ASA et l'importer dans le centre de gestion et Récupérer les paquets et les profils AnyConnect.
6	Ordinateur local	Lancez l'outil de migration Secure Firewall sur votre machine locale, voir Lancer l'outil de migration Secure Firewall.
7	Outil de migration Secure Firewall	(Facultatif) téléchargez le fichier de configuration ASA obtenu à partir de l'interface de ligne de commande ASA, consultez Téléverser l'ASA Si vous prévoyez de vous connecter à ASA en direct, passez à l'étape 8.
8	Outil de migration Secure Firewall	Vous pouvez vous connecter à Live ASA directement à partir de l'outil de migration de pare-feu sécurisé. Pour plus d'informations, consultez Se connecter à l'ASA à partir de l'outil de migration Secure Firewall.
9	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 .
10	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
11	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

	Espace de travail	Étapes
12	Outil de migration Secure Firewall	L'outil de migration de Secure Firewall vous permet de mapper la configuration ASA avec les interfaces de défense contre les menaces. Pour connaître les étapes détaillées, reportez-vous à Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager.
13	Outil de migration Secure Firewall	Pour vous assurer que la configuration ASA est correctement migrée, mappez les interfaces ASA aux objets d'interface de défense contre les menaces, aux zones de sécurité et aux groupes d'interfaces appropriés. Pour connaître les étapes détaillées, consultez Mapper les interfaces ASA à des zones de sécurité et à des groupes d'interfaces.
14	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 et valider la configuration.
15	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.
16	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 Transférer la configuration migrée vers Centre de gestion.
17	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 ASAgéré par , 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.

Procédure

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 des 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.

Prochaine étape

Obtenir le fichier de configuration d'ASA

Obtenir le fichier de configuration d'ASA

Vous pouvez utiliser une des méthodes suivantes pour obtenir un fichier de configuration :

- Exporter le fichier de configuration , à la page 4
- Se connecter à l'ASA à partir de l'outil de migration Secure Firewall, à la page 9

Exporter le fichier de configuration

Cette tâche n'est requise uniquement que si vous voulez téléverser manuellement un fichier de configuration . Si vous voulez vous connecter à un à partir de l'outil de migration Secure Firewall, passez à Se connecter à l'ASA à partir de l'outil de migration Secure Firewall, à la page 9.

Remarque Ne pas coder à la main ou apporter des modifications à la configuration après avoir exporté le fichier. Ces changements ne seront pas migrés vers défense contre les menaces et ils créeront des erreurs dans la migration ou causeront son échec. Par exemple, ouvrir et sauvegarder le fichier de configuration dans le terminal peut ajouter un espace blanc ou des lignes vides que l'outil de migration Secure Firewall ne peut pas analyser.

Assurez-vous que le fichier de configuration exporté ne contient pas le mot-clé "--More--" en tant que texte, car cela peut faire échouer la migration.

Procédure

Étape 1 Utilisez la commande **show running-config** pour le dispositif ASA ou le contexte que vous migrez et copiez la configuration à partir de là. Voir Afficher la configuration en cours d'exécution

Vous pouvez également utiliser Adaptive Security Device Manager (ASDM) pour le dispositif ADA ou le contexte que vous souhaitez migrer et choisir **Fichier** > **Afficher la configuration en cours d'exécution dans une nouvelle fenêtre** pour obtenir le fichier de configuration.

Remarque Pour un multi-contexte, vous pouvez utiliser la commande **show tech-support** pour obtenir la configuration de tous les contextes dans un seul fichier.

Étape 2 Sauvegardez la configuration soit comme `.cfg` ou `.txt`.

Vous ne pouvez pas téléverser la configuration vers l'outil de migration Secure Firewall si elle a une extension différente.

Étape 3 Transférez le fichier de configuration vers votre ordinateur où vous avez téléchargé l'outil de migration Secure Firewall.

Exporter le certificat PKI à partir d'ASA et l'importer dans le centre de gestion

Avant de commencer

L'outil de migration Secure Firewall prend en charge la migration des VPN basés sur des certificats vers le centre de gestion.

ASA utilise le modèle du point de confiance pour stocker les certificats dans la configuration. Un point de confiance est un conteneur dans lequel les certificats sont stockés. Le point de confiance ASA peut stocker jusqu'à deux certificats.

Le point de confiance ASA ou les certificats dans le fichier de configuration ASA contiennent des valeurs de hachage. Ainsi donc, vous ne pouvez pas directement les importer dans un centre de gestion.

Dans le centre de gestion de destination, migrez manuellement le point de confiance ASA ou les certificats VPN en tant qu'objets PKI dans le cadre de l'activité de pré-migration.

Procédure

Étape 1 Utilisez la commande suivante pour exporter le certificat PKI via la CLI à partir de la configuration ASA source avec les clés vers un fichier PKCS12.

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

Étape 2 Importez le certificat PKI dans un centre de gestion (**Gestion d'objet Objets PKI)**.

Pour plus d'informations, référez-vous au guide de configuration du pare-feu pour obtenir plus de renseignements.

Les objets PKI créés manuellement peuvent maintenant être utilisés dans l'outil de migration Secure Firewall dans la **page de mise en revue et de validation** sous la section **Point de confiance** dans **Accès à distance VPN**.

Récupérer les paquets et les profils AnyConnect

Les profils AnyConnect sont facultatifs et peuvent être téléversés via le centre de gestion ou l'outil de migration Secure Firewall.

Avant de commencer

- Le VPN d'accès à distance sur le centre de gestion demande au moins un paquet AnyConnect.
- Si la configuration consiste en un paquet de navigateur Hostscan et externe, vous devez téléverser ces paquets.
- Tous les paquets doivent être ajoutés au centre de gestion en tant qu'activité pré-migration.
- Dap.xml et Data.xml doivent être ajoutés via l'outil de migration Secure Firewall

Procédure

Étape 1 Utilisez la commande suivante pour copier le paquet demandé de la source ASA vers un serveur FTP ou TFTP.

```
Copy <source file location:/source file name> <destination>
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Example
of copying Anyconnect Package.
ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Example
of copying External Browser Package.
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example of copying
Hostscan Package.
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect
Profile.
```

Étape 2 Importer les paquets téléchargés dans le centre de gestion (**fichier de gestion des objets** > **VPN** > **AnyConnect**)

1. Les fichiers Dap.xml et Data.xml doivent être téléchargés vers le centre de gestion à partir de l'outil de migration Secure Firewall dans la section **Examiner et valider** > **fichier VPN AnyConnect** > **pour l'accès à distance**.
2. Les profils AnyConnect peuvent être téléchargés directement vers le centre de gestion ou via l'outil de migration Secure Firewall dans la section **Examiner et valider** > **fichier VPN AnyConnect** > **pour l'accès à distance**.

Les fichiers téléversés manuellement peuvent maintenant être utilisés dans l'outil de migration Secure Firewall.

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 Téléverser l'ASA, à la page 9 .

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.
- 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.

Procédure

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.

  Remarque Si vous n'avez pas de compte Cisco.com, créez-le sur la page de connection de Cisco.com.

- Connectez-vous avec les identifiants par défaut suivants :
  - **Nom d'utilisateur** : admin
  - Mot de passe : Admin123

Passez à l'étape 8si vous avez utilisé votre compte Cisco.com pour vous connecter.

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 avez exporté la configuration sur votre ordinateur, passez au Téléverser l'ASA.
- Si vous souhaitez extraire des informations d'un dossier en utilisant l'outil de migration Secure Firewall, passez à Se connecter à l'ASA à partir de l'outil de migration Secure Firewall, à la page 9

Téléverser l'ASA

Avant de commencer

Exporter le fichier de configuration au format `.cfg` ou `.txt` à partir de l'appareil ASAASA .

Remarque Ne téléversez pas un fichier de configuration codé à la main ou modifié manuellement. Les éditeurs de texte ajoutent des lignes vides et d'autres éléments au fichier qui peuvent faire échouer la migration.

Procédure

Étape 1 Dans l'écran **Extraire** les **informations ASA** , dans la section **Téléversement manuel**, cliquez sur **Téléverser** pour charger un fichier de configuration ASA .

Étape 2 Naviguez vers où le fichier de configuration est situé et cliquez sur **Ouvrir**

L'outil de migration Secure Firewall téléverse le fichier de configuration. Pour les fichiers de configuration volumineux, cette étape prend plus de temps. La console fournit un journal ligne par ligne de la progression, y compris la ligne de configuration ASA avec FPS qui est en cours d'analyse. Si vous ne voyez pas la console, vous pouvez la trouver dans une fenêtre séparée derrière l'outil de migration Secure Firewall. La section **Choix de contexte** identifie si la configuration téléversée correspond au ASA multi-contexte.

Étape 3 Examinez la section **Sélection du contexte** et choisissez le contexte que vous voulez migrer.

Prochaine étape

Préciser les paramètres de destination pour l'outil de migration Secure Firewall, à la page 11

Se connecter à l'ASA à partir de l'outil de migration Secure Firewall

L'outil de migration Secure Firewall peut se connecter à un dispositif ASA que vous souhaitez migrer et extraire les informations de configuration requises.

Avant de commencer

- Télécharger et lancer l'outil de migration Secure Firewall.
- Pour les ASA à contexte unique, obtenez l'adresse IP de gestion, les informations d'identification de l'administrateur et le mot de passe d'activation.
- Pour les ASA en mode multi-contexte, obtenez l'adresse IP du contexte **d'administration**, les informations d'identification de l'administrateur et le mot de passe d'activation.

Remarque Si l'ASA n'est pas configuré avec l'option **Activer le mot de passe**, vous pouvez laisser le champ vide dans l'outil de migration Secure Firewall.

Procédure

Étape 1 Sur l'écran **Extraire les informations ASA**, dans la section **Connecter à l'ASA**, cliquez sur **Connecter** pour vous connecter au périphérique ASA que vous souhaitez migrer.

Étape 2 Sur l'écran **Connexion à l'ASA**, saisissez les informations suivantes :

1. Dans le champ **Adresse IP/Nom d'hôte de l'ASA**, entrez l'adresse IP de gestion ou le nom d'hôte (pour un ASA à contexte unique) ou l'adresse IP du contexte d'administration ou le nom d'hôte (pour un ASA à contextes multiples).
2. Dans les champs **Nom d'utilisateur**, **Mot de passe**et **Activer le mot de passe**, saisissez les informations d'identifiant administrateur appropriés.

   Remarque Si l'ASA n'est pas configuré avec l'option **Activer le mot de passe**, vous pouvez laisser le champ vide dans l'outil de migration Secure Firewall.

3. Cliquez sur **Ouvrir une session**.

Lorsque l'outil de migration Secure Firewall se connecte à l'ASA, il affiche message de connexion réussie au message ASA Pour un ASA multicontexte, l'outil de migration Secure Firewall identifie et liste les contextes.

Étape 3 Choisissez le contexte ASA que vous voulez migrer à partir de la liste déroulante **Contexte**

Étape 4 (Facultatif) Sélectionnez **Collecter les comptes de résultat**.

Lorsque cette case est cochée, cet outil calcule le nombre de fois qu'une règle ASA a été utilisée et la dernière fois que la règle a été utilisée depuis la mise en service de l'ASA ou le dernier redémarrage de l'ASA, et affiche ces informations sur la page **Examiner et valider**. Cela vous permet d'évaluer l'efficacité et la pertinence de la règle avant la migration.

Étape 5 Cliquez sur **Débuter l'extraction**

L'outil de migration Secure Firewall se connecte à l'ASA et débute l'extraction des informations de configuration. Lorsque l'extraction se termine avec succès, la section **Sélection du contexte** identifie si la configuration téléversée correspond à un ASA à contexte simple ou multiple.

Étape 6 Examinez la section **Sélection** du contexte et choisissez le contexte ASA que vous voulez migrer.

Étape 7 Cliquez sur **Démarrer l'analyse**.

La section **Résumé de l'analyse** affiche le statut de l'analyse. L'outil de migration Secure Firewall analyse le fichier de configuration et le déconnecte de l'ASA.

Étape 8 Examinez le résumé des éléments détectés et analysés par l'outil de migration Secure Firewall dans le fichier de configuration téléversé.

Étape 9 Cliquez sur **Suivant** pour choisir les paramètres cibles.

Prochaine étape

Préciser les paramètres de destination pour l'outil de migration Secure Firewall, à la page 11

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 Centre de gestion des cibles pour la migration pris en charge.
- Créez un compte dédié à l'outil de migration Secure Firewall dans centre de gestion avec des privilèges suffisants pour accéder à l'API REST, comme décrit dans la section Comptes d'utilisateur pour l'accès à la gestion.
- (Facultatif) Si vous souhaitez faire migrer des configurations spécifiques à un dispositif, comme des interfaces et des itinéraires, ajoutez le défense contre des 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.

Procédure

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 des menaces, vous pouvez seulement migrer vers les appareils défense contre des 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 des menacesqui sont gérés parcentre de gestion. Vous pouvez voir la progression de cette étape dans la console.

Étape 3 Cliquez sur **Procéder**.

Dans la section **Choisir la défense contre les menaces** , vous pouvez soit sélectionner un dispositif défense contre des menacesvers lequel vous souhaitez migrer, soit, si vous n'avez pas de dispositif défense contre des menaces, migrer les stratégies partagées (listes de contrôle d'accès, NAT et objets) de la ASAconfiguration vers le centre de gestion.

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 l'ASA du .

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

  Remarque Au minimum, le dispositif défense contre des menacesnatif que vous choisissez doit avoir le même nombre d'interfaces physiques ou de canaux de port que la configuration de l'ASA que vous migrez. Au minimum, l'instance de conteneur du dispositif défense contre des 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 l'ASA . 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.

Tableau 1 : ASA Fonctionnalités et versions Centre de gestion ou Défense contre les menacesprises en charge du pare-feu

Fonctionnalités de pare-feu	Version du centre de gestion ou de la défense contre les menaces prise en charge
avec déploiement à distance	6.7 ou plus récent
VPN carte cryptographique site-à-site	6.6 ou plus récent
Virtual Tunnel Interface (VTI) et basée sur les itinéraires (VTI)	6.7 ou plus récent
Objets de routage dynamique et BGP	7.1 ou plus récent
VPN d'accès à distance	• Centre de gestion 7.2 ou plus récent • Threat Defense 7.0 ou plus récent
EIGRP	• Centre de gestion 7.2 ou plus récent • Threat Defense 7.0 ou plus récent
PBR	• Centre de gestion 7.3 ou plus récent • Threat Defense 7.3 ou plus récent
ECMP	• Centre de gestion 7.1 ou plus récent • Threat Defense 6.5 ou plus récent

Remarque Pour migrer les interfaces VPN site à site, VTI et basées sur les routes (VTI), défense contre des menaces doit être configuré surcentre de gestion.

- Pour l'ASA 5505, les configurations spécifiques à l'appareil (interface et routes) et les stratégies partagées (NAT, ACL et objets) ne peuvent être migrées que lorsque la plateforme de défense contre des menaces cible prise en charge est Firewall 1010 avec la version centre de gestion 6.5 ou ultérieure.

  Remarque
  - Si la cible défense contre des menaces n'est pas FPR-1010 ou si la cible centre de gestion est antérieure à la version 6.5, la prise en charge de la migration de l'ASA 5505 ne s'applique qu'aux politiques partagées. Les caractéristiques de l'appareil ne seront pas migrées.
  - Vous pouvez sélectionner uniquement FPR-1010 dans la liste déroulante **Choisir l'appareil** car la configuration source est ASA 5505.
  - La prise en charge de la migration ASA-SM ne concerne que les stratégies partagées. Les caractéristiques de l'appareil ne seront pas migrées.

- Cliquez sur **Continuer sans défense contre les menaces** pour faire migrer la configuration vers centre de gestion.

  Lorsque vous procédez sansdéfense contre des menaces , l'outil de migration de Secure Firewall ne transfère aucune configuration ou politique vers défense contre des 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 défense contre des 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.

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 des menaces, l'outil de migration Secure Firewall sélectionne automatiquement les fonctionnalités disponibles pour la migration à partir de la configuration de l'ASA 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 Secure Firewall sélectionne automatiquement les fonctionnalités disponibles pour la migration à partir de la configuration de l'ASA du dans la section **Configuration partagée**. Vous pouvez modifier la sélection par défaut, selon vos besoins.

  Remarque La section **Configuration de l'appareil** n'est pas disponible lorsque vous n'avez pas choisi d'appareil destinataire défense contre des menacesvers où migrer

  Remarque La section **Configuration de l'appareil** n'est pas disponible lorsque vous avez choisi **Migrer le gestionnaire d'appareil Firepower (Configurations partagées uniquement)**.

- L'outil de migration Secure Firewall prend en charge les fonctions de contrôle d'accès suivantes pendant la migration :
  - Remplir les zones de sécurité de destination—Active le mappage des zones de destination pour l'ACL pendant la migration.

    La logique de recherche de route est limitée aux routes statiques et aux routes connectées, alors que les PBR, les routes dynamiques et les NAT ne sont pas pris en compte. La configuration du réseau de l'interface est utilisée pour dériver les informations de l'itinéraire connecté.

    Compte tenu de la nature des groupes d'objets réseau Source et Destination, cette opération peut entraîner une explosion des règles.

  - Migrer les règles de tunnel en tant que préfiltre - Le mappage des règles de protocole de tunnel encapsulé par l'ASA du vers les règles de tunnel du préfiltre présente les avantages suivants :
    - Inspection en profondeur - Pour le trafic encapsulé et pour améliorer les performances avec le fastpathing.
    - Amélioration des performances : vous pouvez accélérer ou bloquer toutes les autres connexions qui bénéficient d'un traitement anticipé.

    L'outil de migration Secure Firewall identifie les règles de trafic du tunnel encapsulé dans la configuration source et les migre en tant que règles de tunnel préfiltré. Vous pouvez vérifier la règle de tunnel migré sous la politique Préfiltrer La politique Préfiltrer est associée à la stratégie de contrôle d'accès sur centre de gestion.

    Les protocoles étant migrés comme des règles de tunnel préfiltrés sont les suivants :

- GRE (47)
- Encapsulation IPv4 (4)
- Encapsulation IPv6 (41)
- Tunnellisation Teredo (UDP : 3544)

Remarque Si vous choisissez de ne pas choisir l'option Préfiltrer, toutes les règles de traffic tunnelisé seront migrées comme des règles non prises en charge.

Les règles de tunnel ACL (GRE et IPnIP) dans la configuration de l'ASA sont actuellement migrées comme bidirectionnelles par défaut. Vous pouvez maintenant spécifier la direction de la règle pour la destination comme bidirectionnelle ou unidirectionnelle dans l'option d'état du contrôle d'accès.

- L'outil de migration Secure Firewall prend en charge les interfaces et les objets suivants pour la migration des tunnels VPN :
  - Basée sur la règle (carte cryptographique) - Si le centre de gestion et défense contre des menaces cible est la version 6.6 ou plus récente.
  - Basée sur l'itinéraire (VTI) - Si le centre de gestionet défense contre des menacescible est la version 6.7 ou plus récente.
- 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'ASA de ne seront pas migrés. Cela optimise le temps de migration et nettoie les objets inutilisés de la configuration.
- (Facultatif) Dans la section **Optimisation**, sélectionnez **Recherche de groupe d'objets** pour une utilisation optimale de la mémoire par politique d'accès sur défense contre des menaces .
- (Facultatif) Dans la section **Groupement en ligne**, l'outil de migration Secure Firewall vous permet d'effacer les règles d'accès des noms d'objets réseau et service prédéfinis qui commencent par CSM ou DM. Si vous décochez cette option, les noms d'objets prédéfinis seront conservés durant la migration. Pour plus d'informations, référez-vous à Regroupement en ligne.

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

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.

Prochaine étape

Examiner le rapport pré-migration, à la page 17

Regroupement en ligne

Groupement d'objet par ASDM et ASA géré par CSM

Lorsque vous saisissez plusieurs éléments (objets ou valeurs en ligne) dans l'adresse source ou de destination, ou dans le service source ou de destination, CSM ou ASDM crée automatiquement un groupe d'objets. Les conventions d'appellation de ces groupes d'objets utilisés par CSM et ASDM sont respectivement CSM_INLINE et DM_INLINE lors du déploiement de la configuration sur l'appareil ASA concerné.

Remarque Pour modifier le comportement du regroupement d'objets, dans **Outils** > **Préférences**, sélectionnez **Développement automatique des objets de réseau et de service avec la préférence de table de règles de préfixe spécifiée**.

Voici le fragment de code de configuration extrait à l'aide de la commande **show run** sur une ASA gérée par ASDM.

```
object network host1
 host 10.1.1.100
object network fqdn_obj1
 fqdn abc.cisco.com
object-group network DM_INLINE_NETWORK_1
 network-object 10.21.44.189 255.255.255.255
 network-object 10.21.44.190 255.255.255.255
object-group network DM_INLINE_NETWORK_2
 network-object 10.21.44.191 255.255.255.255
 network-object object host1
 network-object object fqdn_obj1


access-list CSM_DM_ACL extended permit tcp object-group DM_INLINE_NETWORK_1 object-group
DM_INLINE_NETWORK_2
```

Dans l'exemple ci-dessus, la liste d'accès CSM_DM_ACL sur l'interface ASDM n'affiche pas le groupe DM_INLINE comme réseau source et destination de la règle, mais affiche le contenu du groupe DM_INLINE.

Groupement en ligne - ASDM/CSM

La fonctionnalité de regroupement en ligne de l'outil de migration Secure Firewall vous permet d'analyser la **configuration en cours d'exécution** des dispositifs ASA gérés par ASDM ou CSM. Il fournit une option pour préserver la même représentation de l'interface utilisateur des règles de liste d'accès que sur ASDM ou CSM. Si cette option n'est pas retenue, les règles migrées feront référence aux groupes DM_INLINE, comme indiqué dans le document ASA **show running-configuration.**

Remarque Le fichier de configuration de l'ASA source utilisé par l'outil de migration Secure Firewall serait toujours **show run** ou **show tech** collecté à partir de l'ASA ou via une connexion en direct à l'ASA (SSH). L'outil de migration Secure Firewall ne prend pas en charge aucune autre forme de fichiers ou méthodes de configuration.

Les figures suivantes montrent comment les champs Source et Réseau destination de l'ACE ou de la RULE changent en fonction de l'activation ou de la désactivation de l'option de regroupement en ligne.

Illustration 1 : Avec regroupement en ligne-ASDM/CSM activé

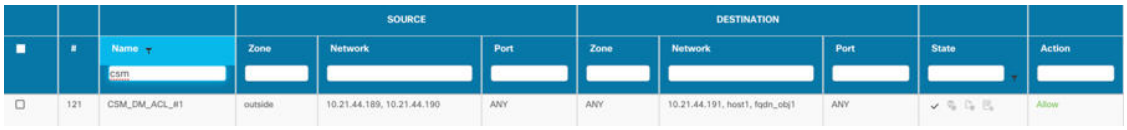


Illustration 2 : Avec regroupement en ligne-ASDM/CSM désactivé

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.

Procédure

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 :

- **Résumé général** - Méthode utilisée pour extraire les informations de configuration du ASA ou pour se connecter à une configuration de .

  Si vous vous connectez à une ASA active, le mode de pare-feu détecté sur l'ASAASA , et pour le mode de contexte multiple, le contexte que vous avez choisi pour la migration.

Un résumé des éléments de configuration des dispositifs ASA qui peuvent être migrés avec succès et des défense contre des menacesfonctionnalités spécifiques des ASA sélectionnées pour la migration.

Lors de la connexion à un dispositif géré par FDM, le résumé comprend des informations sur le nombre d'occurrences - le nombre de fois où une règle de dispositif géré par l'ASA a été rencontrée et les informations sur l'horodatage.

- **Lignes de configuration avec des erreurs** - Détails des éléments de configuration ASA 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 configuration 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 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 dispositifs ASAASA 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 des 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 ASAASA , 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 ASAASA 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

Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager

Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager

L'appareil défense contre des menaces doit avoir un nombre d'interfaces physiques et de canaux de port égal ou supérieur à celui utilisé par ASAASA. Ces interfaces ne doivent pas avoir les mêmes noms sur les deux appareils. Vous pouvez choisir comment associer les interfaces.

Sur l'écran **Associer l'interface Threat Defense**, l'outil de migration Secure Firewall récupère une liste des interfaces sur l'appareil défense contre des menaces. Par défaut, l'outil de migration Secure Firewall mappe les interfaces dans ASAASA avec leet le dispositif défense contre des menaces en fonction de leurs identités d'interface. Par exemple, l'interface « gestion seule » de l'interface du ASA est automatiquement mappée à l'interface « gestion seule » du défense contre des menacesdispositif et n'est pas modifiable.

Le mappage de l'interface de l'ASA avec à l'interface défense contre des menaces diffère en fonction du type de périphérique défense contre des menaces :

- Si la cible défense contre des menaces est de type natif :
  - Le défense contre des menacesdoit avoir un nombre égal ou supérieur d'interfaces ASA ou d'interfaces de données de canal de port (PC) utilisées (à l'exclusion des interfaces de gestion uniquement et des sous-interfaces dans la configuration de dispositifs gérés par un ASA). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre des 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 des menaces est de type contenant :
  - Le défense contre des menacesdoit avoir un nombre égal ou supérieur d'interfaces ASA ou 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 ASA avec FPS). Si le nombre est moindre, ajouter le type d'interface requis sur le défense contre des menaces cible. Par exemple, si le nombre d'interfaces physiques et de sous-interfaces physiques sur la cible défense contre des menaces est inférieur de 100 à celui de l'ASA , vous pouvez créer des interfaces physiques ou des sous-interfaces physiques supplémentaires sur la cible défense contre des menaces.
  - Les sous-interfaces ne sont pas créés par l'outil de migration Secure Firewall Seul le mappage d'interface est autorisé entre les interfaces physiques, les canaux de port ou les sous-interfaces.

Avant de commencer

Assurez-vous de vous être connecté au centre de gestion et choisi la destination comme défense contre des menaces Pour en savoir plus, consultez Préciser les paramètres de destination pour l'outil de migration Secure Firewall, à la page 11.

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

Procédure

Étape 1 Si vous souhaitez modifier le mappage d'une interface, cliquez sur la liste déroulante du **nom de l'interface de défense contre les menaces** et choisissez l'interface que vous souhaitez mapper à l'interface de l'ASA .

Vous ne pouvez pas modifier le mappage des interfaces de gestion. Si une interface défense contre des menaces a déjà été attribuée à une interface de périphérique ASA , 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 des menacesà toutes les sous.

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

Prochaine étape

Mappez les interfaces des ASA aux objets d'interface, aux zones de sécurité et aux groupes d'interfaces appropriésdéfense contre des menaces. Pour plus d'informations, voir Mapper les interfaces ASA à des zones de sécurité et à des groupes d'interfaces.

Mapper les interfaces ASA à des zones de sécurité et à des groupes d'interfaces

Remarque Si la configuration de votre ASAde ne comprend pas de listes d'accès ni de règles NAT ou si vous choisissez de ne pas migrer ces règles, vous pouvez ignorer cette étape et passer à Optimiser, examiner et valider la configuration, à la page 21.

Pour s'assurer que la configuration du de l'ASAest migrée correctement, mappez les interfaces duASA aux objets d'interface, aux zones de sécurité et aux groupes d'interfaces appropriésdéfense contre des menaces. Dans une configuration ASA 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.
- Groupes d'interfaces - Une interface peut appartenir à plusieurs groupes d'interfaces.

L'outil de migration Secure Firewall permet le mappage un à un des interfaces avec les zones de sécurité et les groupes d'interfaces ; lorsqu'une zone de sécurité ou un groupe d'interfaces 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 plus d'informations sur les zones de sécurité et les groupes d'interface dans centre de gestion, référez-vous à Objets d'interface : groupes d'interfaces et zones de sécurité .

Procédure

Étape 1 Sur l'écran **Mapper les zones de sécurité et les groupes d'interfaces**, passez en revue les interfaces, les zones de sécurité et les groupes d'interfaces disponibles.

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 ASA 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.

c) Dans la colonne **VRF mappé**, affichez les configurations VRF dérivées des contextes de sécurité, qui sont mappés à l'interface.

Étape 3 Vous pouvez mapper manuellement ou auto-créer les zones de sécurité et les groupes d'interface.

Étape 4 Pour mapper manuellement les zones de sécurité et les groupes d'interface, 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 ou groupe d'interface.
c) Saisissez le nom de la zone de sécurité dans la colonne **Zone de sécurité**. Le nombre maximal de caractères est de 48. De même, vous pouvez ajouter un groupe d'interfaces.
d) Cliquez sur **Close** (Fermer).

Pour mapper les zones de sécurité et les groupes d'interface par auto-création, faites ce qui suit :

a) Cliquez sur **Auto-créer**.
b) Dans la boîte de dialogue **Auto-créer**, cochez une ou les deux cases **Groupes d'interface** et **Mappage de zone**.
c) Cliquez sur **Auto-créer**.

L'outil de migration Secure Firewall donne à ces zones de sécurité le même nom que l'interface l'ASA , comme à **l'extérieur** ou à **l'intérieur**, et affiche un « (A) » après le nom pour indiquer qu'il a été créé par l'outil de migration du pare-feu sécurisé. Les groupes d'interface ont un suffixe `_ig` ajouté, tel que **outside_ig** ou **inside_ig**. En outre, les zones de sécurité et les groupes d'interface ont le même mode que l'interface ASA du . Par exemple, si l'interface logique ASA du est en mode L3, la zone de sécurité et le groupe d'interface créés pour l'interface sont également en mode L3.

Étape 5 Lorsque vous avez mappé toutes les interfaces aux zones de sécurité et groupes d'interface appropriés, cliquez sur **Suivant**.

Optimiser, examiner et valider la configuration

Procédure

Étape 1 (Facultatif) Sur l'écran , cliquez sur **Optimiser l'ACL** pour exécuter le code d'optimisation et effectuez les opérations suivantes :

a) Pour télécharger les règles d'optimisation d'ACL, cliquez sur **Télécharger**.
b) Sélectionnez les règles et choisissez **Actions** > **Migrer comme désactivé** ou **Ne pas migrer** et appliquez l'une des actions.
c) Cliquez sur **Save** (enregistrer).
L'opération de migration passe de **Ne pas migrer** à **désactivé** ou vice-versa.

Vous pouvez effectuer une sélection en bloc des règles à l'aide des options suivantes

- Migrer - Pour migrer vers le statut par défaut.
- Ne pas migrer - Pour ignorer la migration des ACL
- Migrer comme désactivé - Pour migrer les ACL avec le champ ***État*** réglé à ***Désactiver***
- Migrer comme activé - Pour migrer les ACL avec le champ ***État*** réglé à ***Activer***

Étape 2 Sur optimiser,l'écran **Examiner et valider la configuration**, cliquez sur **Règles de contrôle d'accès** et faites ceci :

a) Pour chaque entrée dans le tableau, examinez les mappages et vérifiez qu'ils soient corrects.

Une règle de politique d'accès migrée utilise le nom de l'ACL comme préfixe et y ajoute le numéro de la règle de l'ACL pour faciliter le mappage vers le fichier de configuration d'ASA. Par exemple, si une ACL ASAest nommée « inside_access », la première ligne de règle (ou ACE) de l'ACL sera nommée « inside_access_#1 ». Si une règle doit être étendue en raison de combinaisons TCP ou UDP, d'un objet de service étendu ou pour toute autre raison, l'outil de migration Secure Firewall ajoute un suffixe numéroté au nom. Par exemple, si la règle d'autorisation est développée en deux règles de migration, elles sont nommées « inside_access _#1-1 » et « inside_access_#1-2 ».

Pour toute règle comprenant un objet non pris en charge, l'outil de migration Secure Firewall ajoute un suffixe « _UNSUPPORTED » au nom.

b) Si vous ne souhaitez pas migrer une ou plusieurs stratégies de liste de contrôle d'accès, cochez la case des lignes concernées, choisissez **Actions** > **Ne pas migrer**, puis cliquez sur **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**.

Dans la boîte de dialogue **Action découlant d'une règle**, dans le menu déroulant **Actions**, vous pouvez choisir les onglets **SCA** ou **Préfiltre** :

- SCA - Chaque règle de contrôle d'accès comporte une action qui détermine la manière dont le système traite et enregistre le trafic correspondant. Vous pouvez effectuer une action d'autorisation, de confiance, de surveillance, de blocage ou de blocage avec réinitialisation sur une règle de contrôle d'accès.
- Préfiltre - L'action découlant d'une règle détermine comment le système traite et enregistre le trafic correspondant. Vous pouvez faire soit un fastpath ou un bloc.

Astuces Les stratégies IPS et de fichiers attachées à une règle de contrôle d'accès seront automatiquement supprimées pour toutes les actions de la règle, à l'exception de l'option Autoriser.

Catégorie de règle ACL - L'outil de migration Secure Firewall préserve les sections de règle dans la configuration ASA gérée par CSM et les migre en tant que catégories ACL sur centre de gestion.

Avertissement relatif à la capacité et à la limite des règles - L'outil de migration Secure Firewall compare le nombre total d'ACE pour les règles migrées avec la limite d'ACE prise en charge sur la plate-forme cible.

En fonction du résultat de la comparaison, l'outil de migration Secure Firewall affiche un indicateur visible et un message d'avertissement si le nombre total d'ACE migrés dépasse le seuil ou s'il s'approche du seuil de la limite supportée par le dispositif cible.

Vous pouvez optimiser ou décider de ne pas migrer si les règles dépassent la colonne Compte ACE. Vous pouvez aussi terminer la migration et utiliser ces informations pour optimiser les règles après un transfert sur le centre de gestion avant le déploiement.

Remarque L'outil de migration Secure Firewall ne bloque aucune migration malgré l'avertissement.

Vous pouvez désormais filtrer le nombre d'ACE dans l'ordre croissant, décroissant, égal, supérieur et inférieur.

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 3 Cliquez sur les onglets suivants et examinez les éléments de configuration :

- **Règles NAT**
- **Objets (objets de liste d'accès, objets de réseau, objets de port, objets VPN et objets de route dynamique)**
- **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.

Les objets Liste d'accès affichent les listes d'accès standard et étendues utilisées dans BGP, EIGRP et AD VPN.

Si vous ne souhaitez pas migrer une ou plusieurs règles NAT ou interfaces de routage, cochez la case des lignes concernées, choisissez **Actions** > **Ne pas migrer**, puis cliquez sur **Enregistrer**.

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

Étape 4 (Facultatif) Tout en examinant votre configuration, vous pouvez renommer un ou plusieurs objets réseau, port ou VPN dans l'onglet **Objets réseau**ou dans l'onglet **Objets port**, ou dans l'onglet **Objets VPN** en choisissant **Actions** > **Renommer**.

Les règles d'accès et politiques NAT référant aux objets renommés sont aussi mises à jour avec de nouveaux noms d'objet.

Étape 5 Dans la section **Objets de routage dynamique**, tous les objets pris en charge étant migrés sont affichés :

- Liste de politiques
- Liste des préfixes
- Route-Carte
- Liste de communautés
- Chemin d'accès AS
- Accès-Liste

Étape 6 Dans la section **Routes**, les routes suivantes sont affichées :

- Statiques - Affiche toutes les routes statiques IPv4 et IPv6
- BGP - Affiche toutes les routes BGP.
- EIGRP - Affiche toutes les routes EIGRP.

  Pour EIGRP, les clés d'authentification sont obtenues si la configuration `more system:running` est téléchargée et que les clés ne sont pas chiffrées. Si la clé est chiffrée dans la configuration de la source, vous pouvez fournir manuellement la clé dans la section de l'interface dans EIGRP. Vous pouvez choisir le type d'authentification (chiffrée, non chiffrée, autorisée ou aucune) et fournir la clé selon le cas.
- ECMP - Affiche toutes les zones ECMP.

  Remarque La seule action pouvant être effectuée dans cette section est de renommer les zones ECMP.
- PBR - Affiche toutes les routes PBR.

Étape 7 Dans la section **VPN d'accès à distance**, tous les objets correspondant au VPN d'accès à distance sont migrés de l'ASA vers le centre de gestion et sont affichés :

- **Fichiers Anyconnect** - Les paquets AnyConnect, les fichiers Hostscan (Dap.xml, Data.xml, Hostscan Package), les paquets External Browser et les profils AnyConnect doivent être récupérés à partir du dispositif ASA source et doivent être disponibles pour la migration.

  Dans le cadre de l'activité de pré-migration, téléchargez tous les paquets AnyConnect vers le centre de gestion. Vous pouvez téléverser directement les profils AnyConnect vers le centre de gestion ou à partir de l'outil de migration Secure Firewall.

  Sélectionnez les paquets AnyConnect, Hostscan ou External Browser préexistants récupérés depuis le centre de gestion. Vous devez sélectionner au moins un paquet AnyConnect. Vous devez sélectionner Hostscan, dap.xml, data.xml, ou un navigateur externe si disponible dans la configuration source. Les profils AnyConnect sont facultatifs.

  Dap.xml doit être le bon fichier à récupérer de l'ASA. Les validations sont effectuées sur dap.xml qui sont disponibles dans le fichier de configuration. Vous devez téléverser et choisir tous les fichiers

nécessaires pour la validation. Si la mise à jour n'est pas effectuée, elle sera considérée comme incomplète et l'outil de migration Secure Firewall ne procédera pas à la validation.

- **AAA** - Les serveurs d'authentification de type Radius, LDAP, AD, LDAP, SAML et Local Realm sont affichés. Mettez à jour les clés pour tous les serveurs AAA. À partir de l'outil de migration Secure Firewall 3.0, les clés pré-partagées sont récupérées automatiquement pour un ASA Live Connect. Vous pouvez aussi téléverser la configuration source avec les clés cachés utilisant le fichier **more system: running-config**. Pour récupérer la clé d'authentification AAA en format texte clair, suivez les étapes ci-dessous :

  Remarque Ces étapes devraient être effectuées à l'extérieur de l'outil de migration Secure Firewall

  1. Connectez-vous à l'ASA via la console SSH.
  2. Entrez la commande *more system:running-config* .
  3. Allez à la section **aaa-server et utilisateur local**pour trouver toute la configuration AAA et les valeurs de clé respectives en format texte clair.

```
ciscoASA#more system:running-config

!

aaa-server Test-RADIUS (inside) host 2.2.2.2

 key <key in clear text>     <-----The radius key is now displayed in clear text
format.

aaa-server Test-LDAP (inside) host 3.3.3.3

ldap-login-password <Mot de passe en clair> <-----Le mot de passe LDAP/AD/LDAPS est
désormais affiché en clair.

username Test_User password <Password in clear text> <-----The Local user
        password is shown in clear text.
```

  Remarque Si le mot de passe de l'utilisateur local est crypté, vous pouvez vérifier en interne le mot de passe ou en configurer un nouveau dans l'outil de migration Secure Firewall.

- LDAPS nécessite le domaine dans le centre de gestion. Vous devez mettre à jour le domaine pour le type de chiffrement LDAPS.
- Le domaine unique primaire AD est requis pour centre de gestion sur un serveur AD. Si un domaine unique est identifié, il sera affiché sur l'outil de migration Secure Firewall. S'il y a conflit, vous devez saisir un domaine primaire AD unique pour transférer avec succès les objets

  Pour un serveur AAA avec le chiffrement réglé à LDAPS, ASA supporte l'adresse IP et le nom d'hôte ou le domaine mais le centre de gestion prend en charge seulement le nom d'hôte ou le domaine. Si la configuration ASA contient le nom d'hôte ou le domaine, celui-ci est récupéré et affiché. Si la configuration de l'ASA contient l'adresse IP pour LDAPS, entrez un domaine dans la section **AAA**sous **VPN d'accès à distance** . Vous devez saisir le domaine qui peut être résolu à l'adresse IP du serveur AAA.

  Pour les serveurs AAA de type AD (le type de serveur est Microsoft dans la configuration de l'ASA), le **domaine primaire AD** est un champ obligatoire à configurer sur un centre de gestion. Ce champ n'est pas configuré séparément sur l'ASA et est extrait de la configuration LDAP-base-dn sur l'ASA.

```
Si le ldap-base-dn est : ou=Test-Ou,dc=gcevpn,dc=com
```

Le **domaine primaire AD** est le champ commençant par dc, avec dc=gcevpn et dc=com qui forme le domaine primaire. Le domaine primaire AD serait gcevpn.com.

Fichier exemple de LDAP-base-dn :

```
cn=asa,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:
```

Ici, dc=abec, et dc=com seraient combinés comme abc.com pour former le domaine primaire AD.

```
cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:
```

Le domaine primaire AD est fwsecurity.cisco.com.

Le domaine primaire AD est récupéré automatiquement et affiché sur l'outil de migration Secure Firewall.

Remarque La valeur du domaine primaire AD doit être unique pour chaque objet Realm. En cas où un conflit serait détecté ou si l'outil de migration Firewall est incapable de trouver la valeur dans la configuration ASA, vous devez saisir un domaine primaire AD pour le serveur spécifique. Saisissez le domaine primaire AD pour valider la configuration.

- **Ensemble des adresses -** Tous les ensembles IPv4 et IPv6 sont affichés ici.
- **Stratégies de groupe** - Cette section affiche les stratégies de groupe avec les profils de client, les profils de gestion, les modules de client et les stratégies de groupe sans profils. Si le profil a été ajouté dans la section du fichier AnyConnect, il est affiché tel que pré-sélectionné. Vous pouvez choisir ou enlever le profil d'utilisateur, le profil de gestion et le profil de module de client.

  L'attribut personnalisé lié à la politique de groupe spécifique est affiché dans l'onglet **Attribut personnalisé AnyConnect**. Vous pouvez choisir l'attribut personnalisé et le valider.
- **Profil de connexion** - Tous les profils de connections/groupes tunnels sont affichés ici.
- **Point de confiance** - La migration des points de confiance ou objets PKI de l'ASA vers le centre de gestion fait partie de l'activité de pré-migration et est nécessaire à la réussite de la migration du VPN AD. Mettez en correspondance le point de confiance pour Global SSL, IKEv2 et l'interface dans la section **Interface d'accès à distance** pour passer aux étapes suivantes de la migration. Les points de confiance Global SSL et IKEv2 sont obligatoires si le protocole LDAPS est activé. Si un objet SAML existe, les points de confiance pour SAML IDP et SP peuvent être mappés dans la section SAML. Le certificat SP est facultatif. Le point de confiance peut également être modifié pour un groupe de tunnels spécifique. Si la configuration du point de confiance SAML outrepassé est disponible dans l'ASA source, elle peut être sélectionnée dans l'option **Passer outre SAML**.

  Pour plus d'informations sur l'exportation de certificats PKI à partir d'ASA, voir Exporter le certificat PKI à partir d'ASA et l'importer dans le centre de gestionet l'importer dans ce dernier.
- **Cartes de certificats -** Les cartes de certificats sont affichées ici.
- **Équilibrage de la charge VPN** - Les configurations d'équilibrage de la charge VPN sont affichées ici.

  Pour l'équilibrage de charge VPN, l'outil de migration Secure Firewall récupère la clé de chiffrement si la configuration **more system : running-config** est téléchargée. Vous pouvez mettre à jour manuellement la clé de chiffrement en utilisant **Actions** > **Mettre à jour les clés**

Étape 8 (Facultatif) Pour télécharger les détails pour chaque élément de configuration dans la grille, cliquez sur **Télécharger**.

Étape 9 Après avoir complété votre examen, cliquez sur **Valider**.

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 10 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.

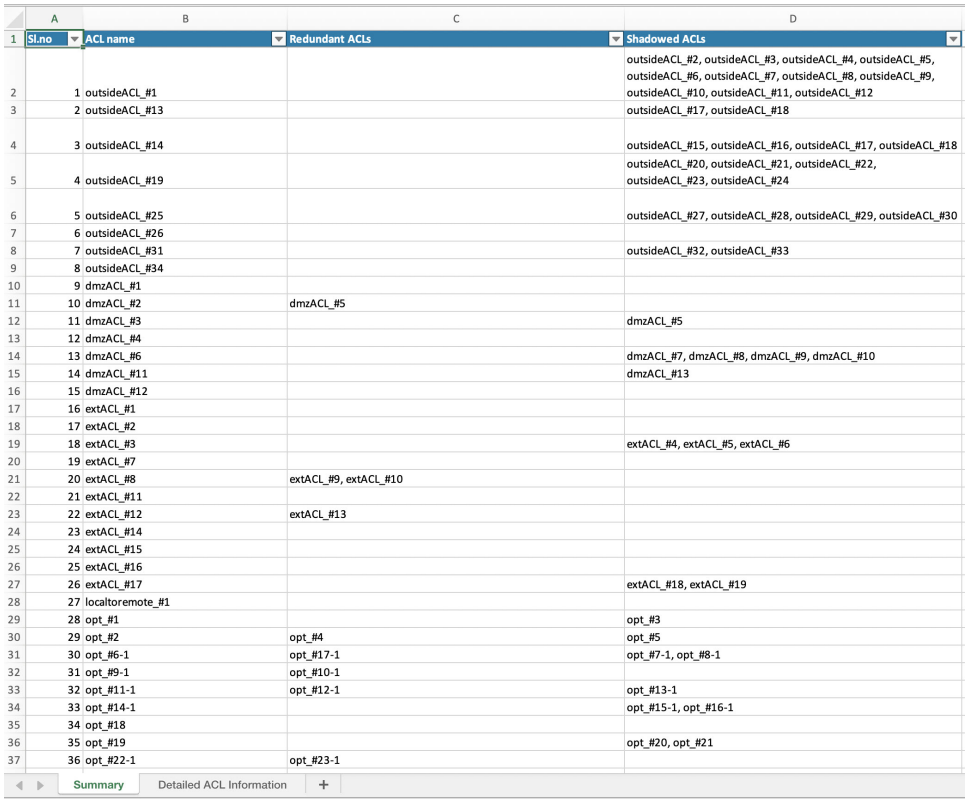
e) Cliquez sur **Résoudre**
f) Lorsque vous avez résolu tous les conflits d'objet sur un onglet, cliquez sur **Sauvegarder**
g) Cliquez sur **Valider**pour revalider la confirmation et confirmer que vous avez résolu tous les conflits d'objet.

Étape 11 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 28

Création de rapports pour l'optimisation d'ACL

Le rapport d'optimisation ACL affiche les informations suivantes :

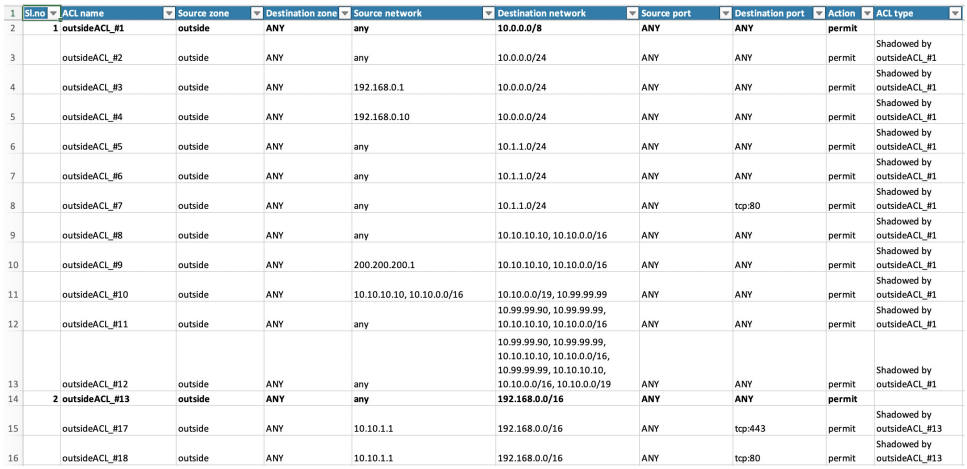
- Feuille de résumé - Affiche le résumé de l'optimisation ACL.



Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
2	outsideACL_#13		outsideACL_#17, outsideACL_#18
3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
6	outsideACL_#26		
7	outsideACL_#31		outsideACL_#32, outsideACL_#33
8	outsideACL_#34		
9	dmzACL_#1		
10	dmzACL_#2	dmzACL_#5	
11	dmzACL_#3		dmzACL_#5
12	dmzACL_#4		
13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
14	dmzACL_#11		dmzACL_#13
15	dmzACL_#12		
16	extACL_#1		
17	extACL_#2		
18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
19	extACL_#7		
20	extACL_#8	extACL_#9, extACL_#10	
21	extACL_#11		
22	extACL_#12	extACL_#13	
23	extACL_#14		
24	extACL_#15		
25	extACL_#16		
26	extACL_#17		extACL_#18, extACL_#19
27	localtoremote_#1		
28	opt_#1		opt_#3
29	opt_#2	opt_#4	opt_#5
30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
31	opt_#9-1	opt_#10-1	
32	opt_#11-1	opt_#12-1	opt_#13-1
33	opt_#14-1		opt_#15-1, opt_#16-1
34	opt_#18		
35	opt_#19		opt_#20, opt_#21
36	opt_#22-1	opt_#23-1	

Summary | Detailed ACL Information

- Informations détaillées ACL - Affiche les détails de l'ACL de base. Chaque ACL vient avec une étiquette de type d'ACL (Ombre ou Redondant) pour identifier l'ACL de base pour comparaison et son association avec la catégorie d'optimisation.



Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	**outsideACL_#1**	**outside**	**ANY**	**any**	**10.0.0.0/8**	**ANY**	**ANY**	**permit**	
	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#12	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
2	**outsideACL_#13**	**outside**	**ANY**	**any**	**192.168.0.0/16**	**ANY**	**ANY**	**permit**	
	outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

Transférer la configuration migrée vers Centre de gestion

Vous ne pouvez pas pousser la configuration de l'ASA 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.

Procédure

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 ASA à centre de gestion.

La nouvelle fonctionnalité d'optimisation de l'outil de migration Secure Firewall vous permet d'obtenir rapidement les résultats de la migration à l'aide des filtres de recherche.

L'outil de migration Secure Firewall permet également d'optimiser le téléchargement des fichiers CSV et d'appliquer les actions par page ou sur toutes les règles.

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 et valider la configuration, à la page 21

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.

Procédure

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 ASA a été migrée :

- **Résumé de la migration** - Résumé de la configuration qui a été migrée avec succès de l'ASA de vers Défense contre les menaces, y compris des informations sur ASA , centre de gestionle nom d'hôte et le domaine, le dispositifDéfense 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 l'ASA 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 l'ASA 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 interfaces de la

configuration de l'ASA du vers les interfaces du dispositif de défense contre les menaces. 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 d'interface source vers les zones de sécurité et les groupes d'interfaces de défense contre les menaces** - Détails des interfaces logiques et des noms des ASA du migrés avec succès et comment vous les avez mappés vers les zones de sécurité et les groupes d'interfaces 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 l'ASA 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 l'ASA 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 ASA 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 ASA de qui ont été étendues d'une seule ASArègle de point en plusieurs règles Défense contre les menaces au 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 l'ASA 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 les règles de politique de contrôle d'accès de l'ASA 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' ASA 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 d'accès de l'ASA 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.
- **Règles de contrôle d'accès qui ont échoué la recherche** de zone- Détails des règles de contrôle d'accès de l' de qui échouent à l'opération Recherche de route et qui sont renseignées dans le**rapport de post-migration**. L'outil de migration Secure Firewall effectue l'opération de recherche de route sur la base des informations de route (statique et connectée) dans la configuration source pour remplir les zones de sécurité de destination dans les règles d'accès.
- **Règles de contrôle d'accès pour les protocoles tunnellisés** - Détails des règles tunnellisées qui sont migrées en tant que règles tunnellisées de préfiltrage lors de la migration.

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 des ASA que vous devez migrer manuellement sur le dispositif de défense contre les menaces.

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 IP SLA
- Recherche groupée d’objets

- Objets temporels
- Objets VPN
- Tunnels de réseau privé virtuel (VPN) de site à site
- 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 défense contre 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 l'ASA de .

Désinstaller l'outil de migration Secure Firewall

Tous les composants sont stockés dans le même dossier que l'outil de migration Secure Firewall.

Procédure

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 : ASA 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.

Procédure

Étape 1 Utilisez la commande show **running-config** pour le ou le contexte que vous migrez et enregistrez une copie de la configuration du . Voir Afficher la configuration en cours d'éxécution.

Vous pouvez également utiliser Adaptive Security Device Manager (ASDM) pour le dispositif ou le contexte que vous souhaitez migrer et choisir **Fichier > Afficher la configuration en cours d'exécution dans une nouvelle fenêtre**pour obtenir le fichier de configuration.

Remarque Pour un contexte multiple, vous pouvez utiliser la commande **show tech-support** pour obtenir la configuration de tous les contextes dans un seul fichier.

Étape 2 Examinez le fichier de configuration d'ASA.

Étape 3 DéployezSérie Firepower 2100 l'appareil 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 4 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 5 (Facultatif) Si la configuration du dispositif géré par le des canaux de port, créez des canaux de port (EtherChannels) sur le dispositif cibleSérie Firepower 2100.

Pour plus d'informations, consultez Configurez des EtherChannels et les interfaces redondantes.

Étape 6 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 3.

Étape 7 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 11.

Étape 8 Mappez les interfaces ASA les interfaces avec les interfaces Défense contre les menaces.

Remarque L'outil de migration Secure Firewall vous permet de mapper un type d'interface au type di'interface de défense contre les menaces.

Par exemple, vous pouvez mapper un canal de port dans un à une interface physique dans Défense contre les menaces.

Pour plus d'informations, voir Mapper les configurations ASA aux interfaces de défense contre les menaces de Secure Firewall Device Manager.

Étape 9 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 l'ASA aux zones de sécurité.

Pour plus d'informations, voir Mapper les interfaces ASA à des zones de sécurité et à des groupes d'interfaces.

Étape 10 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 11 Examinez le rapport post-migration, installez manuellement et déployez les autres configurations vers défense contre les menance et complétez la migration.

Pour plus de renseignements, consultez la section Examiner le rapport de post-migration et terminer la migration, à la page 30.

Étape 12 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 34.

Procédure

Étape 1 Connectez-vous au via la console SSH et changez pour le mode de configuration d'interface.

Étape 2 Arrêtez les interfaces du à l'aide de la commande **shutdown.**

Étape 3 (Facultatif) Accédez au centre de gestion et configurez le routage dynamique pour le dispositif Série Firepower 2100.

Pour plus d'informations, référez-vous à Routage dynamique

Étape 4 Effacez le cache du protocole de résolution d'adresses (ARP) sur l'infrastructure de commutation environnante

Étape 5 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 6 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 7 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 l'ASA , 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 8 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.

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.