Certificats

- Exigences et conditions préalables pour les certificats, à la page 1
- Lignes directrices et limites des certificats VPN Cisco Secure Firewall Threat Defense, à la page 1
- Gestion des certificats Défense contre les menaces, à la page 2
- Installation d’un certificat à l’aide de l’inscription autosignée , à la page 6
- Installation d'un certificat à l’aide de l’inscription EST, à la page 6
- Installation d’un certificat à l’aide de l’inscription SCEP, à la page 7
- Installation d’un certificat à l’aide de l’inscription manuelle, à la page 8
- Installation d’un certificat à l’aide d’un fichier PKCS12, à la page 9
- Dépannage des certificats Défense contre les menaces, à la page 9
- Historique pour les certificats, à la page 10

Exigences et conditions préalables pour les certificats

Domaines pris en charge

N’importe quel

Rôles utilisateur

Admin

Administrateur de réseau

Lignes directrices et limites des certificats VPN Cisco Secure Firewall Threat Defense

- Lorsqu’un objet d’inscription de PKI est associé à un périphérique , puis installé sur celui-ci, le processus d’inscription de certificat démarre immédiatement. Le processus est automatique pour les types d’inscriptions autosigné et SCEP; il ne nécessite aucune action supplémentaire de la part de l’administrateur. L’inscription manuelle de certificats nécessite une intervention de l’administrateur.

- Lorsque l'inscription du certificat est terminée, un point de confiance (Trustpoint) existe sur le périphérique avec le même nom que Objets d'Inscription du certificat. Utilisez ce point de confiance dans la configuration de votre méthode d'authentification VPN.
- Les périphériques défense contre les menaces prennent en charge l'inscription de certificats à l'aide du service de l'autorité de certification Microsoft et des services de l'autorité de certification fournis sur les périphériques de sécurité adaptatifs Cisco (ASA) et le routeur Cisco IOS.
- Les périphériques défense contre les menaces ne peuvent pas être configurés en tant qu'autorité de certification (CA).

Directives pour la gestion des certificats entre domaines et périphériques

- L'inscription au certificat peut être effectuée dans un domaine parent ou enfant.
- Lorsque l'inscription est effectuée à partir d'un domaine parent, l'objet d'inscription du certificat doit également se trouver dans le même domaine. Si le point de confiance d'un périphérique est remplacé dans le domaine enfant, la valeur remplacée est déployée sur le périphérique.
- Lorsque l'inscription du certificat est effectuée sur un périphérique dans un domaine enfant, l'inscription est visible pour le domaine parent ou un autre domaine enfant. En outre, l'ajout de certificats supplémentaires est possible.
- Lorsqu'un domaine enfant est supprimé, les inscriptions de certificats sur les périphériques contenus sont automatiquement supprimées.
- Une fois qu'un appareil dispose de certificats inscrits dans un domaine, il peut être inscrit dans n'importe quel autre domaine. Les certificats peuvent être ajoutés dans l'autre domaine.
- Lorsque vous déplacez un périphérique d'un domaine à un autre, les certificats sont également déplacés en conséquence. Vous recevrez une alerte pour supprimer les inscriptions sur ces périphériques.

Gestion des certificats Défense contre les menaces

Consultez Infrastructure de l'infrastructure PKI et certificats numériques pour une présentation des certificats numériques.

Consultez Objets d'Inscription du certificat pour obtenir une description des objets utilisés pour inscrire et obtenir des certificats sur les périphériques gérés.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Certificates (certificats)**.

Vous pouvez voir les colonnes suivantes pour chaque périphérique répertorié sur cet écran :

- **Name** (nom) : répertorie les périphériques auxquels des points de confiance sont déjà associés. Développez le périphérique pour voir la liste des points de confiance associés.
- **Domain** (Domaine) : affiche les certificats inscrits dans un domaine spécifique.
- **Enrollment Type** (type d'inscription) : affiche le type d'inscription utilisé pour un point de confiance (Trustpoint).

- **Status** (État) : fournit l'état du certificat de l'**autorité de certification** et **du certificat d'identité**. Vous pouvez afficher le contenu du certificat, lorsqu'il est `disponible`, en cliquant sur la loupe.

  Lorsque vous affichez les informations sur le certificat d'autorité de certification, vous pouvez afficher la hiérarchie de toutes les autorités de certification qui ont émis votre certificat d'autorité de certification.

  Si l'inscription échoue, cliquez sur l'état pour afficher le message d'échec.

- Cliquez sur **Enable weak-crypto** à droite pour activer l'utilisation du chiffrement faible dans les certificats. Lorsque vous cliquez sur le bouton à bascule, vous recevez un avertissement à confirmer avant d'activer les chiffrements faibles. Cliquez sur **Yes** (oui) pour activer les chiffrements faibles.

  Remarque Lorsqu'une inscription de certificat échoue en raison de l'utilisation du chiffrement faible, vous recevez un message pour activer ce chiffrement. Vous pouvez choisir d'activer le chiffrement faible lorsque vous devez spécifiquement l'utiliser.

- La colonne supplémentaire répertorie les icônes permettant d'effectuer les tâches suivantes :
  - **Export Certificate**(exporter le certificat) : cliquez pour exporter et télécharger une copie du certificat. Vous pouvez choisir d'exporter au format PKCS12 (chaîne complète de certificats) ou PEM (certificat d'identité uniquement).

    Vous devez fournir une phrase secrète pour exporter un certificat PKCS12 pour importer le fichier ultérieurement.
  - **Re-Enroll certificate** (Réinscrire le certificat) : réinscrire un certificat existant.
  - **Refresh Certificate status** (Actualiser l'état du certificat) : actualiser un certificat pour synchroniser l'état du certificat du périphérique Firepower Threat Defense avec le centre de gestion Cisco Firepower Management Center.
  - **Delete certificate** (Supprimer les certificats) : pour supprimer tous les certificats associés à un point de confiance.

Étape 2 Choisissez **(+) Add** pour associer et installer un objet d'inscription sur un périphérique.

Lorsqu'un objet d'inscription de certificat est associé à un périphérique, puis installé sur celui-ci, le processus d'inscription de certificat démarre immédiatement. Le processus est automatique pour les inscriptions de type autosigné et SCEP, ce qui signifie qu'il ne nécessite aucune action supplémentaire de l'administrateur. L'inscription manuelle de certificats nécessite une action supplémentaire de l'administrateur.

Remarque L'inscription d'un certificat sur un périphérique ne bloque pas l'interface utilisateur, et le processus d'inscription s'exécute en arrière-plan, ce qui permet à l'utilisateur d'effectuer l'inscription de certificat sur d'autres périphériques en parallèle. La progression de ces opérations parallèles peut être surveillée sur la même interface utilisateur. Les icônes respectives affichent l'état d'inscription du certificat.

Sujets connexes

Installation d'un certificat à l'aide de l'inscription autosignée , à la page 6
Installation d'un certificat à l'aide de l'inscription SCEP, à la page 7
Installation d'un certificat à l'aide de l'inscription manuelle, à la page 8
Installation d'un certificat à l'aide d'un fichier PKCS12, à la page 9

Mettre automatiquement à jour les offres groupées d'autorité de certification

Vous pouvez configurer le centre de gestion pour mettre à jour automatiquement les certificats d'autorité de certification à l'aide des commandes de l'interface de ligne de commande. Par défaut, les certificats d'autorité de certification sont automatiquement mis à jour lors de l'installation ou de la mise à niveau vers la version 7.0.5.

Remarque Dans un déploiement uniquement IPv6, la mise à jour automatique des certificats d'autorité de certification peut échouer, car certains serveurs Cisco ne prennent pas en charge IPv6. Dans ce cas, forcez la mise à jour des certificats d'autorité de certification à l'aide de la commande **configure cert-update run-now force**.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de la FMC à l'aide de SSH ou, si elle est virtuelle, ouvrez la console de la machine virtuelle.

Étape 2 Vous pouvez vérifier si les certificats d'autorité de certification du système local sont les plus récents ou non :

configure cert-update test

Cette commande compare le groupe d'autorités de certification du système local avec le dernier groupe d'autorités de certification (du serveur Cisco). Si l'ensemble d'autorités de certification est à jour, aucune vérification de connexion n'est exécutée et le résultat du test s'affiche comme suit :

Exemple :

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Si l'ensemble d'autorités de certification est périmé, la vérification de la connexion est exécutée sur le lot d'autorités de certification téléchargé, et le résultat du test est affiché.

Exemple :

En cas d'échec de la vérification de la connexion :

```
> configure cert-update test
Test failed, not able to fully connect.
```

Exemple :

Lorsque la vérification de la connexion est réussie ou que le groupe de l'autorité de certification est déjà à jour :

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Étape 3 (Facultatif) Pour mettre à jour instantanément les groupes d'autorités de certification :

configure cert-update run-now

Exemple :

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

Lorsque vous exécutez cette commande, la connectivité SSL est vérifiée sur les certificats de l'autorité de certification (du serveur Cisco). Si la vérification de la connectivité SSL échoue même pour un des serveurs Cisco, le processus est interrompu.

Exemple :

```
> configure cert-update run-now
Certs failed some connection checks.
```

Pour procéder à la mise à jour malgré les échecs de connexion, utilisez le mot-clé **force**.

Exemple :

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

Étape 4 Si vous ne souhaitez pas que les groupes d'autorités de certification soient automatiquement mis à jour, désactivez la configuration :

configure cert-update auto-update disable

Exemple :

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

Étape 5 Pour réactiver la mise à jour automatique des groupes d'autorités de certification :

configure cert-update auto-update enable

Exemple :

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

Lorsque vous activez la mise à jour automatique sur les certificats d'autorité de certification, le processus de mise à jour est exécuté quotidiennement à une heure définie par le système.

Étape 6 (Facultatif) Affichez l'état de la mise à jour automatique des certificats d'autorité de certification :

show cert-update

Exemple :

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

Installation d'un certificat à l'aide de l'inscription autosignée

Procédure

Étape 1 Sur l'écran **Devices > Certificates** (Périphériques > certificats), choisissez **Add** (ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (Ajouter un nouveau certificat).

Étape 2 Sélectionnez un périphérique dans la liste **Devices** (Périphériques).

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez un objet d'inscription de certificat du type Auto-signé dans la liste déroulante.
- Cliquez sur **(+)**pour ajouter un nouvel objet d'inscription de certificat, voir Ajout d'objets d'Inscription du certificat.

Étape 4 Appuyez sur **Add** (ajouter) pour lancer le processus d'inscription automatique autosigné.

Pour les points de confiance de type inscription autosignés, l'état du certificat de l' **autorité de certification** sera toujours affiché, car le périphérique géré agit comme sa propre autorité de certification et n'a pas besoin d'un certificat d'autorité de certification pour générer son propre certificat d'identité.

Le **certificat d'identité** ira de En cours à Disponible pendant que le périphérique crée son propre certificat d'identité autosigné.

Étape 5 Cliquez sur la loupe pour afficher le certificat d'identité autosigné créé pour ce périphérique.

Prochaine étape

Une fois l'inscription terminée, un point de confiance (Trustpoint) existe sur le périphérique avec le même nom que l'objet d'inscription de certificat. Utilisez ce point de confiance dans la configuration de votre méthode d'authentification VPN de site à site et d'accès à distance

Installation d'un certificat à l'aide de l'inscription EST

Avant de commencer

Remarque L'utilisation de l'inscription EST établit une connexion directe entre le périphérique géré et le serveur d'autorité de certification. Assurez-vous donc que votre périphérique est connecté au serveur CA avant de commencer le processus d'inscription.

Remarque La capacité d'EST à inscrire automatiquement un périphérique à l'expiration de son certificat n'est pas prise en charge.

Procédure

Étape 1 Dans l'écran **Devices – Certificates** (périphériques – certificats), cliquez sur **Add** (Ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (ajouter un nouveau certificat).

Étape 2 Sélectionnez un périphérique dans la liste **Devices** (Périphériques).

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez l'objet d'inscription de certificat EST dans la liste déroulante **Cert Enrollment** (Inscription de certificat).
- Cliquez sur **(+)**pour ajouter un nouveau Objets d'Inscription du certificat, consultez Ajout d'objets d'Inscription du certificat.

Étape 4 Cliquez sur **Add** (Ajouter) pour inscrire le certificat sur le périphérique.

Le **certificat d'identité** passera de `En cours` à `Disponible` pendant que le périphérique obtiendra son certificat d'identité à l'aide d'EST de l'autorité de certification spécifiée. Parfois, une actualisation manuelle peut être requise pour obtenir le certificat d'identité.

Étape 5 Cliquez sur la loupe pour afficher le certificat d'identité créé et installé sur ce périphérique.

Installation d'un certificat à l'aide de l'inscription SCEP

Avant de commencer

Remarque L'inscription SCEP établit une connexion directe entre le périphérique géré et le serveur d'autorité de certification. Assurez-vous donc que votre périphérique est connecté au serveur CA avant de commencer le processus d'inscription.

Procédure

Étape 1 Sur l'écran **Devices > Certificates** (Périphériques > certificats), choisissez **Add** (ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (Ajouter un nouveau certificat).

Étape 2 Sélectionnez un périphérique dans la liste **Devices** (Périphériques).

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez un objet d'inscription de certificat de type SCEP dans la liste déroulante.
- Cliquez sur **(+)**pour ajouter un nouvel objet d'inscription de certificat, voir Ajout d'objets d'Inscription du certificat.

Étape 4 Appuyez sur **Add**(ajouter) pour lancer le processus d'inscription automatique.

Pour les points de confiance de type d'inscription SCEP, l'état du certificat de l' **autorité de certification** passera de En cours à Disponible, car le certificat d'autorité de certification est obtenu auprès du serveur de l'autorité de certification et installé sur le périphérique.

Le **certificat d'identité** passera de `InProgress` (En cours) à `Available` (Disponible) lorsque le périphérique obtiendra son certificat d'identité à l'aide du SCEP de l'autorité de certification précisée. Parfois, une actualisation manuelle peut être requise pour obtenir le certificat d'identité.

Étape 5 Cliquez sur la loupe pour afficher le certificat d'identité créé et installé sur ce périphérique.

Prochaine étape

Une fois l'inscription terminée, un point de confiance (Trustpoint) existe sur le périphérique avec le même nom que l'objet d'inscription de certificat. Utilisez ce point de confiance dans la configuration de votre méthode d'authentification VPN de site à site et d'accès à distance

Installation d'un certificat à l'aide de l'inscription manuelle

Procédure

Étape 1 Sur l'écran **Devices > Certificates** (Périphériques > certificats), choisissez **Add** (ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (Ajouter un nouveau certificat).

Étape 2 Sélectionnez un périphérique dans la liste **Devices** (Périphériques).

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez un objet d'inscription de certificat de type Manuel dans la liste déroulante.
- Cliquez sur **(+)**pour ajouter un nouvel objet d'inscription de certificat, voir Ajout d'objets d'Inscription du certificat.

Étape 4 Appuyez sur **Add** (Ajouter) pour commencer le processus d'inscription.

Étape 5 Exécutez l'activité appropriée avec votre serveur d'autorité de certification PKI pour obtenir un certificat d'identité.

a) Cliquez sur **Identity Certificate** (certificat d'identité) afin d'afficher et de copier la requête de signature de certificat (CSR).

b) Exécutez l'activité appropriée avec votre serveur d'autorité de certification PKI pour obtenir un certificat d'identité utilisant cette requête de signature de certificat (CSR).

Cette activité est complètement indépendante du Cisco Secure Firewall Management Center ou du périphérique géré. Une fois terminé, vous obtiendrez un certificat d'identité pour le périphérique géré. Vous pouvez le placer dans un fichier.

c) Pour terminer le processus manuel, installez le certificat d'identité obtenu sur le périphérique géré.

Revenez à la boîte de dialogue Cisco Secure Firewall Management Center et sélectionnez **Browse Identity Certificate** (Parcourir le certificat d'identité) pour choisir le fichier de certificat d'identité.

Étape 6 Sélectionnez **Import** pour importer le certificat d'identité.

L'état du certificat d'identité sera `Availalble` (Disponible) une fois l'importation terminée.

Étape 7 Cliquez sur la loupe pour afficher le **certificat d'identité** de ce périphérique.

Prochaine étape

Une fois l'inscription terminée, un point de confiance (Trustpoint) existe sur le périphérique avec le même nom que l'objet d'inscription de certificat. Utilisez ce point de confiance dans la configuration de votre méthode d'authentification VPN de site à site et d'accès à distance

Installation d'un certificat à l'aide d'un fichier PKCS12

Procédure

Étape 1 Accédez à l'écran **Devices > Certificates** (périphériques > Certificats), choisissez **Add** (ajouter) pour ouvrir la boîte de dialogue **Add New Certificate** (ajouter un nouveau certificat).

Étape 2 Choisissez un périphérique géré préconfiguré dans la liste déroulante des **périphériques**.

Étape 3 Associez un objet d'inscription de certificat à cet appareil de l'une des manières suivantes :

- Choisissez un type PKCS Objets d'Inscription du certificat dans la liste déroulante.
- Cliquez sur **(+)**pour ajouter un nouveau Objets d'Inscription du certificat, consultez Ajout d'objets d'Inscription du certificat.

Étape 4 Appuyez sur **Add**(ajouter).

L'état du certificat de l'autorité de certification et du certificat d'identité passe de `En cours` à `Disponible` , au fur et à mesure qu'il installe le fichier PKCS12 sur le périphérique.

Remarque Lorsque vous téléversez le fichier PKCS12 pour la première fois, celui-ci est stocké dans le centre de gestion Cisco Firepower Management Center dans le cadre de l'objet CertEnrollment. Pour toute inscription ayant échoué en raison d'une phrase secrète incorrecte ou d'un échec de déploiement, réessayez d'inscrire le certificat PKCS12 sans téléverser à nouveau le fichier. La taille de fichier PKCS12 ne doit pas dépasser 24 Ko.

Étape 5 Une fois l'état `disponible` affiché, cliquez sur la loupe pour afficher le certificat d'identité de cet appareil.

Prochaine étape

Le certificat (point de confiance) du périphérique géré porte le même nom que le fichier PKCS12. Utilisez ce certificat dans votre configuration d'authentification VPN.

Dépannage des certificats Défense contre les menaces

Consultez Lignes directrices et limites des certificats VPN Cisco Secure Firewall Threat Defense, à la page 1 pour déterminer si les variations dans votre environnement d'inscription de certificat peuvent être à l'origine d'un problème. Considérez ensuite les éléments suivants :

- Assurez-vous qu'il existe une voie de routage vers le serveur d'autorité de certification à partir du périphérique.

Si le nom d'hôte du serveur de l'autorité de certification est indiqué dans l'objet d'inscription, utilisez Flex Config pour configurer le DNS correctement afin d'atteindre le serveur. Vous pouvez également utiliser l'adresse IP du serveur de l'autorité de certification.

- Si vous utilisez un serveur d'autorité de certification Microsoft 2012, le modèle IPsec par défaut n'est pas accepté par le périphérique géré et doit être modifié.

  Pour configurer un modèle fonctionnel, suivez ces étapes en utilisant la documentation de MS CA comme référence.

  1. Dupliquez le modèle IPsec (Offline Request).
  2. Dans **Extensions > Politiques d'application**, sélectionnez *Système final de sécurité IP*, plutôt que *Sécurité IP IKE en amont*.
  3. Définissez les autorisations et le nom du modèle.
  4. Ajoutez le nouveau modèle et modifiez les paramètres du registre pour refléter le nouveau nom du modèle.

- Sur le centre de gestion, vous pourriez recevoir l'alerte d'intégrité suivante liée au périphérique défense contre les menaces :

  ```
  Code – F0853; Description : le certificat par défaut du trousseau de clés n'est pas
  valide. Raison : expiré
  ```

  Dans ce cas, utilisez la commande suivante pour régénérer le certificat par défaut dans la CLI CLISH :

  ```
  > system support regenerate-security-keyring default
  ```

Historique pour les certificats

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Améliorations apportées à l'inscription manuelle	6.7	N'importe lequel	Vous pouvez désormais créer uniquement un certificat d'autorité de certification, sans certificat d'identité. Vous pouvez également générer une requête de signature de certificat (CSR) sans certificat d'autorité de certification et obtenir un certificat d'identité de l'autorité de certification.
Chaîne d'autorité de certification PKCS	6.7	N'importe lequel	Vous pouvez afficher et gérer la chaîne des autorités de certification (AC) qui délivrent vos certificats. Vous pouvez également exporter une copie des certificats.

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.