Certificats

Les certificats numériques fournissent une identification numérique aux fins d'authentification. Les certificats sont utilisés pour les connexions SSL (Secure socket Layer), TLS (Transport Layer Security) et DTLS (Datagram TLS), comme HTTPS et LDAPS. Les rubriques suivantes expliquent comment créer et gérer les certificats.

Certificats

Les certificats numériques fournissent une identification numérique aux fins d'authentification. Un certificat numérique contient des renseignements permettant d'identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l'entreprise, le service ou l'adresse IP. Un certificat numérique comprend également une copie de la clé publique de l'utilisateur ou du périphérique. Les certificats sont utilisés pour les connexions SSL (Secure socket Layer), TLS (Transport Layer Security) et DTLS (Datagram TLS), comme HTTPS et LDAPS.

Vous pouvez créer les types de certificat suivants :

- Certificats internes : les certificats d'identité internes sont des certificats pour des systèmes ou des hôtes spécifiques. Vous pouvez les générer vous-même à l'aide de la boîte à outils OpenSSL ou les obtenir auprès d'une autorité de certification. Vous pouvez également générer un certificat autosigné. Lorsque les certificats internes expirent ou deviennent non valides pour une raison quelconque, vous pouvez les régénérer à partir de la commande CLI CLISH suivante :

```
> system support regenerate-security-keyring
  String  Certificate to be regenerated, default or fdm
```

- Certificats d'autorité de certification (CA) internes : les certificats d'autorité de certification internes sont des certificats que le système peut utiliser pour signer d'autres certificats. Ces certificats varient des certificats d'identité internes en ce qui concerne l'extension des contraintes de base et l'indicateur de l'autorité de certification, qui sont activés pour les certificats d'autorité de certification mais désactivés pour les certificats d'identité. Vous pouvez les générer vous-même à l'aide de la boîte à outils OpenSSL ou les obtenir auprès d'une autorité de certification. Vous pouvez également générer un certificat d'autorité de certification interne autosigné. Si vous configurez des certificats d'autorité de certification internes autosignés, l'autorité de certification s'exécute sur le périphérique lui-même.

- Un certificat d'une autorité de certification de confiance (CA) est utilisé pour signer d'autres certificats. Il est autosigné et appelé certificat racine. Un certificat émis par un autre certificat CA s'appelle un certificat subordonné.

Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur. Les autorités de certification délivrent des certificats numériques dans le cadre d'une PKI, qui utilise le chiffrement par clé publique ou privée pour assurer la sécurité. Une autorité de certification peut être un tiers de confiance, tel que VeriSign, ou une autorité de certification privée (interne) que vous établissez dans votre organisation. Les autorités de certification sont chargées de gérer les demandes de certificats et d'émettre des certificats numériques. Pour en savoir plus, consultez Cryptographie à clé publique, à la page 2.

Cryptographie à clé publique

Dans le chiffrement à clé publique, comme le système de chiffrement RSA, chaque utilisateur dispose d'une paire de clés contenant une clé publique et une clé privée. Les clés agissent comme des compléments, et tout ce qui est chiffré avec l'une des clés peut être déchiffré avec l'autre.

En termes simples, une signature se forme lorsque les données sont chiffrées avec une clé privée. La signature est jointe aux données et envoyée au récepteur. Le récepteur applique la clé publique de l'expéditeur aux données. Si la signature envoyée avec les données correspond au résultat de l'application de la clé publique aux données, la validité du message est établie.

Ce processus repose sur le récepteur ayant une copie de la clé publique de l'expéditeur et sur un degré élevé de confiance que cette clé appartient à l'expéditeur, et non à une personne se faisant passer pour l'expéditeur.

L'obtention de la clé publique d'un expéditeur est normalement gérée en externe ou par le biais d'une opération effectuée lors de l'installation. Par exemple, la plupart des navigateurs Web sont configurés avec les certificats racine de plusieurs autorités de certification par défaut.

Vous pouvez en savoir plus sur les certificats numériques et le chiffrement à clé publique en vous rendant sur openssl.org, sur Wikipedia ou d'autres sources. Une bonne compréhension du chiffrement SSL/TLS vous aidera à établir des connexions sécurisées avec votre périphérique.

Types de certificats utilisés par fonctionnalité

Vous devez créer le bon type de certificat pour chaque fonctionnalité. Les fonctionnalités suivantes nécessitent des certificats.

Politiques d'identité (Identity Policies, portail captif) : certificat interne

(Facultatif) Le portail captif est utilisé dans les politiques d'identité. Les utilisateurs doivent accepter ce certificat lors de l'authentification à l'appareil afin de s'identifier et d'associer leur adresse IP à leur nom d'utilisateur. Si vous ne fournissez pas de certificat, l'appareil utilise un certificat généré automatiquement.

Identité du domaine (politiques d'identité et VPN d'accès distant) : Certificat de l'autorité de certification de confiance

(Facultatif) Si vous utilisez une connexion cryptée pour votre serveur d'annuaire, le certificat doit être accepté pour effectuer l'authentification avec le serveur d'annuaire. Les utilisateurs doivent s'authentifier lorsque les politiques VPN d'identité et d'accès à distance le demandent. Un certificat n'est pas nécessaire si vous n'utilisez pas le chiffrement pour le serveur d'annuaire.

Serveur Web de gestion (paramètres système d'accès de gestion) : Certificat interne

(Facultatif.) Firepower Device Manager est une demande basée sur le Web, elle fonctionne donc sur un serveur Web. Vous pouvez télécharger un certificat que votre navigateur accepte comme valide pour éviter de recevoir un avertissement d'autorité non fiable.

VPN d'accès distant : Certificat interne

(Requis) Le certificat interne est destiné à l'interface extérieure, qui établit l'identité de l'appareil pour les client AnyConnect lorsqu'ils établissent une connexion avec l'appareil. Les clients doivent accepter ce certificat.

VPN de site à site : Certificats d'autorité de certification interne et de confiance

Si vous utilisez l'authentification par certificat pour une connexion VPN de site à site, vous devez sélectionner le certificat d'identité interne utilisé pour authentifier l'homologue local dans la connexion. Bien que cela ne fasse pas partie de la définition de connexion VPN, vous devez également télécharger les certificats d'autorité de certification de confiance utilisés pour signer les certificats d'identité des homologues locaux et distants, afin que le système puisse authentifier les homologues.

SSL Decryption Policy (politique de déchiffrement SSL) : Certificats et groupes de certificats internes, d'autorité de certification interne et d'autorité de certification de confiance

(Requis) La politique de déchiffrement SSL utilise des certificats aux fins suivantes :

- Les certificats internes sont utilisés pour les règles connues de déchiffrement des clés.
- Les certificats d'autorité de certification interne sont utilisés pour déchiffrer les règles de nouvelle signature lors de la création de la session entre le client et le périphérique Cisco Firewall Threat Defense.
- Les certificats d'autorité de certification de confiance sont utilisés indirectement pour déchiffrer les règles de nouvelle signature lors de la création de la session entre le périphérique Cisco Firewall Threat Defense et le serveur. Les certificats d'autorité de certification de confiance sont utilisés pour vérifier l'autorité de signature du certificat du serveur. Vous pouvez configurer ces certificats directement ou dans un groupe de certificats dans les paramètres de politiques. Le système comprend un grand nombre de certificats d'autorité de certification de confiance, qui sont réunis dans le groupe d'autorités de confiance de Cisco. Vous n'avez donc pas besoin de télécharger de certificats supplémentaires.

Exemple : génération d'un certificat interne à l'aide d'OpenSSL

L'exemple suivant utilise les commandes OpenSSL pour générer un certificat de serveur interne. Vous pouvez obtenir OpenSSL à partir de OpenSSL.org. Consultez la documentation d'OpenSSL pour obtenir des renseignements précis. Les commandes utilisées dans cet exemple peuvent changer et vous pouvez avoir d'autres options disponibles que vous pourriez souhaiter utiliser.

Cette procédure vise à vous donner une idée de la façon d'obtenir un certificat à charger vers . Cisco Firewall Threat Defense.

Remarque Les commandes OpenSSL affichées ici ne sont que des exemples. Ajustez les paramètres en fonction de vos exigences de sécurité.

Procédure

Étape 1 Générez une clé.

```
openssl genrsa -out server.key 4096
```

Étape 2 Générez une demande de signature de certificat (CSR).

```
openssl req -new -key server.key -out server.csr
```

Étape 3 Générez un certificat autosigné avec la clé et la CSR.

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Étant donné que le Firepower Device Manager ne prend pas en charge les clés chiffrées, essayez d'ignorer le mot de passe de défi en appuyant simplement sur Entrée lors de la génération d'un certificat autosigné.

Étape 4 Chargez les fichiers dans les champs appropriés lors de la création d'un objet de certificat interne dans Firepower Device Manager.

Vous pouvez également copier/coller le contenu du fichier. Les exemples de commandes créent les fichiers suivants :

- server.crt : chargez ou collez le contenu dans le champ Server Certificate (Certificat de serveur).
- server.key : chargez ou collez le contenu dans le champ Certificate Key (Clé du certificat). Si vous avez fourni un mot de passe lors de la génération de la clé, vous pouvez la déchiffrer à l'aide de la commande suivante. Le résultat est envoyé à stdout, où vous pouvez le copier.

  ```
  openssl rsa -in server.key -check
  ```

Configurer les certificats

Firewall Threat Defense prend en charge les certificats X509 au format PEM ou DER. Utilisez OpenSSL pour générer des certificats si nécessaire, les obtenir d'une autorité de certification de confiance ou créer des certificats autosignés.

Pour en savoir plus sur ces certificats, consultez Certificats, à la page 1.

Pour en savoir plus sur le type utilisé pour chaque fonctionnalité, consultez Types de certificats utilisés par fonctionnalité, à la page 2.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de certificat lors de la modification d'une propriété de certificat en cliquant sur le lien **Create New Certificate** (Créer un certificat) affiché dans la liste des objets.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Le système est livré avec les certificats prédéfinis suivants, que vous pouvez utiliser tels quels ou remplacer.

- DefaultInternalCertificate
- DefaultWebserverCertificate
- NGFW-Default-InternalCA

Le système comprend également de nombreux certificats d'autorité de certification de confiance provenant d'autorités de certification tierces. Ceux-ci sont utilisés par les politiques de déchiffrement SSL pour les actions de déchiffrement et de réauthentification. Le groupe Cisco-Trusted-Authorities comprend tous ces certificats et est le groupe par défaut utilisé par la politique de déchiffrement SSL.

Vous pouvez cliquer sur les filtres de recherche prédéfinis pour limiter la liste aux certificats **System-defined (définis par le système)** ou **User-defined** (définis par l'utilisateur).

Vous pouvez également utiliser le filtre **Weak Key** pour trouver des certificats dont les clés sont différentes des longueurs de clé prises en charge. Les clés sont considérées comme faibles même si elles sont plus longues que les longueurs prises en charge. Nous vous recommandons de remplacer ces certificats par des certificats dont les clés ont des longueurs prises en charge. Voici les longueurs prises en charge :

- Les clés RSA peuvent être de 2 048, 3 072 ou 4 096 bits.
- Les clés ECDSA peuvent être de 256, 384 ou 521 bits.
- Les clés EDDSA peuvent être de 256 bits.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un nouvel objet de certificat, utilisez la commande pour le type de certificat dans le menu **+**.
- Pour créer un groupe de certificats, cliquez sur  et sélectionnez **Add Certificate Group** (Ajouter un groupe de certificats).
- Pour afficher ou modifier un certificat ou groupe, cliquez soit sur l'icône de modification () soit sur l'icône d'affichage () du certificat.
- Pour supprimer un certificat ou groupe non référencé, cliquez sur l'icône de la corbeille () du certificat.

Pour des informations détaillées sur la création ou la modification de certificats, consultez les rubriques suivantes :

- Charger les certificats d'identité interne et d'autorité de certification interne, à la page 6
- Génération de certificats internes autosignés et de certificats d'autorité de certification internes, à la page 7
- Téléchargement des certificats de l'autorité de certification de confiance, à la page 9

• Configuration des groupes de certificats CA de confiance, à la page 11

Charger les certificats d'identité interne et d'autorité de certification interne

Les certificats d'identité internes sont des certificats pour des systèmes ou des hôtes spécifiques.

Les certificats d'autorité de certification internes sont des certificats que le système peut utiliser pour signer d'autres certificats. Ces certificats varient des certificats d'identité internes en ce qui concerne l'extension des contraintes de base et l'indicateur de l'autorité de certification, qui sont activés pour les certificats d'autorité de certification mais désactivés pour les certificats d'identité.

Vous pouvez générer ces certificats vous-même à l'aide de la boîte à outils OpenSSL ou les obtenir auprès d'une autorité de certification, puis les télécharger en utilisant la procédure suivante. Pour obtenir un exemple de génération d'une clé, consultez Exemple : génération d'un certificat interne à l'aide d'OpenSSL, à la page 3.

Vous pouvez également générer des certificats d'identité interne et d'autorité de certification interne autosignés. Si vous configurez des certificats d'autorité de certification internes autosignés, l'autorité de certification s'exécute sur le périphérique lui-même. Pour en savoir plus sur la création de certificats autosignés, consultez Génération de certificats internes autosignés et de certificats d'autorité de certification internes, à la page 7.

Pour en savoir plus sur les fonctionnalités qui utilisent ces certificats, consultez Types de certificats utilisés par fonctionnalité, à la page 2.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur + > **Add Internal Certificate** (Ajouter un certificat interne), puis cliquez sur **Upload Certificate and Key** (Charger le certificat et la clé).
- Cliquez sur + > **Add Internal CA Certificate** (Ajouter un certificat d'autorité de certification interne), puis cliquez sur **Upload Certificate and Key** (Charger le certificat et la clé).
- Pour modifier ou afficher un certificat, cliquez sur l'icône d'information (). La boîte de dialogue affiche le sujet du certificat, l'émetteur et la période de validité. Cliquez sur Replace Certificate (Remplacer le certificat) pour charger un nouveau certificat et une nouvelle clé. Vous pouvez également coller le certificat et la clé dans la boîte de dialogue.

Étape 3 Entrez un nom (**Name**) pour le certificat.

Le nom est utilisé dans la configuration uniquement comme nom d'objet, il ne fait pas partie du certificat lui-même.

Étape 4 Cliquez sur **Upload Certificate** (Charger le certificat) (ou **Replace Certificate** (Remplacer le certificat) lors de la modification) et sélectionnez le fichier de certificat (par exemple, *.crt). Les extensions de fichier autorisées sont.pem, .cert, .cer, .crt et .der. Vous pouvez également coller le certificat.

Le certificat doit être un certificat X509 au format PEM ou DER.

Le certificat que vous collez doit inclure les lignes BEGIN CERTIFICATE et END CERTIFICATE. Par exemple :

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

Étape 5 Cliquez sur **Upload Key** (Charger la clé) (ou **Replace Key** (Remplacer la clé) lors de la modification) et sélectionnez le fichier de certificat (par exemple, *.key). L'extension du fichier doit être .key. Vous pouvez également coller la clé pour le certificat.

La clé ne peut pas être chiffrée et elle doit être une clé RSA.

Par exemple :

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQClSu1BknrMjzw/5FZ9YgdMLDUGJlbYgkjN7mVrkjyLQx2TYsem
r8iTiKB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkBhOsPs1A8e60r5mImeDrtw+
Cc0O5cSfnlTAw5CgcGkcxTCaGIZmXMkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdLqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2STlZ3jERMZd29fjIRuJ9jpFC2lIDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuv6db8Rh+7l
MUOx09tvbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

Étape 6 Cliquez sur **OK**.

Si la taille de clé est inférieure à la taille minimale que nous autorisons pour les certificats autosignés générés, vous serez averti que le certificat ne répond pas aux exigences minimales recommandées. Cliquez sur **Proceed** (Continuer) pour charger le certificat quand même, mais nous vous recommandons de créer un nouveau certificat plus fort.

Génération de certificats internes autosignés et de certificats d'autorité de certification internes

Les certificats d'identité internes sont des certificats pour des systèmes ou des hôtes spécifiques.

Les certificats d'autorité de certification internes sont des certificats que le système peut utiliser pour signer d'autres certificats. Ces certificats varient des certificats d'identité internes en ce qui concerne l'extension des contraintes de base et l'indicateur de l'autorité de certification, qui sont activés pour les certificats d'autorité de certification mais désactivés pour les certificats d'identité.

Vous pouvez générer un certificat d'identité interne autosigné et des certificats d'autorité de certification internes ; autrement dit, les certificats sont signés par le périphérique lui-même. Si vous configurez des

certificats d'autorité de certification internes autosignés, l'autorité de certification s'exécute sur le périphérique. Le système génère le certificat et la clé.

Vous pouvez également créer ces certificats à l'aide d'OpenSSL ou les obtenir d'une autorité de certification de confiance et les téléverser. Pour en savoir plus, consultez Charger les certificats d'identité interne et d'autorité de certification interne, à la page 6.

Pour en savoir plus sur les fonctionnalités qui utilisent ces certificats, consultez Types de certificats utilisés par fonctionnalité, à la page 2.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **+** > **Add Internal Certificate** (Ajouter un certificat interne), puis sur **Signed Certificate** (Certificat autosigné).
- Cliquez sur **+** > **Add Internal CA Certificate** (Ajouter un certificat d'autorité de certification interne), puis sur **Certificat autosigné**.

Remarque

Pour modifier ou afficher un certificat, cliquez sur l'icône d'information (). La boîte de dialogue affiche le sujet du certificat, l'émetteur et la période de validité. Cliquez sur **Replace Certificate** (Remplacer le certificat) pour charger un nouveau certificat et une nouvelle clé. Lors du remplacement d'un certificat, vous ne pouvez pas rétablir les caractéristiques d'autosignature expliquées dans les étapes suivantes. Au lieu de cela, vous devez coller ou charger un nouveau certificat, comme décrit dans Charger les certificats d'identité interne et d'autorité de certification interne, à la page 6. Les étapes restantes s'appliquent uniquement aux nouveaux certificats autosignés.

Étape 3 Entrez un nom (**Name**) pour le certificat.

Le nom est utilisé dans la configuration uniquement comme nom d'objet, il ne fait pas partie du certificat lui-même.

Étape 4 Configurez au moins l'un des éléments suivants pour les informations sur le sujet et l'émetteur du certificat.

- **Pays (C)** : le code du pays ISO 3166 à deux lettres à inclure dans le certificat. Par exemple, le code du pays pour les États-Unis est US. Sélectionnez le code du pays dans la liste déroulante.
- **État ou Province (ST)** : l'état ou la province à inclure dans le certificat.
- **Localité ou Ville (L)** : la localité à inclure dans le certificat, par exemple le nom de la ville.
- **Organisation (O)** : le nom de l'organisation ou de l'entreprise à inclure dans le certificat.
- **Unité organisationnelle (OU)** : le nom de l'unité organisationnelle (par exemple, le nom du service) à inclure dans le certificat.
- **Nom commun (CN)** : le nom commun X.500 à inclure dans le certificat. Il peut s'agir du nom du périphérique, du site Web ou d'une autre chaîne de texte. Cet élément est généralement requis pour la réussite des connexions. Par exemple, vous devez inclure un numéro de référence dans le certificat interne utilisé pour le VPN d'accès à distance.

- **Type de clé** : le type de clé à générer pour ce certificat : RSA, ECDSA (algorithme de signature numérique de courbe elliptique) ou EDDSA (algorithme de signature numérique de courbe Edvers).
- **Taille de la clé** : la taille de la clé à générer. En général, les clés plus longues sont plus sécurisées. Cependant, les clés dont la taille de module est plus grande prennent plus de temps à être générées et à être traitées lors de l'échange. Les tailles autorisées varient selon le type de clé.
  - Les clés RSA peuvent être de 2 048, 3 072 ou 4 096 bits.
  - Les clés ECDSA peuvent être de 256, 384 ou 521 bits.

    Les clés EDDSA peuvent être de 256 bits.
- **Période de validité** : durée pendant laquelle le certificat sera considéré comme valide. La valeur par défaut est de 825 jours à compter d'aujourd'hui, quelle que soit la façon dont vous définissez la date d'expiration. Cliquez sur **Set default** (Rétablir les valeurs par défaut) pour revenir aux valeurs par défaut. Vous pouvez configurer la période à l'aide de l'une des méthodes suivantes. Veillez à remplacer les certificats avant leur expiration.
  - **By Date** (Par date) : cliquez sur **Expiration Date** (Date d'expiration) et sélectionnez le dernier jour où le certificat doit être considéré comme valide.
  - **By Number of Days** (Par nombre de jours) : saisissez le nombre de jours, à compter d'aujourd'hui, pendant lesquels le certificat doit être considéré comme valide. Après avoir saisi le nombre, vous pouvez cliquer sur **By Date (Par date)** pour voir la date d'expiration calculée.

Étape 5 Cliquez sur **Save** (enregistrer).

Téléchargement des certificats de l'autorité de certification de confiance

Un certificat d'une autorité de certification de confiance (CA) est utilisé pour signer d'autres certificats. Il est autosigné et appelé certificat racine. Un certificat émis par un autre certificat CA s'appelle un certificat subordonné.

Pour en savoir plus sur les fonctionnalités qui utilisent ces certificats, consultez Types de certificats utilisés par fonctionnalité, à la page 2.

Obtenez un certificat d'autorité de certification de confiance auprès d'une autorité de certification externe ou créez-en un en utilisant votre propre autorité de certification interne, par exemple avec les outils OpenSSL. Ensuite, utilisez la procédure suivante pour télécharger le certificat.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **+** > **Add Trusted CA Certificate** (ajouter un certificat d'autorité de certification de confiance).
- Pour modifier un certificat, cliquez sur l'icône de modification ( ) du certificat.

Étape 3 Entrez un nom (**Name**) pour le certificat.

Le nom est utilisé dans la configuration uniquement comme nom d'objet, il ne fait pas partie du certificat lui-même.

Étape 4 Cliquez sur **Upload Certificate** (télécharger le certificat) (ou **Replace Certificate**, c.-à-d. remplacer le certificat lors de la modification) et sélectionnez le fichier de certificat d'autorité de certification (par exemple * .pem). Les extensions de fichier autorisées sont.pem, .cert, .cer, .crt et .der. Vous pouvez également coller le certificat d'autorité de certification de confiance.

Le nom du serveur dans le certificat doit correspondre au nom d'hôte/adresse IP du serveur. Par exemple, si vous utilisez 10.10.10.250 comme adresse IP mais ad.exemple.com dans le certificat, la connexion échouera.

Le certificat doit être un certificat X509 au format PEM ou DER.

Le certificat que vous collez doit inclure les lignes BEGIN CERTIFICATE et END CERTIFICATE. Par exemple :

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

Étape 5 Définissez l'utilisation de la validation (**Validation Usage**) pour limiter l'utilisation du certificat.

Certaines fonctionnalités vous permettent de choisir si une connexion peut être validée par rapport à un certificat spécifique. Vous devez indiquer dans le certificat que ces fonctionnalités peuvent valablement utiliser le certificat, sinon une connexion est refusée.

Toute fonctionnalité non incluse dans ces options peut être validée par rapport à ce certificat sans autorisation d'utilisation explicite. Par exemple, les politiques de décryptage SSL, et le serveur Web qui héberge le Firepower Device Manager, ignorent l'option Utilisation de la validation. Si vous sélectionnez une option dans ce champ, le certificat sera téléchargé dans la configuration en cours qui s'affiche à l'aide de la commande **show running-config**.

L'objectif principal de ces options est de vous empêcher d'établir des connexions VPN, car elles peuvent être validées par rapport à un certificat particulier.

- **Serveur SSL** : Validez le certificat sur le serveur SSL distant. Utilisé pour le DNS dynamique.
- **Client SSL** : Validez le certificat de la connexion VPN d'accès distant entrant.
- **Client IPsec** : Validez le certificat de la connexion VPN entrante IPsec site vers site.
- **Autre** : les fonctionnalités de validation, telles que LDAPS, qui ne sont pas gérées par le moteur d'inspection Snort. Sélectionnez cette option uniquement si vous rencontrez des problèmes avec une fonctionnalité particulière. Cette option est mutuellement exclusive avec toutes les autres options : vous devez la désélectionner avant de pouvoir sélectionner d'autres options, et désélectionner toutes les options avant de pouvoir sélectionner cette option.

Étape 6 Cliquez sur **OK**.

Configuration des groupes de certificats CA de confiance

Utilisez des groupes de certificats d'autorité de certification externes de confiance dans les paramètres de la politique de déchiffrement SSL pour préciser les certificats auxquels la politique de déchiffrement SSL doit faire confiance. Si un utilisateur final tente de se connecter à un site dont le certificat de l'émetteur ne fait pas partie des certificats de confiance, l'utilisateur reçoit un message lui demandant de faire confiance au certificat. Ainsi, le fait de ne pas avoir le certificat dans la liste de confiance est un inconvénient pour l'utilisateur final, mais n'empêche pas en soi la connexion (ce que vous pourriez faire avec des règles de contrôle d'accès).

Le groupe par défaut est Cisco-Trusted-Authorities. Vous ne devrez créer votre propre groupe que si :

- Vous souhaitez faire confiance aux certificats qui ne font pas partie du groupe par défaut. Vous devez ensuite sélectionner le groupe par défaut et votre nouveau groupe dans les paramètres de la politique de déchiffrement SSL.
- Vous souhaitez faire confiance à une liste de certificats plus limitée que le groupe par défaut. Vous devez ensuite créer un groupe qui a une liste complète de certificats de confiance, pas seulement votre delta, et le sélectionner comme seul groupe dans les paramètres de la politique de déchiffrement SSL.

Avant de commencer

Chargez tous les certificats d'autorités de certification de confiance que vous ajouterez au groupe, s'ils ne sont pas déjà présents dans le système.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Certificates** (certificats) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un groupe de certificats, cliquez sur  et sélectionnez **Add Certificate Group** (Ajouter un groupe de certificats).
- Pour modifier un groupe de certificats, cliquez sur l'icône de modification () du groupe.

Étape 3 Entrez un **Name** (Nom) pour le groupe de certificats et, au besoin, une description.

Étape 4 Cliquez sur le signe + pour ajouter des certificats au groupe.

Ajoutez tous les certificats dont vous avez besoin dans le groupe. Vous pouvez cliquer sur **Create New Trusted CA Certificate** (Créer un nouveau certificat d'AC approuvée) pour en charger de nouveaux pendant que vous créez le groupe.

Si vous n'avez plus besoin d'un certificat dans le groupe, cliquez sur l'icône X (à droite) pour le certificat.

Étape 5 Cliquez sur **OK**.

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.