Erreur d'abandon TLS du module de services NGFW en raison d'une défaillance de la connexion ou d'une erreur de validation de certificat

Contenu

Introduction

Ce document décrit comment résoudre un problème particulier avec l'accès aux sites Web HTTPS via le module de services Cisco NGFW (Next-Generation Firewall) avec déchiffrement activé.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Procédures de connexion SSL (Secure Sockets Layer)
- Certificats SSL

Components Used

Les informations de ce document sont basées sur le module de services Cisco NGFW avec Cisco Prime Security Manager (PRSM) version 9.2.1.2(52).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

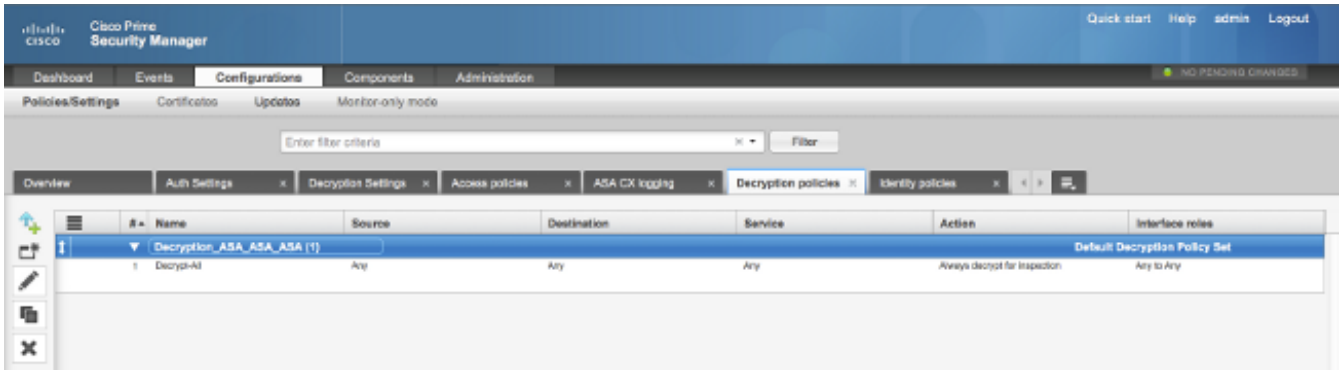
Informations générales

Le déchiffrement est une fonctionnalité qui permet au module de services NGFW de déchiffrer les flux chiffrés SSL (et d'inspecter la conversation qui est par ailleurs chiffrée) et d'appliquer des politiques sur le trafic. Pour configurer cette fonctionnalité, les administrateurs doivent configurer un certificat de déchiffrement sur le module NGFW, qui est présenté aux sites Web HTTPS d'accès client à la place du certificat de serveur d'origine.

Pour que le déchiffrement fonctionne, le module NGFW doit faire confiance au certificat présenté par le serveur. Ce document explique les scénarios lorsque la connexion SSL échoue entre le module de services de pare-feu de nouvelle génération et le serveur, ce qui provoque l'échec de certains sites Web basés sur HTTPS lorsque vous tentez de les atteindre.

Pour les besoins de ce document, ces stratégies sont définies sur le module de services de pare-feu de nouvelle génération avec PRSM :

- **Stratégies d'identité** : Il n'existe aucune stratégie d'identité définie.
- **Stratégies de déchiffrement** : La stratégie **Décrypt-All** utilise cette configuration :

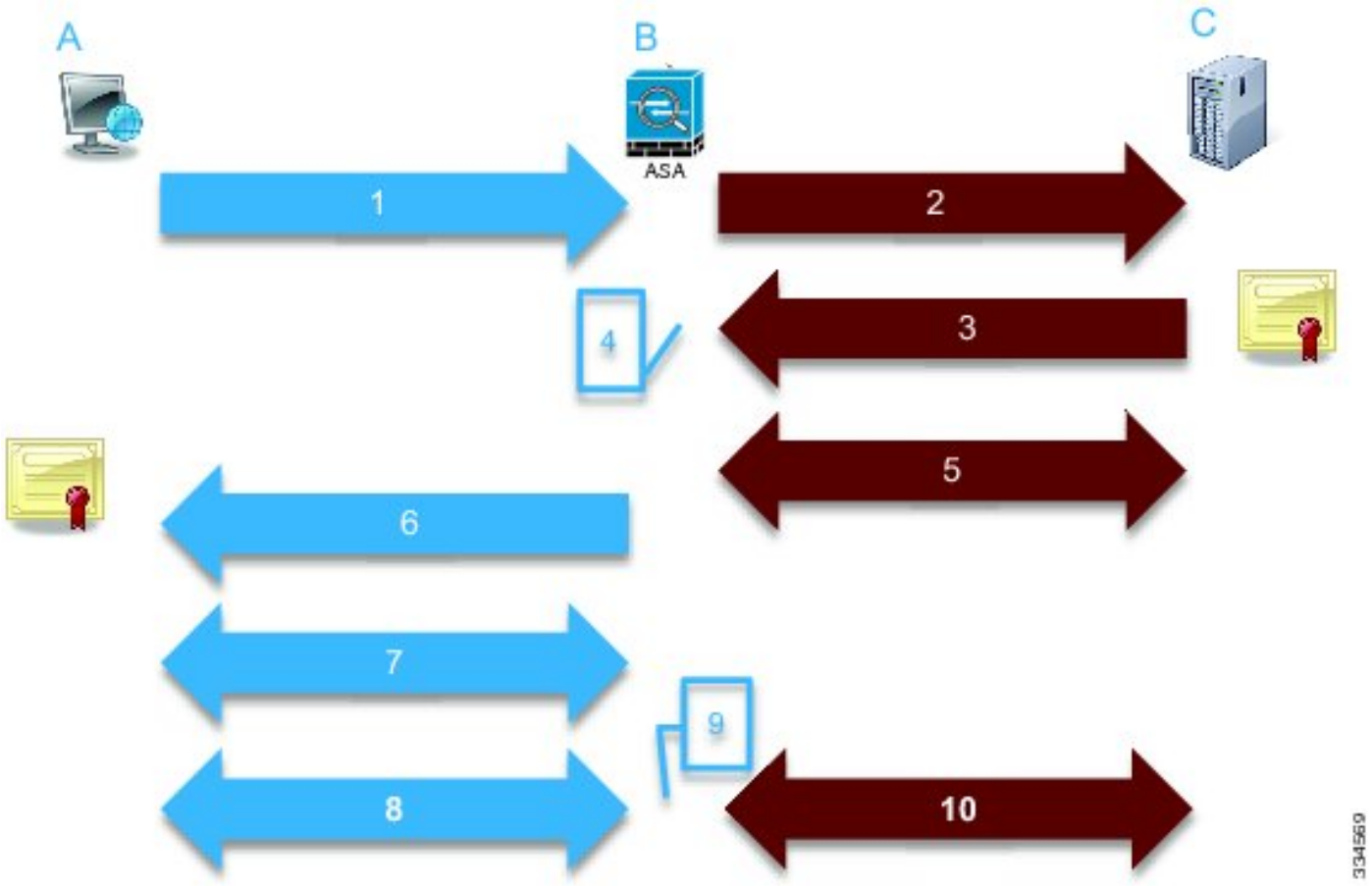


- **Stratégies d'accès** : Il n'existe aucune stratégie d'accès définie.
- **Paramètres de déchiffrement** : Ce document suppose qu'un **certificat de déchiffrement** est configuré sur le module de services du pare-feu de nouvelle génération et que les clients lui font confiance.

Lorsqu'une stratégie de déchiffrement est définie sur le module de services du pare-feu de nouvelle génération et est configurée comme décrit précédemment, le module de services du pare-feu de nouvelle génération tente d'intercepter tout le trafic chiffré SSL via le module et de le déchiffrer.

> **Note**: Une explication pas à pas de ce processus est disponible dans la section Flux de trafic décrypté du Guide de l'utilisateur pour ASA CX et Cisco Prime Security Manager 9.2.

Cette image représente la séquence d'événements :



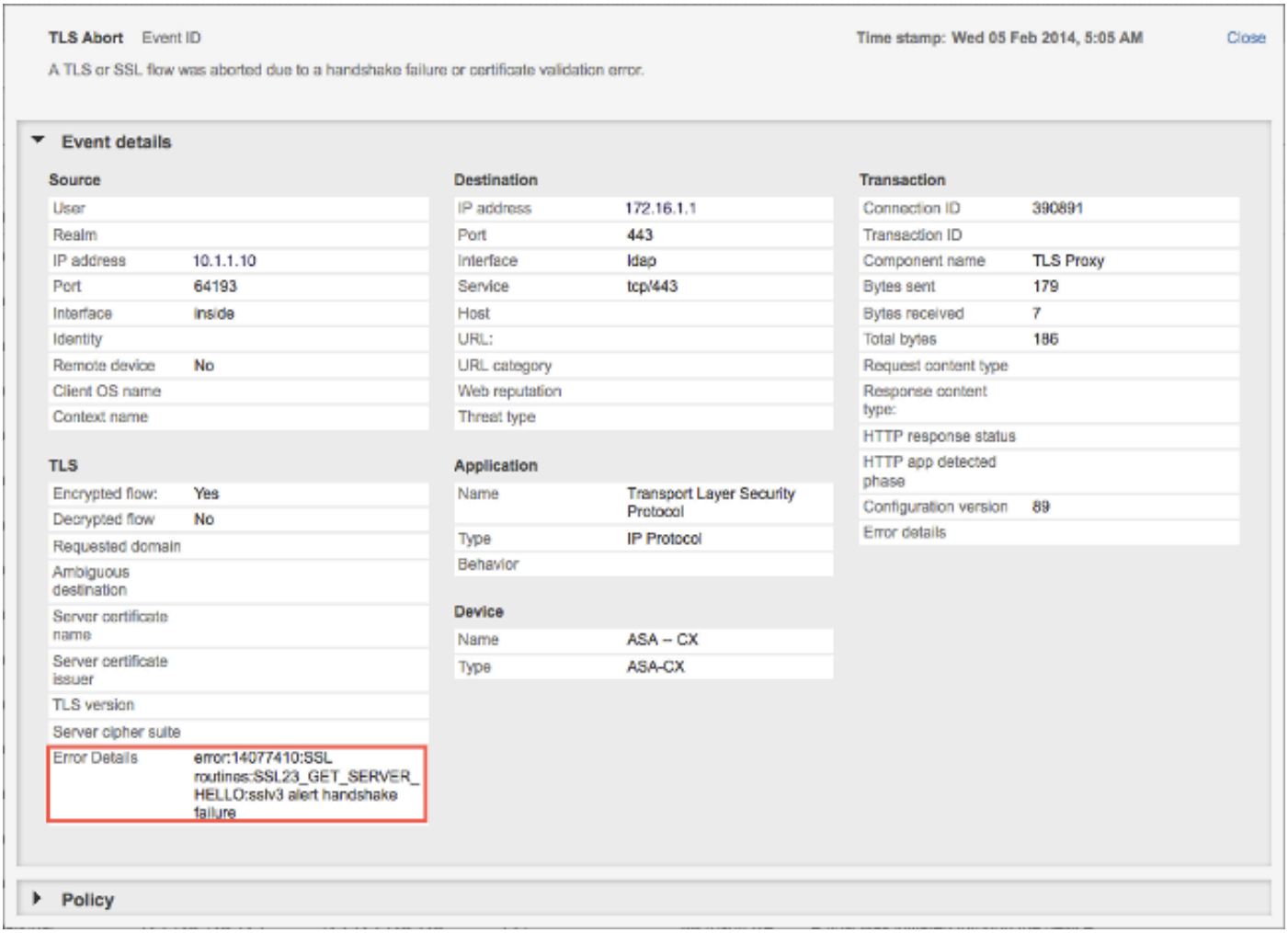
Dans cette image, **A** est le client, **B** est le module de services de pare-feu de nouvelle génération et **C** est le serveur HTTPS. Pour les exemples fournis dans ce document, le serveur HTTPS est un Cisco Adaptive Security Device Manager (ASDM) sur un appareil de sécurité adaptatif Cisco (ASA).

Il y a deux facteurs importants à prendre en compte dans ce processus :

- Dans la deuxième étape du processus, le serveur doit accepter l'une des suites de chiffrement SSL présentées par le module de services du pare-feu de nouvelle génération.
- Dans la quatrième étape du processus, le module de services de pare-feu de nouvelle génération doit faire confiance au certificat présenté par le serveur.

Problème

Si le serveur ne peut accepter aucun des chiffrements SSL présentés par le module de services NFGW, vous recevez un message d'erreur similaire à celui-ci :



Il est important de prendre note des informations sur les détails de l'erreur (mises en surbrillance), qui indiquent :

```
error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
```

Lorsque vous affichez le fichier **/var/log/cisco/tls_proxy.log** dans l'archive de diagnostics de module, les messages d'erreur suivants s'affichent :

```
2014-02-05 05:21:42,189 INFO  TLS_Proxy   - SSL alert message received from
 server (0x228 = "fatal : handshake failure") in Session: x2fd1f6

2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410:
 SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while
 connecting to server for Session: x2fd1f6
```

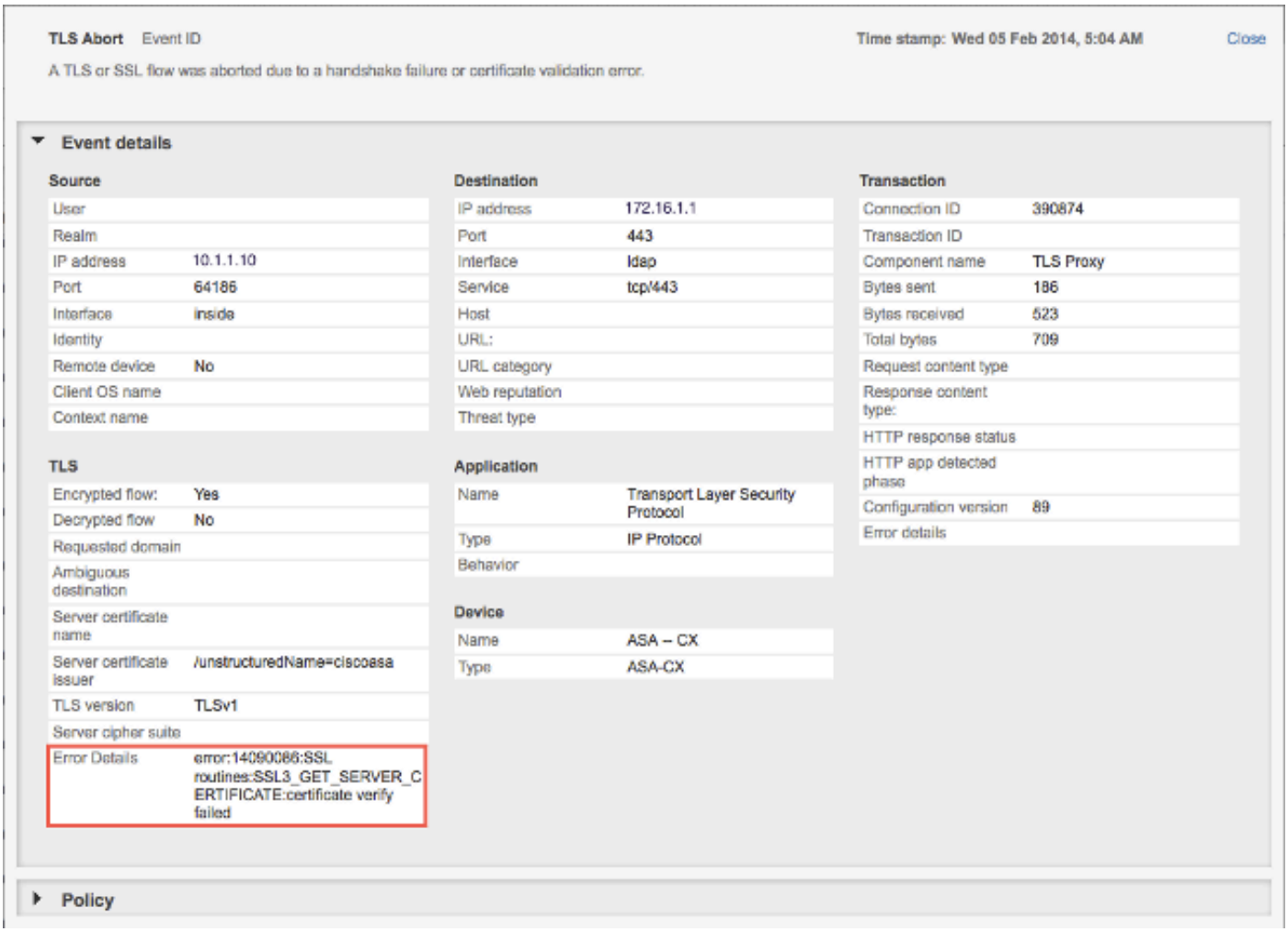
Solution

Une cause possible de ce problème est qu'une licence 3DES/AES (Triple Data Encryption Standard/Advanced Encryption Standard) (souvent appelée K9) n'est pas installée sur le module. Vous pouvez télécharger gratuitement la licence K9 pour le module et la télécharger via PRSM.

Si le problème persiste après l'installation de la licence 3DES/AES, obtenez des captures de paquets pour la connexion SSL entre le module de services NGFW et le serveur, et contactez l'administrateur du serveur afin d'activer les chiffrements SSL appropriés sur le serveur.

Problème

Si le module de services NGFW ne fait pas confiance au certificat présenté par le serveur, vous recevez un message d'erreur similaire à celui-ci :



Il est important de prendre note des informations sur les détails de l'erreur (mises en surbrillance), qui indiquent :

`error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:`**`certificate verify failed`**

Lorsque vous affichez le fichier **/var/log/cisco/tls_proxy.log** dans l'archive de diagnostics de module, les messages d'erreur suivants s'affichent :

```
2014-02-05 05:22:11,505 INFO  TLS_Proxy - Certificate verification failure:
 self signed certificate (code 18, depth 0)

2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from
 server (0x230 = "fatal : unknown CA") in Session: x148a696e

2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086:
 SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while
 connecting to server for Session: x148a696e
```

Solution

Si le module ne peut pas faire confiance au certificat SSL du serveur, vous devez importer le certificat du serveur dans le module avec PRSM afin de vous assurer que le processus de connexion SSL est réussi.

Complétez ces étapes afin d'importer le certificat du serveur :

1. Ignorez le module de services NGFW lorsque vous accédez au serveur afin de télécharger le certificat via un navigateur. Une façon de contourner le module est de créer une politique de déchiffrement qui ne déchiffre pas le trafic vers ce serveur particulier. Cette vidéo vous montre comment créer la stratégie :

   Voici les étapes affichées dans la vidéo :

   Pour accéder au module PRSM sur le CX, accédez à **https://<IP_ADDRESS_OF_PRSM>**. Cet exemple utilise **https://10.106.44.101**.

   Accédez à **Configurations > Policies/Settings > Decryption policies** dans le module PRSM.

   Cliquez sur l'icône située près du coin supérieur gauche de l'écran et sélectionnez l'option **Ajouter une stratégie ci-dessus** afin d'ajouter une stratégie en haut de la liste.

   Nommez la stratégie, laissez la source comme **Any** et créez un objet **de groupe de réseau CX**.
   Note: N'oubliez pas d'inclure l'adresse IP du serveur HTTPS. Dans cet exemple, une adresse IP de **172.16.1.1** est utilisée.Choisissez **Ne pas déchiffrer** pour l'action.

   Enregistrez la stratégie et validez les modifications.
2. Téléchargez le certificat de serveur via un navigateur et téléchargez-le sur le module de services de pare-feu de nouvelle génération via PRSM, comme illustré dans cette vidéo :

   Voici les étapes affichées dans la vidéo :

   Une fois la stratégie précédemment mentionnée définie, utilisez un navigateur pour accéder au serveur HTTPS qui s'ouvre via le module de services de pare-feu de nouvelle génération.
   Note: Dans cet exemple, Mozilla Firefox version 26.0 est utilisé afin de naviguer vers le serveur (un ASDM sur un ASA) avec l'URL **https://172.16.1.1**.Acceptez l'avertissement de sécurité s'il apparaît et ajoutez une exception de sécurité.

   Cliquez sur la petite icône en forme de verrou située à gauche de la barre d'adresse. L'emplacement de cette icône varie en fonction du navigateur utilisé et de la version.

   Cliquez sur le bouton **Afficher le certificat**, puis sur le bouton **Exporter** sous l'onglet Détails

après avoir sélectionné le certificat du serveur.

Enregistrez le certificat sur votre machine personnelle à l'emplacement de votre choix.

Connectez-vous au module PRSM et accédez à **Configurations > Certificates**.

Cliquez sur **Je veux... > Importer le certificat** et choisir le certificat de serveur précédemment téléchargé (à partir de l'étape 4).

Enregistrer et valider les modifications. Une fois terminé, le module de services NGFW doit faire confiance au certificat présenté par le serveur.

3. Supprimez la stratégie qui a été ajoutée à l'étape 1. Le module de services du pare-feu de nouvelle génération est désormais en mesure de mener à bien la connexion avec le serveur.

Informations connexes

- Guide de l'utilisateur pour ASA CX et Cisco Prime Security Manager 9.2
- Support et documentation techniques - Cisco Systems