Erreurs d'arrêt de TLS de Module de services NGFW dues à l'erreur de validation de panne ou de certificat de prise de contact

Contenu

Introduction

Ce document décrit comment dépanner un problème particulier avec l'accès aux sites Web basés sur HTTPS par le Module de services de la deuxième génération du Pare-feu de Cisco (NGFW) avec le déchiffrement activé.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Prises de contact de Secure Sockets Layer (SSL)
- Certificats SSL

Composants utilisés

Les informations dans ce document sont basées sur le Module de services de Cisco NGFW avec la version 9.2.1.2(52) du gestionnaire de Sécurité de perfection de Cisco (PRSM).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

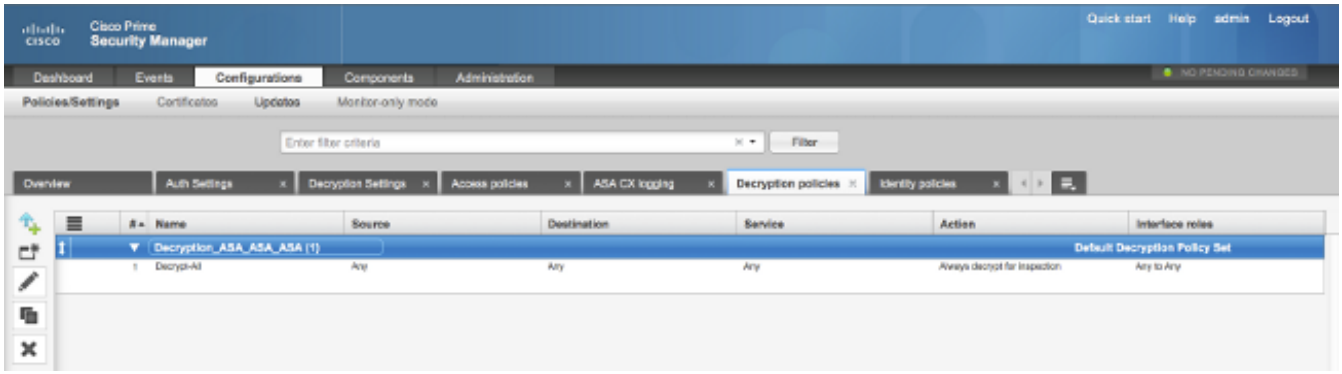
Informations générales

Le déchiffrement est une caractéristique qui permet au Module de services NGFW de déchiffrer des écoulements SSL-chiffrés (et examiner la conversation qui est autrement chiffrée) et d'imposer des stratégies sur le trafic. Afin de configurer cette caractéristique, les administrateurs doivent configurer un certificat de déchiffrement sur le module NGFW, qui est présenté aux sites Web basés sur HTTPS d'accès client au lieu du certificat de serveur d'origine.

Pour que le déchiffrement fonctionne, le module NGFW doit faire confiance au certificat serveur-présenté. Ce document explique les scénarios quand la prise de contact SSL échoue entre le Module de services NGFW et le serveur, qui fait échouer certains sites Web basés sur HTTPS quand vous tentez de les atteindre.

Afin de ce document, ces stratégies sont définies sur le Module de services NGFW avec PRSM :

- **Stratégies d'identité** : Il n'y a aucune stratégie d'identité définie.
- **Stratégies de déchiffrement** : **La Déchiffrage-toute** stratégie utilise cette configuration :

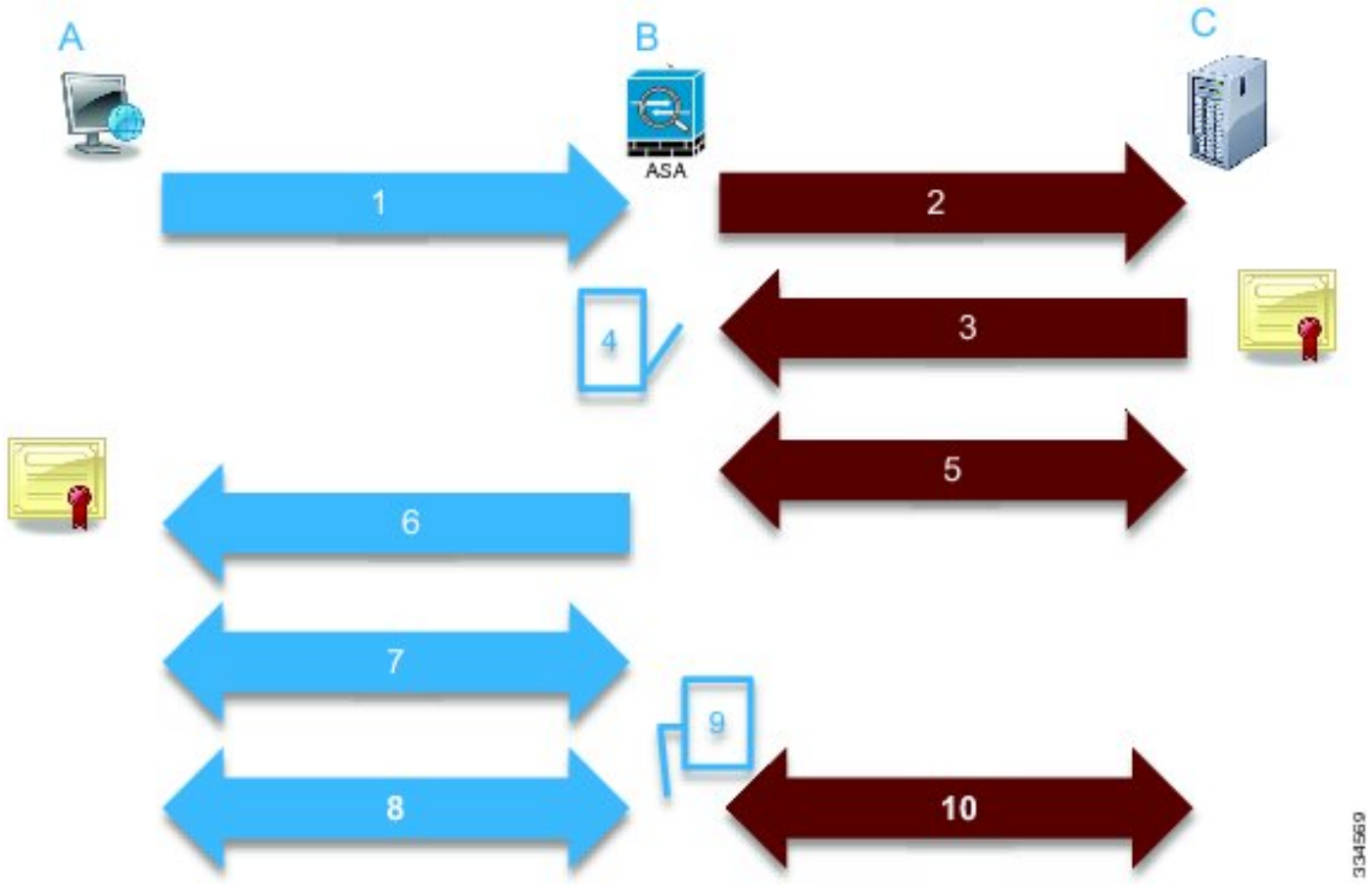


- **Stratégies d'Access** : Il n'y a aucune stratégie définie d'accès.
- **Configurations de déchiffrement** : Ce document suppose qu'un **certificat de déchiffrement** est configuré sur le Module de services NGFW et que les clients lui font confiance.

Quand une stratégie de déchiffrement est définie sur le Module de services NGFW et est configurée comme décrit précédemment, les essais de Module de services NGFW pour intercepter tout les trafic SSL-chiffré par le module et à déchiffrer.

> Remarque: Une explication pas à pas de ce processus est disponible dans la section déchiffrée de la circulation du guide utilisateur pour ASA CX et du directeur de la sécurité principal 9.2 de Cisco.

Cette image dépeint la séquence d'opérations :



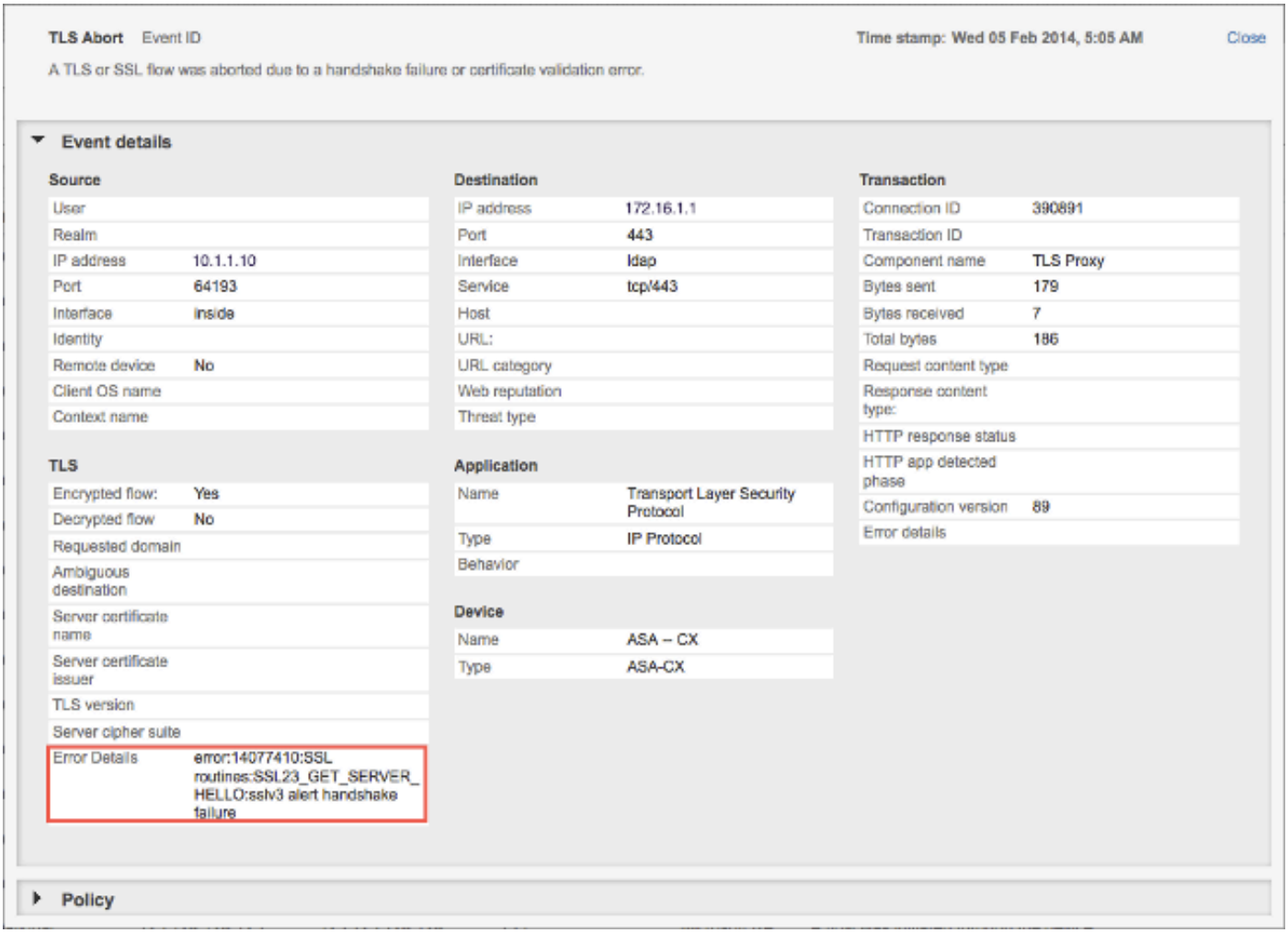
Dans cette image, **A** est le client, **B** est le Module de services NGFW, et le **C** est le serveur HTTPS. Pour les exemples fournis dans ce document, le serveur basé sur HTTPS est un Cisco Adaptive Security Device Manager (ASDM) sur une appliance de sécurité adaptable Cisco (ASA).

Il y a deux importants facteurs au sujet de ce processus que vous devriez considérer :

- Dans la deuxième étape du processus, le serveur doit recevoir une des suites de chiffrement SSL qui sont présentées par le Module de services NGFW.
- Dans la quatrième étape du processus, le Module de services NGFW doit faire confiance au certificat qui est présenté par le serveur.

Problème

Si le serveur ne peut pas recevoir les chiffrements l'uns des SSL qui sont présentés par le Module de services NFGW, vous recevez un message d'erreur semblable à ceci :



Il est important de noter les informations de détails d'erreur (mises en valeur), qui affichent :

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

Quand vous visualisez le fichier de **/var/log/cisco/tls_proxy.log** dans les archives de diagnostics de module, ces messages d'erreur apparaissent :

```
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
```

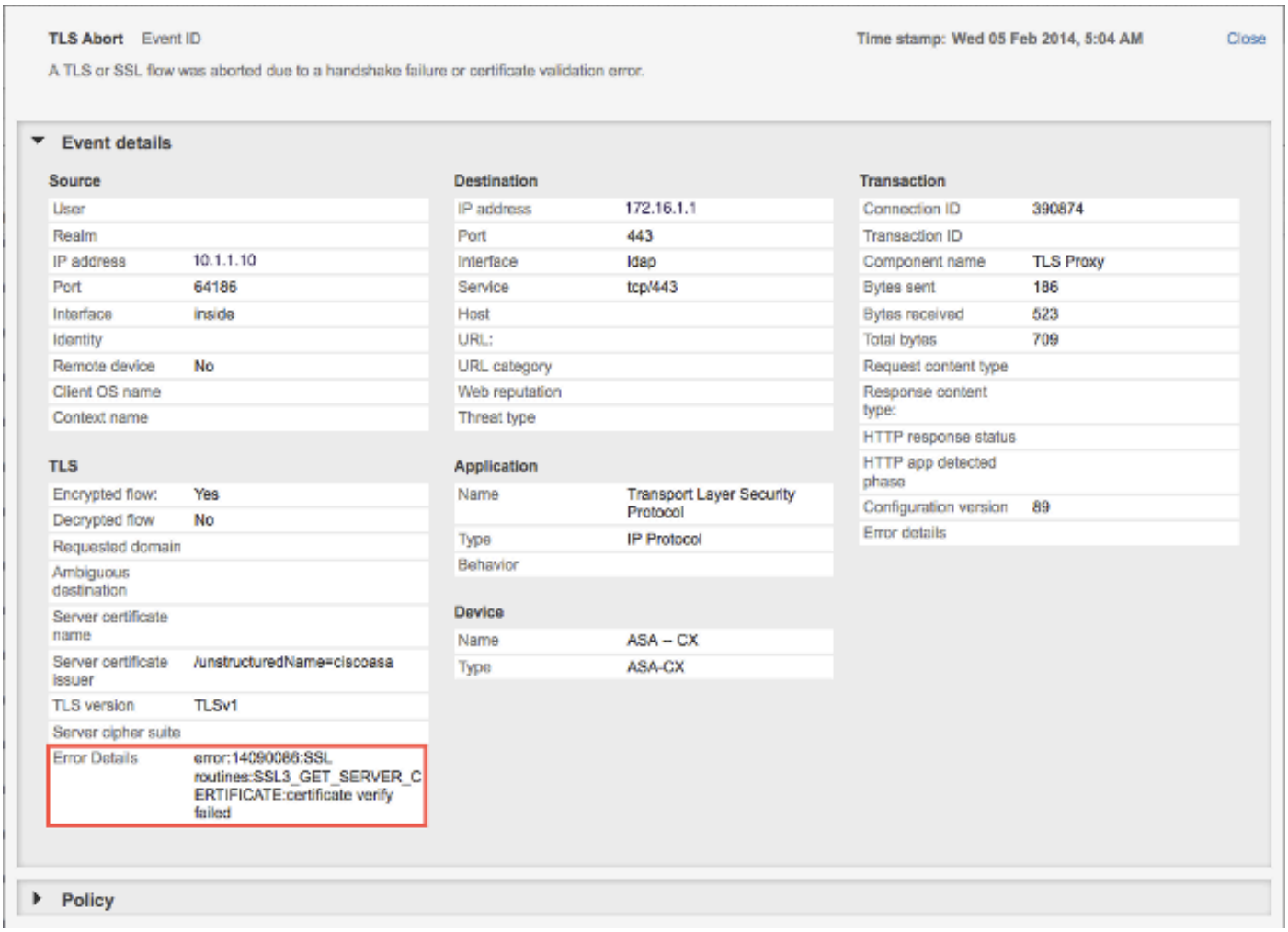
Solution

Une cause possible pour ce problème est qu'un permis triple de norme de chiffrement de données/Advanced Encryption Standard (3DES/AES) (souvent désigné sous le nom de K9) n'est pas installé sur le module. Vous pouvez télécharger le permis K9 pour le module sans frais et le télécharger par l'intermédiaire de PRSM.

Si le problème persiste après que vous installiez le permis 3DES/AES, alors obtenez les captures de paquet pour la prise de contact SSL entre le Module de services NGFW et le serveur, et contactez l'administrateur du serveur afin d'activer les chiffrements appropriés SSL sur le serveur.

Problème

Si le Module de services NGFW ne fait pas confiance au certificat qui est présenté par le serveur, alors vous recevez un message d'erreur semblable à ceci :



Il est important de noter les informations de détails d'erreur (mises en valeur), qui affichent :

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

Quand vous visualisez le fichier de **/var/log/cisco/tls_proxy.log** dans les archives de diagnostics de module, ces messages d'erreur apparaissent :

```
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 de serveur, vous devez importer le certificat de serveur dans le module avec PRSM afin de s'assurer que le processus de prise de contact SSL est réussi.

Terminez-vous ces étapes afin d'importer le certificat de serveur :

1. Sautez le Module de services NGFW quand vous accédez au serveur afin de télécharger le certificat par l'intermédiaire d'un navigateur. Une manière de sauter le module est de créer une stratégie de déchiffrement qui ne déchiffre pas le trafic à ce serveur particulier. Ce vidéo t'affiche comment créer la stratégie :

   Ce sont les étapes qui sont affichées dans le vidéo :

   Afin d'accéder au PRSM sur la CX, naviguez vers **https:// <IP_ADDRESS_OF_PRSM>**. Cet exemple utilise **https://10.106.44.101**.

   Naviguez vers des **stratégies de configurations > de stratégies/configurations > de déchiffrement** dans le PRSM.

   Cliquez sur l'icône qui se trouve près du coin supérieur gauche de l'écran et choisissez l'**ajouter au-dessus de l'**option de **stratégie** afin d'ajouter une stratégie au haut de la liste.

   En nommez la stratégie, laissez la source en tant que, et créez un objet de **groupe de réseau de la CX**.
   Remarque: Souvenez-vous pour inclure l'adresse IP du serveur basé sur HTTPS. Dans cet exemple, une adresse IP de **172.16.1.1** est utilisée.Choose **ne déchiffrent pas** pour l'action.

   Sauvegardez la stratégie et commettez les modifications.
2. Téléchargez le certificat de serveur par un navigateur et téléchargez-le au Module de services NGFW par l'intermédiaire de PRSM, suivant les indications de ce vidéo :

   Ce sont les étapes qui sont affichées dans le vidéo :

   Une fois que la stratégie précédent-mentionnée est définie, utilisez un navigateur afin de naviguer vers le serveur basé sur HTTPS qui s'ouvre par le Module de services NGFW.
   Remarque: Dans cet exemple, la version 26.0 de Mozilla Firefox est utilisée afin de naviguer vers le serveur (un ASDM sur une ASA) avec l'URL **https://172.16.1.1**.Recevez l'alerte de sécurité si on s'affiche et ajoutez une exception de Sécurité.

   Cliquez sur la petite icône en forme de verrouillage située à la gauche de la barre d'adresses. L'emplacement de cette icône varie basé sur le navigateur qui est utilisé et la version.

   Cliquez sur le bouton de **certificat de vue** et puis le bouton d'**exportation** sous l'onglet de détails après que vous sélectionniez le certificat de serveur.

Sauvegardez le certificat sur votre ordinateur personnel à un emplacement de votre choix.

Connectez-vous dans le PRSM et parcourez aux **configurations > aux Certificats**.

Le clic **I veulent à… > le certificat d'importation** et a choisi le certificat de serveur précédent-téléchargé (d'étape 4).

Sauvegardez et commettez les modifications. Une fois complet, le Module de services NGFW devrait faire confiance au certificat qui est présenté par le serveur.

3. Enlevez la stratégie qui a été ajoutée dans l'étape 1. Le Module de services NGFW peut maintenant se terminer la prise de contact avec succès avec le serveur.

Informations connexes

- Guide utilisateur pour ASA CX et directeur de la sécurité 9.2 de perfection de Cisco
- Support et documentation techniques - Cisco Systems