# NGFW-servicesmodule - TLS Afbreken fouten vanwege handschokkingsfouten of certificaatvalidatiefout

## Inhoud



## Inleiding

Dit document beschrijft hoe u een specifiek probleem met toegang tot op HTTPS gebaseerde websites kunt oplossen door middel van de Cisco Next-generation firewall (NGFW) servicemodule met encryptie ingeschakeld.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Socket Layer (SSL) handshake-procedures
- SSL-certificaten

### Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco NGFW-servicemodule met Cisco Prime Security Manager (PRSM) versie 9.2.1.2(52).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

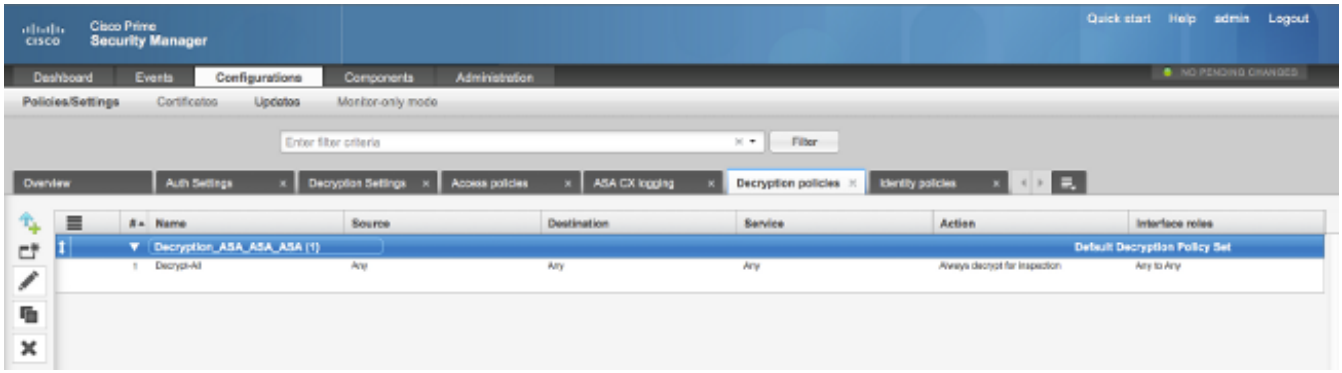
## Achtergrondinformatie

Decryptie is een eigenschap die de NGFW servicemodule toelaat om SSL-gecodeerde stromen te decrypteren (en het gesprek te inspecteren dat anders versleuteld is) en beleid op het verkeer af te dwingen. Om deze optie te kunnen configureren moeten beheerders een decryptie certificaat configureren op de NGFW module, dat wordt aangeboden aan de HTTPS-gebaseerde websites van de client in plaats van het originele servercertificaat.

Om decryptie te kunnen werken, moet de NGFW module het server-aangeboden certificaat vertrouwen. Dit document legt de scenario's uit wanneer de SSL-handdruk tussen de NGFW-servicemodule en de server mislukt, waardoor bepaalde op HTTPS gebaseerde websites defect raken wanneer u probeert deze te bereiken.

Voor de toepassing van dit document worden dit beleid gedefinieerd in de NGFW-servicemodule met PRSM:

- **Identiteitsbeleid**: Er bestaat geen welomschreven identiteitsbeleid.
- **Decryptie beleid**: Het **decrypt-all** beleid gebruikt deze configuratie:

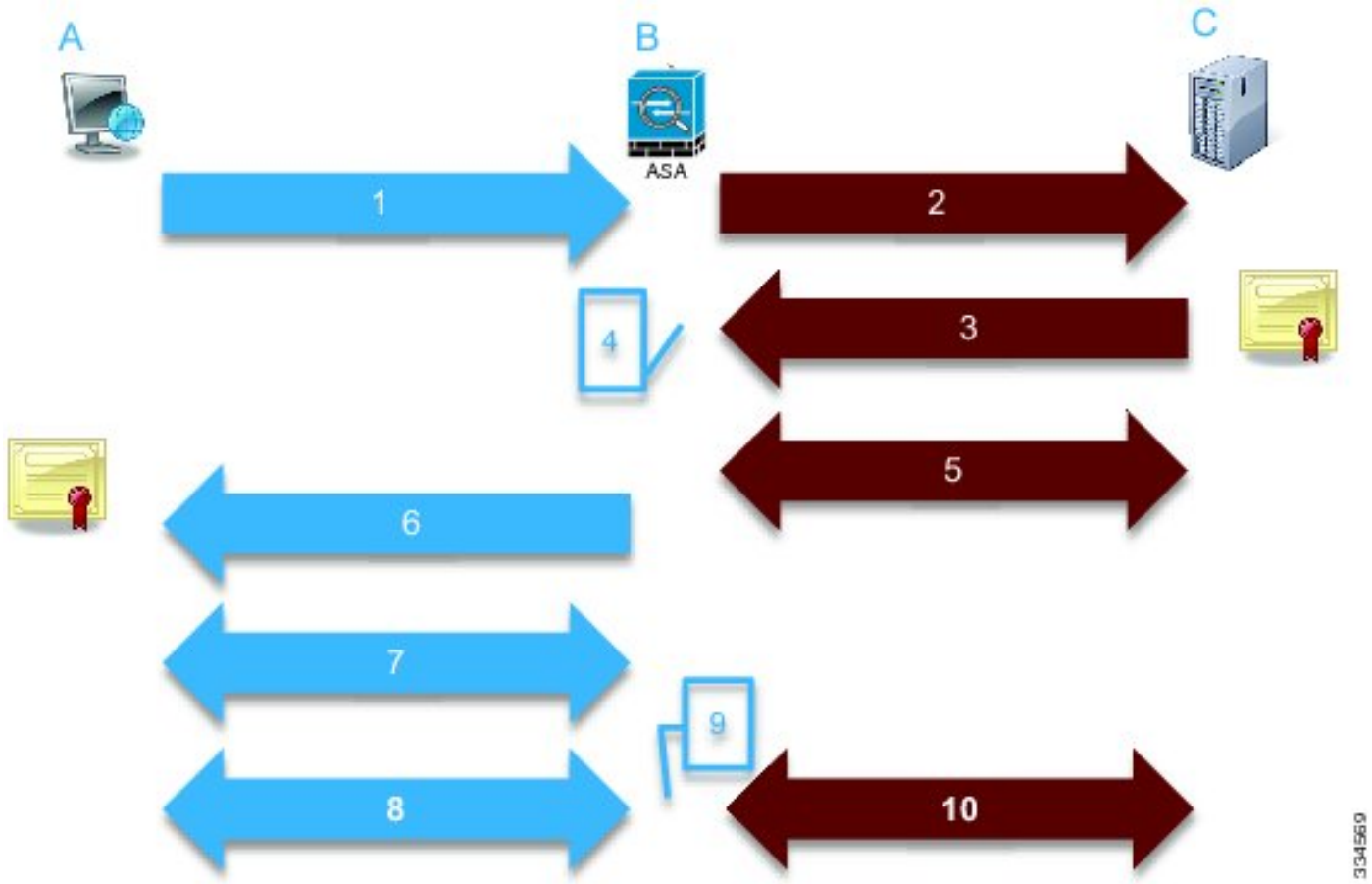



- **Toegangsbeleid**: Er is geen bepaald toegangsbeleid.
- **Instellingen voor decryptie**: In dit document wordt ervan uitgegaan dat een **decryptie-certificaat** is ingesteld op de NGFW-servicemodule en dat de klanten er vertrouwen in hebben.

Wanneer een decryptie beleid op de NGFW servicemodule wordt bepaald en zoals eerder beschreven wordt gevormd, probeert de NGFW servicemodule het volledige SSL-gecodeerde verkeer door de module en decrypt te onderscheppen.

> Opmerking: Een stap-voor-stap verklaring van dit proces is beschikbaar in het gedeelte Decrypted Traffic Flow van de Gebruikersgids voor ASA CX en Cisco Prime Security Manager 9.2.

Dit beeld geeft de opeenvolging van gebeurtenissen weer:



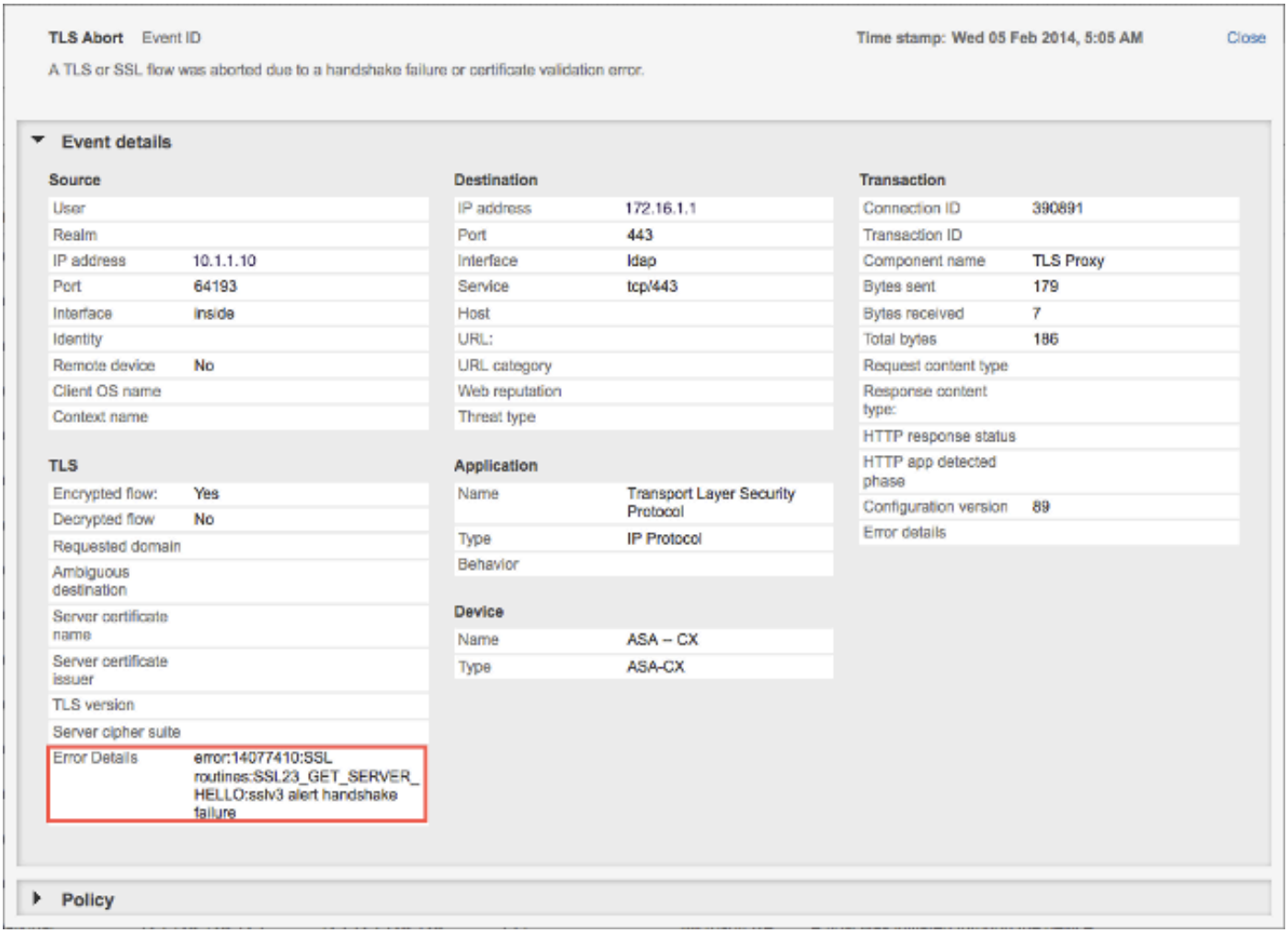

In deze afbeelding is **A** de client, **B** is de NGFW servicemodule en **C** de HTTPS server. Voor de voorbeelden in dit document is de op HTTPS gebaseerde server een Cisco Adaptieve Security Appliance Manager (ASDM) op een Cisco Adaptieve Security Appliance (ASA).

Er zijn twee belangrijke factoren in dit proces die u in overweging moet nemen:

- In de tweede stap van het proces moet de server één van de SSL algoritmen accepteren die door de NGFW servicemodule worden voorgesteld.
- In de vierde stap van het proces moet de NGFW-servicemodule het certificaat vertrouwen dat door de server wordt gepresenteerd.

## Probleem

Als de server geen van de SSL ciphers kan accepteren die door de NFGW servicemodule worden voorgesteld, ontvangt u een gelijkend foutbericht:




Het is belangrijk om nota te nemen van de (gemarkeerde) foutdetails, die aantonen:

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

Wanneer u het **/var/log/cisco/tls_proxy.log-**bestand bekijkt in het diagnostische modulair archief, verschijnen deze foutmeldingen:

```
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
```

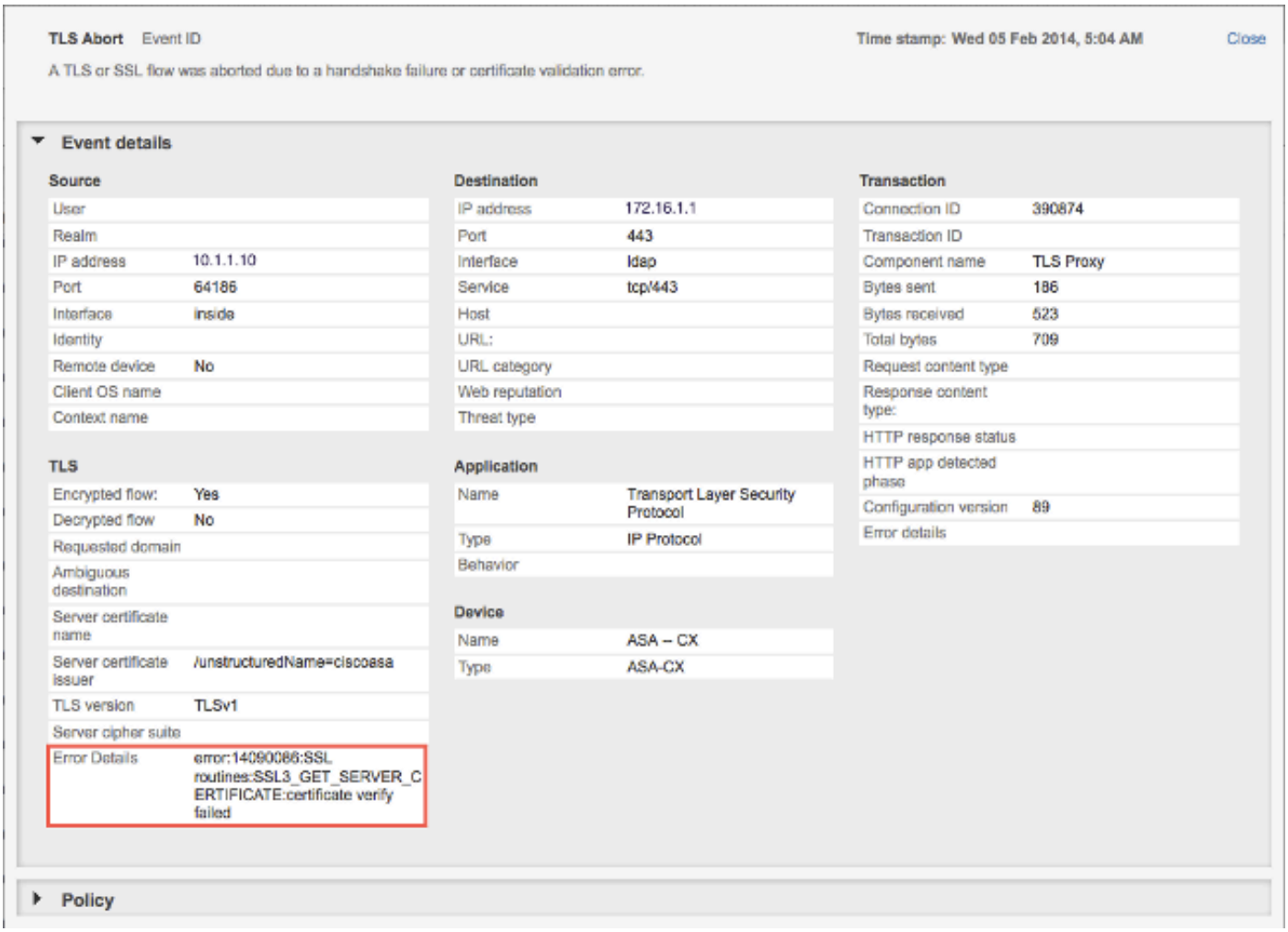
# Oplossing

Eén mogelijke oorzaak voor dit probleem is dat een Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES)-licentie (vaak K9) niet op de module is geïnstalleerd. U kunt de K9 licentie voor de module downloaden zonder kosten en deze uploaden via PRSM.

Als het probleem zich blijft voordoen nadat u de 3DES/AES-licentie hebt geïnstalleerd, kunt u pakketvastlegging verkrijgen voor de SSL-handdruk tussen de NGFW-servicemodule en de server en contact opnemen met de serverbeheerder om het juiste SSL-algoritme(s) op de server mogelijk te maken.

# Probleem

Als de NGFW-servicemodule het certificaat niet vertrouwt dat door de server wordt overgelegd, ontvangt u een gelijkaardig foutbericht:




Het is belangrijk om nota te nemen van de (gemarkeerde) foutdetails, die aantonen:

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

Wanneer u het **/var/log/cisco/tls_proxy.log-**bestand bekijkt in het diagnostische modulair archief, verschijnen deze foutmeldingen:

```
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
```

# Oplossing

Als de module geen vertrouwen heeft in het SSL-certificaat van de server, moet u het servercertificaat in de module met PRSM importeren om er zeker van te zijn dat het SSL-handdrukproces succesvol is.

Voltooi deze stappen om het servercertificaat te importeren:

1. Breek de NGFW servicemodule over wanneer u toegang hebt tot de server om het certificaat te downloaden via een browser. Eén manier om de module te omzeilen is een decryptie beleid te creëren dat geen verkeer naar die specifieke server decrypteert. In deze video is te zien hoe je beleid kunt maken:

   Dit zijn de stappen die in de video worden getoond:

   Om toegang tot PRSM op de CX te krijgen, navigeer dan naar **https://<IP_ADDRESS_OF_PRSM>**. Dit voorbeeld gebruikt **https://10.106.44.101**.

   Navigeer naar **Configuraties > Beleid/Instellingen > Decryptie-beleid** in PRSM.

   Klik op het pictogram dat zich in de linker bovenhoek van het scherm bevindt en kies de optie **Toevoegen boven** beleid om aan de lijst een beleid toe te voegen.

   Geef het beleid een naam, laat de bron als **Any**, en maak een **CX Network group** object. Opmerking: Vergeet niet het IP-adres van de HTTPS-gebaseerde server op te nemen. In dit voorbeeld wordt een IP-adres van **172.16.1.1** gebruikt.Kies **Niet decrypteren** voor de Actie.

   Bewaar het beleid en verbind de veranderingen.
2. Download het servercertificaat via een browser en uploadde het naar de NGFW servicemodule via PRSM, zoals te zien is in deze video:

   Dit zijn de stappen die in de video worden getoond:

   Zodra het eerder genoemde beleid is gedefinieerd, gebruikt u een browser om naar de op HTTPS gebaseerde server te navigeren die door de NGFW servicemodule wordt geopend. Opmerking: In dit voorbeeld wordt Mozilla Firefox versie 26.0 gebruikt om met de URL **https://172.16.1.1** naar de server (een ASDM op een ASA) te navigeren.Accepteer de veiligheidswaarschuwing als deze verschijnt en voeg een beveiligingsuitzondering toe.

   Klik op het kleine slot-vormige pictogram links op de adresbalk. De locatie van dit pictogram varieert op basis van de browser die wordt gebruikt en de versie.

   Klik op de knop **Certificaat bekijken** en vervolgens op de knop **Exporteren** onder het tabblad Details nadat u het servercertificaat hebt geselecteerd.

   Bewaar het certificaat op uw persoonlijke machine op een locatie naar keuze.

Log in op PRSM en blader naar **Configuraties > Certificaten**.

Klik op **Ik wil... > het certificaat importeren** en kies het eerder gedownload servercertificaat (uit Stap 4).

Sla de wijzigingen op en sluit ze aan. Na voltooiing, zou de NGFW servicemodule het certificaat moeten vertrouwen dat door de server wordt aangeboden.

3. Verwijder het beleid dat in Stap 1 was toegevoegd. De NGFW-servicemodule kan nu de handdruk met succes met de server voltooien.

## Gerelateerde informatie

- Gebruikershandleiding voor ASA CX en Cisco Prime Security Manager 9.2
- Technische ondersteuning en documentatie – Cisco Systems