Errori di interruzione TLS modulo servizi NGFW a causa di un errore di handshake o di convalida del certificato

Sommario

Introduzione

In questo documento viene descritto come risolvere un particolare problema con l'accesso ai siti Web basati su HTTPS tramite il modulo dei servizi Cisco Next-Generation Firewall (NGFW) con decrittografia abilitata.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Procedure di handshake SSL (Secure Sockets Layer)
- certificati SSL

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il Cisco NGFW Services Module con Cisco Prime Security Manager (PRSM) versione 9.2.1.2(52).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

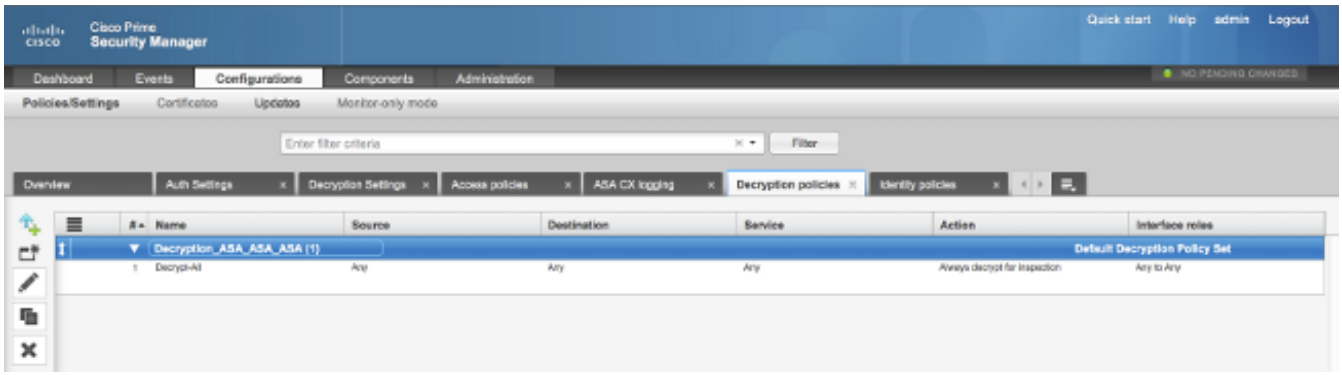
La decrittografia è una funzionalità che consente al modulo dei servizi NGFW di decrittografare i flussi crittografati con SSL (e ispezionare la conversazione altrimenti crittografata) e applicare policy sul traffico. Per configurare questa funzionalità, gli amministratori devono configurare un certificato di decrittografia nel modulo NGFW, che viene presentato ai siti Web basati su HTTPS di accesso client al posto del certificato server originale.

Affinché la decrittografia funzioni, il modulo NGFW deve considerare attendibile il certificato presentato dal server. In questo documento vengono illustrati gli scenari in cui si verifica un errore dell'handshake SSL tra il modulo di servizi NGFW e il server, che provoca l'errore di alcuni siti Web basati su HTTPS quando si tenta di raggiungerli.

Ai fini del presente documento, queste policy sono definite sul modulo servizi NGFW con PRSM:

- **Criteri di identità**: Nessun criterio di identità definito.

- **Criteri di decrittografia**: Il criterio **Decrypt-All** utilizza questa configurazione:



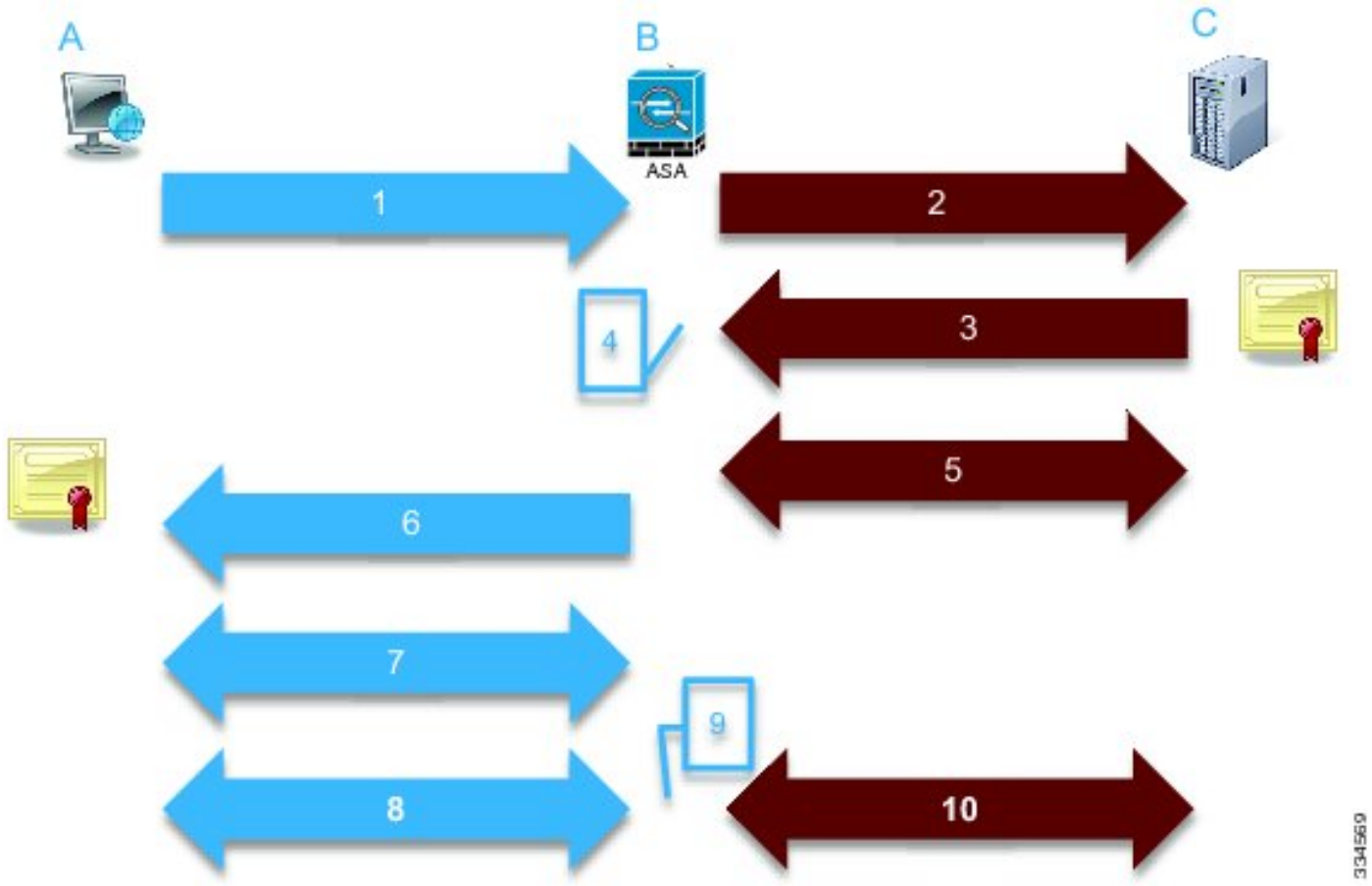
- **Criteri di accesso**: Nessun criterio di accesso definito.

- **Impostazioni decrittografia**: In questo documento si presume che il **certificato di decrittografia** sia configurato nel modulo dei servizi NGFW e che i client lo considerino attendibile.

Quando un criterio di decrittografia viene definito sul modulo dei servizi NGFW e configurato come descritto in precedenza, il modulo dei servizi NGFW tenta di intercettare tutto il traffico crittografato con SSL attraverso il modulo e lo decrittografa.

> **Nota:** Una spiegazione dettagliata di questo processo è disponibile nella sezione Decrypted Traffic Flow della Guida per l'utente di ASA CX e Cisco Prime Security Manager 9.2.

L'immagine mostra la sequenza degli eventi:



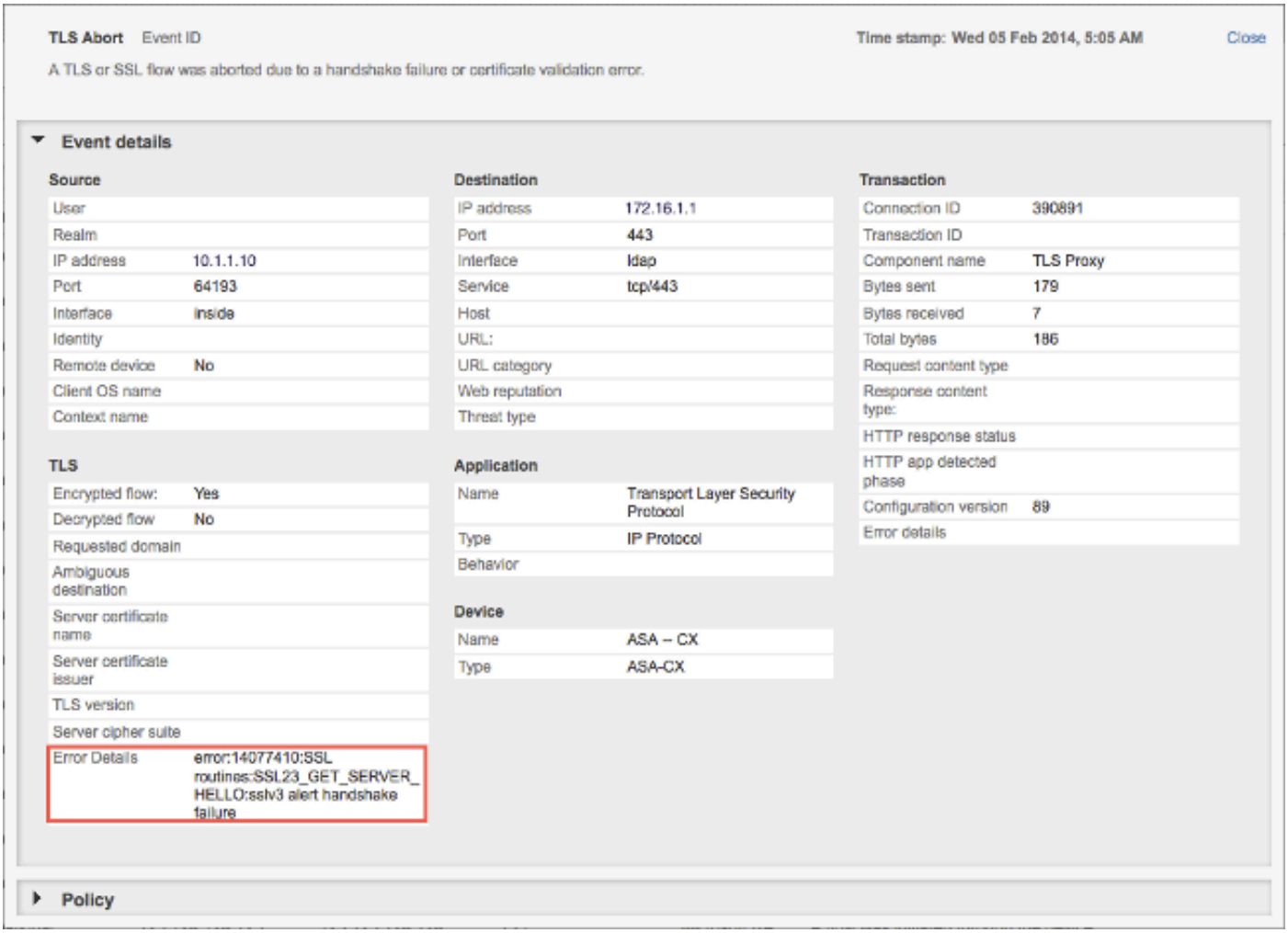
In questa immagine, **A** è il client, **B** è il modulo dei servizi NGFW e **C** è il server HTTPS. Per gli esempi riportati in questo documento, il server basato su HTTPS è un Cisco Adaptive Security Device Manager (ASDM) su una appliance Cisco Adaptive Security (ASA).

In questo processo è necessario considerare due fattori importanti:

- Nella seconda fase del processo, il server deve accettare una delle suite di cifratura SSL presentate dal modulo dei servizi NGFW.
- Nella quarta fase del processo, il modulo dei servizi NGFW deve considerare attendibile il certificato presentato dal server.

Problema

Se il server non accetta nessuna delle cifrature SSL presentate dal modulo dei servizi NFGW, viene visualizzato un messaggio di errore simile al seguente:



Èimportante prendere nota delle informazioni di Dettagli errore (evidenziate), che mostrano:

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

Quando si visualizza il file **/var/log/cisco/tls_proxy.log** nell'archivio di diagnostica del modulo, vengono visualizzati questi messaggi di errore:

```
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
```

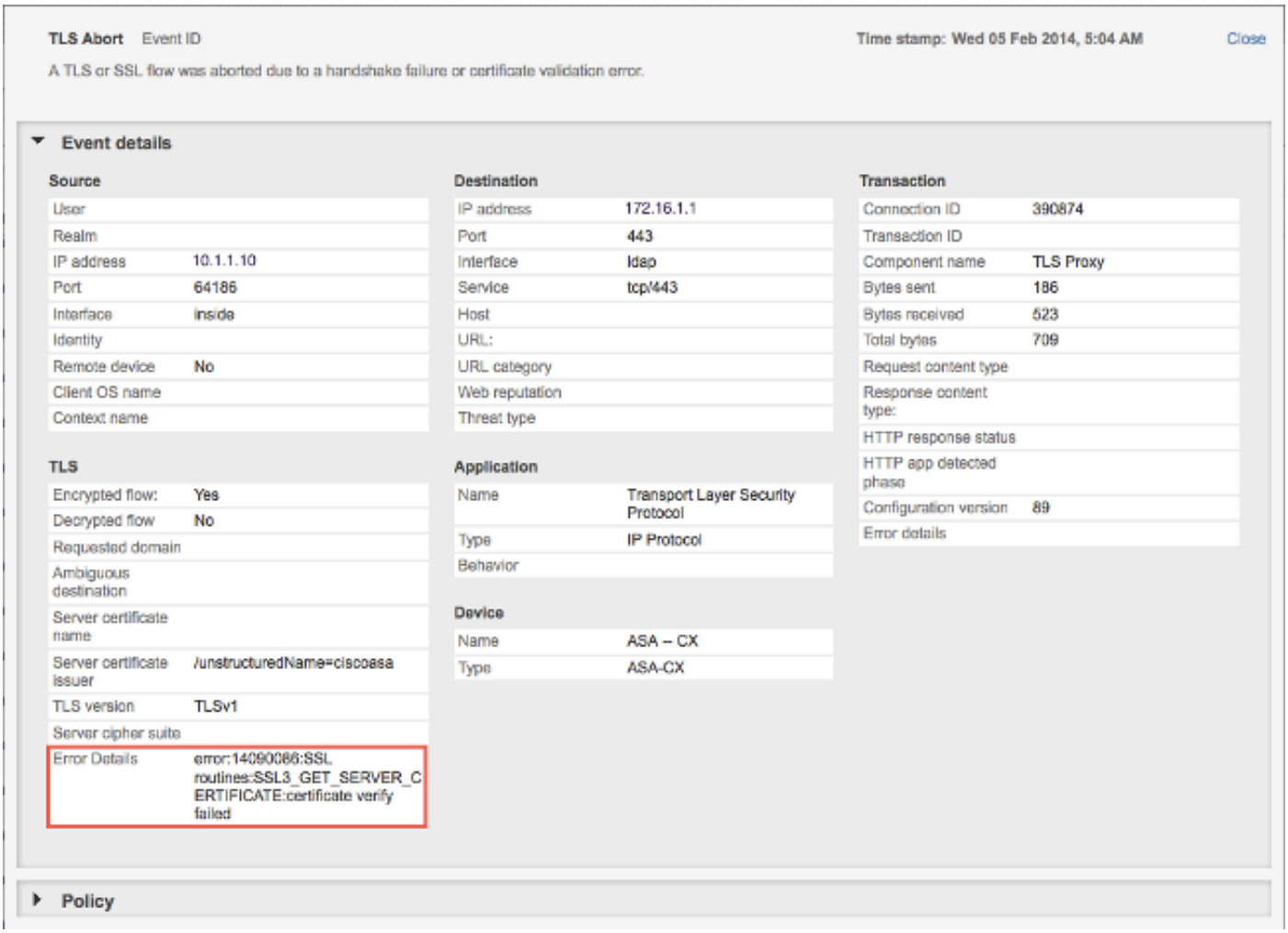
Soluzione

Una possibile causa del problema è che nel modulo non è installata una licenza Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES) (spesso indicata come K9). È possibile scaricare la licenza K9 per il modulo senza costi aggiuntivi e caricarla tramite PRSM.

Se il problema persiste dopo l'installazione della licenza 3DES/AES, ottenere le acquisizioni dei pacchetti per l'handshake SSL tra il modulo dei servizi NGFW e il server e contattare l'amministratore del server per abilitare le cifrature SSL appropriate sul server.

Problema

Se il modulo dei servizi NGFW non considera attendibile il certificato presentato dal server, viene visualizzato un messaggio di errore simile al seguente:



Èimportante prendere nota delle informazioni di Dettagli errore (evidenziate), che mostrano:

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

Quando si visualizza il file **/var/log/cisco/tls_proxy.log** nell'archivio di diagnostica del modulo, vengono visualizzati questi messaggi di errore:

```
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
```

Soluzione

Se il modulo non è in grado di considerare attendibile il certificato SSL del server, è necessario

importare il certificato del server nel modulo con PRSM per assicurarsi che il processo di handshake SSL venga completato correttamente.

Per importare il certificato server, completare i seguenti passaggi:

1. Ignorare il modulo dei servizi NGFW quando si accede al server per scaricare il certificato tramite un browser. Un modo per ignorare il modulo consiste nel creare un criterio di decrittografia che non decrittografi il traffico verso quel particolare server. In questo video viene illustrato come creare il criterio:

   Di seguito sono riportati i passaggi illustrati nel video:

   Per accedere a PRSM sul CX, selezionare **https://<IP_ADDRESS_OF_PRSM>**. In questo esempio viene utilizzato **https://10.106.44.101**.

   Passare a **Configurazioni > Criteri/Impostazioni > Criteri di decrittografia** in PRSM.

   Per aggiungere un criterio all'inizio dell'elenco, fare clic sull'icona situata vicino all'angolo superiore sinistro della schermata e scegliere l'opzione **Aggiungi sopra**.

   Assegnare un nome al criterio, lasciare Origine come **Qualsiasi** e creare un oggetto **gruppo di rete CX**.
   Nota: Ricordarsi di includere l'indirizzo IP del server basato su HTTPS. Nell'esempio, viene usato un indirizzo IP di **172.16.1.1**.Scegliere **Non decrittografare** per l'azione.

   Salvare il criterio ed eseguire il commit delle modifiche.
2. Scaricare il certificato del server tramite un browser e caricarlo nel modulo dei servizi NGFW tramite PRSM, come mostrato in questo video:

   Di seguito sono riportati i passaggi illustrati nel video:

   Una volta definita la regola sopra indicata, utilizzare un browser per passare al server basato su HTTPS che si apre tramite il modulo dei servizi NGFW.
   Nota: Nell'esempio, Mozilla Firefox versione 26.0 viene usato per spostarsi sul server (un'ASDM su un'ASA) con l'URL **https://172.16.1.1**.Accettare l'avviso di protezione se ne viene visualizzato uno e aggiungere un'eccezione di protezione.

   Fare clic sulla piccola icona a forma di lucchetto situata a sinistra della barra degli indirizzi. La posizione di questa icona varia in base al browser utilizzato e alla versione.

   Dopo aver selezionato il certificato server, fare clic sul pulsante **Visualizza certificato** e quindi sul pulsante **Esporta** nella scheda Dettagli.

   Salvare il certificato nel computer personale in un percorso scelto.

Accedere a PRSM e selezionare **Configurazioni > Certificati**.

Fare clic su **Desidero... > Importa certificato** e scegliere il certificato server scaricato in precedenza (dal passaggio 4).

Salvare e confermare le modifiche. Una volta completato, il modulo dei servizi NGFW deve considerare attendibile il certificato presentato dal server.

3. Rimuovere il criterio aggiunto al passaggio 1. Il modulo dei servizi NGFW è ora in grado di completare l'handshake con il server.

Informazioni correlate

- Guida per l'utente di ASA CX e Cisco Prime Security Manager 9.2
- Documentazione e supporto tecnico – Cisco Systems