Resolución de Problemas de Actualización de Definiciones TETRA con Error 3000

Contenido

Introducción

Este documento describe los pasos para resolver el error de definiciones de TETRA con el error 3000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Endpoint

Componentes Utilizados

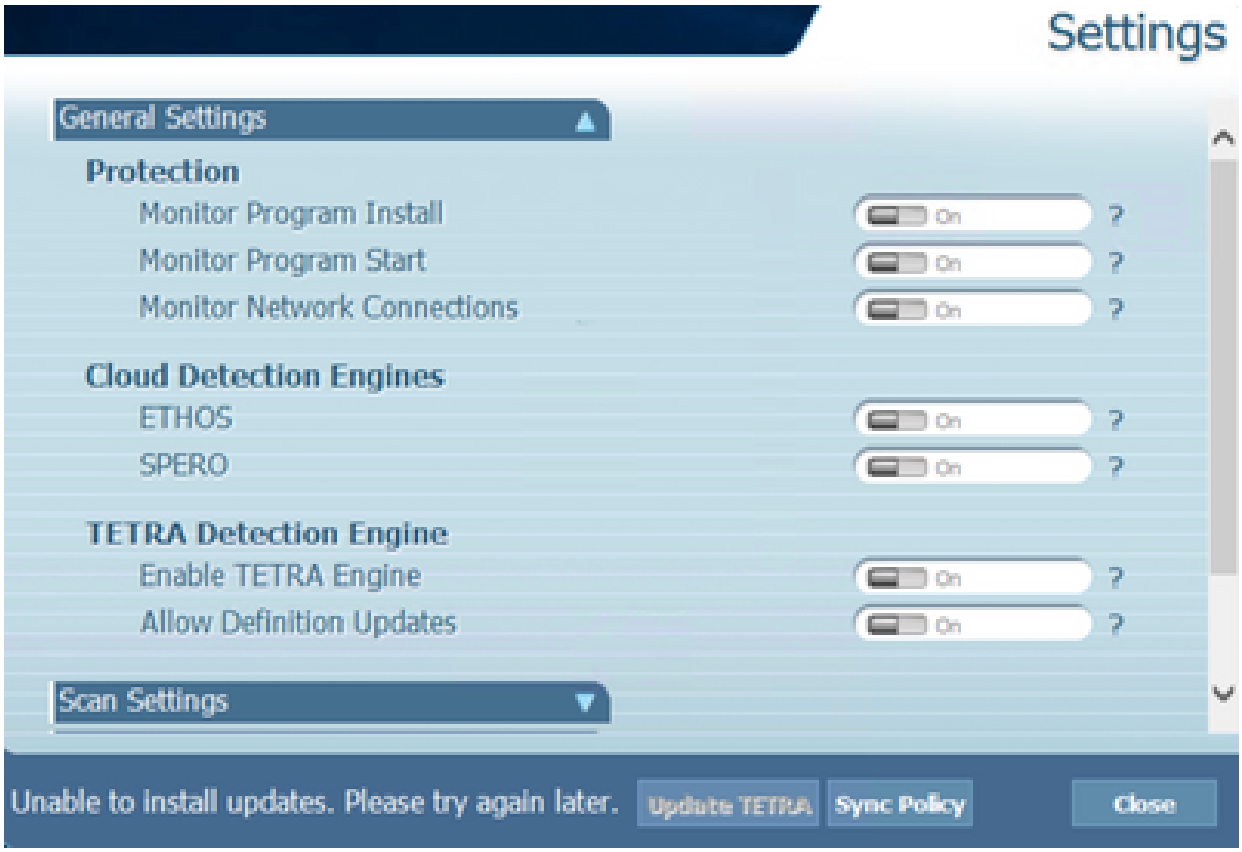
La información de este documento se basa en:

- Cisco Secure Endpoint Connector (cualquier versión)
- Wireshark (cualquier versión)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

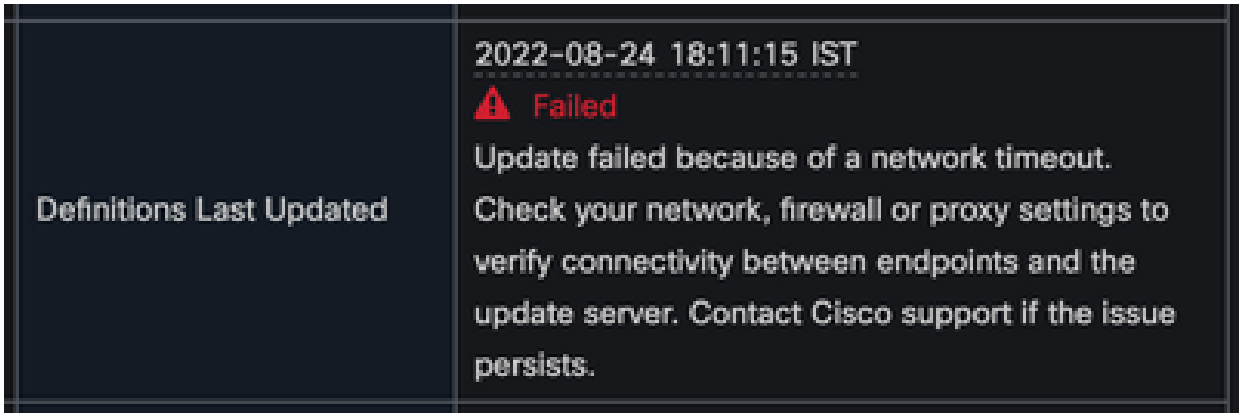
Problema

1. En el terminal, la actualización de las definiciones de TETRA falla con el mensaje de error "No se pueden instalar las actualizaciones. Inténtelo de nuevo más tarde".



2. En Cisco Secure Endpoint Console, se observa el error de falla mencionado:

   "La actualización ha fallado debido a un tiempo de espera de la red. Compruebe la configuración de la red, el firewall o el proxy para verificar la conectividad entre los terminales y el servidor de actualización. Póngase en contacto con el servicio de asistencia de Cisco si el problema continúa."



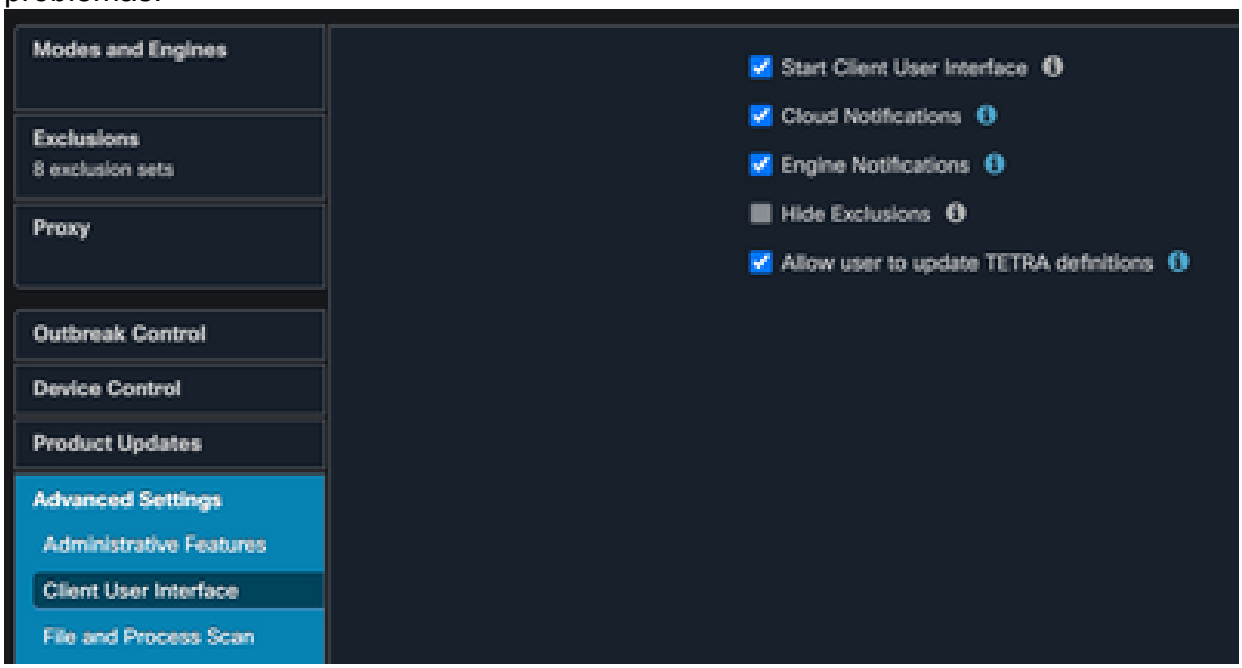
3. En debug sfc.exe.log, las definiciones actualizadas fallaron con el error 3000 que se observa, que significa Unknown_Error como se documentó.
   <#root>

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdateInterface::update updateDir: C:\Progr
(978223515, +0 ms) Aug 04 07:30:23 [11944]: ERROR: TETRAUpdateInterface::update

Update failed with error -3000


(978223515, +0 ms) Aug 04 07:30:23 [11944]: PipeSend: sending message to user interface: 26,
(978223515, +0 ms) Aug 04 07:30:23 [860]: PipeWrite: waiting on pipe event handle
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit defInit: 0, bUpdate: 0
```

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit bUpdate: 0, bReload: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: FASharedPtr<class TETRAUpdateInterface>::Release
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: bUpdated = FALSE, state: 20,
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: sig count: 0, version: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: Config::IsUploadEventEnabled: returns 1, 1
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
```

Solución

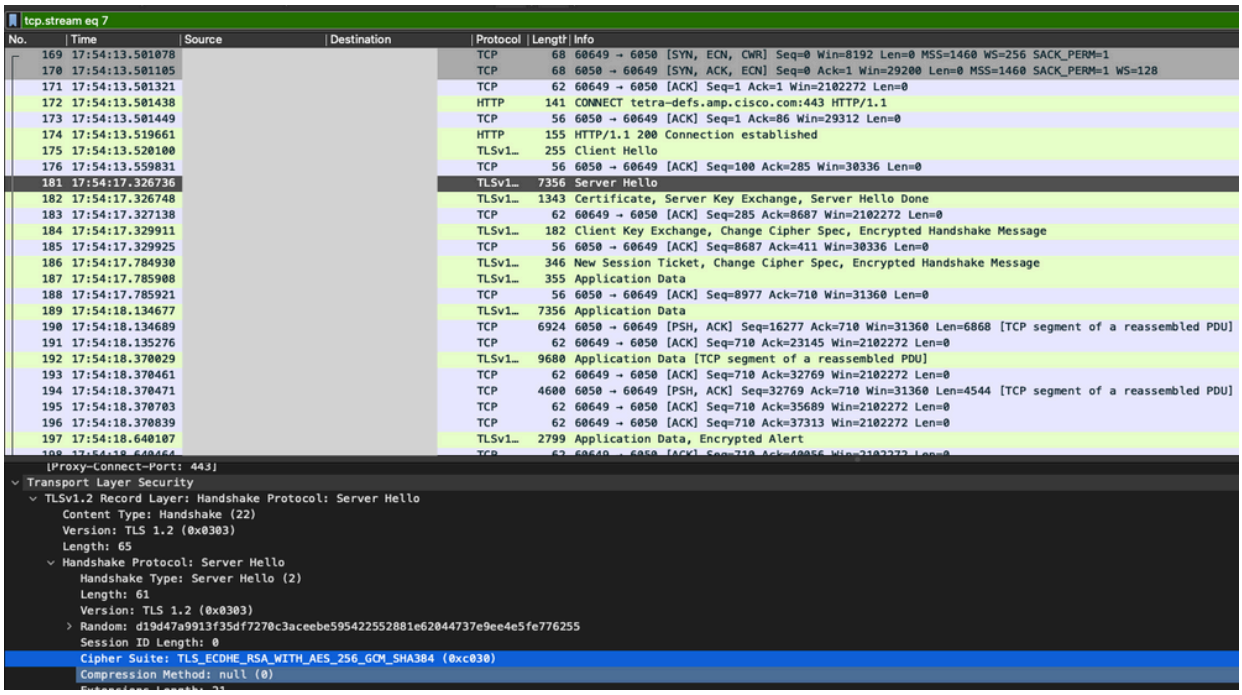
1. Habilite la opción Permitir que el usuario actualice las definiciones de TETRA en Política de AMP > Interfaz de usuario cliente en la Consola. Con este parámetro puede activar la actualización de TETRA según sea necesario durante la resolución de problemas.



2. Además, habilite debug Connector y el registro de nivel de bandeja en el terminal o a través de la política AMP.

3. Por favor tome capturas de paquetes en los terminales exitosos y fallidos de actualización de TETRA para las definiciones de TETRA mientras hace clic en Update TETRA en el terminal.

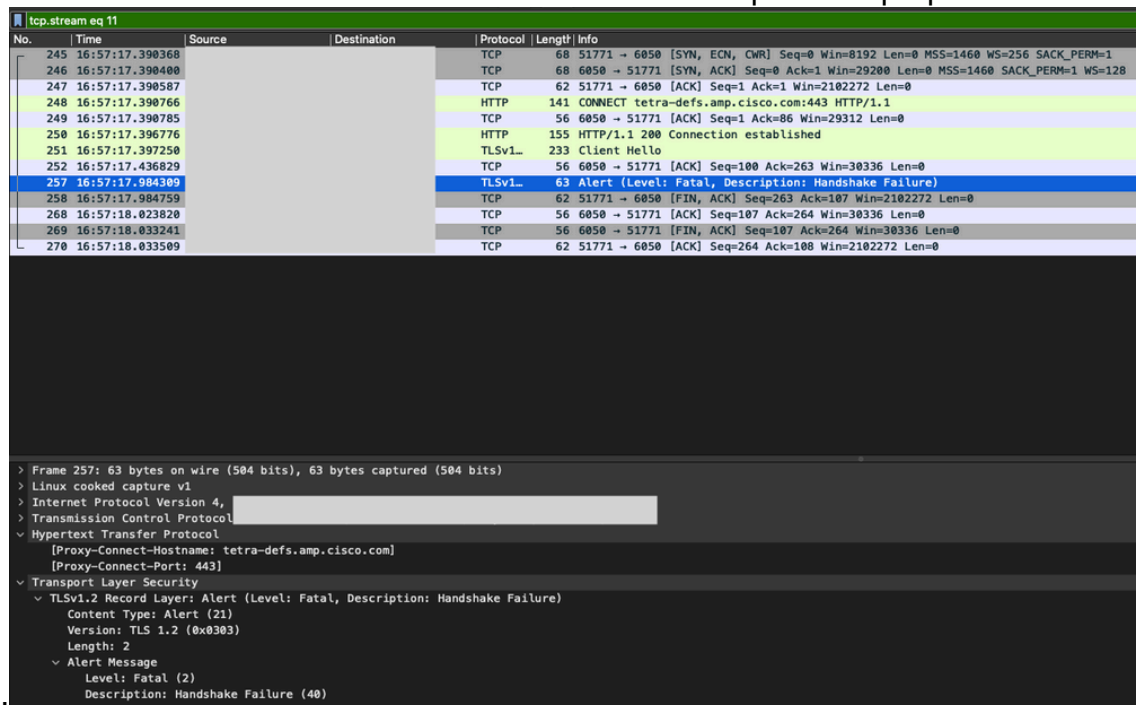
4. En el punto final exitoso de la actualización de TETRA, en el filtro de captura de paquetes los paquetes con http.host == "tetra-defs.amp.cisco.com:443" y luego "siga el tcp.stream" de cada paquete para analizar el tráfico relacionado.
5. En Server Hello packet, puede ver que el servidor acepta el cifrado "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" en Server Hello packet.



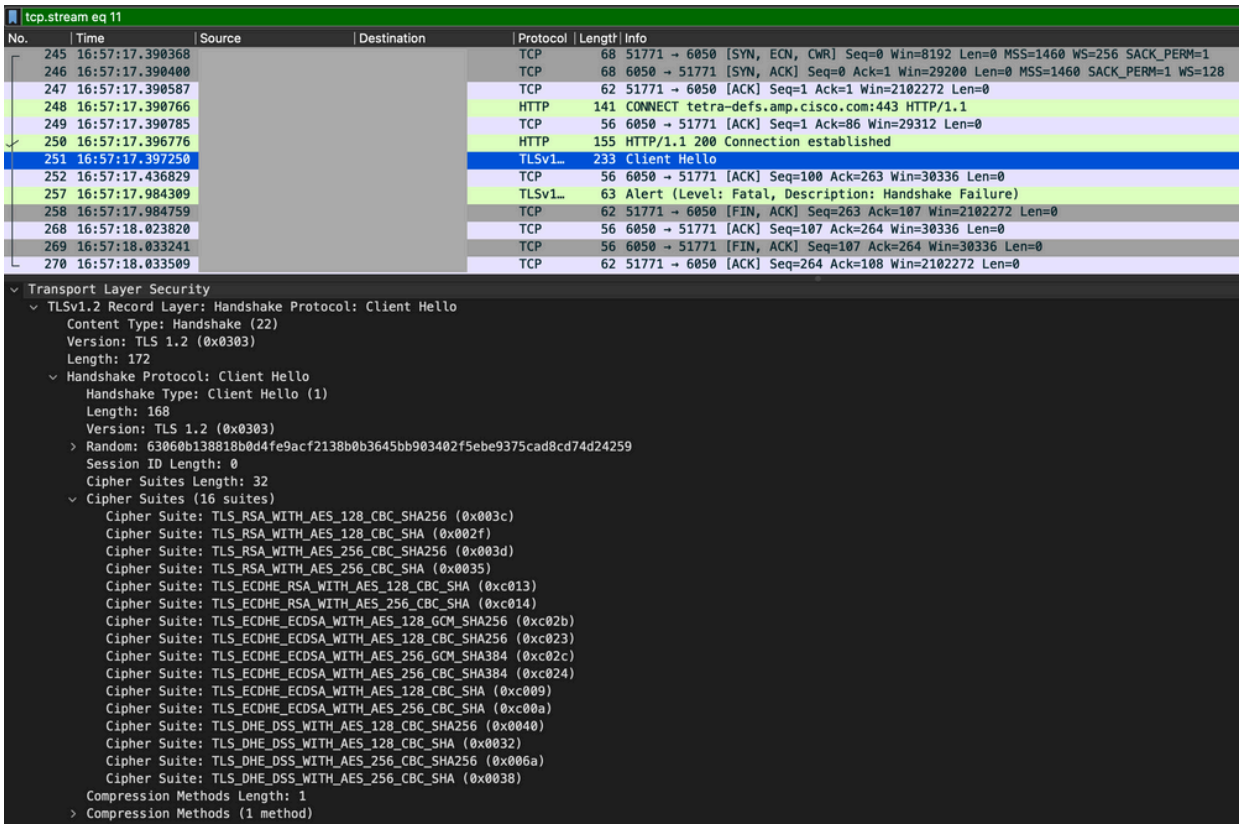
6. El servidor Cisco Secure Endpoint TETRA acepta solo los cifrados mencionados:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_AES_128_GCM_SHA256
```

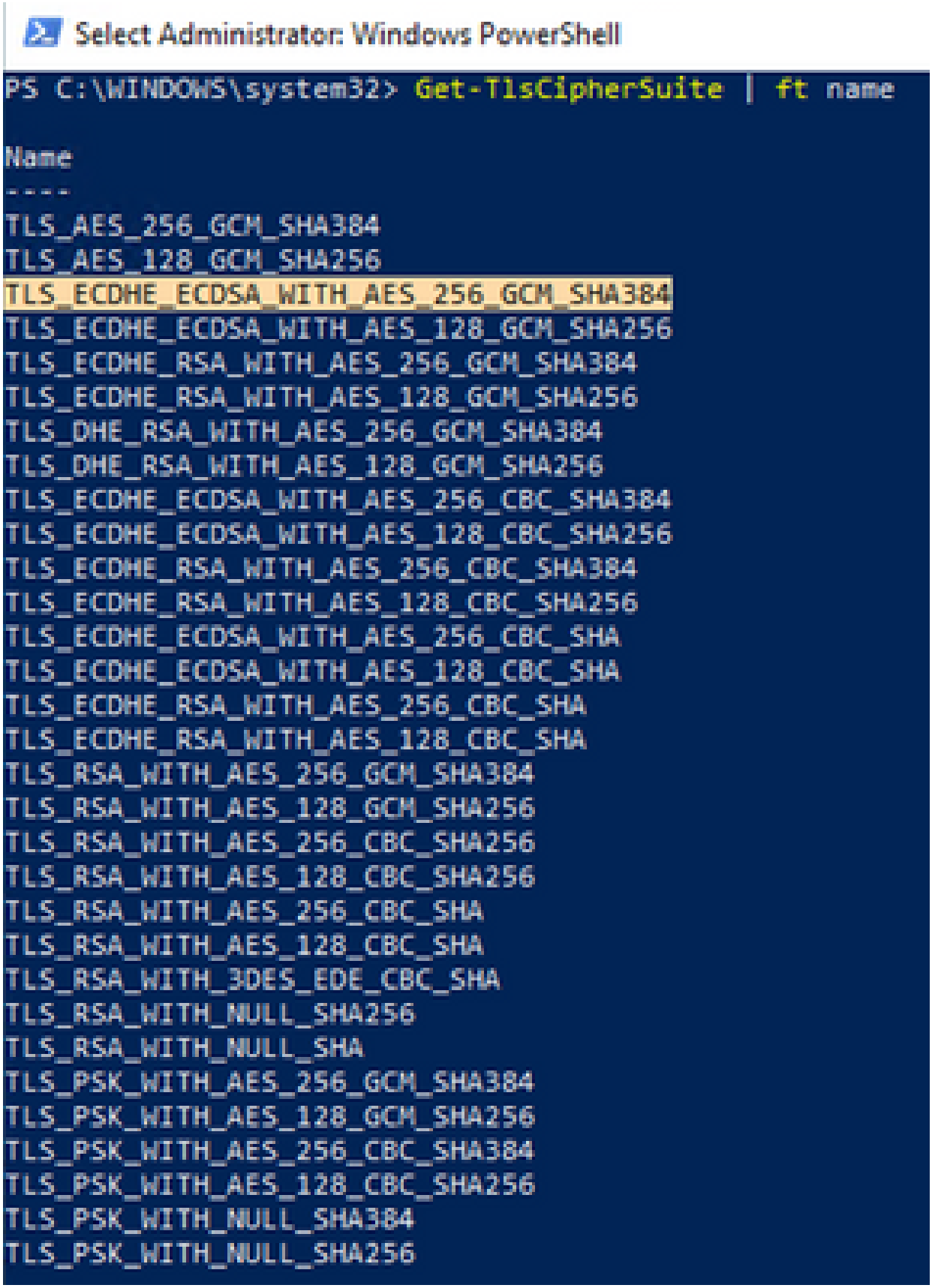
7. En el punto final fallido de la actualización de TETRA, en la captura de paquetes, se observa un error fatal en el intercambio de señales SSL después del paquete Hello del Cliente.



8. En el paquete de saludo del cliente, puede ver los cifrados ofrecidos desde el punto final.

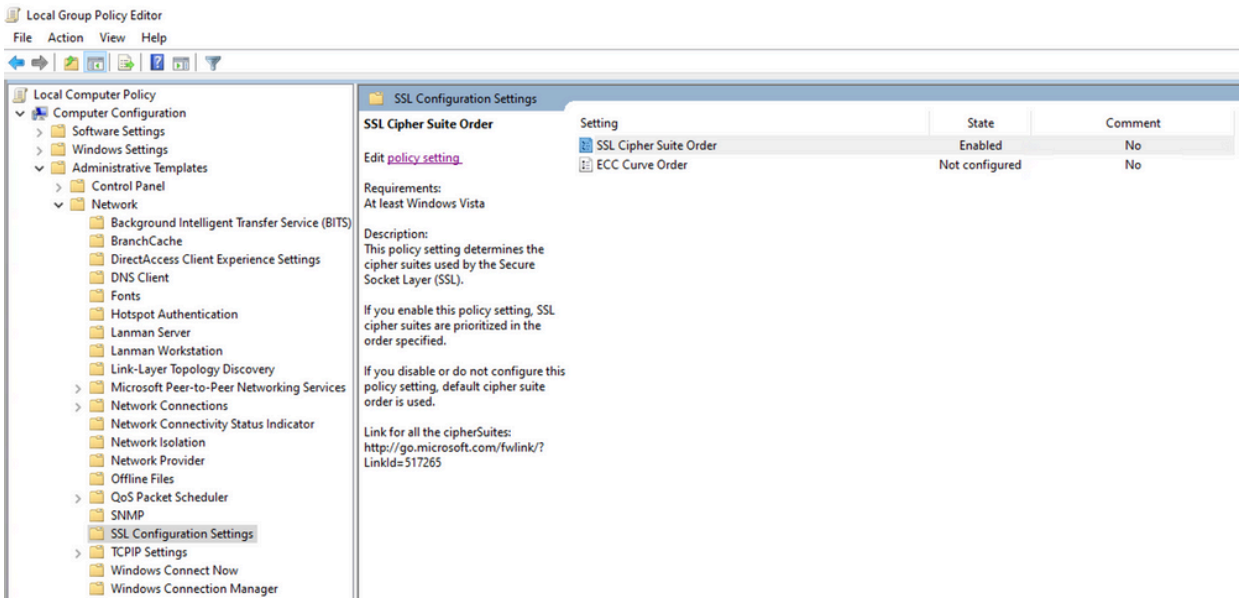


9. Además, puede realizar una verificación cruzada de los Ciphers habilitados en el punto final con Get-TlsCipherSuite | ft name Comando de PowerShell.

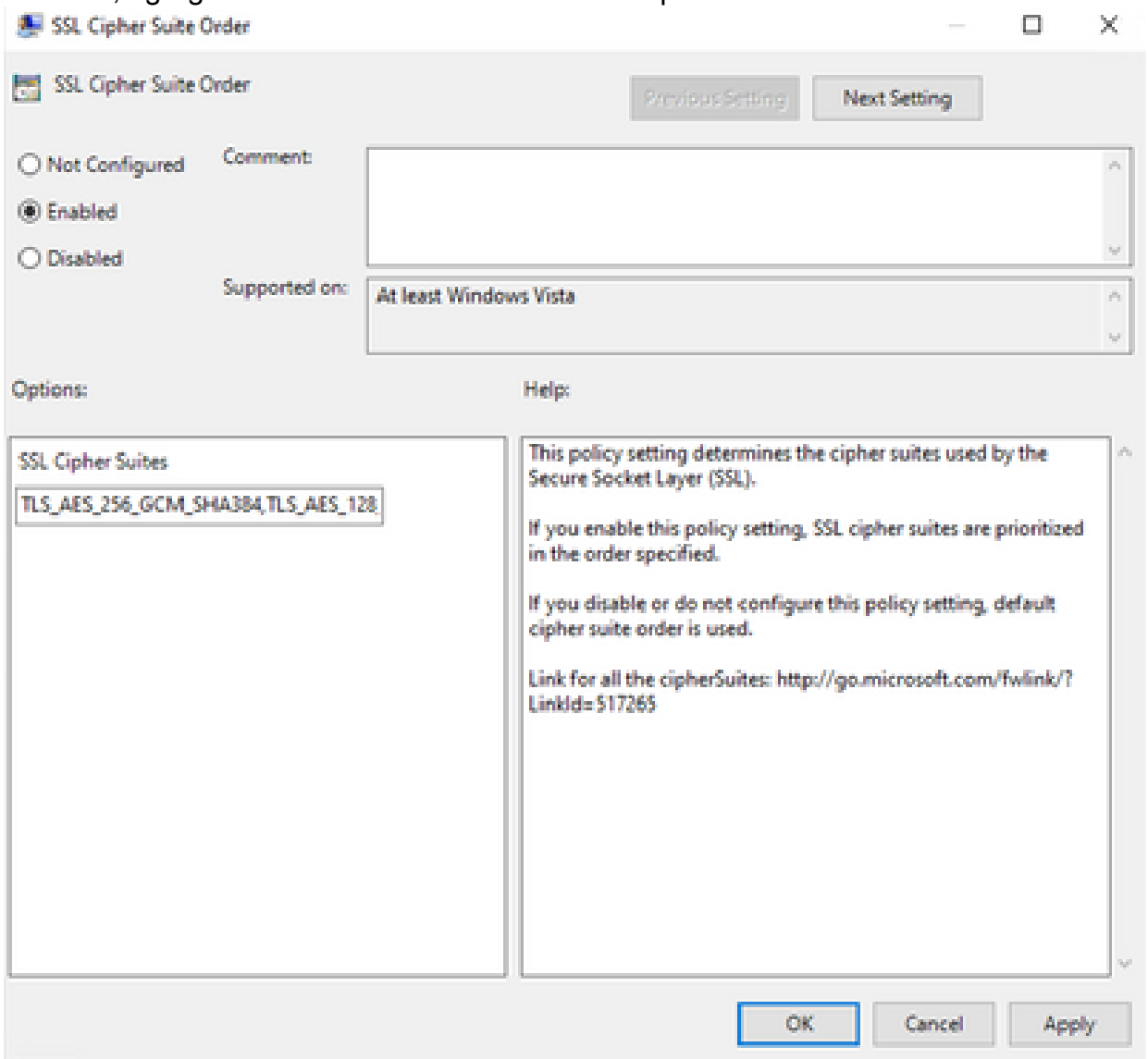


10. En caso de que los cifrados mencionados en el Paso 6 no aparezcan aquí, esa es la razón del fallo del protocolo de enlace SSL.
11. Para solucionar esto, verifique el pedido de SSL Cipher Suite en la política de grupo:

```
Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Templ
```



12. El pedido de Cipher Suite debe ser Not Configured o Disabled y, si se establece en Enabled, agregue los cifrados mencionados en el paso 6 de la lista.



13. Aplique estos cambios y reinicie el terminal para que estos cambios estén disponibles para las aplicaciones.
14. Vuelva a intentar actualizar TETRA una vez que se haya completado el reinicio.

15. En caso de que el problema de las definiciones de TETRA persista, analice los registros y las capturas de nuevo.

Información Relacionada

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).