使用3000错误排除TETRA定义更新故障

目录

简介

本文档介绍对TETRA定义故障进行故障排除的步骤，错误为3000。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Secure Endpoint

使用的组件

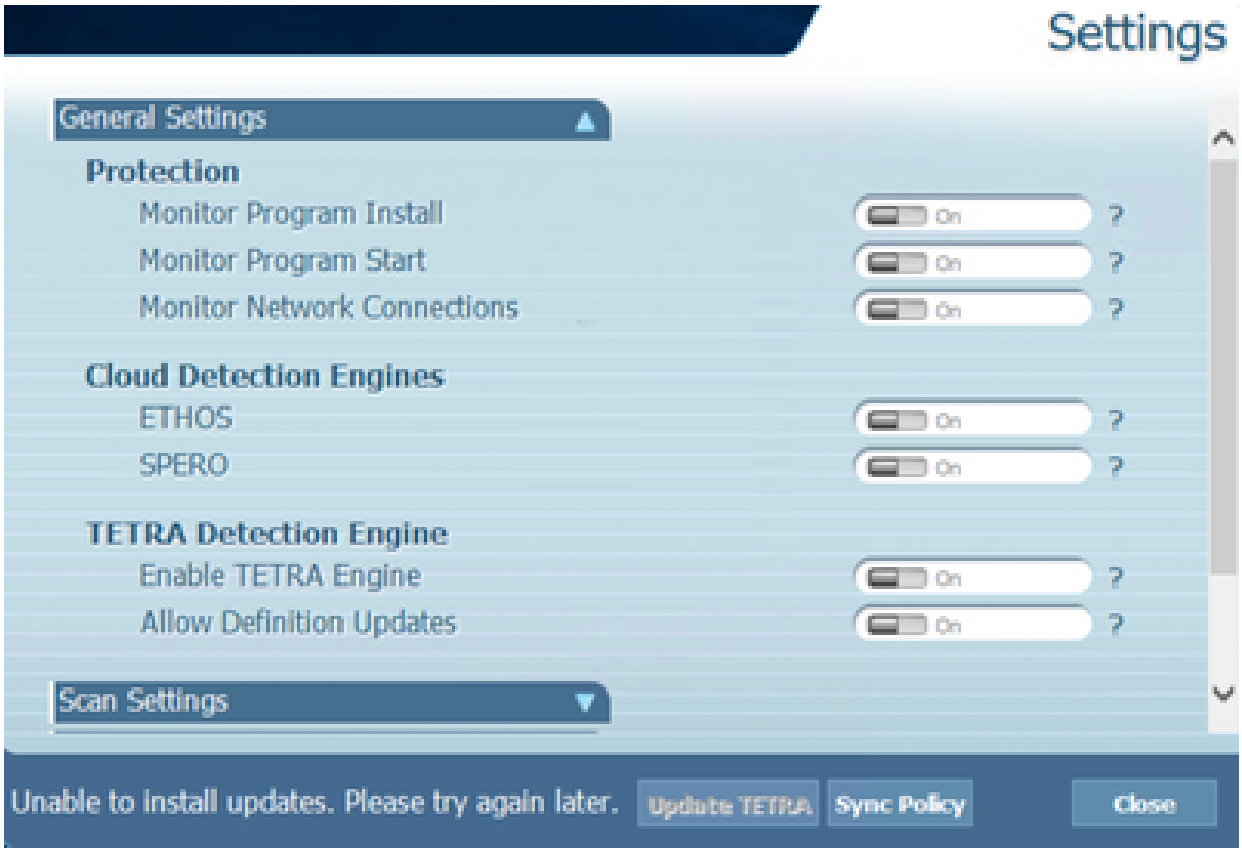
本文档中的信息基于：

- 思科安全终端连接器（任何版本）
- Wireshark（任何版本）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

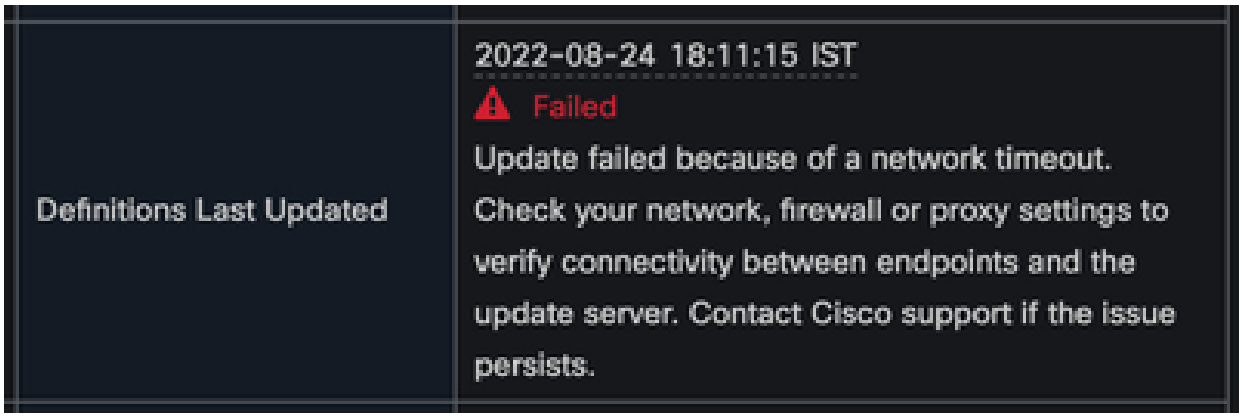
问题

1. 在终端上，TETRA定义更新失败并显示“无法安装更新。请稍后重试”错误消息。



2. 在Cisco Secure Endpoint Console上，观察到所述的故障错误：

“由于网络超时，更新失败。检查您的网络、防火墙或代理设置，以验证终端与更新服务器之间的连接。如果问题仍然存在，请与思科支持部门联系。”



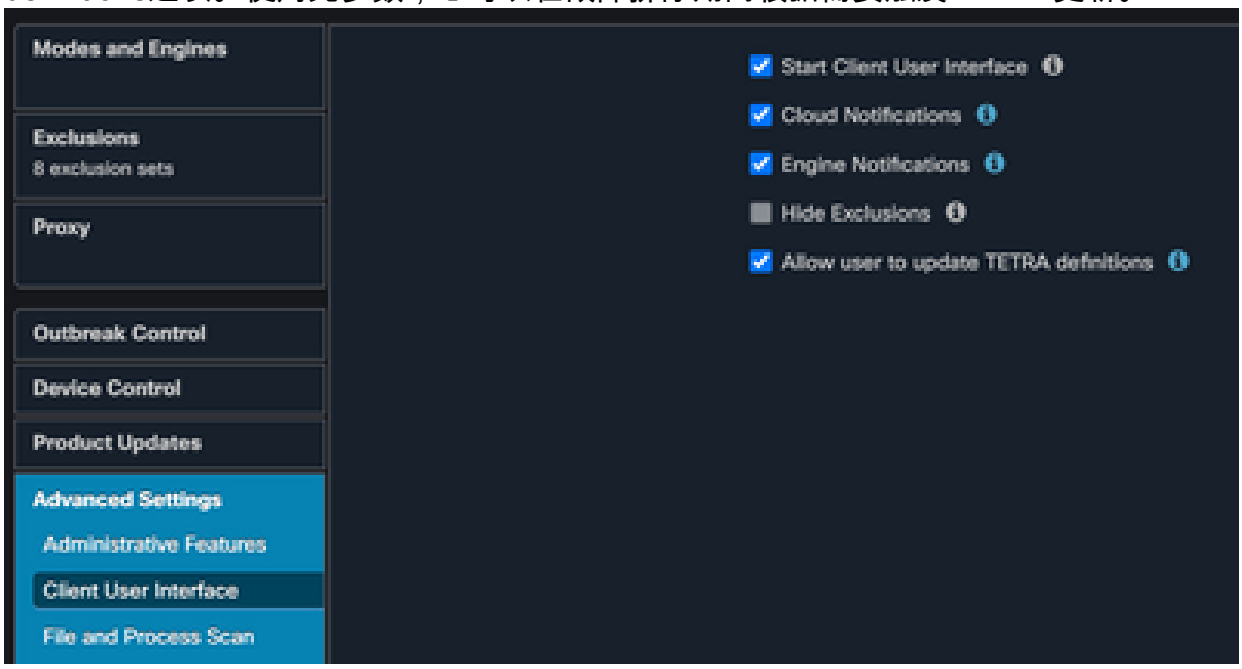
3. 在debug sfc.exe.log中，发现已更新定义失败，错误为3000，这表示Unknown_Error（如记录所示）。
<#root>

```
(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
```

解决方案

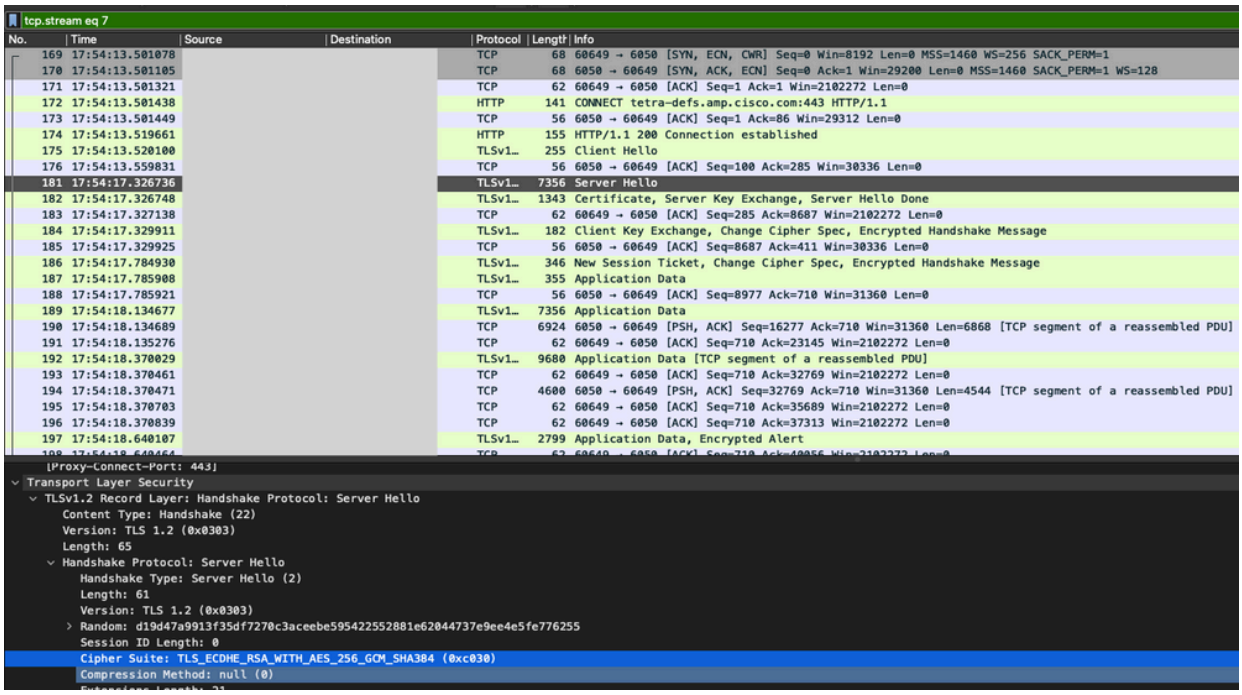
1. 请在控制台的AMP Policy > Client User Interface中启用Allow user to update TETRA definitions选项。使用此参数，您可以在故障排除期间根据需要触发TETRA更新。



2. 此外，在终端上或通过AMP策略启用调试连接器和托盘级别日志。

3. 单击Update TETRA on endpoint时，请在TETRA更新成功和失败的终端上获取TETRA定义的数据包捕获。

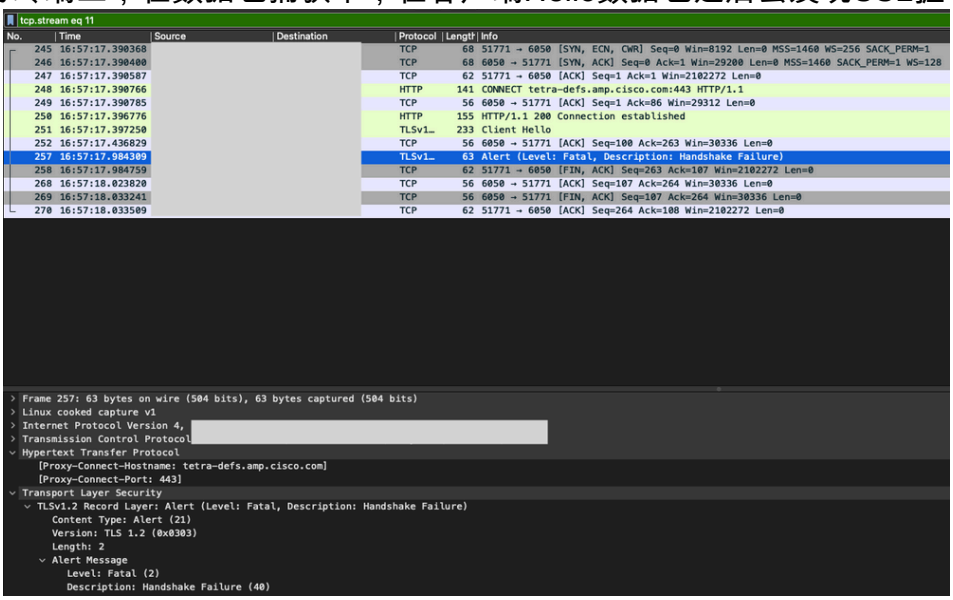
4. 在TETRA更新成功的终端上，数据包捕获使用http.host == "tetra-defs.amp.cisco.com:443"过滤数据包，然后"跟随每个数据包的tcp.stream"分析相关流量。
5. 在服务器Hello数据包中，可以看到服务器在服务器Hello数据包中接受“TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384”密码。



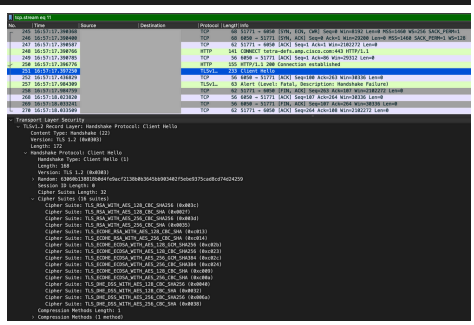
6. 思科安全终端TETRA服务器只接受提到的密码：

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

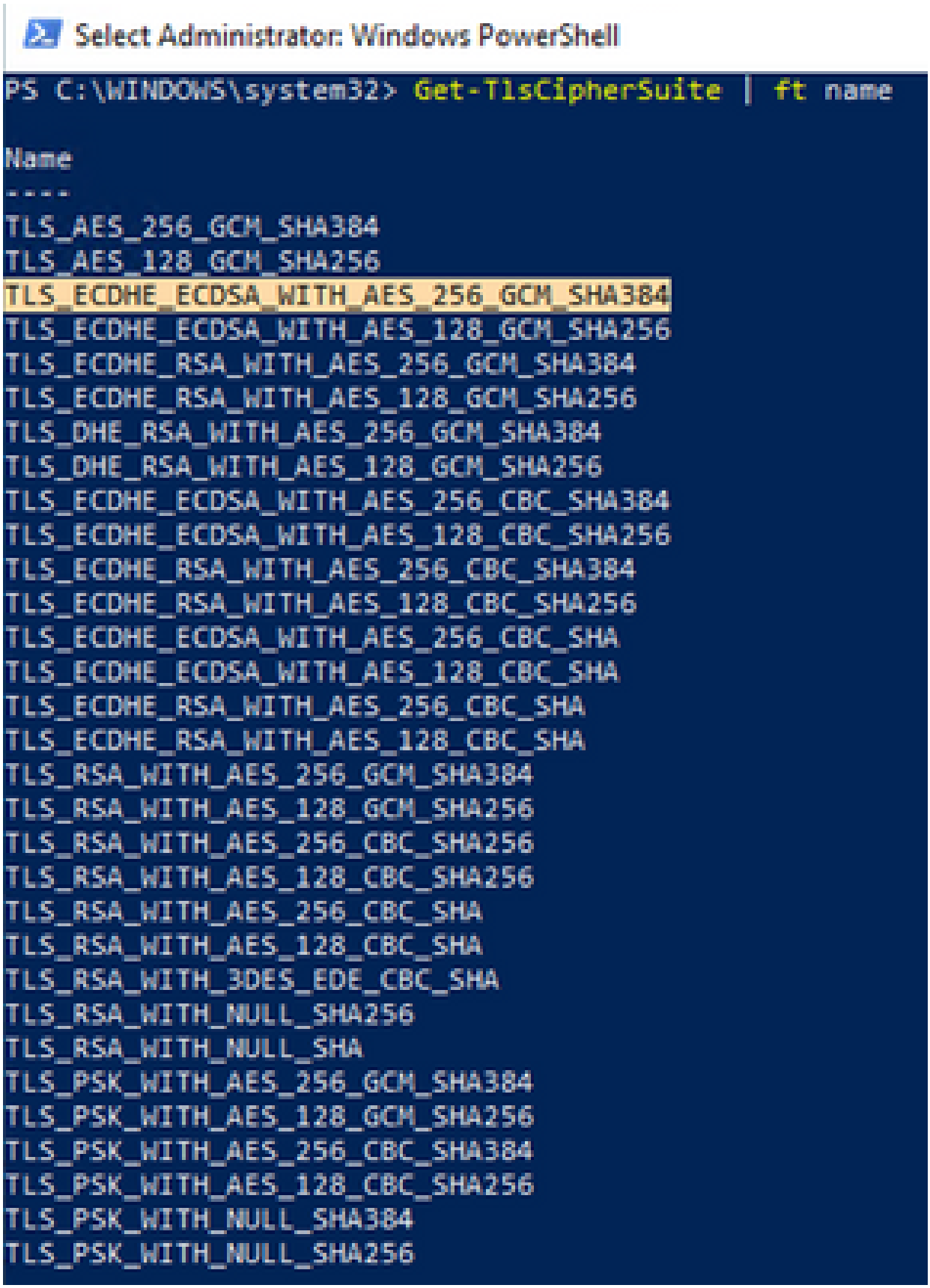
7. 在TETRA更新失败的终端上，在数据包捕获中，在客户端Hello数据包之后会发现SSL握手中出现致命错误。



8. 在Client Hello数据包中，您可以看到终端提供的密码。

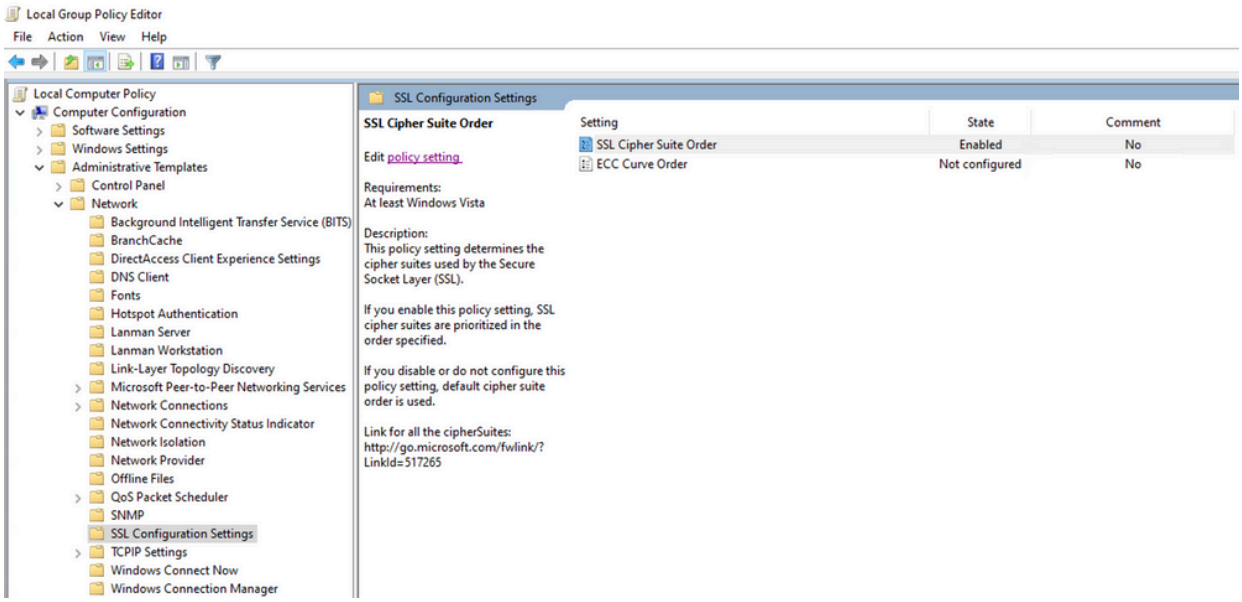


9. 此外，您还可以使用Get-TlsCipherSuite交叉验证终端上启用的密码 | ft name PowerShell命令。

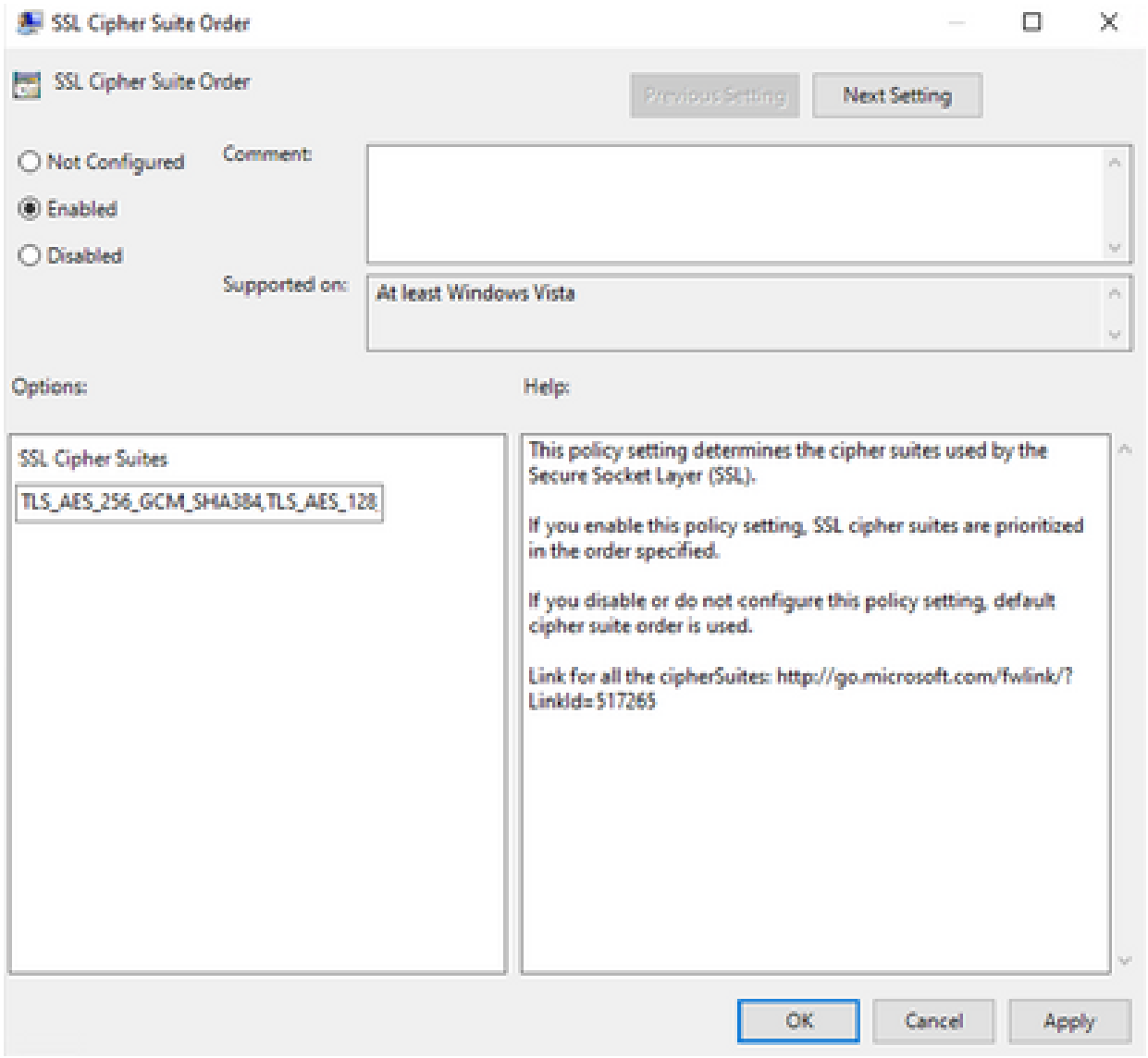


10. 如果此处未列出第6步中提到的密码，则这是SSL握手失败的原因。
11. 要解决此问题，请验证组策略中的SSL密码套件顺序:

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



12. 密码套件顺序必须是Not Configured或Disabled，如果设置为Enabled，请在列表中添加步骤6中提到的密码。



13. 应用这些更改并重新启动终端，使这些更改可用于应用。
14. 重新启动完成后，请重试更新TETRA。

15. 如果TETRA定义问题依然存在，请再次分析日志并捕获数据。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。