Cisco Secure Endpoint - Tetra 정의 업데이트 실패(3000 오류)

목차

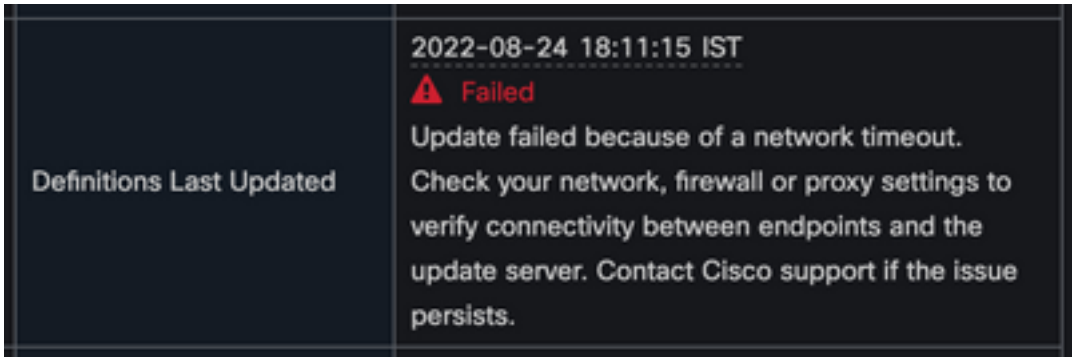
소개

이 문서에서는 오류 3000 오류와 함께 Tetra 정의 오류를 해결하는 단계를 설명합니다.

문제 설명

1. 엔드포인트에서 tetra 정의 업데이트가 실패하고 '업데이트*를 설치할 수 없습니다. 나중에 다시 시도하십시오.*' 오류.

2. AMP Console에서 언급된 오류 메시지가 관찰됩니다. ***실패****네트워크 시간 초과로 인해 업데이트하지 못했습니다. 네트워크, 방화벽 또는 프록시 설정을 확인하여 엔드포인트와 업데이트 서버 간의 연결을 확인합니다. 문제가 계속되면 Cisco 지원에 문의하십시오.*

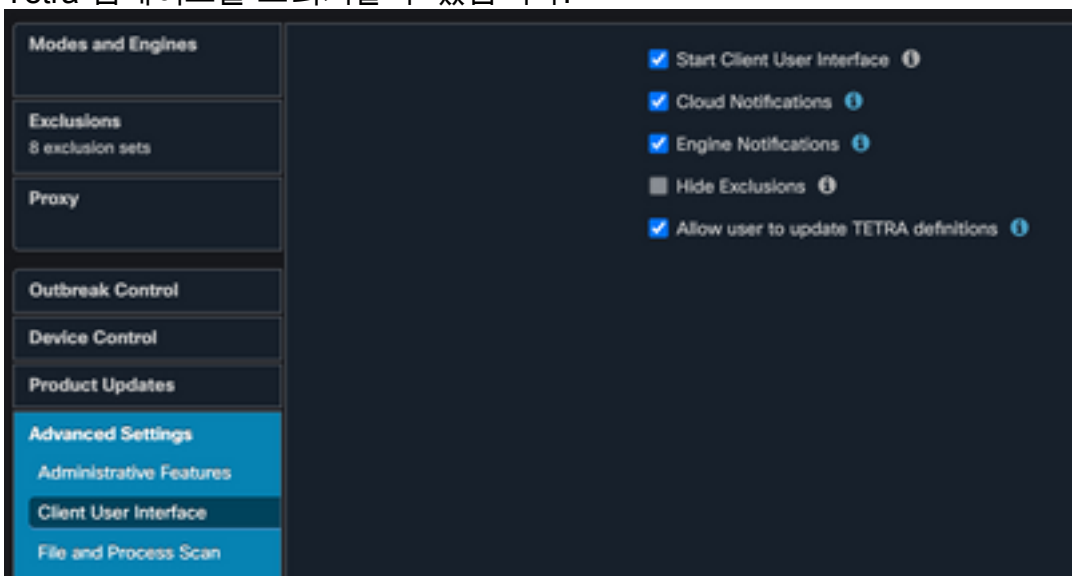


3. debug sfc.exe.log에서는 오류 3000 오류와 함께 업데이트된 정의가 관찰되며, 이는 문서화된 '*Unknown_Error*'를 나타냅니다.

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TetraUpdateInterface::update updateDir:
C:\Program Files\Cisco\AMP\tetra, 20, -3000, -3000, 0, 0, 0
(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, id: 0
(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>::ReleaseInstance count: 1
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTetraUpdate: bUpdated = FALSE, state:
20, status: -3000
(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,
first failure - never, last err code - 4294964296, last upd success - never
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0,
first failure - Thu Aug 4 06:35:16 2022, last err code - 4294964296, last upd success -
never
```

솔루션

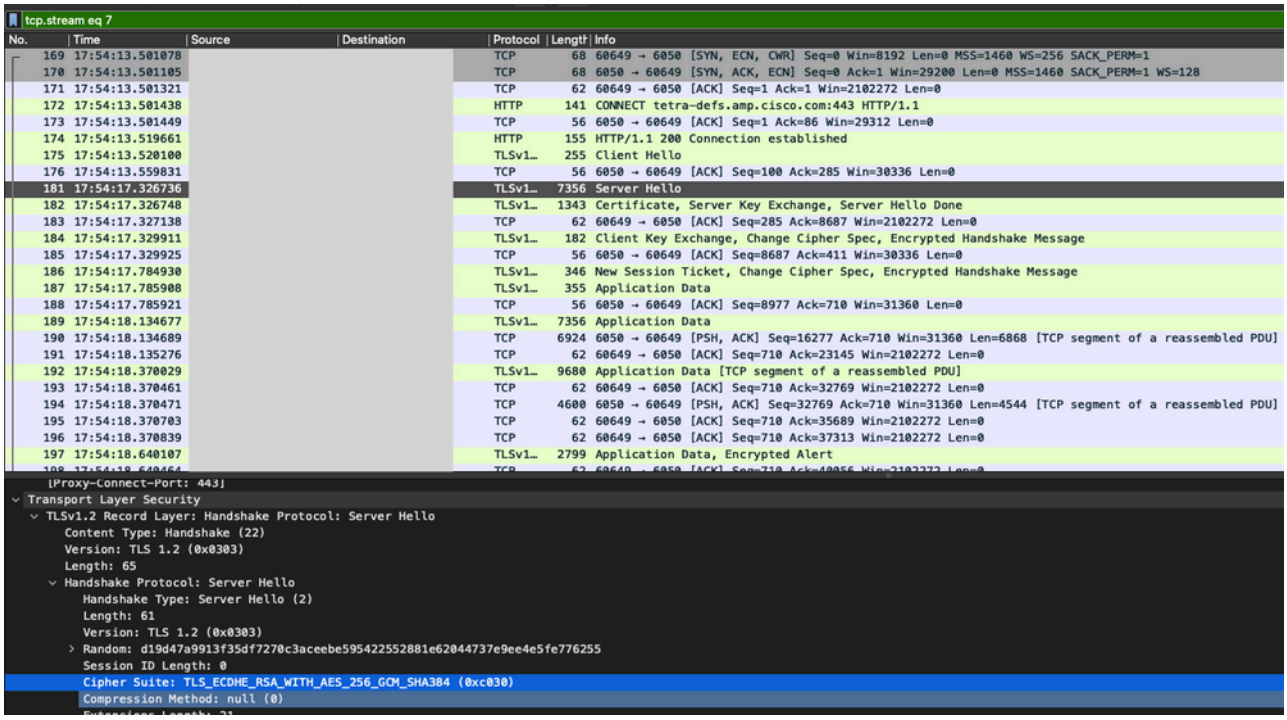
1. 콘솔의 AMP 정책 -> 클라이언트 사용자 인터페이스에서 'Allow user to update Tetra definitions' 옵션을 활성화하십시오. 이 매개변수를 사용하면 문제 해결 중에 필요에 따라 Tetra 업데이트를 트리거할 수 있습니다.



2. 또한 엔드포인트에서 또는 AMP 정책을 통해 디버그 커넥터 및 트레이 레벨 로그를 활성화합니다.

3. 엔드포인트에서 'Update Tetra'를 클릭하는 동안 Tetra 업데이트에 성공하거나 실패한 엔드포인트 모두에서 패킷 캡처를 받으십시오.

4. OnTetra에서 성공한 엔드포인트를 업데이트하면 패킷 캡처에서 패킷을 **http.host == "tetra-defs.amp.cisco.com:443"**으로 필터링한 다음 각 패킷의 tcp.stream을 따라 관련 트래픽을 분석합니다.
5. 'Server Hello' 패킷에서는 Server가 Server Hello 패킷의 'TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384' 암호를 수락하는 것을 볼 수 있습니다.

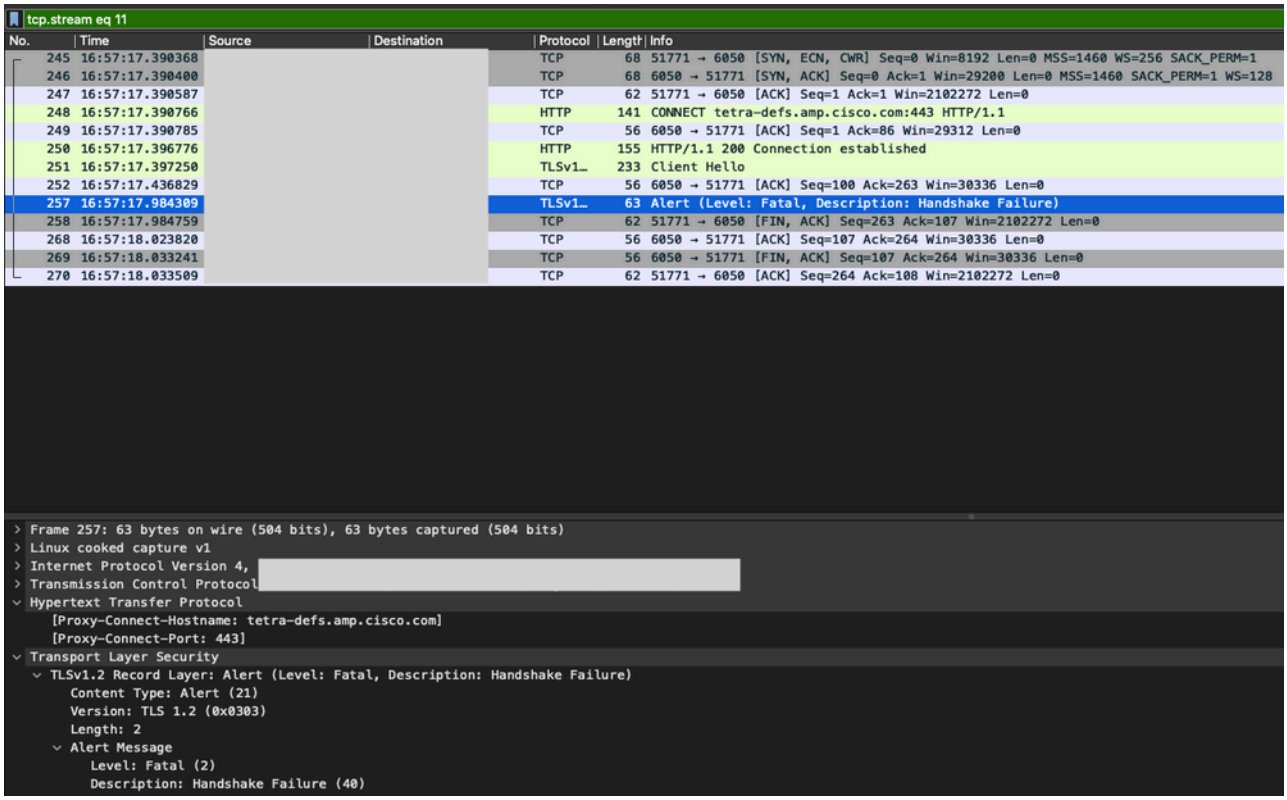


6. AMP Tetra 서버는 다음 암호만 허용합니다.

```
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
```

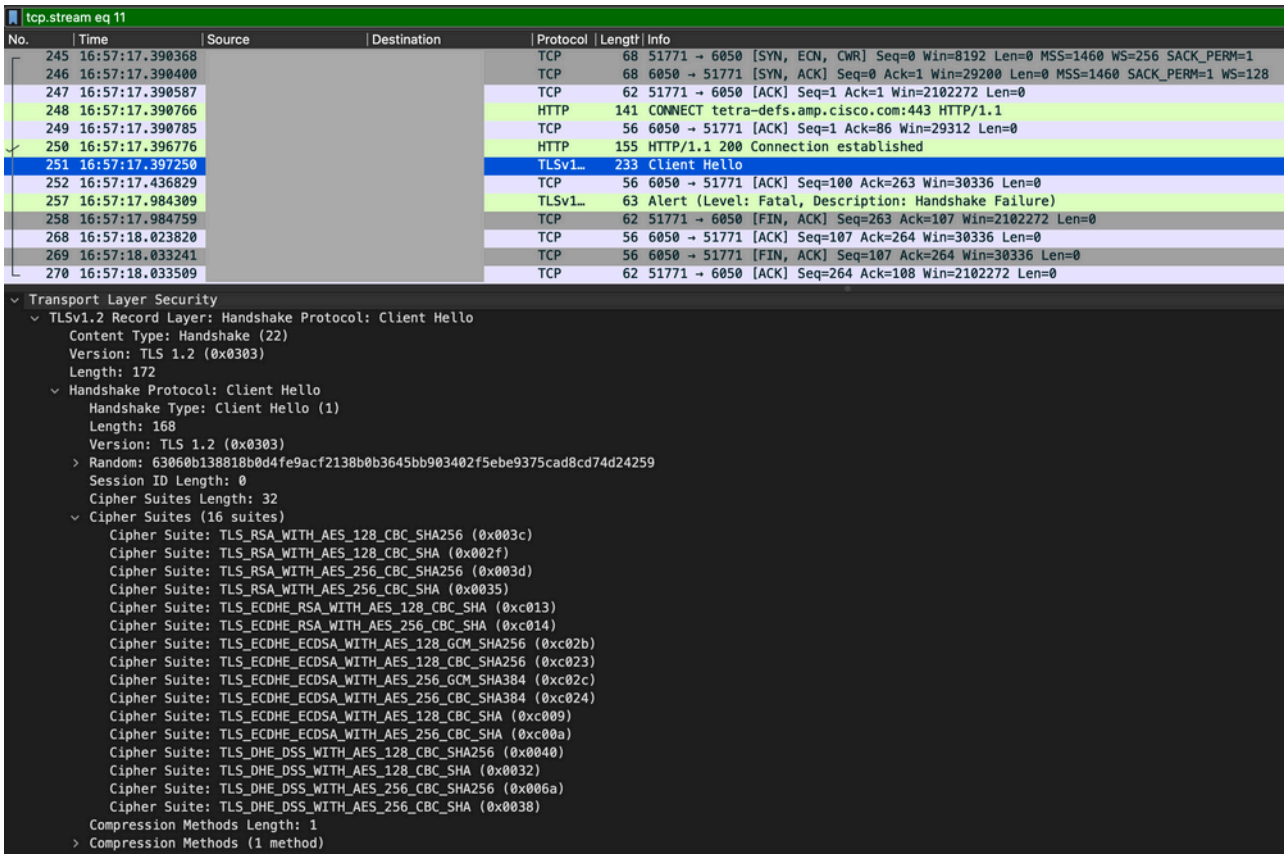
7. Tetra 업데이트 실패 엔드포인트에서 패킷 캡처의 경우 Client Hello 패킷 이후에 SSL 핸드셰이크에 치명적인 오류가 발생합니다

.

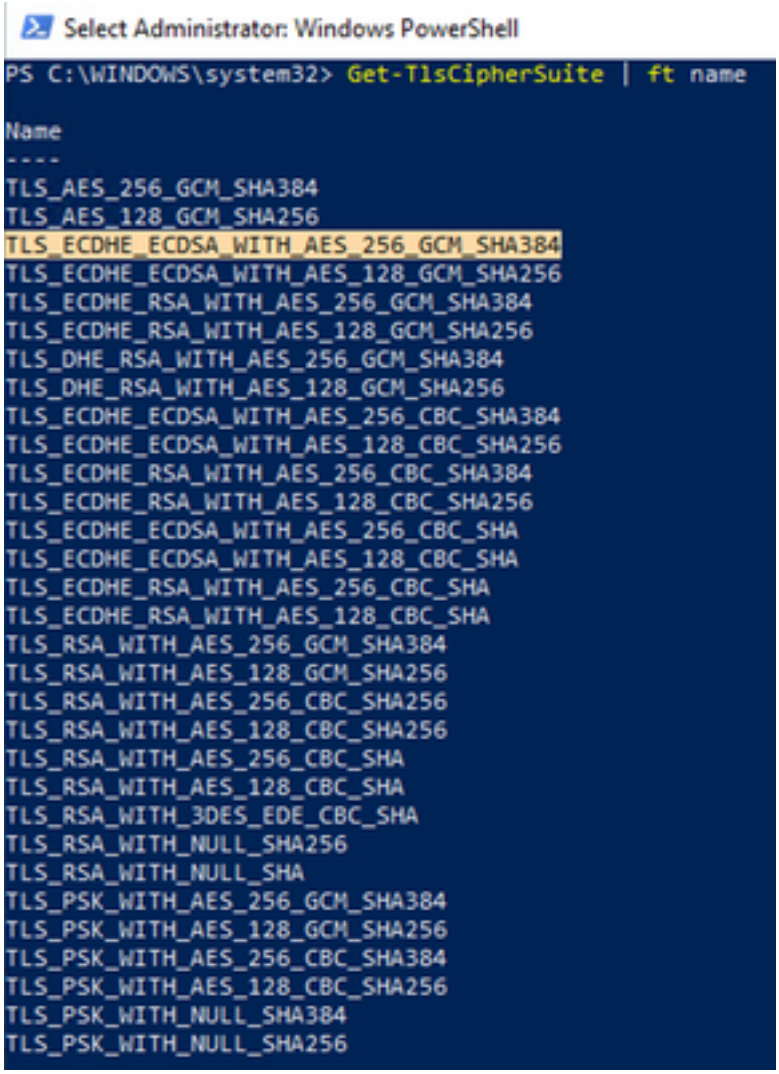


8. Client Hello 패킷에서는 엔드포인트에서 제공된 암호를 볼 수 있습니다

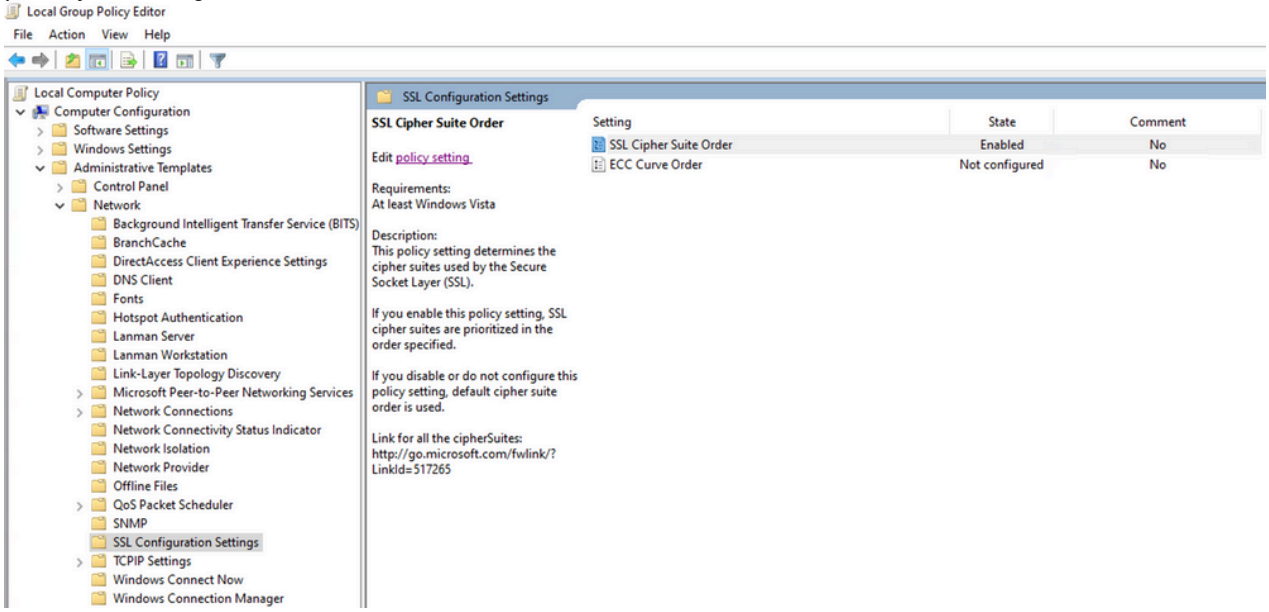
.



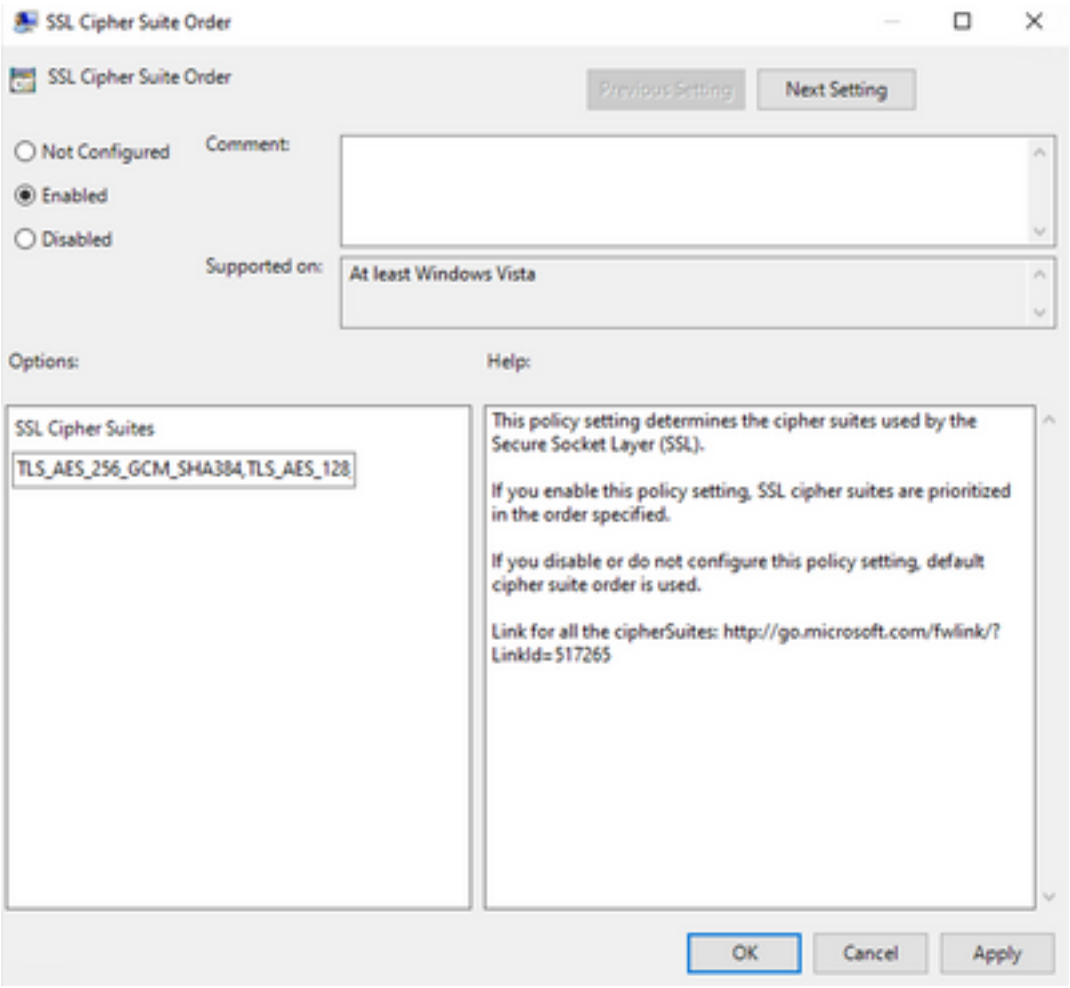
9. 또한 'Get-TlsCipherSuite를 사용하여 엔드포인트에서 활성화된 암호를 교차 확인할 수 있습니다 | ft name' PowerShell 명령입니다.



10. 6단계에서 언급한 암호가 여기에 나열되지 않은 경우 SSL 핸드셰이크 실패의 원인이 됩니다.
11. 이 문제를 해결하려면 그룹 정책에서 'SSL 암호 그룹 순서'를 확인하십시오.
    `Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Templates -> Network -> SSL Configuration Settings -> SSL Cipher Suite Order -> Edit policy setting`



12. 암호 그룹 순서는 '구성되지 않음' 또는 '사용 안 함'이어야 하며, '사용'으로 설정된 경우 6단계에서 언급한 암호를 목록에 추가하십시오.



13. 이러한 변경 사항을 적용하고 엔드포인트를 재부팅하여 애플리케이션에서 이러한 변경 사항을 사용할 수 있도록 합니다.
14. 재부팅이 완료되면 'Update Tetra'를 다시 시도하십시오.
15. Tetra 정의 문제가 지속될 경우 로그를 분석하고 다시 캡처하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.