防火牆從ASA遷移到FTD後，身份服務引擎(ISE)3.3狀態驗證失敗

目錄

問題

報告的問題可能顯示為處於「未知」狀態合規狀態的終結點。此外，無法向使用者顯示狀態調配門戶。

在某些情況下，客戶報告從ASA遷移到FTD後，他們重複使用相同的配置；但是，FTD需要額外的和特定的設定才能使狀態VPN正常工作。

環境

- 思科身分識別服務引擎(ISE)版本3.3
- 帶兩個節點的ISE部署
- 思科安全使用者端版本5.1.7.80
- Firepower威脅防禦(FTD)版本7.4.1.1
- 終端通過VPN連線
- 狀態驗證的相關IP地址：72.163.1.80(enroll.cisco.com)

解析

這些步驟詳細說明了遷移到FTD後用於識別、診斷和解決ISE狀態驗證問題的工作流。為了清楚起見，每個步驟都有說明，並直接引用在環境中觀察到的日誌和配置指示符。

第1步：收集DART套件以驗證探測

檢查嘗試VPN連線的端點的狀態狀態是否有任何錯誤或停滯狀態。檢視ISE狀態代理日誌(ISEPosture.txt)以瞭解指示伺服器伺服器無效或不可訪問狀態的錯誤消息。

指示問題的日誌摘錄示例：

2026/01/05 15:38:26 [警告] csc_iseagent函式：目標：:parsePostureStatusResponse執行緒ID:0x32D0檔案：Target.cpp行： 370級別：警告頭端為空。內容可能不是「X-ISE-PDP」的形式。

2026/01/05 15:38:26 [資訊] csc_iseagent函式：目標：：探測執行緒ID: 0x32D0檔案：Target.cpp行： 212級別：調試重定向的狀態192.168.1.254為5 <伺服器無效。>

2026/01/05 15:38:28 [資訊] csc_iseagent函式： SwiftHttpRunner::http_discovery_callback執行緒

Id: 0x1AD8檔案： SwiftHttpRunner.cpp行： 519級別
： info Time out for Redirection target enroll.cisco.com。

2026/01/05 15:38:28 [資訊] csc_iseagent函式： SwiftHttpRunner::http_discovery_callback執行緒Id: 0x1AD8檔案： SwiftHttpRunner.cpp行： 580級別：資訊啟用下一輪計時器。

2026/01/05 15:38:28 [資訊] csc_iseagent函式： GetCurrentUserName執行緒ID: 0x1AD8檔案：ImpersonateUser.cpp行： 60級別：資訊當前登入使用者的使用者名稱是basheer.mohamed。

2026/01/05 15:38:29 [資訊] csc_iseagent函式： hs_transport_winhttp_get執行緒ID: 0x698C檔案：hs_transport_winhttp.c行： 4912級別： debug請求超時。

2026/01/05 15:38:29 [資訊] csc_iseagent函式：目標：:probeDiscoveryUrl執行緒ID: 0x698C檔案：Target.cpp行： 269級別：debug GET request to URL(http://enroll.cisco.com/auth/discovery?architecture=9)，返回狀態–1 <操作失敗。>

2026/01/05 15:38:29 [資訊] csc_iseagent函式：目標：：探測執行緒ID: 0x698C檔案：Target.cpp行： 212級別：調試重定向的狀態target enroll.cisco.com為6 <無法訪問。>

在這種情況下，無法訪問enroll.cisco.com，從而導致發現過程失敗。

第2步：確認ISE授權配置檔案和即時日誌

驗證RADIUS即時日誌是否正確推送到終結點。它必須包含訪問接受和URL重定向引數以進行狀態驗證。

範例：

訪問型別= ACCESS_ACCEPT

cisco-av-pair = url-redirect-acl=redirect

cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=4cb1f740-e371-11e6-92ce-005056873bd0&action=cpp

對於此特定示例，我們已確認重定向正在按預期工作；但是，發現過程失敗，因為網關被報告為無效的伺服器。在VPN整合方案中可以預料到此行為，因為終結點不依賴VPN網關進行發現。請改用 the endpoint attempts to reach the ISE node using enroll.cisco.com。

步驟3.驗證FTD中的ACL設定

驗證重新導向ACL以及為分割通道設定的ACL中是否明確允許enroll.cisco.com。

要檢查兩個ACL，您可以在FMC中導航到Object > Object Management > Access List > Extended。

要檢查VPN中是否配置了拆分隧道，請導航至Devices > VPN > Remote Access > Choose the VPN and Connection Profile settings > Edit Group Policy > Split Tunnel。

注意：如果未在VPN策略上配置拆分隧道，則不需要此驗證，因此此場景中不需要拆分隧道ACL。

原因

問題的根本原因是遷移到Firepower威脅防禦(FTD)後，網路策略中缺少所需的發現IP地址(72.163.1.80, enroll.cisco.com)。

如果沒有此IP，思科安全客戶端無法在通過VPN連線時發現ISE策略服務節點，導致狀態狀態保持為掛起狀態。此外，終端上禁用位置服務導致狀態驗證不完整。

相關內容

- 思科支援

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。