Identity Services Engine (ISE) 3.3 Validierung des Status nach Firewall-Migration von ASA zu FTD fehlgeschlagen

Inhalt

Problem

Das gemeldete Problem kann als Endpunkt auftreten, der noch den Status "Unbekannt" aufweist. Außerdem kann dem Benutzer das Posture Provisioning Portal nicht angezeigt werden.

In einigen Szenarien haben Kunden berichtet, dass sie nach der Migration von ASA zu FTD dieselbe Konfiguration wiederverwendet haben. FTD benötigt jedoch zusätzliche und spezifische Einstellungen, damit Posture VPN ordnungsgemäß funktioniert.

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.3
- ISE-Bereitstellung mit zwei Knoten
- Cisco Secure Client Version 5.1.7.80
- Firepower Threat Defense (FTD) Version 7.4.1.1
- Über VPN verbundene Endpunkte
- Relevante IP-Adresse für die Statusüberprüfung: 72.163.1.80 (enroll.cisco.com)

Auflösung

Diese Schritte beschreiben den Workflow für die Identifizierung, Diagnose und Behebung des ISE-Statusüberprüfungsproblems nach der Migration zu FTD. Jeder Schritt wird der Übersichtlichkeit halber mit direkten Verweisen auf Protokolle und Konfigurationsindikatoren erläutert, die in der Umgebung beobachtet wurden.

Schritt 1: Sammeln Sie ein DART-Paket ein, um die Sonden zu überprüfen.

Überprüfen Sie den Status von Endpunkten, die eine VPN-Verbindung herstellen, auf Fehler oder blockierte Zustände. Überprüfen Sie die ISE-Statusagentenprotokolle (ISEPosture.txt) auf Fehlermeldungen, die auf ungültige Server oder einen nicht erreichbaren Status hinweisen.

Beispiel für einen Protokollauszug, der das Problem angibt:

2026/01/05 15:38:26 [Warnung] csc_iseagent Funktion: Ziel::parsePostureStatusResponse Thread ID: 0x32D0 Datei: Target.cpp Zeile: 370 Ebene: warn Headend ist leer. Möglicherweise

hat der Inhalt nicht das Format 'X-ISE-PDP'.

2026/01/05 15:38:26 [Information] csc_iseagent Funktion: Target::Probe Thread Id: 0x32D0 Datei: Target.cpp Zeile: 212 Ebene: debug Status of Redirection target 192.168.1.254 is 5 <Ungültiger Server.>

2026/01/05 15:38:28 [Information] csc_iseagent Funktion: SwiftHttpRunner::http_discovery_callback Thread ID: 0x1AD8 Datei: SwiftHttpRunner.cpp Zeile: 519 Level: info Time out for Redirection target enroll.cisco.com.

2026/01/05 15:38:28 [Information] csc_iseagent Funktion: SwiftHttpRunner::http_discovery_callback Thread ID: 0x1AD8 Datei: SwiftHttpRunner.cpp Zeile: 580 Level: info Aktivieren des nächsten Round-Timers.

2026/01/05 15:38:28 [Information] csc_iseagent Funktion: GetCurrentUserName Thread ID: 0x1AD8 Datei: ImpersonateUser.cpp Zeile: 60 Ebene: info Benutzername des momentan angemeldeten Benutzers ist basheer.mohamed.

2026/01/05 15:38:29 [Information] csc_iseagent Funktion: hs_transport_winhttp_get Thread ID: 0x698C Datei: hs_transport_winhttp.c Zeile: 4912 Ebene: debug Die Anfrage ist abgelaufen.

2026/01/05 15:38:29 [Information] csc_iseagent Funktion: Target::probeDiscoveryUrl Thread Id: 0x698C Datei: Target.cpp Zeile: 269 Ebene: debug GET request to URL (http://enroll.cisco.com/auth/discovery?architecture=9), return status -1 <Operation Failed.>.

2026/01/05 15:38:29 [Information] csc_iseagent Funktion: Target::Probe Thread Id: 0x698C Datei: Target.cpp Zeile: 212 Ebene: debug Status of Redirection target enroll.cisco.com is 6 <Nicht erreichbar.>.

In diesem Fall ist enroll.cisco.com nicht erreichbar, wodurch der Erkennungsprozess fehlschlägt.

Schritt 2: Bestätigen des ISE-Autorisierungsprofils und der Live-Protokolle

Überprüfen Sie, ob das RADIUS-Livelog korrekt an den Endpunkt weitergeleitet wurde. Es muss die Parameter "Access Accept" und "URL Redirect" für die Statusüberprüfung enthalten.

Beispiel:

Zugriffstyp = 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

Für dieses Beispiel haben wir bestätigt, dass die Umleitung wie erwartet funktioniert. Der Erkennungsvorgang schlägt jedoch fehl, da das Gateway als ungültiger Server gemeldet wird. Dieses Verhalten kann in einem VPN-Integrationsszenario erwartet werden, da der Endpunkt für

die Erkennung nicht auf das VPN-Gateway angewiesen ist. Stattdessen wird
the endpoint attempts to reach the ISE node using enroll.cisco.com.

Schritt 3: Überprüfen der ACLs-Einstellungen im FTD

Stellen Sie sicher, dass enroll.cisco.com in der Umleitungs-ACL und in der für den Split-Tunnel konfigurierten ACL explizit zulässig ist.

Um beide ACLs zu überprüfen, können Sie im FMC zuObject > Object Management > Access List > Extended navigieren.

Um zu überprüfen, ob Split Tunnel im VPN konfiguriert ist, navigieren Sie zu Devices > VPN > Remote Access > Choose the VPN and Connection Profile settings > Edit Group Policy > Split Tunnel.

Hinweis: Wenn Split Tunnel in der VPN-Richtlinie nicht konfiguriert ist, ist diese Validierung nicht erforderlich. Daher wird in diesem Szenario die Split Tunnel-ACL nicht benötigt.

Ursache

Die Ursache des Problems war das Fehlen der erforderlichen Ermittlungs-IP-Adresse (72.163.1.80, enroll.cisco.com) in der Netzwerkrichtlinie nach der Migration zu Firepower Threat Defense (FTD).

Ohne diese IP-Adresse konnte der Cisco Secure Client den ISE-Richtliniendienstknoten bei der Verbindung über VPN nicht erkennen, was dazu führte, dass der Status "Wartend" (Ausstehend) blieb. Darüber hinaus trugen deaktivierte Standortdienste auf Endpunkten zu einer unvollständigen Statusüberprüfung bei.

Verwandte Inhalte

- Cisco Support

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.