Identity Services Engine (ISE) 3.3 Posture Validation Fails After Firewall Migration from ASA to FTD

Contents

Issue

The reported issue can present as the endpoint remaining in an "Unknown" posture compliance status. Additionally,

In some scenarios, customers have reported that after migrating from ASA to FTD, they reused the same configurati

Environment

- Cisco Identity Services Engine (ISE) version 3.3
- ISE deployment with two nodes
- Cisco Secure Client version 5.1.7.80
- Firepower Threat Defense (FTD) version 7.4.1.1
- Endpoints connecting via VPN
- Relevant IP address for posture validation: 72.163.1.80 (enroll.cisco.com)

Resolution

These steps detail the workflow for identifying, diagnosing, and resolving the ISE posture validation issue after migr

Step 1: Collect a DART Bundle to Verify Probes

Check the posture status of endpoints attempting VPN connectivity for any errors or stuck states. Review the ISE po

Example log excerpt indicating the issue:

2026/01/05 15:38:26 [Warning] csc_iseagent Function: Target::parsePostureStatusResponse Thread Id: 0x32D0 File
ISE-PDP'..

2026/01/05 15:38:26 [Information] csc_iseagent Function: Target::Probe Thread Id: 0x32D0 File: Target.cpp Line: 2

2026/01/05 15:38:28 [Information] csc_iseagent Function: SwiftHttpRunner::http_discovery_callback Thread Id: 0x

2026/01/05 15:38:28 [Information] csc_iseagent Function: SwiftHttpRunner::http_discovery_callback Thread Id: 0x

2026/01/05 15:38:28 [Information] csc_iseagent Function: GetCurrentUserName Thread Id: 0x1AD8 File: Imperson

2026/01/05 15:38:29 [Information] csc_iseagent Function: hs_transport_winhttp_get Thread Id: 0x698C File: hs_tra

2026/01/05 15:38:29 [Information] csc_iseagent Function: Target::probeDiscoveryUrl Thread Id: 0x698C File: Targ
1 **<Operation Failed.>.**

2026/01/05 15:38:29 [Information] csc_iseagent Function: Target::Probe Thread Id: 0x698C File: Target.cpp Line: 2

In this case, enroll.cisco.com is not reachable, which causes the discovery process to fail.

Step 2: Confirm ISE Authorization Profile and Live Logs

Verify that the RADIUS livelog is correctly pushed to the endpoint. It must include Access Accept and URL redirec

Example:

Access Type = ACCESS_ACCEPT

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

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

For this specific example, we have confirmed that the redirection is working as expected; however, the discovery pro

Step 3. Verify the ACLs Settings in the FTD

Verify that enroll.cisco.com is explicitly permitted in the redirection ACL as well as in the ACL configured for the S

To check both ACLs, in the FMC you can navigate to**Object > Object Management > Access List > Extended**.

To check if Split Tunnel is configured in the VPN, navigate to **Devices > VPN > Remote Access > Choose the VPN**

Note: If Split Tunnel is not configured on the VPN policy, this validation is not required, hence the Split Tunnel AC

Cause

The root cause of the issue was the absence of the required discovery IP address (72.163.1.80, enroll.cisco.com) in th

Without this IP, Cisco Secure Client was unable to discover the ISE Policy Service Node when connecting over VPN

Related Content

- Cisco Support