防火墙从ASA迁移到FTD后，身份服务引擎(ISE)3.3状态验证失败

目录

问题

报告的问题可能显示为处于“未知”状态合规状态的终结点。此外，无法向用户显示状态调配门户。

在某些情况下，客户报告从ASA迁移到FTD后，他们重复使用相同的配置；但是，FTD需要额外的和特定的设置才能使状态VPN正常工作。

环境

- 思科身份服务引擎(ISE)版本3.3
- 带两个节点的ISE部署
- 思科安全客户端5.1.7.80版
- Firepower威胁防御(FTD)版本7.4.1.1
- 通过VPN连接的终端
- 状态验证的相关IP地址：72.163.1.80(enroll.cisco.com)

分辨率

这些步骤详细说明了用于在迁移到FTD之后识别、诊断和解决ISE终端安全评估验证问题的工作流。为了清楚起见，每个步骤都进行了说明，并直接引用了环境中的日志和配置指示符。

第1步：收集DART套件以验证探针

检查尝试进行VPN连接的终端的状态是否有任何错误或停滞状态。查看ISE状态代理日志(ISEPosture.txt)，了解指示无效服务器服务器或不可访问状态的错误消息。

指示问题的日志摘录示例：

2026/01/05 15:38:26 [警告] csc_iseagent函数：目标：:parsePostureStatusResponse线程ID: 0x32D0文件：Target.cpp行： 370级别：警告头端为空。内容可能未采用“X-ISE-PDP”形式。

2026/01/05 15:38:26 [信息] csc_iseagent函数：目标：：探测线程Id: 0x32D0文件： Target.cpp行： 212级别：调试重定向状态目标192.168.1.254为5 <服务器无效。>

2026/01/05 15:38:28 [信息] csc_iseagent函数： SwiftHttpRunner::http_discovery_callback线程Id: 0x1AD8文件： SwiftHttpRunner.cpp行： 519级别
： info Time out for Redirection target enroll.cisco.com。

2026/01/05 15:38:28 [信息] csc_iseagent函数： SwiftHttpRunner::http_discovery_callback线程Id: 0x1AD8文件： SwiftHttpRunner.cpp行： 580级别：信息启用下一轮计时器。

2026/01/05 15:38:28 [信息] csc_iseagent函数： GetCurrentUserName线程ID: 0x1AD8文件： ImpersonateUser.cpp行： 60级别：info当前登录用户的用户名是basheer.mohamed。

2026/01/05 15:38:29 [信息] csc_iseagent函数：hs_transport_winhttp_get线程ID:0x698C文件：hs_transport_winhttp.c行：4912级别：debug请求已超时。

2026/01/05 15:38:29 [信息] csc_iseagent函数：目标：:probeDiscoveryUrl线程Id:0x698C文件：Target.cpp行：269级别：debug GET request to URL(http://enroll.cisco.com/auth/discovery?architecture=9)，返回状态–1 <操作失败。>

2026/01/05 15:38:29 [信息] csc_iseagent函数：目标：：探测线程Id: 0x698C文件： Target.cpp行： 212级别：调试重定向的状态：target enroll.cisco.com为6 <无法访问。>

在这种情况下，无法访问enroll.cisco.com，从而导致发现过程失败。

第2步：确认ISE授权配置文件和实时日志

验证RADIUS实时日志是否正确推送到终结点。它必须包含访问接受和URL重定向参数以进行状态验证。

示例：

访问类型= 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

对于此特定示例，我们已确认重定向按预期工作；但是，发现过程失败，因为网关被报告为无效服务器。在VPN集成方案中可以预期出现此行为，因为终端不依赖VPN网关进行发现。相反，the endpoint attempts to reach the ISE node using enroll.cisco.com。

步骤3.检验FTD中的ACL设置

验证重定向ACL以及为分割隧道配置的ACL中是否明确允许enroll.cisco.com。

要检查两个ACL，在FMC中您可以导航到对象>对象管理>访问列表>扩展。

要检查VPN中是否配置了拆分隧道，请导航到Devices > VPN > Remote Access > Choose the VPN and Connection Profile settings > Edit Group Policy > Split Tunnel。

注：如果未在VPN策略上配置拆分隧道，则不需要进行此验证，因此本场景中不需要拆分隧道ACL。

原因

问题的根本原因是迁移到Firepower威胁防御(FTD)后，网络策略中缺少所需的发现IP地址(72.163.1.80, enroll.cisco.com)。

如果没有此IP，思科安全客户端无法在通过VPN连接时发现ISE策略服务节点，导致状态状态保持为挂起状态。此外，终端上禁用位置服务导致状态验证不完整。

相关内容

- 思科支持

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）。