安全访问证书检查状态检查身份验证失败

目录

问题

尝试使用证书检查功能使用终端安全评估配置文件部署安全访问时，所有登录尝试都会失败，尽管在DART捆绑日志中无法识别失败的特定原因。用户尝试使用SAML IDP身份验证，同时还希望通过安全评估检查机制实施证书验证，但此配置会导致一致的身份验证失败，即使后端证书匹配成功。

环境

- 思科安全访问 — 安全客户端远程访问（VPN、状态、专用资源）
- SAML IDP身份验证集成
- 已启用证书检查功能的终端安全评估配置文件
- SAN中具有UPN字段的用户证书与电子邮件地址匹配
- 使用用户、组和终端设备的安全访问租户配置

分辨率

仅当使用多证书身份验证时，才会实施证书终端状态检查，这同时需要用户证书和机器证书验证。由于部署方案涉及仅拥有用户证书且需要使用单个VPN配置文件的用户，因此解决方案涉及实施SAML +单个证书身份验证，而不是依赖状态证书检查。

身份验证配置步骤

步骤 1：配置SAML +单证书身份验证

配置身份验证方法，以将SAML身份验证与单一证书身份验证结合使用，而不是尝试通过状态检查实施证书验证。

步骤 2：配置证书UPN匹配

确保证书的使用者备用名称(SAN)中的UPN字段包含与在“用户”、“组”和“终端设备”下的“安全访问”中为用户配置的auth属性相匹配的用户电子邮件地址。

步骤 3：设置主要身份验证字段

配置主字段以使用证书中的UPN进行身份验证，确保它与Secure Access用户数据库中的用户电子邮件地址相对应。

证书结构要求

必须配置证书结构，以便证书中的UPN或辅助值与安全访问中用户的auth属性相匹配。如果用户提供的证书的UPN或辅助值与安全访问中为该用户配置的auth属性不匹配，则身份验证将被拒绝。

重要配置说明

如果需要实施安全状态证书检查，则需要多证书身份验证（IDP SAML +多证书身份验证），但这需要用户和机器证书。对于用户仅拥有用户证书且需要使用单个VPN配置文件的部署，SAML +单一证书身份验证提供了适当的解决方案，同时仍保持基于证书的安全控制。

原因

仅当配置多证书身份验证时，才会实施证书终端状态检查。将SAML身份验证与状态证书检查配合使用时，系统希望用户和机器证书都存在以进行验证。由于部署仅使用具有SAML身份验证的用户证书，因此尽管后端证书匹配成功，但安全评估证书检查功能始终无法进行身份验证尝试，因为安全评估机制未设计用于单一证书身份验证方案。

相关内容

- 思科技术支持和下载

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）。