

了解安全访问中的SSL证书和握手错误

目录

问题

由于证书和TLS错误而阻止的HTTP流量现在可以在控制面板活动搜索中查看。本文提供常见错误消息列表以及每个错误的简要说明。

环境

- 思科安全访问 — 安全Web网关SSL检查

分辨率

上游证书已过期

网站的证书已过过期日期，因此Cisco Secure Access不信任该证书。此问题将由网站所有者修复，因此请联系网站管理员并通知他们。

上游证书自签名

网站提供其自己签名的证书，而不是由受信任的证书颁发机构颁发的证书。由于没有独立机构为其提供担保，因此思科安全访问无法确认证书是真实的。

您经常会看到资源上的自签名证书，这些证书面向小规模的内部受众 — IT安全设备上的管理员门户

就是一个典型示例。请注意，Cisco Secure Access无法设置为信任自签名证书。

缺少中间证书

Cisco安全访问无法收集所需的所有中间证书，因此无法建立完整的信任链，使其回到根目录。

这一点很重要：网站的证书（“枝叶”）由中间证书签名，而中间证书又可由另一个中间证书签名，以此类推，直至受信任的根。要签出此链，网站必须将其中间证书与自己的证书一起发送。当这些内容缺失时，验证就会中断，因此请让网站的网站管理员知道。

有一个例外：如果证书包含“授权信息访问”(AIA)扩展，思科安全访问可以尝试自行获取缺失的中间体。请记住，仅当同时打开HTTPS解密和文件检查时，此操作才有效。

上游证书缺少主题名称

该证书不包括使用者名称（可分辨名称）或使用者替代名称，这意味着没有明确标识证书所属的内容。否则，思科安全访问无法对其进行验证。网站所有者需要更正此问题。

上游证书缺少公用名

证书没有公用名(CN) — 该字段通常保存站点的主机名，并帮助确认证书实际属于您访问的站点。如今，该检查确实取决于主题备用名(SAN),CN被视为旧字段，但其缺失仍会触发此错误。联系网络管理员来解决问题。

不受信任的上游证书

思科安全访问不信任此证书，通常是因为它无法识别颁发此证书的根CA。

Cisco Secure Access SWG保留受信任根证书颁发机构的内置列表，该列表来源于信誉良好的提供商，并始终保持最新。如果站点的证书追溯到该列表之外的CA，验证将失败。如果您确信根CA是可以信任的，请与技术支持部门联系，我们可以了解一下。

证书中的主机名与预期不同

您请求的地址与证书上的名称不匹配 — 无论是其公用名(CN)还是其任何使用者备用名(SAN)。由于证书似乎不属于您所访问的站点，因此Cisco Secure Access不信任此请求。网络管理员需要解决这个问题。

已撤销上游证书

颁发此证书的证书颁发机构已撤销此证书，也就是说，它不再被视为有效。

思科安全访问使用在线证书状态协议(OCSP)确认这一点，该协议会实时检查证书是否已被吊销。让网站的网站管理员知道以便进行更换。

TLS握手错误

不支持的上游密码

无法完成TLS握手，因为网站不支持Cisco Secure Access SWG使用的任何密码套件。这通常出现在只能提供较弱密码的较旧或过时的服务器上。修复在服务器端，因此请将其传递给网络管理员。

上行TLS版本不匹配

握手失败，因为网站未使用Cisco Secure Access SWG支持的TLS版本。目前，思科安全访问SWG代理可与TLS 1.2和TLS 1.3配合使用，既适用于来自客户端的连接，也适用于它通向目标服务器的连接。

小于1024位的上游DH密钥

握手无法完成，因为网站使用的Diffie-Hellman密钥太弱（低于1024位），思科安全访问无法接受。这是服务器端限制，因此网络管理员需要对其进行强化。

解决方法

可以通过在Cisco安全访问中进行配置更改来解决这些问题。

只有当您信任服务器和证书的真实性时，才能执行此操作。

解决方法：可以使用“选择性解密列表”条目禁用解密，或使用“外部域”条目完全绕过来自思科安全访问的流量。禁用解密时，思科安全访问不执行证书验证。

请注意，在大多数情况下，当流量从Cisco安全访问 — Web浏览器执行类似的证书验证时，浏览器仍会显示错误或警告。

原因

思科安全访问SSL检查代理无法完成TLS握手 — 最常见的原因是目标使用拒绝CSA重新签名证书的证书绑定。

- 证书锁定：客户端硬码预期证书指纹
- CSA CA在终端上不受信任：检查CA证书未部署到受信任的根存储

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）。