

安全访问中的SSL解密证书错误处理

目录

问题

在Cisco Secure Access中启用SSL解密时，用户遇到与证书相关的错误页面。已收到有关三种特定类型的证书错误的多个查询：

- 源服务器证书过期错误
- 证书CN/SAN不匹配错误，其中证书上列出的公用名或主题备用名称与访问的域不匹配
- 源服务器证书中嵌入的导致连接问题的证书撤销列表(CRL)链接

这些证书错误类似于通常在Web浏览器中显示的警告。问题是，Cisco Secure Access能否通过显示警告页面（类似于浏览器或内容过滤器），然后在显示警告后允许访问，或在所有情况下允许访问来处理与证书相关的错误。此外，需要了解禁用SSL解密时的行为以及流量是否通过，无论证书问题如何。

环境

- 思科安全接入 — 互联网接入（漫游模块、VA、DNS、SWG、PAC、IPS、证书）
- 已启用SSL解密功能
- 多个域遇到证书验证问题
- 具有各种证书问题（包括到期和域不匹配）的源服务器

分辨率

证书错误处理限制

与证书相关的错误处理在Cisco安全访问中不可用。该产品不支持：

- 呈现类似于浏览器的证书问题警告页面
- 域特定证书错误处理配置
- 基于目标域的自定义错误处理
- 包含用户覆盖选项的内容过滤器样式警告页面

SSL解密排除解决方法

推荐的方法是使用安全配置文件解密设置从SSL解密中排除有问题的域。可通过以下方式配置此配置：

导航到安全配置文件>解密设置部分以从SSL检查中排除特定域。

从SSL解密中排除域时，会出现以下行为：

- 排除域的流量完全绕过SSL检查
- 安全访问不执行证书验证
- 用户不会遇到安全访问生成的证书错误页面
- 如果证书问题持续存在，则原始证书错误可能仍然显示在用户浏览器中

SSL解密禁用行为

当域或全局禁用SSL解密时，思科安全访问会通过（转发）流量，而不考虑任何证书问题。当解密未启用时，产品不会检查或验证证书，从而有效地允许所有HTTPS流量透明通过。

原因

证书错误是由源服务器上的合法证书验证问题引起的，包括过期证书、CN/SAN不匹配和CRL连接问题。Cisco Secure Access将证书验证作为其SSL解密过程的一部分执行，当这些验证失败时，产品会生成错误页面以防止潜在的不安全连接。这是SSL检查功能的预期安全行为。

相关内容

- [思科安全访问解密配置文档](#)
- [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）。