为IPS和SWG解密旁路配置SSE不解密

目录

问题

即使将财务类别或特定域添加到“不解密”(DND)列表并应用相关访问规则，流向财务类别目标的HTTPS流量仍然显示思科SSE证书，而不是原始网站证书。通过零信任访问客户端(TIA)访问站点时观察到此行为，特别是影响对需要端到端证书可视性的金融相关网站（如https://onlinesbi.sbi.bank.in/）的访问。

预期行为是，当站点或内容类别添加到DND列表时，源网站证书可以呈现给浏览器，而不是思科SSE证书。但是，思科SSE证书继续显示，表明尽管配置了DND，流量解密仍在进行。

环境

- 思科安全服务边缘(SSE)
- 零信任接入客户端(TIA)连接
- 已启用全局IPS解密
- IPS在访问策略上处于活动状态
- 在安全配置文件中的Do Not Decrypt list中配置的财务类别
- 应用了相应安全配置文件的访问规则

分辨率

解决方法包括了解Cisco SSE执行两种不同的解密类型，并为这两种解密类型配置适当的“不解密”设置。

了解SSE解密类型

思科SSE执行两个独立的解密过程：

- SWG（安全Web网关）解密- Web代理解密
- IPS解密 — 入侵防御系统解密

在安全配置文件中配置的Do Not Decrypt条目仅适用于SWG解密，并且不会阻止IPS解密。当启用全局IPS解密且IPS在任何访问策略中处于活动状态时，仍会进行IPS解密，从而导致向浏览器显示Cisco SSE证书。

配置步骤

步骤 1：将站点或内容类别添加到系统提供的不解密列表。

系统提供的Do Not Decrypt List应用于所有IPS配置文件。将站点或内容类别添加到此系统提供的列表会导致提交原始网站证书，从而有效地绕过IPS解密。

步骤 2：确认不需要进行其他策略更改。

无需在访问策略中引用系统提供的不解密列表。列表会自动应用到所有IPS配置文件。

验证测试

可以使用以下验证方法来确认正确的配置：

方法 1：将域添加到系统提供的不解密列表

将特定域添加到系统提供的不解密列表可能会导致显示原始网站证书而不是思科SSE证书。

方法 2：暂时禁用全局IPS解密（仅用于测试）

暂时禁用全局IPS解密还会导致检测到测试站点的源证书，从而确认IPS解密是思科SSE证书呈现的原因。

预期结果

正确配置后：

- 添加到“系统提供的不解密列表”的站点或内容类别会显示其原始网站证书。
- 对于指定的站点或类别，SWG和IPS解密均被绕过。
- 浏览器显示实际的网站证书而不是Cisco SSE证书。

原因

发生此问题的原因是Cisco SSE执行两个不同的解密过程：SWG解密和IPS解密。在安全配置文件中配置的“不解密”条目仅绕过SWG解密。当启用全局IPS解密且IPS在访问策略中处于活动状态时，IPS解密继续独立进行，导致即使站点包含在安全配置文件DND列表中，也会向浏览器显示Cisco SSE证书。

要完全绕过两种解密类型，必须将站点或内容类别添加到系统提供的不解密列表，该列表适用于所有IPS配置文件，并防止SWG和IPS都解密。

相关内容

- 创建有效的不解密列表以进行安全访问
- 排除故障并收集基本信息以实现安全访问
- 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）。