评估FTD上SSL/TLS解密的性能影响和最佳实践

目录

问题

用户计划对防火墙威胁防御(FTD)设备启用SSL/TLS解密，并需要在实施前了解对设备性能的潜在影响。主要问题包括：

- 影响防火墙吞吐量、延迟和整体流量处理性能。
- 启用解密后，预期CPU和内存利用率会增加。
- 特定FTD型号的规模调整指南和性能基准。
- 对并发解密会话的建议限制。
- 生产部署的最佳实践和先决条件。

环境

- Firepower 4115。其他硬件平台也可能受到影响。
- FTD版本7.4.2（内部版本172）。 其他软件版本也可能受到影响。
- SSL/TLS解密功能注意事项。
- 生产环境部署规划。

分辨率

SSL/TLS解密确实会增加Firepower 4115的处理开销，但实际影响在很大程度上取决于解密的流量数量以及解密后应用了何种检查。

性能影响分析

SSL/TLS解密的影响包括：

- 有效吞吐量更低。
- 延时长.
- Snort/检查CPU使用率提高。
- 在没有实际流量量变曲线分析的情况下，无法准确预测固定百分比的CPU和内存增加。

FPR 4115性能基准

思科发布的Firepower 4115基准规格：

- TLS硬件解密吞吐量：6.5 Gbps.
- 防火墙+ AVC吞吐量：33 Gbps.
- 使用AVC的最大并发会话数：1500万。
- 每秒使用AVC的最大新连接数：21万。

重要的规模调整说明：6.5 Gbps TLS硬件解密基准基于特定测试条件。如果解密大部分流量，使用入侵/文件/恶意软件策略检查已解密的流量，或处理许多短期TLS会话，则生产吞吐量会降低。

思科不会为FTD 7.4.2上的Firepower 4115发布单独的“最大并发解密会话数”。实际上，容量是使用流量混合、并发会话、连接速率、密码套件和检测策略负载进行验证的。

推荐的生产部署方法

步骤 1：从有限的试点开始

- 最初不要启用宽泛的“解密所有”规则。
- 从选定的用户、子网或目标类别开始。
- 对于不需要检查的流量，使用Do Not Decrypt保持默认处理保守性。

步骤 2：排除通常因解密而中断的流量

- 银行/金融网站。
- 医疗门户网站。
- 证书固定的应用。
- 一些软件即服务(SaaS)和终端安全/云应用。
- 敏感的关键业务应用，除非经过明确测试。

步骤 3：保持SSL规则简单且有序谨慎

- 将特定的Do Not Decrypt exclusions置于更广泛的解密规则之上。
- 尽可能避免过于宽泛或复杂的匹配。
- 请勿将TLS版本或密码套件条件用于Decrypt-Resign/Known-Key规则，因为思科记录这会导致不可预知的行为。

步骤 4：验证证书就绪性

- 对于出站Decrypt-Resign，签名CA证书必须由客户端终端信任。
- 对于入站已知密钥解密，防火墙必须具有正确的服务器证书/私钥材料。

步骤 5：在推广期间监控

- 跟踪总体CPU，更重要的是，跟踪Snort/检查CPU利用率。
- 每秒跟踪并发连接和新的连接。
- 查看连接事件中的SSL流状态/握手错误。
- 注意TLS超订用指示灯和特定于应用的故障。

有关如何监控CPU检查的详细信息：

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- 像TAC工程师一样思考：思科安全防火墙最常见痛点的指南

要每秒跟踪连接和新的连接，请检查：

- 日志记录最佳实践

要跟踪连接事件检查和TLS超订用指示器检查中的SSL流状态/握手错误：

- 排除TLS/SSL超订用故障

步骤 6：回滚或缩小范围（如果看到）：

- 持续检测CPU饱和。
- 用户可见延迟增加。
- TLS握手失败。
- 解密后业务应用程序失败。
- 超订用或SSL错误过多。

步骤 7：考虑TLS 1.3的影响

采用TLS 1.3会影响可视性和行为，因为某些握手和检查特征与TLS 1.2不同。

原因

SSL/TLS解密需要额外的计算资源来解密、检查和重新加密流量流。性能影响因流量模式、应用于已解密流量的检查策略以及特定部署配置而异。如果没有适当的规划和逐步实施，组织可能会在生产环境中遇到意外的性能降级。

相关内容

- 思科安全防火墙管理中心设备配置指南 — 解密规则
- 思科安全防火墙解密策略指南
- 解密策略规则顺序的最佳实践
- 使用思科安全防火墙7.7简化解密
- 解密规则最佳实践
- Cisco Firepower 4100系列产品手册
- 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）。