验证思科安全访问中的IPS解密

目录

问题

当通过安全客户端使用带RAVPN（远程访问VPN）的思科安全访问时，组织需要验证是否对流向特定网站的流量正确执行IPS（入侵防御系统）解密和检查。主要挑战在于确认TLS解密和检查进程是否通过标准管理UI日志以外的其他方法（如活动搜索）正常运行。具体验证要求包括确定可支持测试验证并提供管理接口以外IPS操作的其他确认的客户端证书检查或调试/报告机制。

环境

- 具有RAVPN功能的思科安全访问(CSA)
- 用于远程访问VPN连接的思科安全客户端
- 已启用IPS解密和检测功能
- 需要解密以进行安全检查的TLS/SSL流量
- 从RAVPN客户端到外部网站的Web流量

分辨率

有两种方法可以验证IPS解密和检查是否在Cisco安全访问中对远程访问VPN流量正常工作：

方法 1：管理UI活动搜索（主要方法）

思科安全访问管理界面中的活动搜索功能提供了最可靠的方法来确认IPS解密和检查操作。此界面显示详细日志和分析信息，显示安全服务何时解密并检查流量。

要访问“活动搜索”，请执行以下操作：

导航到Cisco Secure Access管理控制面板并找到Activity Search功能以查看特定用户会话和目标网站的流量检测日志和解密状态。

要启用解密日志，可以在全局设置中启用此设置：

控制面板(Dashboard)->安全(Secure)->访问策略(Access Policy)->规则默认值和全局设置(Rule Defaults and Global Settings)->全局设置(Global Settings)->解密日志记录(Decryption Logging)。

方法 2：客户端证书验证

作为额外的验证方法，您可以执行客户端证书检查以确认流量解密已发生。

当思科安全访问成功解密并检查TLS流量时，它会向客户端提供自己的证书，而不是原始网站证书。

要通过证书检查验证解密，请执行以下操作：

1.检查网站证书
在浏览器中打开证书详细信息，查看颁发者和有效期。

如果证书由思科安全访问根CA颁发，有效期约为10天，则表示在防火墙级别解密入侵防御系统。

如果证书有效期约为5天，则表示基于安全网络网关的解密。

2.验证证书颁发者（DC命名）

此客户端证书验证方法与主要活动搜索方法一起用作补充确认技术，从而进一步确保IPS解密过程按预期运行。

入侵防御系统不解密：

如果以下情况发生入侵防御系统的解密：

·它在全局设置下启用，并且

·至少为一个访问策略规则启用了入侵防御系统（我相信，即使该规则被禁用，此条件仍然适用）

要绕过入侵防御系统解密的域

使用系统提供的不解密列表并在系统提供的不解密列表中添加域。

或

在Cisco Secure Access全局设置下使用基于源的解密 —

注意：如果在安全访问的网络隧道配置上没有配置出站NAT，则此操作会起作用。

原因

需要多种验证方法是因为需要在企业环境中验证安全策略实施。尽管管理UI日志提供了全面的可视性，但客户端验证方法提供了额外的确认点，这些确认点对于合规性测试、故障排除和验证方案非常有用，在这些情况下，直接访问管理接口可能会受到限制，或者全面测试过程需要多个验证点。

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）。