# 使用Eicar进行测试文件检查

## 目录



## 简介

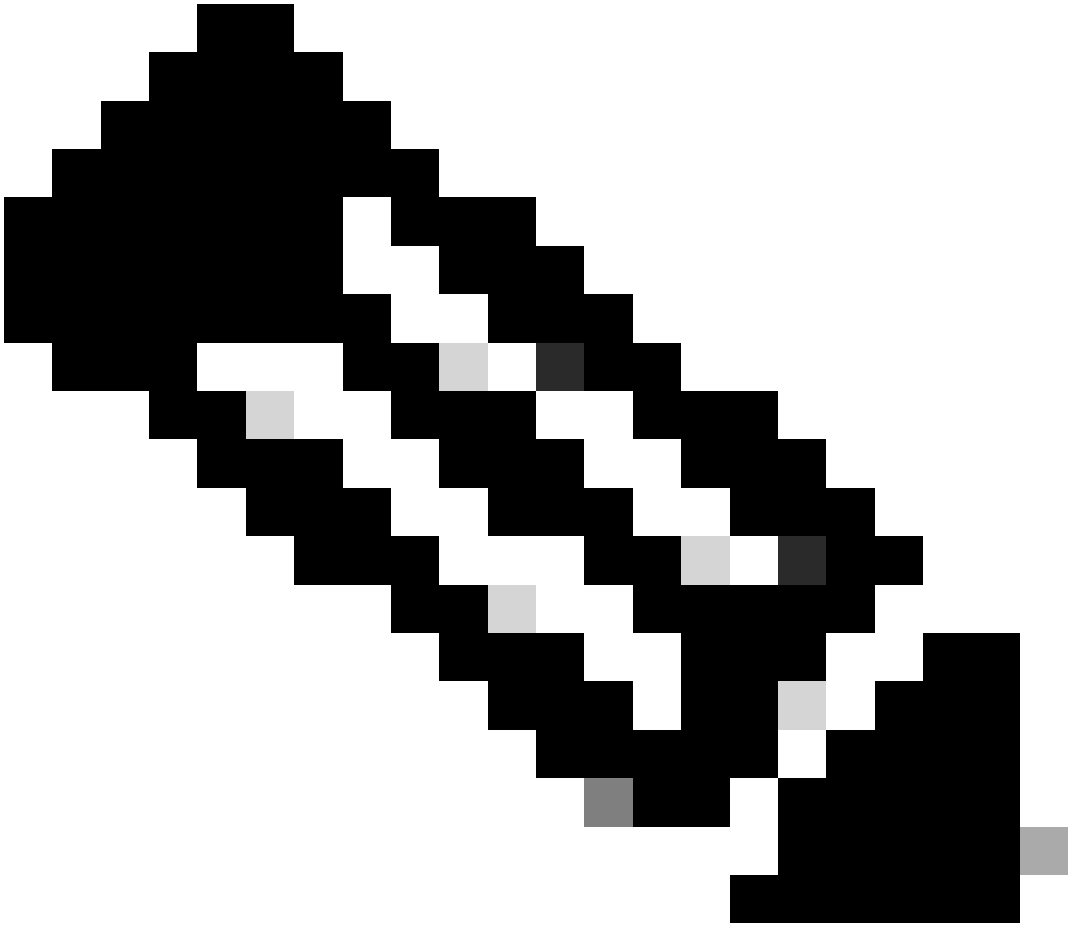
本文档介绍如何使用Eicar测试文件检测。

## 概述

目前，使用eicar.org测试下载文件测试是否启用文件检查功能时，启用或禁用“SSL解密”时，您会看到不同的行为。如果启用了SSL解密，则仅下载eicar.org上的Umbrella File Inspection AV扫描。

## 了解Eicar的检测流程

要启用eicar.org的阻止，请启用SSL解密。



注意：即使通过HTTP访问站点，也需要SSL解密。如果未启用SSL解密，代理将绕过通过HTTPS提供流量的域。

- Umbrella智能代理决定是否向DNS层的代理发送域。
- DNS请求在HTTP/HTTPS连接之前发生，这意味着当域受代理服务器约束时，HTTP和HTTPS流量始终受代理服务器约束。
- 当HTTP/HTTPS流量到达智能代理时，第一步是执行重定向以识别用户。

没有SSL解密，无法进行此重定向，这意味着我们可能无法在某些场景（例如漫游用户）中正确识别用户。

为防止这些用户中断HTTPS请求，除非启用SSL解密，否则Umbrella不使用同时为HTTP/HTTPS流量提供服务的代理域(如eicar.org)。

## 总结.....

为了从该功能获得最佳的安全性和有效性，我们强烈建议安装Cisco Root CA并启用SSL解密。这允

许eicar.org测试文件被阻止，并增加了通过我们的智能代理进行文件检查的域数。

以下是预期行为的摘要：

- SSL解密关闭
  - Eicar.org站点在https://www.eicar.org/download/eicar.com上未被阻止。由于禁用了SSL解密，因此根本不会代理域。
  - 我们自己的测试站点托管工具被阻止：http://proxy.opendnstest.com/download/eicar.com
- SSL解密打开
  - 在http://www.eicar.org/download/eicar.com和https://www.eicar.org/download/eicar.com上被AV扫描阻止Eicar

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）。