了解Umbrella控制面板中的新功能

目录

简介

本文档介绍通过Umbrella控制面板中的目标列表阻止文件检测和自定义URL。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Umbrella控制面板。

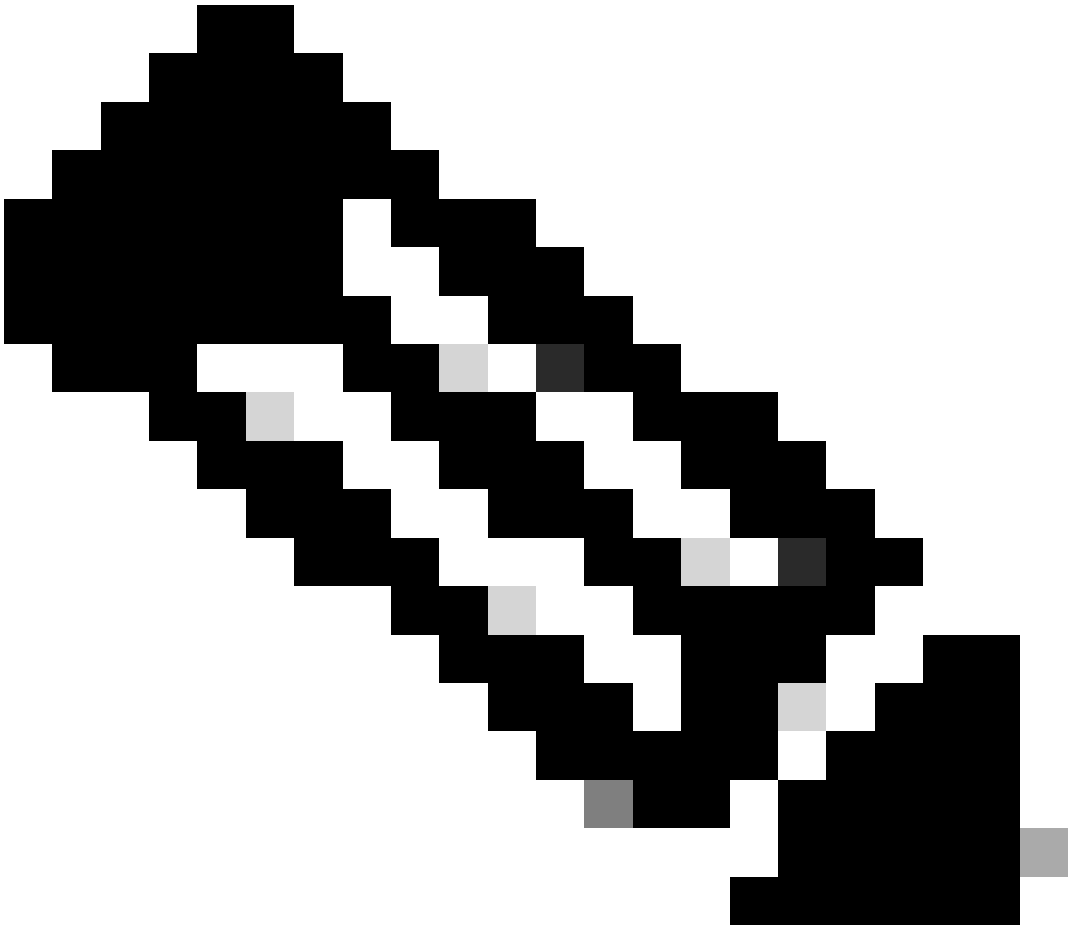
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

新功能

Umbrella正在引入一组新的功能，可改善您的功能。通过此更改，您现在可以在控制面板中看到两个新功能：

- 文件检测会扫描身份下载的文件，以查看它们是否包含恶意代码，如果包含恶意代码，则将其阻止。
- 通过自定义阻止的URL，您可以阻止目标列表中您自己的URL集。现在，您可以灵活地阻止特定页面，而不会阻止整个域。

为了帮助您利用这一新功能，您可以使用新的和更新的报告以及新的策略创建体验。文件检查功能是为未来版本规划的几个功能之一，其核心是推进智能代理基础设施，以便为您提供更多基于云的安全性。



> 注意：这些功能正在以小增量向我们的客户推出，随着Umbrella在此版本中的发展，这些更新在可用性方面受到限制。如果您在控制面板中收到有关这些功能的警报，您会收到这些警报。如果您想了解有关这些功能的更多信息，请联系umbrella-support@cisco.com。

文件检查功能仅适用于具有Umbrella Insights或Umbrella Platform套件的客户。请阅读有关套件的详细信息，如有疑问，请与您的思科客户代表联系。

如何利用这些功能

可在以下几个位置访问这些新功能：策略向导允许您从摘要页面启用文件检查，并且可以通过目标列表将自定义URL添加到阻止的目标列表。此外，还可以从Destination Lists management页面专门管理自定义URL阻止。

在报告端，Umbrella控制面板的“报告”(reports)导航部分已更新，以便您可以轻松找到新的和更新的

报告。阅读本文中有关如何启用这些功能的更多内容，并查看一些报告。

文件检查

文件检查是智能代理的一项功能，通过增加扫描文件以查找可疑域中托管的恶意内容来扩展其范围和功能。可疑域既不可信，也不知道是恶意的。

使用Umbrella策略向导，文件检测易于实施。导航到Policies > Policy List，展开策略或选择+(Add)图标以创建新策略。在策略向导中，确保在摘要页面上启用了File Inspection，或在启用智能代理后(在Advanced Settings下)，从新策略中选择Inspect Files。 阅读此功能的完整文档中的详细信息。

测试文件检查

从在启用了文件检查的策略中注册的设备：

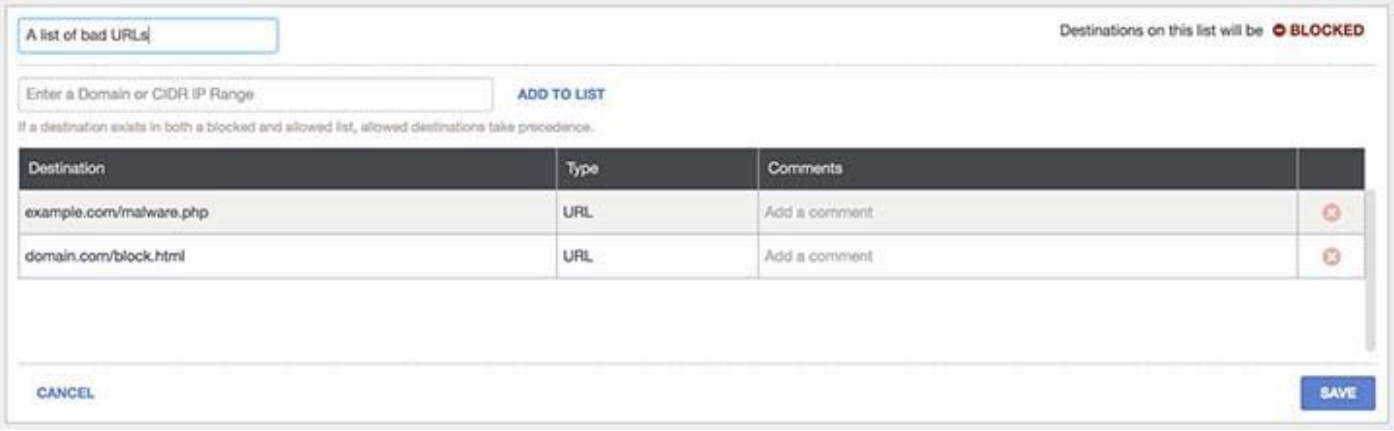
1.浏览http://proxy.opendnstest.com/download/eicar.com。

2.系统将显示此屏幕截图的阻止页面。

Umbrella阻止页面

启用要在目标列表中阻止的URL

要阻止URL，只需将其输入已阻止目标列表，或仅针对URL创建新的已阻止目标列表。为此，请导航到Policies > Destination Lists，展开Destination列表，添加URL，然后选择Save。



Umbrella阻止目标列表

阅读此功能的完整文档中的详细信息。

为了使Umbrella基础设施检查URL以确定它是否与您的受阻止目标列表中定义的匹配，您必须执行以下操作：

- 智能代理和SSL解密必须作为策略的一部分启用。有关详细信息，请阅读Umbrella文档。
- 使用此策略必须在计算机上安装Cisco Umbrella Root CA — 确保也过滤https连接。有关详细信息，请阅读Umbrella文档。

必须正确指定URL，以便策略中的内容与用户尝试访问（随后被阻止）的内容匹配。 有关可以使用或无法使用哪些URL的详细信息，请阅读自定义URL目标列表操作方法。

报告

Umbrella现在有了新的改进报告：

- 安全概述报告：通过图表和图形，您可以轻松查看网络活动的快照。您可以快速查看身份及其流量中的活动，说明问题可能发生在何处。在Umbrella文档中了解更多有关信息。
- 安全活动报告：突出显示Umbrella威胁情报已标记但不必阻止的安全事件。这包括通过智能代理和文件检查过滤的安全事件。在Umbrella文档中了解更多有关信息。

- 活动搜索报告：帮助您从各种身份中查找每个DNS、URL和IP请求的结果，按降序日期和时间排序。此报告可以列出Umbrella在选定时间段内所有与安全相关的活动，并允许您使用过滤器来优化搜索，以便仅查看您想要查看的内容。在Umbrella文档中了解更多有关信息。

这些报告也很容易获得。

发送Umbrella反馈

Umbrella非常想知道您对这些新功能的看法。如果您有任何疑问或意见，Umbrella希望收到您的回复！请将您的反馈发送至umbrella-support@cisco.com，并尽可能详细地提供您的反馈。例如，屏幕截图、您使用的浏览器、您的操作系统和您使用这些功能的场景。

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）。