为Umbrella配置SWG策略

目录

简介

本文档介绍如何配置与Umbrella配合使用的Web策略。

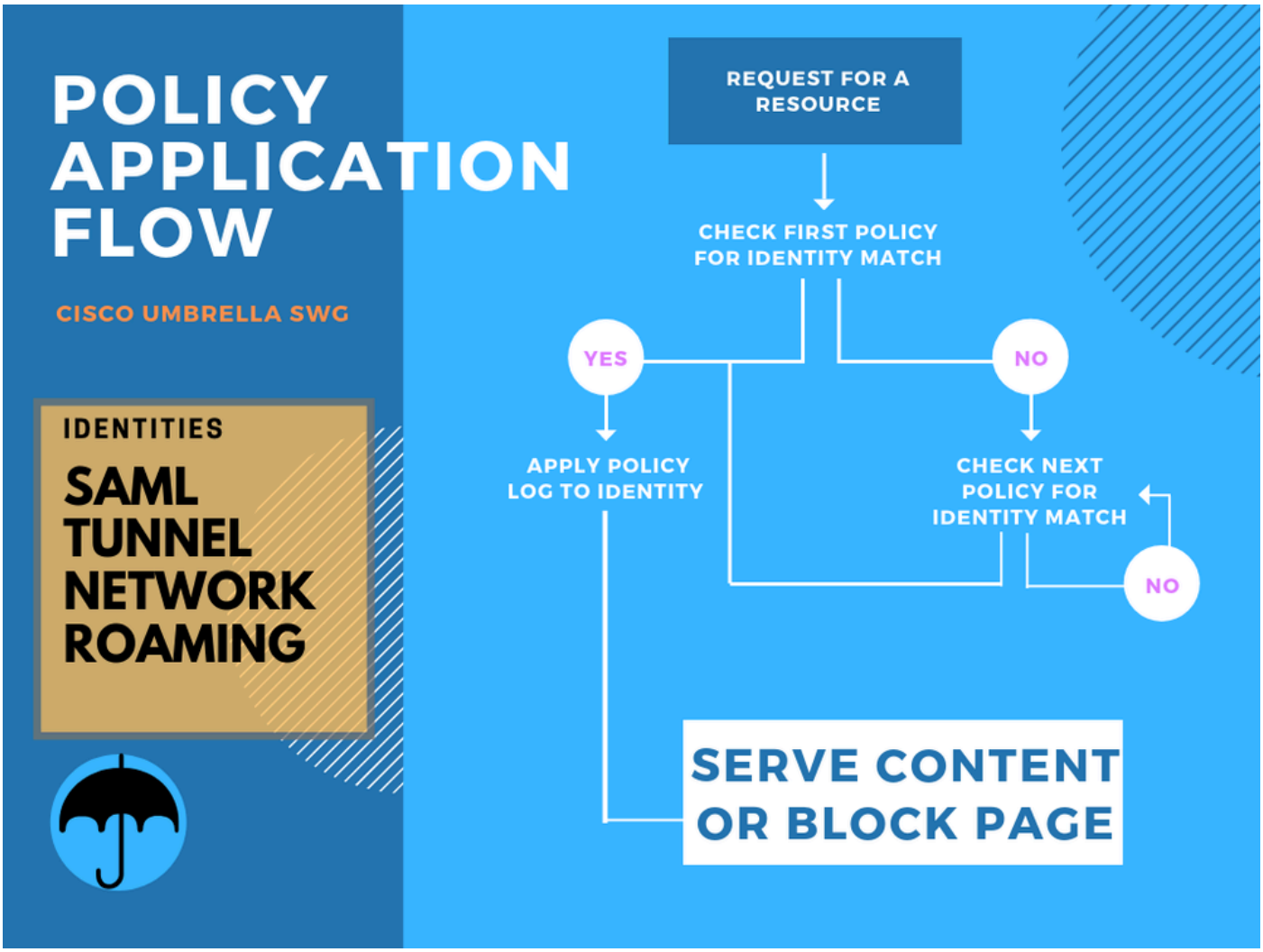
背景信息

欢迎使用Umbrella安全Web网关(SWG)。 部署后，最重要的步骤是定义Web策略，以确保收到的基线行为符合您的预期。现在，此策略流准确镜像DNS层策略。

Umbrella网络策略

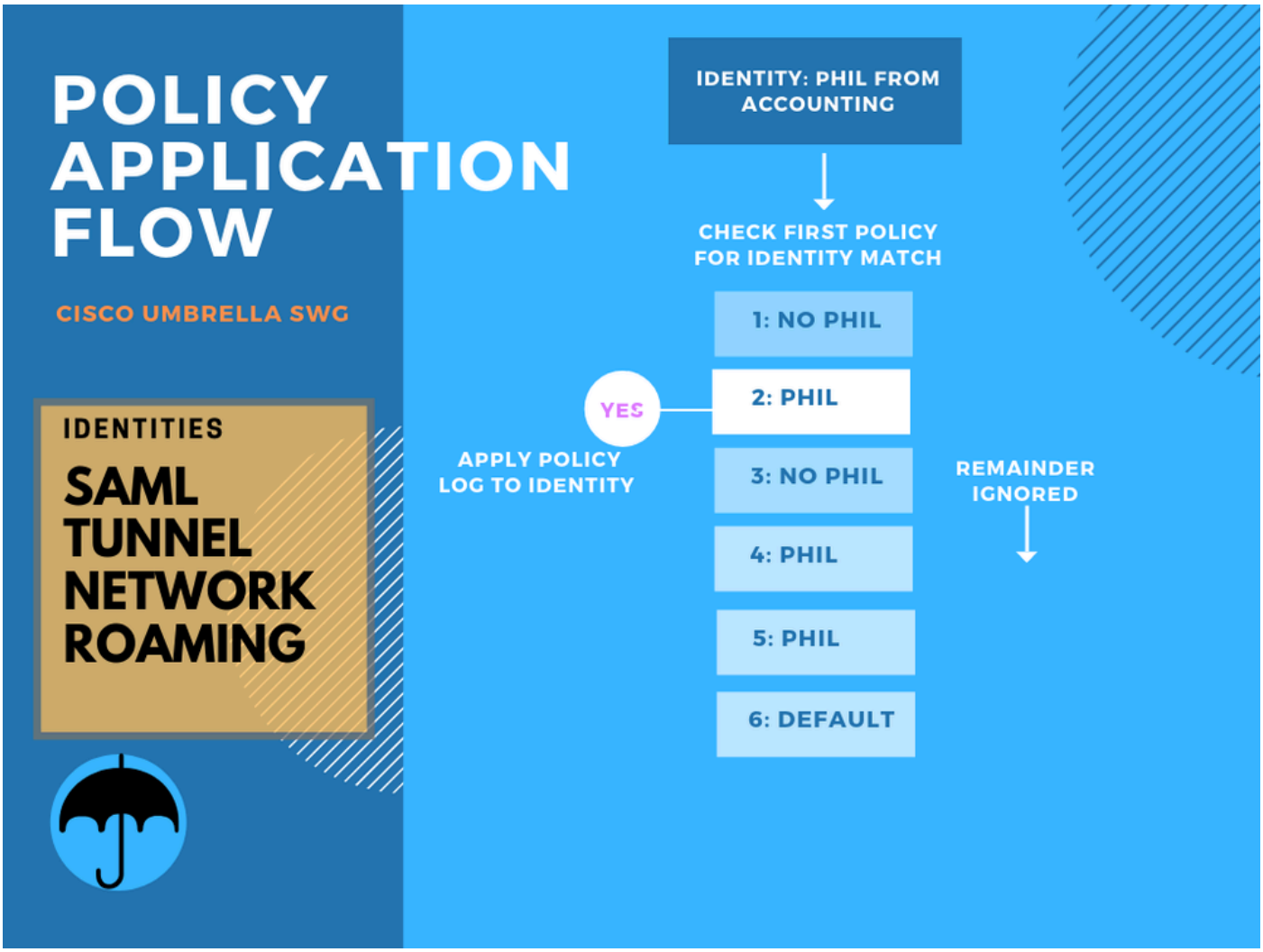
Umbrella Web策略使用顶部匹配应用算法。也就是说，将应用与当前身份集匹配的第一个策略，并忽略所有后续策略匹配。这是所有Umbrella策略的基础，可能不同于任何预先存在的对基于代理的Web策略的期望。

策略功能如此流程图所示。应用与查询中包含的任何身份的第一个策略匹配，而不考虑任何进一步的策略。



流程图 — SWG.png

由于此流量对于不是来自Umbrella DNS策略的流量来说是新的，下面是一个策略集示例，其中几个策略应用于同一用户或组。请注意仅使用应用于Phil（或Phil的用户组）的第一个策略，并忽略所有剩余匹配。其他匹配项不会在Umbrella策略中聚合，只是简单地被忽略。



流程图 — flow.png

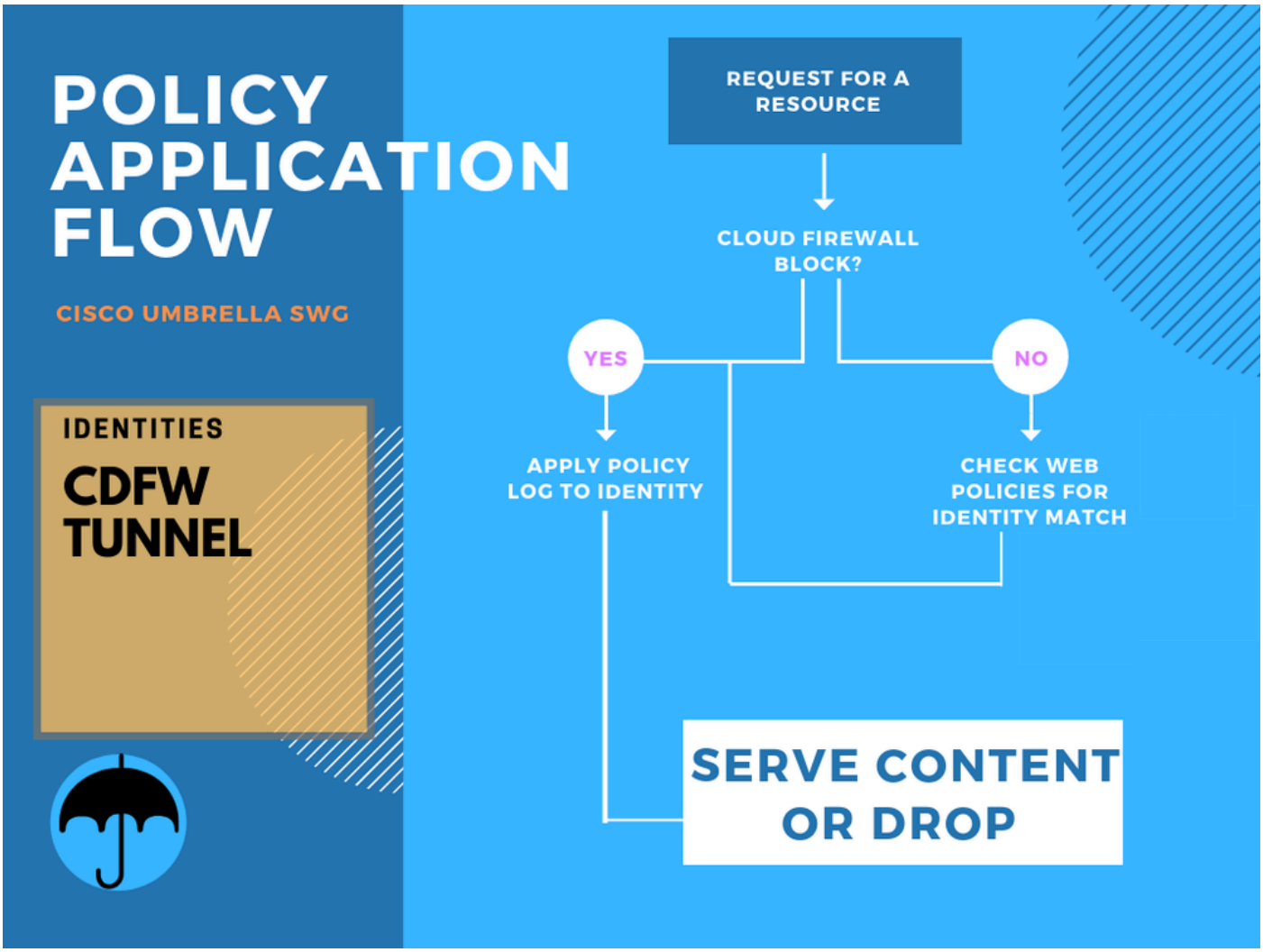
因此，这些功能在Umbrella SWG策略中不可用：

- 嵌套策略
- 允许并阻止横跨任何策略的应用程序或网站的例外项
    - 示例：Phil的策略例外项是允许Facebook、允许Instagram和允许Dropbox例外项，但Phillis仅是允许Facebook和允许Instagram。
        - 在Umbrella策略中，这是两个独特的策略。
            - 允许Facebook、Instagram、Dropbox申请到Phil
            - 允许Facebook、Instagram应用到Phillis
        - 每个允许或阻止的单个应用的组合必须创建一个新策略，并将适用用户添加到该策略中。

此外，任何非HTTP/S的流量都会收到此类流量的DNS层策略。

有关云交付防火墙和SWG的重要说明

Umbrella CDFW通过Umbrella SWG发送任何允许的HTTP/S流量，因此也应用策略。定义策略后，策略应用流与SWG流的工作方式相同。



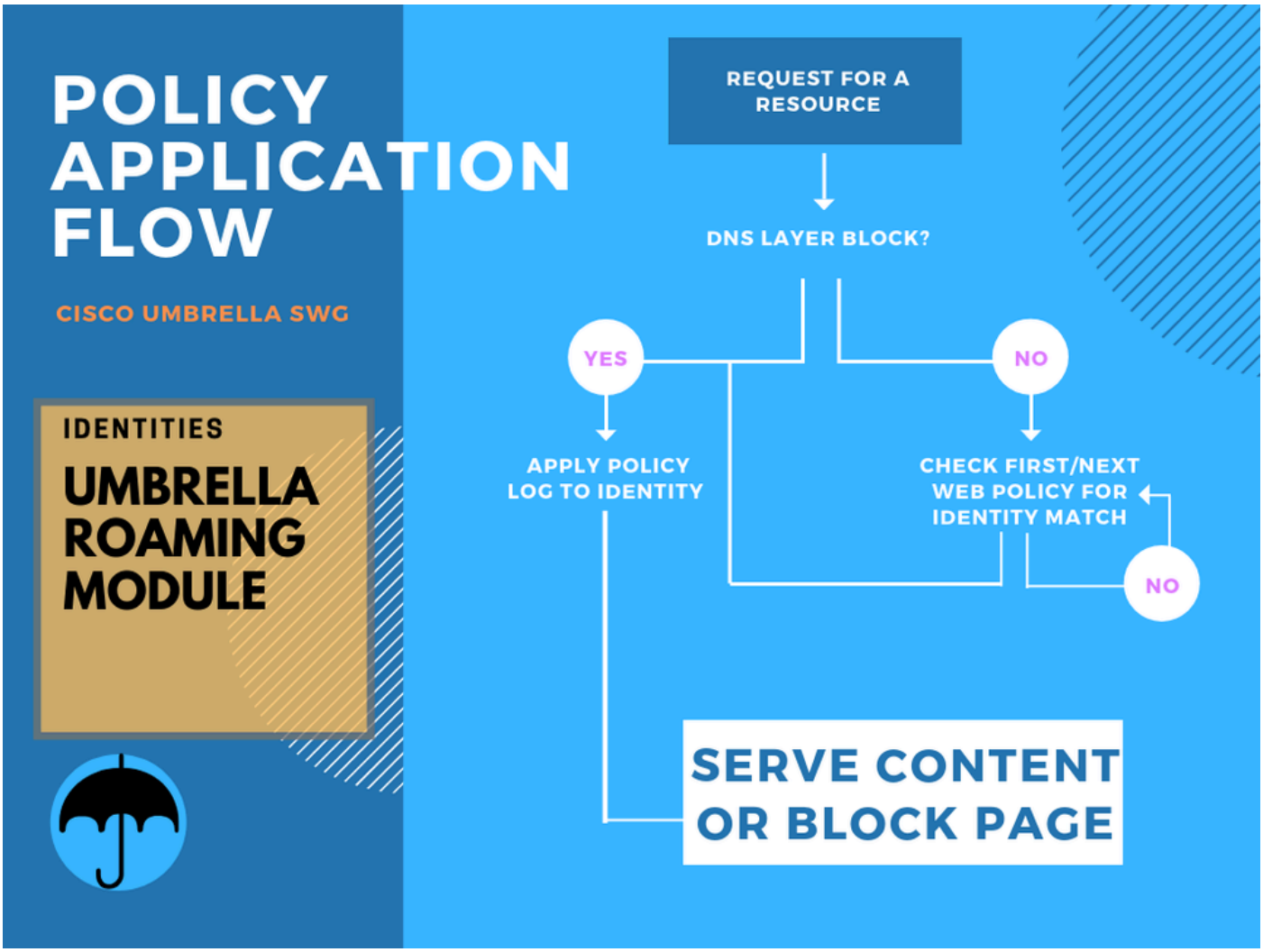
Flowchart-cdfw.png

有关漫游安全模块策略的重要说明

使用Umbrella漫游模块时，策略的实际效果与网内策略不同。漫游模块与网内代理配置或PAC文件不兼容，仅支持网外使用案例。在网络上时可以将其禁用。

将漫游模块与SWG策略配合使用时，DNS策略首先对所有块（包括安全块）生效。如果DNS策略的结果不是阻止，则应用代理策略。此外，对于非HTTP/S流量的任何流量，DNS策略都以独占方式应用。因此，策略应用顺序如下：

1. DNS策略（用于阻止）
2. SWG策略



流程图模块.png

想要了解更多信息？观看我们的教程视频：Umbrella Web策略。

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）。