在Umbrella安全互联网网关中使用基于规则的策略

目录

简介

基于规则的策略过渡概述

常见问题解答

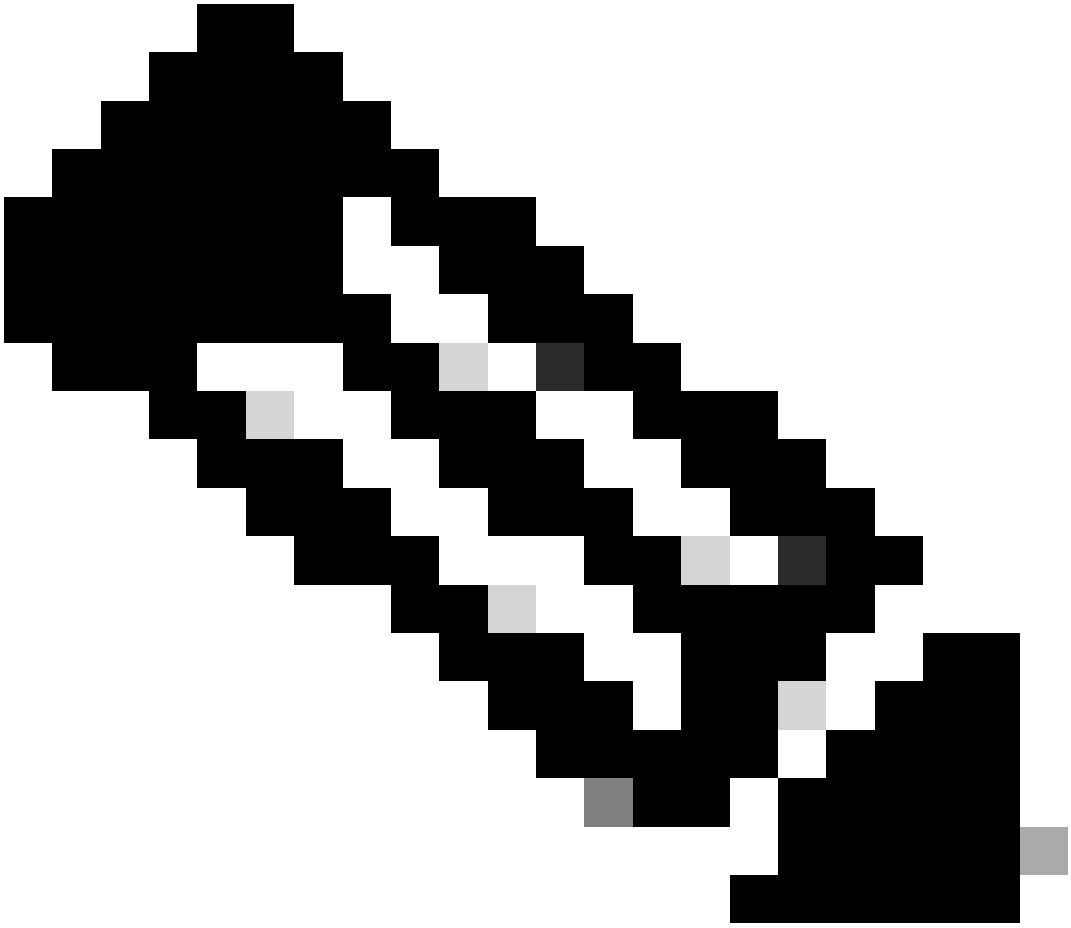
- 什么是Web策略？
- 什么是规则集？
- 为什么使用规则集？
- 可在规则集中配置哪些设置？
- 什么是规则？
- 为什么使用规则？
- 支持哪些身份？
- 支持哪些目标？
- 支持哪些操作？
- 可在规则中配置哪些设置？
- 如何评估规则集？
- 如何评估规则？
- 规则是否应用于与规则集匹配的同一身份？
- 如何知道事务中使用了哪个规则？
- 在哪里可以找到规则集的在线文档？

简介

本文档介绍Umbrella安全互联网网关(SIG)中基于规则的策略功能，并回答常见问题。

基于规则的策略过渡概述

2021年3月31日，基于规则的策略开始向Umbrella SIG客户普遍提供。Umbrella SIG客户在数周内逐渐从传统Web策略过渡到基于规则的策略。客户通过Umbrella控制面板收到有关过渡日期和窗口的通知。此更改不会影响Umbrella DNS客户或DNS策略设置。



注意：本FAQ旨在解决新用户和经验丰富的Umbrella用户关于从传统Web策略向规则集转变的快速问题。 有关更详细的文档，请参阅更新的Umbrella管理指南。

常见问题解答

什么是Web策略？

Web策略是Umbrella组织中所有规则集的集合。

什么是规则集？

规则集是应用于规则集内规则的一组规则和设置的逻辑容器。

为什么使用规则集？

规则集可以表示特定地理位置、办公室组或需要管理的用户，这些管理不同于组织其他部分。

可在规则集中配置哪些设置？

配置规则集中提供的设置。这些设置仅适用于该规则集中的规则：

- 规则集名称
- 规则集标识
- 阻止页面
- 租户控制
- 文件分析
- 文件类型控制
- HTTPS检测
- PAC文件
- 规则集日志记录
- SAML
- 安全设置

有关详细说明，请参阅：配置规则集。

什么是规则？

规则是定义身份和目标都匹配时要执行的操作的语句。

为什么使用规则？

规则允许精细或广泛的访问控制。例如，低优先级的规则可以阻止所有用户的各种网站，而高优先级的规则可以允许访问目标组的特定站点，所有这些站点都位于同一规则集内。

支持哪些身份？

规则集和规则都支持以下身份：

- AD用户
- AD组
- 漫游计算机（AnyConnect终端）
- 内部网络
- 隧道
- 网络

支持哪些目标？

规则支持以下目标：

- 内容类别
- 应用程序设置
- 目标列表

支持哪些操作？

规则支持以下操作：

- 允许
- 阻止
- 警告
- 隔离

可在规则中配置哪些设置？

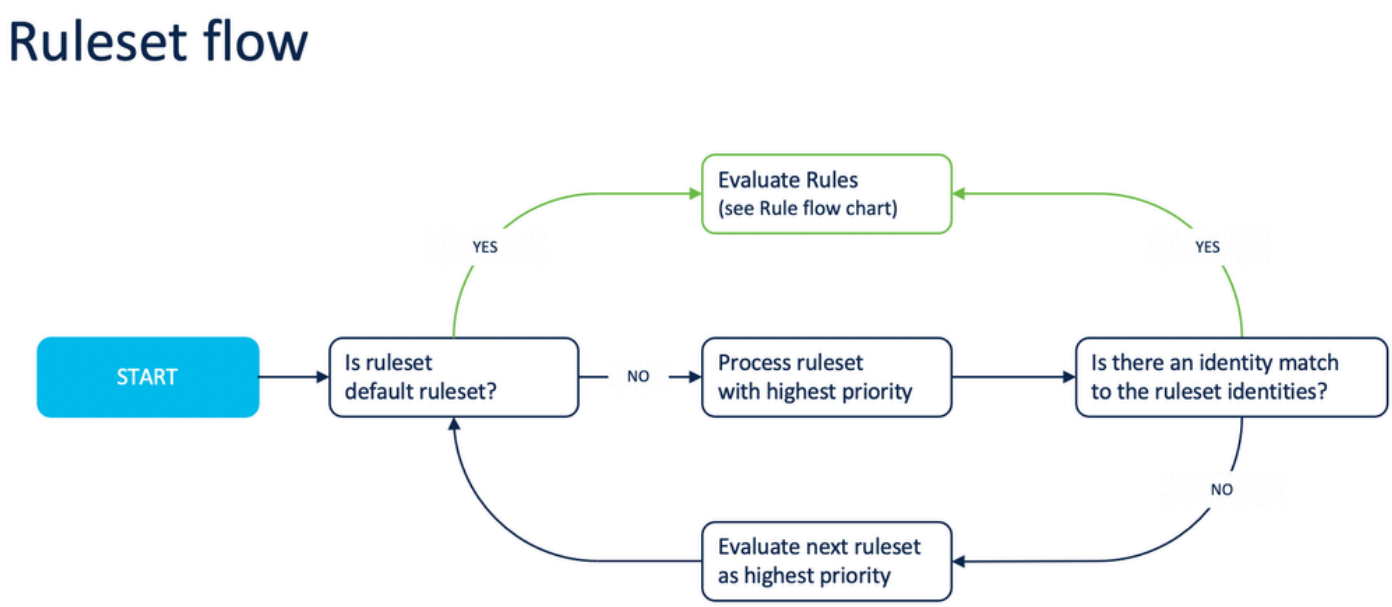
规则可以配置为：

- 规则名称
- 操作
- 身份
- 目的地
- 时间/日安排

有关详细信息，请参阅将规则添加到规则集。

如何评估规则集？

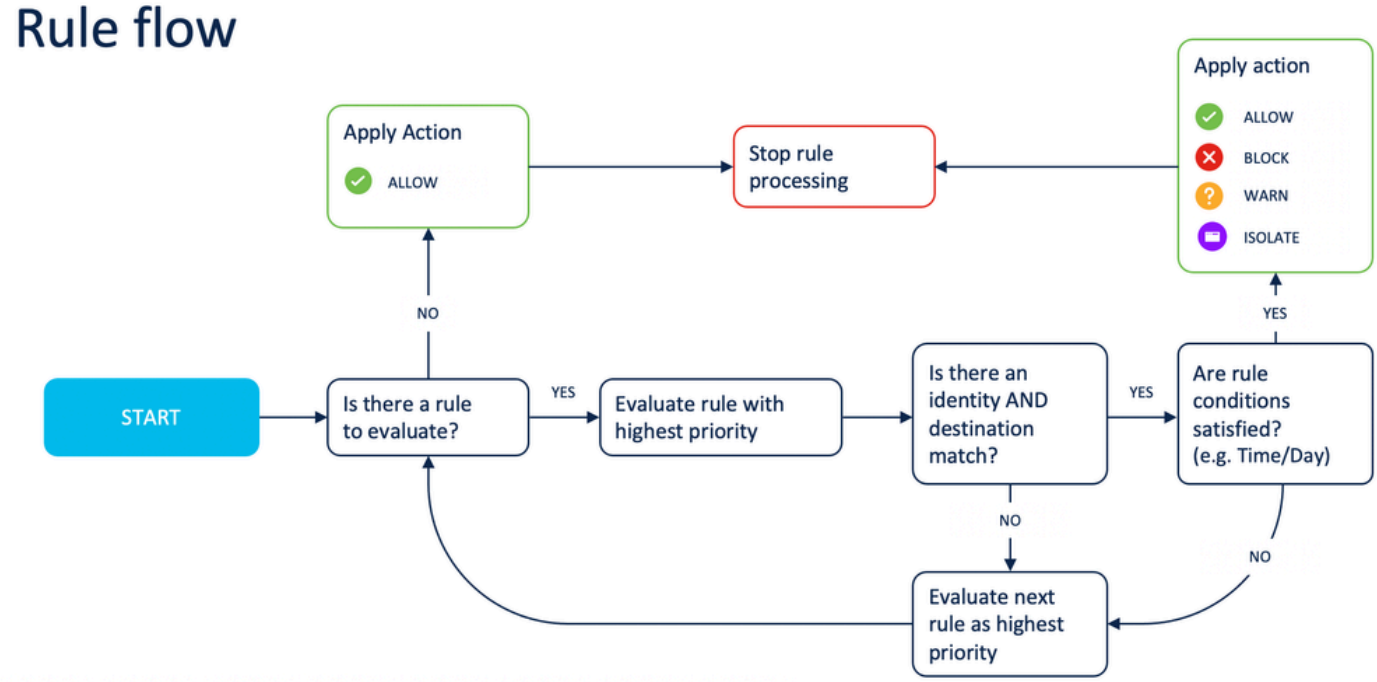
规则集根据可用标识以自上而下的层次结构进行评估。首先评估具有最高优先级的规则集。如果未出现匹配项，则会评估下一个最高优先级的规则集，以此类推。如果任何规则集中没有出现匹配项，则应用默认规则集。



Screen_Shot_2021-04-07_at_2.37.22_PM.png

如何评估规则？

根据可用的标识和目标，自上而下地评估选定规则集中的规则。仅当身份和目标都匹配时，规则才适用。然后应用为规则配置的操作（允许、阻止、警告或隔离）。



Screen_Shot_2021-05-10_at_10.33.03_AM.png

规则是否应用于与规则集匹配的同一身份？

规则可以与规则集匹配相同的身份，但情况并非总是如此。当Umbrella收到Web请求时，它将收集所有存在的身份。然后，系统会根据同一身份池评估选定规则集中的规则，这些规则还必须与目标匹配。规则使用的实际标识可能与匹配规则集的标识不同。

示例：

- JDoe从网络B工作。
- 组织有以下规则集：
  - 规则集1:网络 A
  - 规则集2:网络 B
  - 规则集3:网络 C

只有规则集2适用于JDoe。在规则集2内：

- 规则 1：身份ASmith，目标域B，操作允许
- 规则 2：身份营销、目标SomeSocialApp、操作允许
- 规则 3：身份网络B、目标内容类别（域B、SomeSocialApp）、操作块

结果：

- JDoe被阻止进入域B（规则3）。
- 作为Marketing的成员，JDoe可以访问SomeSocialApp（规则2）。

规则评估顺序决定结果。更具体的身份（用户、组）放在更具体的身份（网络）之前。 第一个匹配成功。

如何知道事务中使用了哪个规则？

“活动搜索”(Activity Search)报告可捕获事务中使用的规则集和规则。此信息可在URL请求的完整详细信息下找到。该字段当前标记为“Policy/Rule”，但随着客户从传统Web策略过渡到规则集，该字段将更改为“Ruleset/Rule”。

在哪里可以找到规则集的在线文档？

请参阅Umbrella管理员指南管理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）。