使用基本域不匹配的FTD访问控制策略中的子域排除FQDN对象故障(&N)

目录

问题

在思科防火墙威胁防御(FTD)访问控制策略中配置完全限定域名(FQDN)对象时，基本域条目不会自动匹配子域。例如，在创建允许配置为“example.com”的目标对象的策略时，会阻止子域“maps.example.com”，而不是允许通过同一策略规则。此行为引发了以下问题：基本域能否用作所有子域的通配符；在FTD策略中实施通配符FQDN匹配的正确配置方法是什么？

环境

- FTD版本7.2。其它版本也可能会受到影响。
- FMC版本7.2。其他版本也可能受到影响。
- 访问控制策略中配置的FQDN对象。

分辨率

- 观察到的行为是FQDN对象的预期操作。
- 在Cisco FMC中，FQDN对象设计为匹配确切的域名，不会自动用作子域的通配符。
- 要正确配置子域匹配，必须使用URL过滤和URL条件而不是FQDN对象。

配置子域匹配的URL过滤

要匹配FMC中的域及其所有子域，请使用以下配置步骤：

步骤1.导航到Access Control Policy Rule Configuration

在FMC中，导航到Policies > Access Control > Access Control Policy > [Your Policy Name] > Rules。

步骤2.创建或编辑访问控制规则

创建新规则或编辑要在其中实施子域匹配的现有访问控制规则。

步骤3.配置URL条件

在规则配置中，添加URL条件而不是使用FQDN对象。配置URL条件以包含具有匹配子域的相应通配符语法的基本域。

步骤4.应用URL过滤策略

确保在访问控制策略中启用并正确配置URL过滤以有效处理URL条件。

步骤5.部署配置

将配置更改部署到目标FTD设备，以实施子域匹配功能。

备用配置方法

如果URL过滤不适用于特定使用案例，请考虑为每个需要显式匹配的子域创建多个FQDN对象，或者如果域解析为可预测IP地址空间，则使用具有IP地址范围的网络对象。

原因

思科FMC中的FQDN对象旨在执行确切的域名匹配，而不是通配符匹配。这是系统的预期行为。FQDN对象功能不包括隐式子域匹配功能，需要使用URL过滤条件来实现所需的子域匹配行为。

相关内容

- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214698-understand-fqdn-feature-on-firepower-thr.html
- https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/214505-configure-fqdn-based-object-for-access-c.html
- 思科漏洞ID CSCwf000588
- 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）。