DNS Allow Rule Not Matching when following a Deny Any/Any Rule

目录

- 问题
- 环境
- 分辨率
- 原因
- 相关内容

问题

当Internet访问策略配置有允许DNS流量的Permit Any/Any规则，后跟策略底部的Deny Any/Any规则时，DNS请求可能与Permit规则不匹配。相反，DNS请求将根据后续规则进行评估，最终可能被全局阻止阻止。

例如，策略可以配置如下：

1. 允许— DNS流量/任何目标
2. 拒绝 — 任何协议/任何目标

在此配置中，DNS流量与预期的Permit规则不匹配，可以通过后续的Deny Any/Any规则阻止。

为什么这会令人困惑

Cisco Secure Access允许管理员选择应用协议，例如：

- DNS

- 基于HTTPS的DNS(DoH)
- 基于TLS的DNS(DoT)

配置互联网访问策略规则时。

这可能导致使用应用协议条件始终可以独立允许或拒绝DNS流量。但是，DNS流量受特定策略评估行为的制约，在此规则配置中，应用协议或基于服务的条件（服务对象）可能不会按预期进行评估。

环境

- 此问题适用于具有以下内容的环境：
  - 思科安全访问(SSE)
  - 包含多个规则的Internet访问策略
  - 基于协议/应用的规则和最终拒绝任何/任何规则的组合
  - DNS流量应匹配前一个Permit规则，但被后续规则或全局阻止阻止

分辨率

当前不支持保证Permit Any/Any DNS规则将独立匹配DNS流量的配置，在此策略结构中后跟Deny Any/Any规则。

当设计包含最终Deny Any/Any规则的Internet访问策略时，客户应了解此策略评估限制。

如果必须允许DNS流量，则应该使用适用于要评估的DNS流量的受支持规则条件来设计策略。

原因

DNS流量的评估方式与一般应用流量不同，不是根据基于服务的条件进行的。

当策略规则包含无法应用于正在评估的DNS流量的条件时，规则不匹配。然后，策略评估将继续执行下一个适用规则。

例如：

```
Rule 1: Permit DNS / Any
           |
           |-- DNS traffic does not match
           |
Rule 2: Deny Any / Any
           |
           |-- DNS traffic matches
           |
         BLOCK
```

因此，将Permit DNS规则直接置于Deny Any/Any规则之上并不能保证允许DNS流量。

相关内容

https://securitydocs.cisco.com/docs/csa/olh/121998.dita

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）。