DNS Allow Rule Not Matching When then a Deny Any/Any Rule

目錄

- 問題
- 環境
- 解析
- 原因
- 相關內容

問題

當Internet訪問策略配置了允許DNS流量的Permit Any/Any規則，以及策略底部的Deny Any/Any規則時，DNS請求可能與Permit規則不匹配。相反，DNS請求將根據後續規則進行評估，並且最終可能被全域性塊阻止。

例如，策略可以配置如下：

1. 允許 - DNS流量/任何目的地
2. Deny — 任何協定/任何目標

在此配置中，DNS流量與預期的Permit規則不匹配，並且可以被後續的Deny Any/Any規則阻止。

為什麼這會讓人困惑

Cisco Secure Access允許管理員選擇應用協定，例如：

- DNS

- 使用HTTPS的DNS(DoH)
- 使用TLS的DNS(DoT)

配置網際網路訪問策略規則時。

這可能導致人們預期，使用應用協定條件時，DNS流量始終可以獨立允許或遭到拒絕。但是，DNS流量受特定策略評估行為的制約，在此規則配置中，應用協定或基於服務的條件（服務對象）可能不會按照預期進行評估。

環境

- 此問題適用於具有以下特徵的環境：
  - 思科安全存取(SSE)
  - 包含多個規則的Internet訪問策略
  - 基於協定/應用的規則和最終拒絕任何/任何規則的組合
  - DNS流量應匹配前一個Permit規則，但被後續規則或全域性阻止阻止

解析

當前沒有支援的配置可保證Permit Any/Any DNS規則在此策略結構中的Deny Any/Any規則後獨立匹配DNS流量。

客戶在設計包含最終Deny Any/Any規則的Internet訪問策略時，應瞭解此策略評估限制。

如果必須允許DNS流量，則應該使用適用於要評估的DNS流量的受支援的規則條件來設計策略。

原因

DNS流量的評估方式與一般應用流量的評估方式不同，不會根據基於服務的條件進行評估。

當策略規則包含無法應用於正在評估的DNS流量的條件時，規則不匹配。然後，策略評估將繼續執行下一個適用規則。

舉例來說：

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

因此，將Permit DNS規則直接置於Deny Any/Any規則之上並不能保證允許DNS流量。

相關內容

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。