DNS Allow Rule Not Matching When Followed by a Deny Any/Any Rule

Contents

- Issue
- Environment
- Resolution
- Cause
- Related Content

Issue

When an Internet Access policy is configured with a Permit Any/Any rule intended to allow DNS traffic, followed by a Deny Any/Any rule at the bottom of the policy, DNS requests may not match the Permit rule. Instead, the DNS requests are evaluated against subsequent rules and may ultimately be blocked by the global block.

For example, a policy may be configured as follows:

1. **Permit** — DNS traffic / Any destination
2. **Deny** — Any protocol / Any destination

In this configuration, the DNS traffic does not match the intended Permit rule and can be blocked by the subsequent Deny Any/Any rule.

Why this can be confusing

Cisco Secure Access allows administrators to select application protocols such as:

- DNS
- DNS over HTTPS (DoH)

- DNS over TLS (DoT)

when configuring an Internet Access policy rule.

This can lead to the expectation that DNS traffic can always be independently allowed or denied using an application protocol condition. However, DNS traffic is subject to specific policy-evaluation behavior, and application protocol or service-based conditions (Service object) may not be evaluated as expected in this rule configuration.

Environment

- This issue applies to environments with:
    - Cisco Secure Access (SSE)
    - Internet Access policies containing multiple rules
    - A combination of protocol/application-based rules and a final Deny Any/Any rule
    - DNS traffic that is expected to match a preceding Permit rule but is instead blocked by a subsequent rule or the global block

Resolution

There is currently no supported configuration that guarantees a Permit Any/Any DNS rule will match DNS traffic independently when followed by a Deny Any/Any rule in this policy structure.

Customers should be aware of this policy-evaluation limitation when designing Internet Access policies that contain a final Deny Any/Any rule.

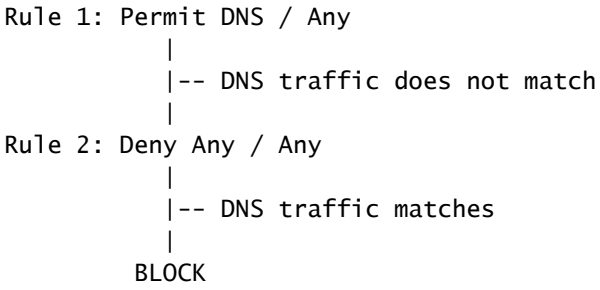
If DNS traffic must be permitted, the policy should be designed using supported rule conditions that are applicable to the DNS traffic being evaluated.

Cause

DNS traffic is not evaluated against service-based conditions in the same manner as general application traffic.

When a policy rule contains conditions that cannot be applied to the DNS traffic being evaluated, the rule does not match. Policy evaluation then continues to the next applicable rule.

For example:



Therefore, placing a Permit DNS rule immediately above a Deny Any/Any rule does not guarantee that the DNS traffic will be permitted.

Related Content

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